CITRIX

XenApp et XenDesktop 7.15 LTSR

Contents

Nouveautés

January 23, 2019

À propos de cette version

À propos de la Mise à jour cumulative 3 (CU3)

À propos de la Mise à jour cumulative 2 (CU2)

À propos de la Mise à jour cumulative 1 (CU1)

À propos de 7.15 LTSR (version initiale)

Mise à jour cumulative 3 (CU3)

February 28, 2019

À propos de cette version

La mise à jour cumulative 3 (CU3) de XenApp et XenDesktop 7.15 LTSR résout plus de 200 problèmes signalés depuis la publication de la version 7.15 LTSR CU2.

7.15 LTSR (informations générales)

Problèmes résolus depuis XenApp et XenDesktop 7.15 LTSR CU2

Problèmes connus dans cette version

Téléchargements

Télécharger 7.15 LTSR CU3

Nouveautés dans cette mise à jour cumulative

La redirection du contenu du navigateur est un composant nouvellement compatible de XenApp et XenDesktop 7.15 LTSR, disponible sous forme de téléchargement distinct. Pour plus d'informations sur la direction du contenu du navigateur dans cette mise à jour cumulative, consultez la section *Redirection du contenu du navigateur* sous Composants compatibles XenApp et XenDesktop 7.15 LTSR CU3.

Nouveaux déploiements

Comment effectuer un nouveau déploiement CU3 ?

Vous pouvez configurer un nouvel environnement XenApp et XenDesktop basé sur CU3, à l'aide du metainstaller CU3. Avant d'effectuer cette configuration, nous vous recommandons de vous familiariser avec le produit :

Consultez la section XenApp et XenDesktop 7.15 LTSR (version initiale) et prêtez une attention particulière aux sections Vue d'ensemble technique, Installer et configurer et Sécurité avant de commencer à planifier votre déploiement. Assurez-vous que votre installation correspond à la configuration système requise pour tous les composants.

Déploiements existants

Que dois-je mettre à jour ?

CU3 fournit des mises à jour pour les composants de base de 7.15 LTSR. Rappel : Citrix vous recommande de mettre à niveau tous les composants LTSR de votre déploiement vers CU3. Par exemple : si Provisioning Services fait partie de votre déploiement LTSR, mettez à jour les composants Provisioning Services vers CU3. Si Provisioning Services ne fait pas partie de votre déploiement, vous n'avez pas besoin de l'installer ni de le mettre à jour.

Composants de base CU3 XenApp et XenDesktop 7.15 LTSR

Composants LTSR 7.15 de base	Version	Remarques
VDA pour OS de bureau	7.15.3000	
VDA pour OS de serveur	7.15.3000	
Delivery Controller	7.15.3000	
Citrix Studio	7.15.3000	
Citrix Director	7.15.3000	
Expérience Gestion des stratégies de groupe	3.1.3000	
StoreFront	3.12.3000	
Provisioning Services	7.15.9	
Serveur d'impression universelle	7.15.3000	

Composants LTSR 7.15 de base	Version	Remarques
Enregistrement de session	7.15.3000	Édition Platinum uniquement
Linux VDA	7.15.3000	Consultez la documentation VDA Linux pour en savoir plus sur les plates-formes prises en charge
Profile Management	7.15.3000	
Service d'authentification fédérée	7.15.3000	

Composants compatibles XenApp et XenDesktop 7.15 LTSR CU3

Les composants suivants, dans les versions indiquées ci-dessous, sont compatibles avec les environnements LTSR. Ils ne bénéficient pas des avantages du programme LTSR (cycle de vie prolongé et mises à jour cumulatives contenant uniquement des corrections). Citrix peut vous demander de mettre à niveau vers une version plus récente de ces composants dans vos environnements 7.15 LTSR :

Plates-formes et composants compatibles avec LTSR 7.15 CU3	Version
Application Layering	4.15.0
*Redirection du contenu du navigateur	15.15
Citrix SCOM Management Pack pour Serveur de licences	1.2
Citrix SCOM Management Pack pour Provisioning Services	1.19
Citrix SCOM Management Pack pour StoreFront	1.13
Citrix SCOM Management Pack pour XenApp et XenDesktop	3.14
Pack d'optimisation HDX RealTime	2.4.2000
Serveur de licences	11.15.0.0 Build 25000
Réinitialisation en libre-service des mots de passe	1.1.10.0
Workspace Environment Management	4.7

***Redirection du contenu du navigateur**

Permet de rediriger le contenu d'un navigateur Web vers une machine cliente et de créer un navigateur correspondant incorporé dans l'application Citrix Workspace. Cette fonctionnalité décharge l'utilisation du réseau, le traitement des pages et le rendu graphique sur le point de terminaison. Cela améliore l'expérience utilisateur lors de la navigation sur des pages Web complexes, notamment des pages Web intégrant HTML5 ou WebRTC. Seule la fenêtre d'affichage (zone visible de l'utilisateur d'une page Web) est redirigée vers le point de terminaison.
La redirection du contenu du navigateur ne redirige pas l'interface utilisateur (barre d'adresse, barre d'outils, etc.) du navigateur sur le VDA. Pour plus d'informations, consultez la section Redirection du contenu du navigateur.

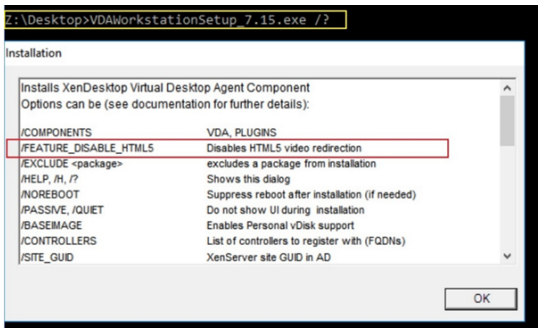
Configuration système requise :

Cette configuration système concerne spécifiquement BCR.msi avec XenApp et XenDesktop 7.15 LTSR CU3. Ignorez la configuration système requise en matière de redirection de contenu du navigateur répertoriée dans toutes les autres versions de XenApp, XenDesktop et Citrix Virtual Apps and Desktops.

- Version 7.15 LTSR CU3 sur le Delivery Controller et le VDA
- Application Citrix Workspace pour Windows 1809 ou version ultérieure
- Citrix Receiver pour Linux 13.9 ou version ultérieure
- BCR.msi, disponible depuis la page Téléchargements de Citrix

Installation :

1. Installez ou mettez à niveau le VDA avec la version 7.15 LTSR CU3 à l'aide de l'option de ligne de commande /FEATURE_DISABLE_HTML5.



   Cette option supprime la fonction de redirection vidéo HTML5, qui doit être effectuée avant d'exécuter BCR.msi. BCR.msi ajoute la fonctionnalité lors de l'installation et ajoute également les services de redirection de contenu du navigateur. Lorsque cette étape est terminée, ouvrez la console services.msc et vérifiez que le **service de redirection vidéo Citrix HDX HTML5** n'est pas répertorié.

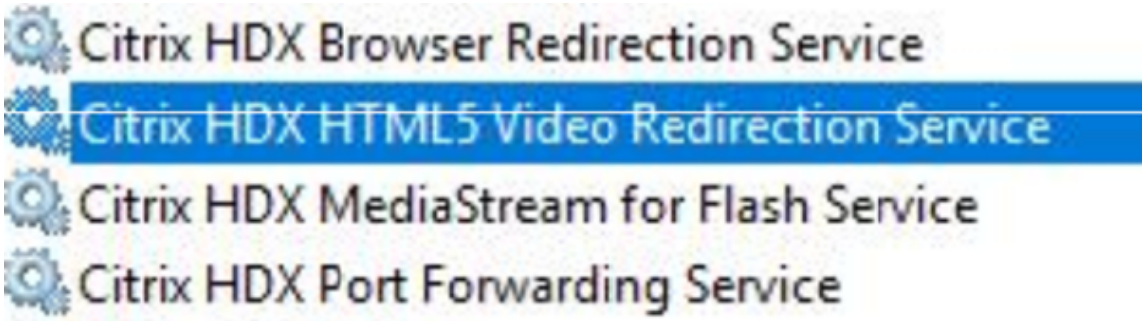
2. Démarrez l'installation de redirection de contenu du navigateur avec BCR.msi. Selon votre système, BCR.msi installe ses fichiers sous :

C:\Program Files\Citrix\ICAService

ou

C:\Program Files(86)\Citrix\ICAService

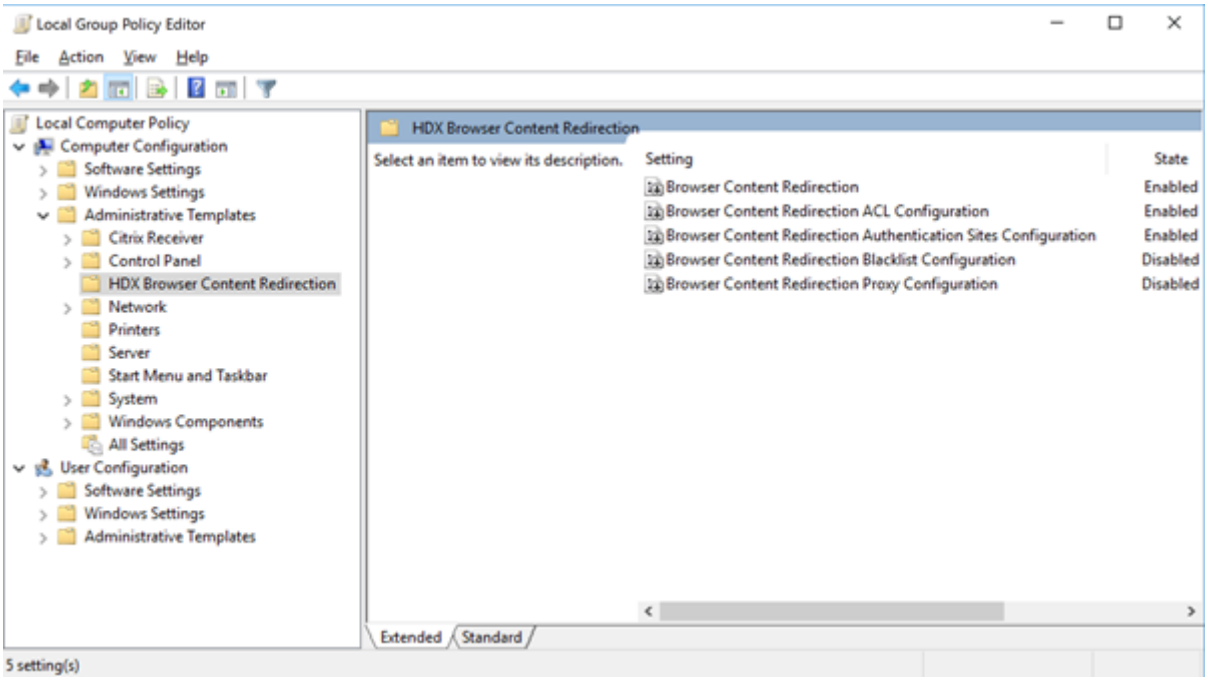
Comme l'installation est rapide, la boîte de dialogue peut se fermer rapidement. Si cela se produit, réexécutez services.msc et vérifiez que les services ont bien été ajoutés.



Stratégies :

Vous pouvez contrôler les stratégies en utilisant les registres HKEY_LOCAL_MACHINE sur le VDA ou le modèle d'administration Citrix **Redirection du contenu du navigateur HDX** pour la console de gestion des stratégies de groupe.

Vous pouvez télécharger le modèle à partir de la page des téléchargements citrix.com sous Citrix Virtual Apps and Desktops (XenApp & XenDesktop) > XenApp 7.15 LTSR / XenDesktop 7.15 LTSR > Composants. Citrix Studio ne contient pas ces stratégies.



Pour de plus amples informations sur la stratégie, consultez la section Paramètres de stratégie Redi-

rection du contenu du navigateur. Pour obtenir des informations de dépannage, consultez l'article CTX230052 du centre de connaissances.

Versions compatibles de l'application Citrix Workspace et Citrix Receiver

Pour faciliter la maintenance et pour garantir des performances optimales, Citrix vous recommande de mettre à niveau vers la dernière version de l'application Citrix Workspace dès qu'elle est disponible. Les dernières versions sont disponibles en téléchargement sur https://www.citrix.com/downloads/workspace-app/.

À des fins de commodité, pensez à vous inscrire au flux RSS Citrix Receiver pour être notifié lorsqu'une nouvelle version de Citrix Receiver est disponible.

Pour Citrix Receiver pour Windows, Citrix a annoncé un programme LTSR spécial. Pour de plus amples informations sur ce programme, consultez la page Étapes du cycle de vie de Citrix Receiver.

Plus précisément, les versions suivantes et toutes les versions ultérieures de l'application Citrix Workspace sont compatibles avec 7.15 LTSR CU3 :

Versions de l'application Citrix Workspace compatibles avec 7.15 LTSR	Version
Application Citrix Workspace pour Android	1810 et versions ultérieures
Application Citrix Workspace pour Chrome	1809.1 et versions ultérieures
Application Citrix Workspace pour HTML5	1809.1 et versions ultérieures
Application Citrix Workspace pour iOS	1810 et versions ultérieures
Application Citrix Workspace pour Mac	1809 et versions ultérieures
Application Citrix Workspace pour Linux	1809 et versions ultérieures
Application Citrix Workspace pour Windows (Store)	1809 et versions ultérieures
Citrix Receiver pour Windows	4.9.4000 (LTSR)

Exclusions notables pour XenApp et XenDesktop 7.15 LTSR

Les fonctionnalités, plates-formes et composants suivants ne bénéficient pas des avantages et des étapes de cycle de vie du programme 7.15 LTSR. Plus précisément, le cycle de vie prolongé et les mises à jour cumulatives contenant uniquement des corrections sont exclus. Les mises à jour des fonctionnalités et composants exclus sont disponibles au travers des versions régulières.

Fonctions exclues
Framehawk
Intégration de StoreFront Citrix Online

Composants exclus
Personal vDisk : exclu pour les machines Windows 10 ; pour les machines Windows 7, prise en charge LTSR limitée jusqu'au 14 janvier 2020 (exigences de CU s'appliquent)
AppDisks

Plates-formes Windows exclues *
Windows 2008 32bits (pour le serveur d'impression universelle)

* Citrix se réserve le droit de mettre à jour la prise en charge des plates-formes en fonction des étapes du cycle de vie des fournisseurs tiers.

Installer et mettre à niveau les outils d'analyse

Lorsque vous utilisez le programme d'installation du produit complet pour déployer et mettre à niveau les composants XenApp ou XenDesktop, des informations anonymes sur le processus d'installation sont collectées et stockées sur la machine sur laquelle vous installez/mettez à niveau le composant. Ces données sont utilisées pour aider Citrix à améliorer l'expérience de ses clients avec l'installation. Pour plus d'informations, veuillez consulter l'article https://more.citrix.com/XD-INSTALLER.

Migration XenApp 6.5

Le processus de migration XenApp 6.5 vous aide à effectuer une transition rapidement et efficacement depuis une batterie XenApp 6.5 vers un site exécutant XenApp 7.15 LTSR CU3. Ceci est utile dans les déploiements contenant un grand nombre d'applications et de stratégies de groupe Citrix : réduisant le risque d'introduction d'erreurs par inadvertance lors du déplacement manuel des applications et des stratégies de groupe Citrix vers le nouveau site XenApp.

Après avoir installé les composants principaux XenApp 7.15 LTSR CU3 et créé un site, le processus de migration suit cette séquence :

- Exécutez le programme d'installation de XenApp 7.15 CU3 sur chaque tâche XenApp 6.5, qui effectue une mise à niveau automatique vers un nouveau Virtual Delivery Agent pour OS de serveur à utiliser dans le nouveau site.
- Exécutez les applets de commande d'exportation PowerShell sur un Controller XenApp 6.5, qui permet d'exporter les paramètres de stratégie et d'application Citrix vers des fichiers XML.
- Modifiez les fichiers XML, le cas échéant, pour affiner les éléments que vous voulez importer dans le nouveau site. En personnalisant les fichiers, vous pouvez importer les paramètres de stratégie et d'application dans votre site XenApp 7.15 LTSR CU3 par étape : certaines maintenant et d'autres ultérieurement.
- Exécutez les applets de commande d'importation PowerShell sur le nouveau Controller XenApp 7.15 CU3, qui importe les paramètres depuis les fichiers XML vers le nouveau site XenApp.

Reconfigurez le nouveau site si nécessaire, puis testez-le.

Pour plus d'informations, voir Migrer XenApp 6.x.

Problèmes résolus

February 28, 2019

Citrix Director

- Les tentatives de suppression de l'attribution d'utilisateurs depuis un poste de travail à l'aide de Citrix Studio, PowerShell ou Citrix Director, par un administrateur délégué doté d'un rôle personnalisé peuvent échouer. Le problème se produit lorsque les administrateurs personnalisés disposent des autorisations nécessaires pour effectuer les opérations sur les groupes de mise à disposition, mais ne disposent pas d'autorisations sur les catalogues de machines. [LC8174]
- Les tentatives de recherche d'utilisateurs lors de leur affectation à des machines sont susceptibles d'échouer. L'utilisateur sélectionné apparaît comme null. [LC8395]
- Citrix Director peut signaler Multi-Stream ICA comme inactif lors de l'utilisation du **protocole UDT (protocole de transfert des données basé sur UDP)**. Le problème se produit lorsque HDX WMI Provider n'est pas mis à jour pour prendre en compte les sessions EDT ou UDT. [LC8960]
- L'utilisation de l'UC par le processus w3wp.exe peut être très importante sur Citrix Director. [LC9222]
- Lorsque vous définissez la langue du navigateur sur une langue autre que l'anglais et que vous démarrez Citrix Director, le volet Détails de la session peut afficher une session comme étant active, même si aucune session n'est en cours d'exécution. [LC9392]

- Lorsque vous utilisez Citrix Director, Microsoft Internet Explorer 11 peut afficher des barres de défilement non fonctionnelles dans la section **Détails de la machine** de la page **Filtres** > **Machines** > **Toutes les machines**. [LC9505]
- Les appels Google Analytic sont établis sur Citrix Director sur le tableau de bord et le tableau de bord des applications, même après la désactivation des téléchargements automatiques, sous la clé de registre HKEY_LOCAL_MACHINE\Software\Citrix\MetaInstall. Les téléchargements automatiques sont désactivés conformément à la procédure décrite dans la section « Installer et mettre à niveau les outils d'analyse » de Citrix Insight Services. [LC9736]
- Les rapports générés au format CSV pour les performances d'ouverture de session dans Citrix Director peuvent utiliser le fuseau horaire UTC au lieu de l'heure locale. [LC9854]
- Certains administrateurs risquent de ne pas pouvoir accéder à certains domaines ajoutés à la liste de domaines web.config. Par conséquent, lorsque vous recherchez une session d'utilisateur, une exception se produit et les détails de la session ne sont pas affichés. [LC9865]
- La valeur **ExportCsvDrilldownLimit** peut ne pas être appliquée aux rapports personnalisés dans Citrix Director. [LD0004]

Stratégie Citrix

- Lorsque vous appliquez la stratégie de bouclage en mode de fusion à un VDA et ajoutez l'URL StoreFront à un groupe de diffusion du VDA dans Citrix Studio, des icônes en double des applications publiées peuvent apparaître. [LC8889]
- Les tentatives de création d'un catalogue de machines peuvent échouer avec une exception indiquant que le résumé ne peut pas être créé. De plus, lors de l'utilisation de l'assistant de création de catalogue et avant l'apparition de l'exception, la liste déroulante supposée répertorier les domaines est vide. [LC9636]
- Lorsque vous exécutez l'outil Résultats de stratégie de groupe à partir de la console de gestion des stratégies de groupe sur un ordinateur installé avec VDA 7.15.2000, le message d'erreur suivant s'affiche : **An error occurred while generating report: Not Found** [LC9825]
- Le service de gestion des impressions Citrix (cpsvc.exe) peut s'arrêter de façon inattendue. Le problème se produit en cas d'entrées illisibles dans la clé de registre d'impression qui est connectée à un objet de stratégie de groupe (GPO). [LC9921]
- Le moteur de stratégie de groupe peut ne pas réussir à insérer toutes les valeurs dans la clé de registre **ApplicationStartDetails**. Par conséquent, les tentatives de démarrage d'applications peuvent échouer. [LC9942]
- Lorsque des entrées de registre sont pré-renseignées manuellement pour les clés de session sous la clé de registre HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix, les clés peuvent ne pas être mises à jour au démarrage de la session. [LC9977]

- Lorsque vous essayez d'appliquer une stratégie Citrix dans Citrix Studio à l'aide du filtre Unité d'organisation, le message d'erreur suivant peut s'afficher : **Une erreur inconnue s'est produite**.

  L'exception suivante apparaît :
  Collection was modified; enumeration operation may not execute.[LD0044]

- Lorsque vous essayez de sauvegarder une stratégie de groupe, puis que vous l'importez avec la version 3.1.2 de la console de gestion des stratégies de groupe (GPMC), celle-ci peut ne plus répondre. Cependant, la stratégie est importée. [LD0173]

Citrix Studio

- Les tentatives de suppression de l'attribution d'utilisateurs depuis un poste de travail à l'aide de Citrix Studio, PowerShell ou Citrix Director, par un administrateur délégué doté d'un rôle personnalisé peuvent échouer. Le problème se produit lorsque les administrateurs personnalisés disposent des autorisations nécessaires pour effectuer les opérations sur les groupes de mise à disposition, mais ne disposent pas d'autorisations sur les catalogues de machines. [LC8174]
- Lorsque l'un des Delivery Controller se déconnecte ou devient indisponible, Citrix Studio peut prendre quelques minutes pour s'ouvrir et afficher le message suivant :

  This snap-in is not responding. [LC8993]

- Les tentatives d'annulation de publication et de suppression des packages App-V du VDA peuvent échouer. [LC9161]
- Lorsque vous essayez de voir la page **Allocation de machine** pour la deuxième fois après avoir sélectionné **Modifier le groupe de mise à disposition** dans le volet **Actions**, la page **Allocation de machine** peut être vide et les détails tels que le nom de la machine et les utilisateurs ne pas s'afficher. [LC9465]
- Les tentatives de suppression du **dossier d'application** dans Citrix Studio après avoir déplacé l'application publiée depuis **Groupe d'applications** peuvent échouer avec une erreur d'autorisation. [LC9520]
- Après la mise à niveau de Citrix Studio vers la mise à jour cumulative 2 de la version 7.15, il est possible que les stratégies ne soient pas localisées. Pour plus d'informations, consultez l'article CTX234711 du centre de connaissances. [LC9613]
- Les tentatives de création d'un catalogue de machines peuvent échouer avec une exception indiquant que le résumé ne peut pas être créé. De plus, lors de l'utilisation de l'assistant de création de catalogue et avant l'apparition de l'exception, la liste déroulante supposée répertorier les domaines est vide. [LC9636]

- Lorsque vous essayez de supprimer des applications App-V du groupe de mise à disposition, les applications peuvent être supprimées. Un message d'erreur s'affiche. [LC9985]
- Lorsque vous essayez d'appliquer une stratégie Citrix dans Citrix Studio à l'aide du filtre Unité d'organisation, le message d'erreur suivant peut s'afficher : **Une erreur inconnue s'est produite**.

  L'exception suivante apparaît :
  Collection was modified; enumeration operation may not execute. [LD0044]
- Une exception se produit lorsque vous essayez d'appliquer une stratégie Citrix dans Citrix Studio à l'aide du filtre Unité d'organisation (OU) ou d'ajouter une unité d'organisation dans l'assistant de catalogue. [LD0112]

Controller

- Les tentatives de suppression de l'attribution d'utilisateurs depuis un poste de travail à l'aide de Citrix Studio, PowerShell ou Citrix Director, par un administrateur délégué doté d'un rôle personnalisé peuvent échouer. Le problème se produit lorsque les administrateurs personnalisés disposent des autorisations nécessaires pour effectuer les opérations sur les groupes de mise à disposition, mais ne disposent pas d'autorisations sur les catalogues de machines. [LC8174]
- Les VDA peuvent avoir par intermittence un état d'alimentation non valide dans Citrix Studio. Studio indique que l'état d'alimentation est désactivé, **OFF**, même lorsque le VDA est en cours d'exécution. [LC8898]
- Lorsque l'un des Delivery Controller se déconnecte ou devient indisponible, Citrix Studio peut prendre quelques minutes pour s'ouvrir et afficher le message suivant :

  This snap-in is not responding [LC8993].
- Vous importez des modifications depuis le broker principal vers la base de données LHC (Local Host Cache, cache d'hôte local) et supprimez un utilisateur ou une machine d'Active Directory sans le ou la supprimer de Citrix Studio. En conséquence, des erreurs peuvent survenir et le cache d'hôte local n'est pas mis à jour. [LC9054]
- Des blocages peuvent se produire sur XenApp avec un **ID d'événement d'application 2013** pendant le temps de connexion maximal. Ce message d'erreur s'affiche :

  Une exception inattendue s'est produite lors du traitement d'une demande HTTP par Citrix Broker Service. [LC9134]
- Lorsque vous mettez à niveau XenApp 7.6 vers XenApp 7.15, les autorisations pour le dossier Licensing sur le Delivery Controller sous **C:\Windows\ServiceProfiles\NetworkService\Licensing** sont remplacées. [LC9445]

- L'utilisation de la mémoire du service de haute disponibilité Citrix (HighAvailabilityService.exe) peut dépasser 2 Go. [LC9446]
- Lorsque vous envoyez une commande de redémarrage au VDA cible à partir de Citrix Studio, le VDA cible peut s'arrêter. [LC9479]
- Les tentatives de suppression du **dossier d'application** dans Citrix Studio après avoir déplacé l'application publiée depuis **Groupe d'applications** peuvent échouer avec une erreur d'autorisation. [LC9520]
- L'infrastructure de bureau virtuel (VDI) hébergée sur les hôtes ESXi peut passer à un état d'alimentation inconnu et ne se met pas automatiquement sous tension. Le problème se produit après que les machines virtuelles (VM) ont été déplacées vers les hôtes ESXi une fois que les hôtes ESXi ne sont plus en mode de maintenance. [LC9619]
- Les tentatives de création d'un catalogue de machines peuvent échouer avec une exception indiquant que le résumé ne peut pas être créé. De plus, lors de l'utilisation de l'assistant de création de catalogue et avant l'apparition de l'exception, la liste déroulante supposée répertorier les domaines est vide. [LC9636]
- Citrix Studio ne montre pas l'option **Start**. Par conséquent, le PC distant ne parvient pas à s'allumer. [LC9702]
- L'utilisation de cette amélioration des performances pour le service de surveillance (Monitor) réduit la consommation élevée d'UC sur le serveur SQL lorsque la base de données de surveillance est volumineuse. [LC9726]
- Les machines virtuelles provisionnées par MCS (Machine Creation Services) peuvent ne pas être créées avec le **Secure Boot** activé. Ce problème peut se produire même lorsque le modèle principal a été créé à l'aide de l'interface EFI (Extensible Firmware Interface) et avec **Secure Boot** activé. [LC9841]
- Par défaut, l'ID Amazon Web Services (AWS) de la machine fournie par Machine Creation Services (MCS) n'est pas persistant. Cela pourrait entraîner l'échec des actions de gestion de l'alimentation de la machine virtuelle sur AWS.

  Pour configurer la persistance de l'identifiant AWS, les options suivantes sont disponibles :

  - Pour activer la persistance de l'ID AWS, définissez l'option Connexion de la propriété avancée de la connexion hôte sur **CreateNewInstanceOnReset=False**.
  - Pour désactiver la persistance de l'ID AWS, définissez l'option Connexion de la propriété d'avance de la connexion hôte sur **CreateNewInstanceOnReset=True** ou supprimez l'option.

  Un délai d'attente de dix secondes est requis avant que la modification de l'option soit effective. [LC9960]

- Les tentatives de création d'une application en utilisant la commande **New-BrokerApplication** avec le paramètre -AdminFolder peuvent ne pas créer le dossier spécifié dans certains scénarios. [LC9982]
- Lorsque vous essayez de supprimer des applications App-V du groupe de mise à disposition, les applications peuvent être supprimées. Un message d'erreur s'affiche. [LC9985]
- Dans un environnement de grande taille où de nombreux groupes d'applications sont utilisés, lorsque vous cliquez sur l'onglet Applications dans Studio, la session expire lors de la récupération des résultats de **Get-BrokerApplicationGroup**. Par conséquent, l'exception suivante apparaît :

  Database could not be connected.

  Avant de lancer l'exception, Studio ne répond plus lors de l'énumération des groupes d'applications. [LD0012]
- Lorsque vous essayez d'appliquer une stratégie Citrix dans Citrix Studio à l'aide du filtre Unité d'organisation, le message d'erreur suivant peut s'afficher : **Une erreur inconnue s'est produite**.

  L'exception suivante apparaît :
  Collection was modified; enumeration operation may not execute. [LD0044]
- Les tentatives de recréation du cache d'hôte local avec un nom de groupe de mise à disposition contenant des caractères spéciaux peuvent échouer avec un **ID d'événement 505**. [LD0068]
- La connexion d'hébergement Citrix Studio peut émettre un message d'avertissement vous invitant à utiliser les connexions d'hébergement HTTPS pour XenServer, même si les connexions HTTPS ne sont pas prises en charge. [LD0210]
- Après avoir mis à niveau XenApp et XenDesktop vers la version 7.15, les programmes de redémarrage initiaux peuvent démarrer immédiatement au lieu de démarrer lors du prochain événement programmé. [LD0308]

Pack d'optimisation HDX RealTime

Identity Assertion

- Les tentatives d'accès au certificat d'authentification disponible dans la session pour la connexion peuvent échouer. [LC9728]
- Lorsque vous utilisez un certificat dans la session du Service d'authentification fédérée pour authentifier une connexion TLS 1.1 (ou version antérieure), la connexion peut échouer. L'ID d'événement 305 est consigné, indiquant un ID de hachage non pris en charge. Le Service d'authentification fédérée ne prend pas en charge le hachage SHAMD5. [LD0018]

Programme d'installation

- Les tentatives d'installation du VDA dans l'environnement sur lequel l'application Adobe Acrobat Reader 2015 DC est déjà installée peuvent générer le message d'erreur suivant :

  Le programme ne peut pas démarrer car mfc120u.dll est absent de votre ordinateur. Essayez de réinstaller le programme pour résoudre le problème. [LC9979]

Linux VDA

- Le VDA Linux peut ne pas appliquer les stratégies Citrix. Le problème se produit lorsque vous configurez une stratégie pour utiliser le type de connexion d'élément Access Control avec NetScaler Gateway. [LC9842]

Profile Management

- Lorsque vous configurez la redirection de dossiers à l'aide de la stratégie Microsoft Active Directory en cliquant sur **Réinitialiser le profil** dans Citrix Director, les dossiers redirigés sont également réinitialisés. Par conséquent, certains dossiers tels que **Documents**, **Images**, **Musique**, **Vidéos** et **Favoris** sont renommés. Toutefois, les dossiers tels que **Menu Démarrer**, **Contacts**, **Téléchargements**, **Liens**, **Recherches** et **Jeux enregistrés** ne sont pas renommés. [LC9237]
- Le service Profile Management peut se fermer de manière inattendue avec le code d'exception 0xc0000374. [LC9355]
- Il est possible que Profile Management ne synchronise pas certains paramètres sur le VDA exécuté sous Microsoft Windows 10, version 1709. [LC9503]
- Avec la stratégie **Registre en réécriture active** activée, la stratégie par défaut de l'exclusion du registre incluant Software\Microsoft\AppV\Client\Integration et Software\Microsoft\AppV\Client\Publishing peut ne pas fonctionner. [LC9550]
- Vous avez une autorisation complète sur le profil utilisateur par défaut. Lors de la première connexion, Profile Management peut supprimer les dossiers exclus configurés via une stratégie du profil utilisateur par défaut. Le problème se produit lorsque la vérification d'exclusion de connexion est configurée pour supprimer les fichiers et les dossiers exclus. [LC9575]
- Profile Management configuré avec le registre en réécriture active traite tous les registres et enregistre toutes les modifications dans un fichier temporaire, que les registres soient exclus ou inclus. Par conséquent, l'utilisation de l'UC est élevée. [LC9624]
- Les sessions 7.15 LTSR CU2 peuvent être lancées en tant qu'écran noir. Le problème se produit avec les sessions exécutées sur XenApp et XenDesktop 7.15 LTSR CU2 et les VDA 7.17 lorsque Pro-

file Management est activé. Pour plus d'informations sur une solution de contournement, consultez l'article CTX235100 du centre de connaissances. [LC9648]

- La stratégie Dossiers en miroir dans Profile Management peut ne pas fonctionner. [LC9691]
- Lorsque Profile Management est activé, des icônes vides peuvent apparaître dans le menu Démarrer des bureaux publiés. Le problème se produit lors de la deuxième ouverture de session ou des ouvertures de session suivantes.

  Remarque : cette correction n'est efficace que sur des nouvelles installations. Pour les scénarios de mise à niveau, vous devez configurer manuellement la stratégie **Dossiers en miroir** dans l'Éditeur de stratégie de groupe HDX ou dans l'Éditeur de stratégie Active Directory. [LC9692]
- La redirection de dossiers AppData (Roaming) peut ne pas fonctionner avec Profile Management et le message d'erreur suivant apparaît :

  Accès refusé.

  Le problème se produit lorsque Profile Management ne lie pas **AppData/Roaming** correctement au dossier partagé et tente d'ajouter /Application Data/Roaming par erreur. [LC9830]

Provisioning Services

Problèmes liés à la console

- L'assistant d'installation XenDesktop peut tenter de se connecter à un hôte Hyper-V incorrect. Le problème se produit lorsqu'il existe plusieurs clusters gérés par le même serveur SCVMM (System Center Virtual Machine Manager). [LC8415]
- Après avoir appliqué le correctif Microsoft KB3186539 sur Provisioning Server sur certaines versions japonaise et chinoise du système d'exploitation Microsoft Windows, la plate-forme Boot Device Manager (BDM) ne peut pas être créée. [LC8743]
- L'outil Boot Device Management (BDM) peut ne pas être mis à jour sur le serveur XenServer créé sur la machine XenServer esclave. [LC8964]
- La piste d'audit de Provisioning Services peut afficher une description de texte incorrecte pour certaines entrées. Les données enregistrées dans la base de données sont correctes, mais la description affichée dans la fenêtre de la piste d'audit est incorrecte. [LC9481]
- La bibliothèque XIP de Provisioning Services pour VMware ESXi ne prend pas en charge TLS v1.2. [LC9629]
- Lorsque vous mettez à niveau le logiciel Provisioning Services Server ou Console, il est possible que les composants logiciels enfichables PowerShell ne soient pas mis à niveau. [LC9718]

- Le démarrage de l'interface UEFI (Provisioning Server Unified Firmware Interface) de Provisioning Server peut ne pas accepter la saisie du menu de démarrage s'il existe plusieurs versions de vDisk. La saisie au clavier cesse de répondre lors du processus de démarrage PXE ou BDM d'une machine cible physique en cours de démarrage en mode Maintenance. [LC9815]
- Lors de l'utilisation de l'assistant d'installation XenDesktop, les tentatives de création de la partition Boot Device Manager (BDM) échouent lors de l'utilisation de la configuration VMware ESX vSAN. [LD0029]

Problèmes liés au serveur

- Une fois qu'un vDisk a été élevé à la version de production, il peut rester monté sur le serveur Provisioning Services. [LC8051]
- La gestion de KMS n'est pas appliquée aux versions de vDisk. [LC8147]
- Le même identificateur de disque est attribué par erreur au vDisk résidant dans différents magasins lorsque le vDisk existant a été ajouté à l'aide de la commande « MCLI Add DiskLocator ». [LC8281]
- Provisioning Services ne parvient pas à monter un vDisk lorsque la taille du secteur logique VHDX est de 512 Mo et que la taille du secteur physique de stockage est de 4 096 Mo. [LC8430]
- Après avoir appliqué le correctif Microsoft KB3186539 sur Provisioning Server sur certaines versions japonaise et chinoise du système d'exploitation Microsoft Windows, la plate-forme Boot Device Manager (BDM) ne peut pas être créée. [LC8743]
- L'outil Boot Device Management (BDM) peut ne pas être mis à jour sur le serveur XenServer créé sur la machine XenServer esclave. [LC8964]
- Lors de la fusion simultanée de deux disques virtuels ou plus, le processus gmtDaemon.exe peut s'arrêter de manière inattendue. [LC9123]
- Lorsque vous créez une version de vDisk de base fusionnée, le processus MgmtDaemon.exe peut se fermer de manière inattendue avec un code d'exception 0xc0000005. [LC9143]
- La piste d'audit de Provisioning Services peut afficher une description de texte incorrecte pour certaines entrées. Les données enregistrées dans la base de données sont correctes, mais la description affichée dans la fenêtre de la piste d'audit est incorrecte. [LC9481]
- Après la mise à niveau de XenApp and XenDesktop de la version 7.13 vers la version 7.15 dans certains environnements Active Directory, les utilisateurs locaux risquent de ne pas pouvoir se connecter à la console Provisioning Services Console. Un message d'erreur de délai d'attente apparaît. [LC9542]
- La bibliothèque XIP de Provisioning Services pour VMware ESXi ne prend pas en charge TLS v1.2. [LC9629]

- Lorsque vous mettez à niveau le logiciel Provisioning Services Server ou Console, il est possible que les composants logiciels enfichables PowerShell ne soient pas mis à niveau. [LC9718]
- Sur Provisioning Services 7.14 et versions ultérieures, l'assistant de configuration peut ne pas réussir à configurer une batterie lorsque vous n'utilisez pas Active Directory. Le problème se produit lorsque Provisioning Services est installé dans un environnement de groupe de travail. [LC9844]
- Lors de l'utilisation de l'assistant d'installation XenDesktop, les tentatives de création de la partition Boot Device Manager (BDM) échouent lors de l'utilisation de la configuration VMware ESX vSAN. [LD0029]
- Après une mise à niveau de Provisioning Services de la version 7.6.x vers 7.15 LTSR CU2 et une tentative d'ouverture de la console Provisioning Services, ce message d'erreur peut s'afficher :

  An unexpected MAPI error occurred [LD0092]

Problèmes liés aux machines cibles

- Les tentatives d'installation d'une machine cible PVS Linux peuvent échouer. Le problème se produit lorsque les dépendances requises sur Ubuntu sont incorrectes. [LC9478]

Remote Broker Provider

- Par défaut, l'ID Amazon Web Services (AWS) de la machine fournie par Machine Creation Services (MCS) n'est pas persistant. Cela pourrait entraîner l'échec des actions de gestion de l'alimentation de la machine virtuelle sur AWS.

  Pour configurer la persistance de l'identifiant AWS, les options suivantes sont disponibles :

  - Pour activer la persistance de l'ID AWS, définissez l'option Connexion de la propriété avancée de la connexion hôte sur **CreateNewInstanceOnReset=False**.
  - Pour désactiver la persistance de l'ID AWS, définissez l'option Connexion de la propriété d'avance de la connexion hôte sur **CreateNewInstanceOnReset=True** ou supprimez l'option.

  Un délai d'attente de dix secondes est requis avant que la modification de l'option soit effective. [LC9960]

Enregistrement de session

Administration

- Un utilisateur du **domaine B** ouvre une session sur le serveur d'enregistrement de session sur le domaine A et tente de mettre à jour la propriété Enregistrement de session. Le GUID de la machine n'est pas généré et une erreur se produit. Le problème se produit parce que l'utilisateur est dans le **domaine B**, mais le serveur d'enregistrement de session est dans le **domaine A**. [LC9562]

Agent

- L'instance publiée de Microsoft Internet Explorer peut s'afficher en tant que **explorer.exe** dans la liste des lecteurs d'enregistrement de session. Le nom de fichier correct est **Iexplore.exe**. [LC9622]

StoreFront

- Lorsque vous zoomez le navigateur à 125 %, le logo personnalisé peut disparaître. [LC9018]
- Lorsque le paramètre **OverrideIcaClientname** est activé, les tentatives d'établissement d'une session distante à partir du client Bureau à distance peuvent échouer. Le problème se produit lorsque la licence n'est pas renouvelée. Un de ces messages d'erreur peut s'afficher :

  « Impossible d'établir la session à distance depuis le client du bureau à distance WR_XxXXxXXX car sa licence n'a pas pu être renouvelée. »

  OU

  « Impossible d'établir la session à distance depuis le client du bureau à distance WR_XxXXxXXX car sa licence temporaire a expiré. » [LC9246]
- Les tentatives d'énumération des applications peuvent échouer après la mise à jour du certificat de Delivery Controller vers TLS v1.2. [LC9337]
- Lorsque vous sélectionnez un site configuré lors de la configuration de XenDesktop, il se peut qu'un magasin par défaut qui utilise le service d'authentification par défaut soit créé dans StoreFront. Si vous supprimez ce magasin, les utilisateurs de Citrix Receiver pour Windows ne peuvent pas ajouter d'autres magasins et ce message s'affiche :

  « Une erreur de protocole s'est produite lors de la communication avec le service d'authentification ». [LC9404]

- Les tentatives de connexion à StoreFront peuvent échouer avec l'erreur **Impossible de traiter votre demande**. Le problème se produit lorsque les applications publiées ont des icônes personnalisées avec une résolution minimale. [LC9521]
- Lorsque vous utilisez le SDK StoreFront pour personnaliser certaines fonctionnalités et configurer l'agrégation du magasin, l'ouverture de session peut échouer avec l'erreur **Impossible de traiter votre demande**. [LC9561]
- La session préliminaire peut ne pas fonctionner après la configuration de **Filtrer les ressources par mots clés**. [LC9642]
- Le fichier ICA peut indiquer le nom de domaine complet (FQDN) du VDA dans l'entrée UDPICA-Port même lorsque vous utilisez la connexion NetScaler Gateway. [LC9760]

Serveur d'impression universelle

Redirection de

- Universal Print Server peut empêcher le service de spouleur d'impression de répondre. [LC9341]

VDA de gestion des profils utilisateur

- Après la mise à niveau du VDA de la version 7.13 à la version 7.15.2000, il est possible que Citrix Director n'affiche pas les dossiers redirigés. Le problème se produit lorsque la redirection de dossiers fonctionne toujours. [LC9968]
- L'utilisation de l'UC par le processus brokeragent.exe peut être élevée. [LD0310]

VDA pour OS de bureau

HDX

- Le service de redirection vidéo Citrix HDX HTML5 (WebSocketService.exe) peut se fermer de manière inattendue et la vidéo ne pas être redirigée sur la page HTML5. [LC8825]
- Lorsqu'une application publiée qui s'exécute sur un VDA utilise un chemin générique tel que %ProgramFiles% ou %ProgramFiles(x86)%, une nouvelle fenêtre d'application dupliquée peut s'ouvrir lors de la reconnexion de la session. [LC9741]

Impression

- Une violation d'accès dans **CpSvc!CDispatcher::UpdateCounters** peut provoquer la fermeture inattendue du service Citrix Print Manager (cpsvc.exe). [LC8804]

- L'imprimante par défaut peut ne pas être définie pour les applications non .net. Microsoft Windows Server 2016 ne parvient pas à mettre à jour la valeur sous la clé de Registre **HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\Device** lorsque l'imprimante par défaut est l'imprimante mappée Citrix. [LC8984]
- L'imprimante par défaut peut être définie de manière incorrecte dans une session. Le problème se produit lorsque l'imprimante par défaut bascule sur une autre imprimante aléatoire. [LC8999]
- Lors de la reconnexion à une session, les imprimantes mappées dans une session peuvent se charger lentement lors de l'utilisation de noms d'imprimante hérités. [LC9079]
- Dans certains fichiers Microsoft Excel, lorsque vous accédez à **Excel** > **Imprimer**, puis sélectionnez une imprimante cliente créée automatiquement à l'aide du pilote Citrix Universal Printer EMF, les caractères de l'aperçu avant impression peuvent apparaître plus petits. [LC9700]
- Le service de gestion des impressions Citrix (cpsvc.exe) peut s'arrêter de façon inattendue. Le problème se produit lorsque **cpwsGetPrinterConnectionsFromPolicy** transmet un pointeur nul à la chaîne de comparaison **[MS] _wcsicmp**. [LC9796]

Session/Connexion

- La webcam peut cesser de répondre dans une session utilisateur. Le problème se produit lorsque vous effectuez l'une des actions suivantes :
  - Lorsque vous utilisez certaines applications tierces pour sélectionner une webcam dans une session utilisateur, les trames vidéo de la webcam ne répondent plus.
  - Lorsque vous utilisez l'outil GraphEdit pour démarrer une webcam virtuelle et sélectionnez l'option Utiliser l'horloge (Use clock) dans le menu.
  - Lors de l'analyse des traces CDF (Citrix Diagnostics Facility), vous constatez qu'un seul échantillon vidéo est distribué lorsque le pipeline de distribution entre le VDA et Citrix Receiver pour Windows est établi. [LC8382]
- La désactivation de Citrix Hooks est susceptible d'échouer lorsque plusieurs exécutables sont ajoutés à **ExcludedImageNames** sous la clé de registre **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHoo** [LC8614]
- Citrix Director peut signaler Multi-Stream ICA comme inactif lors de l'utilisation du **protocole UDT (protocole de transfert des données basé sur UDP)**. Le problème se produit lorsque HDX WMI Provider n'est pas mis à jour pour prendre en compte les sessions EDT ou UDT. [LC8960]
- Des irrégularités dans le mouvement de la souris sont susceptibles de survenir au sein d'un environnement à plusieurs écrans utilisant la configuration H. Vous pouvez démarrer une session Microsoft Skype Entreprise et lancer le partage d'écran avec l'autre utilisateur. Le système d'exploitation transmet un emplacement de souris incorrect au pilote graphique Citrix.

Pour activer cette correction, définissez la clé de registre suivante :

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA

Nom : DisableAppendMouse

Type : DWORD

Données : 00000001

Cependant, si vous utilisez une session HDX après la définition de la clé de registre, certaines fonctionnalités programmant l'emplacement du curseur de la souris sont susceptibles de ne pas fonctionner comme prévu. Ces fonctionnalités sont les suivantes :

- La fonctionnalité d'alignement de la souris.
- La possibilité de synchroniser l'emplacement de la souris entre utilisateurs grâce au partage d'écran GoToMeeting.
- La possibilité de synchroniser l'emplacement de la souris entre utilisateurs grâce au partage d'écran Skype Entreprise. [LC8976]

- Dans certains scénarios, les VDA peuvent se réenregistrer automatiquement avec l'ID d'événement 1048. Par exemple, lorsque vous démarrez deux applications avec des noms similaires, Lotus Notes et Lotus Notes Standard, et fermez la deuxième application que vous avez démarrée, l'entrée de la première application est supprimée du registre. Lorsque cette information est envoyée au Delivery Controller via une notification, cette notification est rejetée et entraîne le réenregistrement. [LC9223]
- HDX RealTime Connector peut se fermer de manière inattendue. La fenêtre d'aperçu vidéo se ferme ou la fenêtre d'aperçu vidéo affiche une zone noire pendant un bref instant, puis se ferme. Le problème se produit lorsque HDX RealTime Media Engine n'est pas installé sur le point de terminaison. [LC9282]
- Le service audio Citrix peut se fermer de manière inattendue, puis redémarrer. Lors de la reconnexion à la même session à partir du second point terminal (client fin), les nouveaux appareils ne sont pas mappés correctement avec la session. [LC9381]
- Si vous sélectionnez la fonction Effacer ou Supprimer le Presse-papiers dans une application publiée qui s'exécute sur un VDA, le Presse-papiers du VDA est effacé mais le texte reste dans le Presse-papiers du point de terminaison. [LC9434]
- Lorsque vous déconnectez une session utilisateur du premier point de terminaison, puis que vous vous reconnectez à la même session à partir du second point de terminaison (client léger), les périphériques audio côté client peuvent être répertoriés dans un ordre incorrect dans le VDA.

  Pour activer cette correction, définissez la clé de registre suivante :

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Audio

  Nom : CleanMappingWhenDisconnect

Type : DWORD

Valeur : 1 [LC9440]

- Les sessions d'applications publiées peuvent se déconnecter et les sessions utilisateur risquent de ne pas se déconnecter correctement des VDA. Lorsque le problème se produit, vous ne pourrez peut-être pas vous reconnecter et ne pourrez pas vous déconnecter de Citrix Studio. Pour remédier à cette situation, définissez les sessions sur Caché à l'aide de la commande PowerShell ou redémarrez le VDA. [LC9444]
- Lors de l'utilisation d'un VDA version 7.15.1000, un nombre anormal d'instructions d'UC provenant de twi3.dll peut passer par le processus Winlogon.exe. [LC9450]
- Si la stratégie Redirection de lecteur client est désactivée, lorsque vous démarrez une application pour la deuxième fois à partir de la machine utilisateur, le démarrage de l'application peut prendre un certain temps. [LC9477]
- Lorsque vous essayez de vous reconnecter à une session existante active à partir d'un autre point de terminaison, ce message d'erreur s'affiche :

  Connexion interrompue ; Receiver tentera de se reconnecter pendant 5 minutes.

  Le problème se produit sur Microsoft Windows 7 avec VDA 7.15 installé. [LC9485]
- Une application Web est ouverte à l'aide du navigateur Microsoft Internet Explorer ou Mozilla Firefox. Lorsque vous ouvrez certains onglets dans l'application, le bureau entier peut cesser de répondre. [LC9508]
- Le compteur de performances d'instance **Total serveur** peut être absent des compteurs **Session ICA**. [LC9537]
- L'association de type de fichier avec Local App Access activé peut ne pas fonctionner lorsque les fichiers se trouvent sur le lecteur DFS (Distributed File System). [LC9538]
- L'ID d'événement 31 **Démarrer l'écoute des connexions** peut ne pas être transmis à l'**observateur d'événements.** [LC9556]
- Avec le **mappage de clavier Unicode** activé, les applications publiées ne peuvent pas être déconnectées. [LC9590]
- Lorsque vous basculez entre les dispositions de clavier, une fenêtre contextuelle peut apparaître. Définissez la clé de registre suivante pour supprimer la fenêtre contextuelle :

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\IcaIme

  Nom : HideNotificationWindow

  Type : DWORD

  Valeur : 1 [LC9592]

- Une application publiée peut se fermer par intermittence immédiatement après le démarrage de l'application en raison d'un échec inattendu. Le problème se produit lorsque les informations sur les processus actifs sont récupérées. [LC9661]
- Après la mise à niveau de XenApp et XenDesktop de la version 7.6 vers la mise à jour cumulative 1 de la version 7.15 LTSR, certains services peuvent s'arrêter ou se fermer de manière inattendue ou ne plus répondre de manière intermittente lors de la connexion. [LC9679]
- Les VDA peuvent ne plus répondre après l'installation de la mise à jour cumulative 2 de XenApp et XenDesktop 7.15 LTSR. [LC9701]
- Une fois que vous avez désactivé certains chiffrements via le registre Microsoft HKEY_LOCAL_MACHINE\SYSTE il est possible que TLS ne soit pas activé. [LC9743]
- Lorsque vous accédez à un poste de travail Windows via un accès PC distant et que vous vous déconnectez de la session Accès PC distant, il est possible que le poste de travail ne soit pas verrouillé. Par conséquent, le poste de travail est accessible à toute personne pouvant atteindre physiquement le poste de travail. [LC9812]
- La touche de langue **Kana** de l'éditeur de méthode d'entrée (IME) japonais peut être automatiquement activée lorsque vous vous connectez à un VDA. [LC9932]
- Avec ce correctif, le mécanisme de processus de liste blanche est ajouté à SCardHook. Lorsque la liste blanche est définie dans le registre, seuls les processus inclus dans la liste blanche peuvent utiliser la redirection de carte à puce.

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard

  Nom: HookProcessWhitelist

  Type : REG_SZ

  Valeur : <process name> [LC9961]
- Lorsque vous déconnectez une session utilisateur du premier point de terminaison, puis que vous vous reconnectez à la même session à partir d'un client léger, les périphériques audio côté client peuvent être répertoriés dans un ordre incorrect dans le VDA.

  Pour activer cette correction, définissez la clé de registre suivante :

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Audio

  Nom : CleanMappingWhenDisconnect

  Type : DWORD

  Valeur : 1 [LD0458]

Exceptions système

- Les serveurs peuvent rencontrer une exception fatale sur picadm.sys et afficher un écran bleu, avec le code bugcheck 0x22. (FILE_SYSTEM). [LC7726]
- Lorsque Enlightened Data Transport (EDT) est activé, les serveurs peuvent rencontrer une exception fatale sous tdica.sys et afficher un écran bleu avec le code bugcheck **SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e)**. [LC8794]
- Les serveurs peuvent rencontrer une exception fatale sur picadm.sys et afficher un écran bleu, avec le code bugcheck0x000000D1(DRIVER_IRQL_NOT_LESS_OR_EQUAL). [LC8830]
- Le VDA peut rencontrer une exception fatale sur wdica.sys et afficher un écran bleu. [LC9695]
- Le processus wfshell.exe peut se fermer de manière inattendue lorsque vous tentez de démarrer une application publiée. Le problème se produit lorsque la stratégie Redirection bidirectionnelle du contenu est activée, alors qu'aucune URL n'est fournie. [LC9705]
- Microsoft Windows Server 2008 R2 rencontrer une exception fatale et afficher un écran bleu avec le code bugcheck **SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (0x1000007E)**. Le problème se produit lorsque XenApp et XenDesktop 7.15 LTSR CU2 est installé sur Microsoft Windows Server. [LC9849]
- Les serveurs peuvent rencontrer une exception fatale sous picavc.sys et afficher un écran bleu avec le code bugcheck **SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e)**. [LD0006]

Expérience utilisateur

- Lorsque vous redimensionnez et tentez de déplacer l'application publiée d'un moniteur à un autre, une bordure blanche peut apparaître autour de l'application. [LC9570]
- Configurez un VDA pour utiliser le **mappage du clavier Unicode** et établissez une session HDX à partir de Citrix Receiver avec l'IME local activé. Lorsque vous tapez un caractère, puis sélectionnez tout ou partie des caractères de sortie dans une application publiée, les nouveaux caractères sont insérés avant les caractères sélectionnés au lieu de les remplacer. [LC9591]
- Lorsque vous modifiez la résolution de l'écran et que vous vous reconnectez à l'application publiée à partir d'un VDA pour OS de bureau, la fenêtre de l'application peut être tronquée. [LC9947]
- Dans un environnement multi-moniteur, dans certains scénarios, l'écran ne se verrouille pas comme prévu. [LD0186]

Interface utilisateur

- Lorsqu'une fenêtre d'application dans une session transparente cesse de répondre, l'icône de la barre des tâches de la fenêtre d'application peut être supprimée et recréée. [LC9807]

VDA pour OS de serveur

HDX

- Le service de redirection vidéo Citrix HDX HTML5 (WebSocketService.exe) peut se fermer de manière inattendue et la vidéo ne pas être redirigée sur la page HTML5. [LC8825]
- Lorsqu'une application publiée qui s'exécute sur un VDA utilise un chemin générique tel que %ProgramFiles% ou %ProgramFiles(x86)%, une nouvelle fenêtre d'application dupliquée peut s'ouvrir lors de la reconnexion de la session. [LC9741]

Impression

- Une violation d'accès dans **CpSvc!CDispatcher::UpdateCounters** peut provoquer la fermeture inattendue du service Citrix Print Manager (cpsvc.exe). [LC8804]
- L'imprimante par défaut peut ne pas être définie pour les applications non .net. Microsoft Windows Server 2016 ne parvient pas à mettre à jour la valeur sous la clé de Registre HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\Device lorsque l'imprimante par défaut est l'imprimante mappée Citrix. [LC8984]
- L'imprimante par défaut peut être définie de manière incorrecte dans une session. Le problème se produit lorsque l'imprimante par défaut bascule sur une autre imprimante aléatoire. [LC8999]
- Lors de la reconnexion à une session, les imprimantes mappées dans une session peuvent se charger lentement lors de l'utilisation de noms d'imprimante hérités. [LC9079]
- Dans certains fichiers Microsoft Excel, lorsque vous accédez à Excel > Imprimer, puis sélectionnez une imprimante cliente créée automatiquement à l'aide du pilote Citrix Universal Printer EMF, les caractères de l'aperçu avant impression peuvent apparaître plus petits. [LC9700]
- Le service de gestion des impressions Citrix (cpsvc.exe) peut s'arrêter de façon inattendue. Le problème se produit lorsque **cpwsGetPrinterConnectionsFromPolicy** transmet un pointeur nul à la chaîne de comparaison **[MS]_wcsicmp**. [LC9796]

Session/Connexion

- Après la mise à niveau du VDA de la version 7.12 à la version 7.13, les lecteurs de badges peuvent ne plus fonctionner. [LC7667]
- La webcam peut cesser de répondre dans une session utilisateur. Le problème se produit lorsque vous effectuez l'une des actions suivantes :

  - Lorsque vous utilisez certaines applications tierces pour sélectionner une webcam dans une session utilisateur, les trames vidéo de la webcam ne répondent plus.
  - Lorsque vous utilisez l'outil GraphEdit pour démarrer une webcam virtuelle et sélectionnez l'option Utiliser l'horloge (Use clock) dans le menu.
  - Lors de l'analyse des traces CDF (Citrix Diagnostics Facility), vous constatez qu'un seul échantillon vidéo est distribué lorsque le pipeline de distribution entre le VDA et Citrix Receiver pour Windows est établi. [LC8382]

- La désactivation de Citrix Hooks est susceptible d'échouer lorsque plusieurs exécutables sont ajoutés à **ExcludedImageNames** sous la clé de registre **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHoo** [LC8614]
- Une fausse session XenApp peut être créée sur un VDA pour un OS de serveur lorsqu'une session de bureau distant se déconnecte et se reconnecte. [LC8706]
- Des irrégularités dans le mouvement de la souris sont susceptibles de survenir au sein d'un environnement à plusieurs écrans utilisant la configuration H. Vous pouvez démarrer une session Microsoft Skype Entreprise et lancer le partage d'écran avec l'autre utilisateur. Le système d'exploitation transmet un emplacement de souris incorrect au pilote graphique Citrix.

  Pour activer cette correction, définissez la clé de registre suivante :

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA

  Nom : DisableAppendMouse

  Type : DWORD

  Valeur : 00000001

  Cependant, si vous utilisez une session HDX après la définition de la clé de registre, certaines fonctionnalités programmant l'emplacement du curseur de la souris sont susceptibles de ne pas fonctionner comme prévu. Ces fonctionnalités sont les suivantes :

  - La fonctionnalité d'alignement de la souris.
  - La possibilité de synchroniser l'emplacement de la souris entre utilisateurs grâce au partage d'écran GoToMeeting.
  - La possibilité de synchroniser l'emplacement de la souris entre utilisateurs grâce au partage d'écran Skype Entreprise. [LC8976]

- Dans certains scénarios, les VDA peuvent se réenregistrer automatiquement avec l'ID d'événement 1048. Par exemple, lorsque vous démarrez deux applications avec des noms similaires, Lotus Notes et Lotus Notes Standard, et fermez la deuxième application que vous avez démarrée, l'entrée de la première application est supprimée du registre. Lorsque cette information est envoyée au Delivery Controller via une notification, cette notification est rejetée et entraîne le réenregistrement. [LC9223]

- HDX RealTime Connector peut se fermer de manière inattendue. La fenêtre d'aperçu vidéo se ferme ou la fenêtre d'aperçu vidéo affiche une zone noire pendant un bref instant, puis se ferme. Le problème se produit lorsque HDX RealTime Media Engine n'est pas installé sur le point de terminaison. [LC9282]
- Vous démarrez Microsoft Excel 2007 dans un bureau publié, ouvrez un fichier .xslm avec macros activées et redimensionnez le fichier en mode fenêtré sur Desktop Viewer. La session pourrait ne plus répondre. Le problème se produit lors de l'utilisation du raccourci clavier **Alt + Entrée**. [LC9379]
- Le service audio Citrix peut se fermer de manière inattendue, puis redémarrer. Lors de la reconnexion à la même session à partir du second point terminal (client fin), les nouveaux appareils ne sont pas mappés correctement avec la session. [LC9381]
- Si vous sélectionnez la fonction Effacer ou Supprimer le Presse-papiers dans une application publiée qui s'exécute sur un VDA, le Presse-papiers du VDA est effacé mais le texte reste dans le Presse-papiers du point de terminaison. [LC9434]
- Les sessions d'applications publiées peuvent se déconnecter et les sessions utilisateur risquent de ne pas se déconnecter correctement des VDA. Lorsque le problème se produit, vous ne pourrez peut-être pas vous reconnecter et ne pourrez pas vous déconnecter de Citrix Studio. Pour remédier à cette situation, définissez les sessions sur Caché à l'aide de la commande PowerShell ou redémarrez le VDA. [LC9444]
- Lors de l'utilisation d'un VDA version 7.15.1000, un nombre anormal d'instructions d'UC provenant de twi3.dll peut passer par le processus Winlogon.exe. [LC9450]
- Si la stratégie Redirection de lecteur client est désactivée, lorsque vous démarrez une application pour la deuxième fois à partir de la machine utilisateur, le démarrage de l'application peut prendre un certain temps. [LC9477]
- Une application Web est ouverte à l'aide du navigateur Microsoft Internet Explorer ou Mozilla Firefox. Lorsque vous ouvrez certains onglets dans l'application, le bureau entier peut cesser de répondre. [LC9508]
- Le compteur de performances d'instance **Total serveur** peut être absent des compteurs **Session ICA**. [LC9537]
- L'association de type de fichier avec Local App Access activé peut ne pas fonctionner lorsque les fichiers se trouvent sur le lecteur DFS (Distributed File System). [LC9538]
- Avec le **mappage de clavier Unicode** activé, les applications publiées ne peuvent pas être déconnectées. [LC9590]
- Lorsque vous basculez entre les dispositions de clavier, une fenêtre contextuelle peut apparaître. Définissez la clé de registre suivante pour supprimer la fenêtre contextuelle :

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\IcaIme

Nom : HideNotificationWindow

Type : DWORD

Valeur : 1 [LC9592]

- Une application publiée peut se fermer par intermittence immédiatement après le démarrage de l'application en raison d'un échec inattendu. Le problème se produit lorsque les informations sur les processus actifs sont récupérées. [LC9661]
- Dans des environnements multi-forêts ou à plusieurs domaines, il se peut que vous ne puissiez pas démarrer la deuxième application lorsque les groupes locaux sont configurés pour une visibilité limitée. [LC9665]
- Après la mise à niveau de XenApp et XenDesktop de la version 7.6 vers la mise à jour cumulative 1 de la version 7.15 LTSR, certains services peuvent s'arrêter ou se fermer de manière inattendue ou ne plus répondre de manière intermittente lors de la connexion. [LC9679]
- Les VDA peuvent ne plus répondre après l'installation de la mise à jour cumulative 2 de XenApp et XenDesktop 7.15 LTSR. [LC9701]
- Une fois que vous avez désactivé certains chiffrements via le registre Microsoft HKEY_LOCAL_MACHINE\SYSTE il est possible que TLS ne soit pas activé. [LC9743]
- Vous connectez un périphérique de stockage USB lors de l'ouverture de session et vous redirigez en mode générique. Le lecteur peut continuer à exister une fois que le périphérique USB a été déconnecté. [LC9783]
- La touche de langue **Kana** de l'éditeur de méthode d'entrée (IME) japonais peut être automatiquement activée lorsque vous vous connectez à un VDA. [LC9932]
- Avec ce correctif, le mécanisme de processus de liste blanche est ajouté à SCardHook. Lorsque la liste blanche est définie dans le registre, seuls les processus inclus dans la liste blanche peuvent utiliser la redirection de carte à puce.

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard

  Nom : HideNotificationWindow

  Type : REG_SZ

  Valeur : <process name> [LC9961]
- Le processus wfshell.exe peut se fermer de manière inattendue. Par conséquent, l'application publiée ne démarre pas. [LD0102]
- Après la mise à niveau du VDA vers la mise à jour cumulative de la version 7.15 ou la mise à niveau depuis la mise à jour cumulative 1 vers la mise à jour cumulative 2 de la version 7.15, les valeurs configurées **AnonymousUserIdleTime** et **MaxAnonymousUsers** sous la clé de registre,

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix pourrait être supprimé. [LD0378]

Cartes à puce

- Vous définissez la valeur de Registre DisableLogonUISuppression sur 0 sous la clé de Registre HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Citrix Virtual Desktop Agent. Lorsque vous démarrez une application publiée, le VDA peut vous demander de taper le code de la carte à puce. Le message **Veuillez attendre le Gestionnaire de session locale** s'affiche dans Citrix Receiver pour Windows et finit par disparaître, car la valeur 0 de **DisableLogonUISuppression** supprime l'invite à entrer un code. Par conséquent, l'invite à entrer un code n'apparaît jamais.

  Pour activer cette correction, définissez la clé de registre suivante :

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Citrix Virtual Desktop Agent

  Nom : DisableLogonUISuppressionForSmartCardPublishedApps

  Type : DWORD

  Valeur : 1 [LC9059]

Exceptions système

- Les serveurs peuvent rencontrer une exception fatale sur picadm.sys et afficher un écran bleu, avec le code bugcheck 0x22. (FILE_SYSTEM). [LC7726]
- Lorsque Enlightened Data Transport (EDT) est activé, les serveurs peuvent rencontrer une exception fatale sous tdica.sys et afficher un écran bleu avec le code bugcheck **SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e)**. [LC8794]
- Les serveurs peuvent rencontrer une exception fatale sur picadm.sys et afficher un écran bleu, avec le code bugcheck0x000000D1(DRIVER_IRQL_NOT_LESS_OR_EQUAL). [LC8830]
- Le VDA peut rencontrer une exception fatale sur wdica.sys et afficher un écran bleu. [LC9695]
- Le processus wfshell.exe peut se fermer de manière inattendue lorsque vous tentez de démarrer une application publiée. Le problème se produit lorsque la stratégie Redirection bidirectionnelle du contenu est activée, alors qu'aucune URL n'est fournie. [LC9705]
- Lorsque vous démarrez une application, le processus wfshell.exe peut se fermer de manière inattendue. Le problème se produit en raison du module défaillant icaendpoint.dll. [LC9737]
- Microsoft Windows Server 2008 R2 rencontrer une exception fatale et afficher un écran bleu avec le code bugcheck **SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (0x1000007E)**. Le problème se produit lorsque XenApp et XenDesktop 7.15 LTSR CU2 est installé sur Microsoft Windows Server. [LC9849]

- Les serveurs peuvent rencontrer une exception fatale sous picavc.sys et afficher un écran bleu avec le code bugcheck **SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e)**. [LD0006]

Expérience utilisateur

- Lorsque vous tentez d'ouvrir un lien hypertexte à partir de certaines applications tierces (telles qu'Aurion) qui s'exécutent sur un VDA pour OS de serveur, une chaîne supplémentaire %1 peut être ajoutée au début de l'URL. [LC8952]
- Lorsque vous redimensionnez et tentez de déplacer l'application publiée d'un moniteur à un autre, une bordure blanche peut apparaître autour de l'application. [LC9570]
- Configurez un VDA pour utiliser le **mappage du clavier Unicode** et établissez une session HDX à partir de Citrix Receiver avec l'IME local activé. Lorsque vous tapez un caractère, puis sélectionnez tout ou partie des caractères de sortie dans une application publiée, les nouveaux caractères sont insérés avant les caractères sélectionnés au lieu de les remplacer. [LC9591]

Interface utilisateur

- Un avis juridique apparaît au début de l'écran d'ouverture de session dans une session utilisateur. Avec Local App Access activé, lorsque vous cliquez sur **OK** sur l'écran d'ouverture de session pour continuer, l'écran peut afficher l'avis juridique pendant plusieurs secondes avant de poursuivre l'ouverture de session. [LC9408]
- Lorsqu'une fenêtre d'application dans une session transparente cesse de répondre, l'icône de la barre des tâches de la fenêtre d'application peut être supprimée et recréée. [LC9807]
- Lorsque vous essayez de démarrer une application publiée, l'écran Citrix Receiver pour Windows peut apparaître dans le coin inférieur droit. [LC9817]

Composants de bureau virtuel - Autre

- Les tentatives d'annulation de publication et de suppression des packages App-V du VDA peuvent échouer. [LC9161]
- Le dépassement de la mémoire cache dans l'optimisation MCSIO (Machine Creation Services) peut nuire aux performances des machines virtuelles XenServer. [LC9351]
- Les requêtes WMI en cours d'exécution sur le VDA peuvent ne plus répondre pendant une durée indéterminée. [LC9510]
- Les tentatives d'exécution de plusieurs instances de la même application App-V dans la même session peuvent échouer. Le problème se produit lorsque le processus en cours d'exécution est différent du processus défini dans le fichier manifeste. [LC9652]

- Lorsque le navigateur Microsoft Edge est exécuté sur le VDA, plusieurs entrées d'application peuvent apparaître sous le **Gestionnaire d'activités** dans Citrix Director pendant que vous recherchez l'utilisateur. [LC9673]

Mise à jour cumulative 2 (CU2)

February 28, 2019

À propos de cette version

La mise à jour cumulative 2 (CU2) de XenApp et XenDesktop 7.15 LTSR résout plus de 150 problèmes signalés depuis la publication de la version 7.15 LTSR CU1.

7.15 LTSR (informations générales)

Problèmes résolus depuis XenApp et XenDesktop 7.15 LTSR CU1

Problèmes connus dans cette version

Téléchargements

Télécharger 7.15 LTSR CU2

Nouveaux déploiements

Comment effectuer un nouveau déploiement CU2 ?

Vous pouvez configurer un nouvel environnement XenApp et XenDesktop basé sur CU2, à l'aide du metainstaller CU2. Avant d'effectuer cette configuration, nous vous recommandons de vous familiariser avec le produit :

Consultez la section XenApp et XenDesktop 7.15 LTSR (version initiale) et prêtez une attention particulière aux sections Vue d'ensemble technique, Installer et configurer et Sécurité avant de commencer à planifier votre déploiement. Assurez-vous que votre installation correspond à la configuration système requise pour tous les composants.

Déploiements existants

Que dois-je mettre à jour ?

CU2 fournit des mises à jour pour les composants de base de 7.15 LTSR. Rappel : Citrix vous recommande de mettre à niveau vers CU2 tous les composants LTSR de votre déploiement. Par exemple : si

Provisioning Services fait partie de votre déploiement LTSR, mettez à jour les composants Provisioning Services vers CU2. Si Provisioning Services ne fait pas partie de votre déploiement, vous n'avez pas besoin de l'installer ni de le mettre à jour.

Composants de base CU2 XenApp et XenDesktop 7.15 LTSR

Composants LTSR 7.15 de base	Version	Remarques
VDA pour OS de bureau	7.15.2000	
VDA pour OS de serveur	7.15.2000	
Delivery Controller	7.15.2000	
Citrix Studio	7.15.2000	
Citrix Director	7.15.2000	
Expérience Gestion des stratégies de groupe	3.1.2000	
StoreFront	3.12.2000	
Provisioning Services	7.15.3	
Serveur d'impression universelle	7.15.2000	
Enregistrement de session	7.15.2000	Édition Platinum uniquement
Linux VDA	7.15.2000	Consultez la documentation VDA Linux pour en savoir plus sur les plates-formes prises en charge
Profile Management	7.15.2000	
Service d'authentification fédérée	7.15.2000	

Composants compatibles CU2 XenApp et XenDesktop 7.15 LTSR

Les composants suivants, dans les versions indiquées ci-dessous, sont compatibles avec les environnements LTSR. Ils ne bénéficient pas des avantages du programme LTSR (cycle de vie prolongé et mises à jour cumulatives contenant uniquement des corrections). Citrix peut vous demander de mettre à niveau vers une version plus récente de ces composants dans vos environnements 7.15 LTSR :

Plates-formes et composants compatibles avec LTSR 7.15 CU2	Version
Application Layering	4.10.0
Citrix SCOM Management Pack pour Serveur de licences	1.2
Citrix SCOM Management Pack pour Provisioning Services	1.19
Citrix SCOM Management Pack pour StoreFront	1.13
Citrix SCOM Management Pack pour XenApp et XenDesktop	3.14
Pack d'optimisation HDX RealTime	2.4
Serveur de licences	11.14.0.1 Build 23101
Réinitialisation en libre-service des mots de passe	1.1.10.0
Workspace Environment Management	4.6

Versions Citrix Receiver compatibles

Pour faciliter la maintenance et pour garantir des performances optimales, Citrix vous recommande de mettre à niveau vers la dernière version de Citrix Receiver dès qu'elle est disponible. Les dernières versions sont disponibles au téléchargement sur téléchargements. À des fins de commodité, pensez à vous inscrire au flux RSS Citrix Receiver pour être notifié lorsqu'une nouvelle version de Citrix Receiver est disponible.

Citrix Receiver ne peut pas bénéficier des avantages du programme LTSR de XenApp et XenDesktop (cycle de vie prolongé et mises à jour cumulatives contenant uniquement des corrections). Citrix peut vous demander de mettre à niveau vers une version plus récente de Citrix Receiver dans vos environnements 7.15 LTSR. Pour Citrix Receiver pour Windows, Citrix a annoncé un programme LTSR spécial. Pour de plus amples informations sur ce programme, consultez la page Étapes du cycle de vie de Citrix Receiver.

Plus spécifiquement, 7.15 LTSR CU2 prend en charge les versions suivantes de Citrix Receiver et toutes les versions ultérieures.

Version Citrix Receiver compatible avec 7.15 LTSR CU2	Version
Citrix Receiver pour Android	3.13.5 ou supérieur

Version Citrix Receiver compatible avec 7.15 LTSR CU2	Version
Citrix Receiver pour Chrome	2.6.5 ou supérieur
Citrix Receiver pour HTML5	2.6.5 ou supérieur
Citrix Receiver pour iOS	7.5.3 ou supérieur
Citrix Receiver pour Linux	13.9.1 ou supérieur
Citrix Receiver pour Mac	12.9 ou version ultérieure
Citrix Receiver pour la plateforme Windows universelle (UWP)	1.0.5 ou version ultérieure
Citrix Receiver pour Windows	4.9 ou version ultérieure

Exclusions notables pour XenApp et XenDesktop 7.15 LTSR

Les fonctionnalités, plates-formes et composants suivants ne bénéficient pas des avantages et des étapes de cycle de vie du programme 7.15 LTSR. Plus précisément, le cycle de vie prolongé et les mises à jour cumulatives contenant uniquement des corrections sont exclus. Les mises à jour des fonctionnalités et composants exclus sont disponibles au travers des versions régulières.

Fonctions exclues
Framehawk
Intégration de StoreFront Citrix Online

Composants exclus
Personal vDisk : exclu pour les machines Windows 10 ; pour les machines Windows 7, prise en charge LTSR limitée jusqu'au 14 janvier 2020 (exigences de CU s'appliquent)
AppDisks

Plates-formes Windows exclues *
Windows 2008 32bits (pour le serveur d'impression universelle)

* Citrix se réserve le droit de mettre à jour la prise en charge des plates-formes en fonction des étapes

du cycle de vie des fournisseurs tiers.

Installer et mettre à niveau les outils d'analyse

Lorsque vous utilisez le programme d'installation du produit complet pour déployer et mettre à niveau les composants XenApp ou XenDesktop, des informations anonymes sur le processus d'installation sont collectées et stockées sur la machine sur laquelle vous installez/mettez à niveau le composant. Ces données sont utilisées pour aider Citrix à améliorer l'expérience de ses clients avec l'installation. Pour plus d'informations, veuillez consulter l'article https://more.citrix.com/XD-INSTALLER.

Migration XenApp 6.5

Le processus de migration de XenApp 6.5 vous aide à effectuer une transition rapidement et efficacement depuis une batterie XenApp 6.5 vers un site exécutant XenApp 7.15 LTSR CU2. Ceci est utile dans les déploiements contenant un grand nombre d'applications et de stratégies de groupe Citrix : réduisant le risque d'introduction d'erreurs par inadvertance lors du déplacement manuel des applications et des stratégies de groupe Citrix vers le nouveau site XenApp.

Après avoir installé les composants principaux XenApp 7.15 LTSR CU2 et créé un site, le processus de migration suit cette séquence :

- Exécutez le programme d'installation de XenApp 7.15 CU2 sur chaque tâche XenApp 6.5, qui effectue une mise à niveau automatique vers un nouveau Virtual Delivery Agent pour OS de serveur à utiliser dans le nouveau site.
- Exécutez les applets de commande d'exportation PowerShell sur un Controller XenApp 6.5, qui permet d'exporter les paramètres de stratégie et d'application Citrix vers des fichiers XML.
- Modifiez les fichiers XML, le cas échéant, pour affiner les éléments que vous voulez importer dans le nouveau site. En personnalisant les fichiers, vous pouvez importer les paramètres de stratégie et d'application dans votre site XenApp 7.15 LTSR CU2 par étape : certaines maintenant et d'autres ultérieurement.
- Exécutez les applets de commande d'importation PowerShell sur le nouveau Controller XenApp 7.15 CU2, qui importe les paramètres depuis les fichiers XML vers le nouveau site XenApp.

Reconfigurez le nouveau site si nécessaire, puis testez-le.

Pour plus d'informations, voir Migrer XenApp 6.x.

Problèmes résolus

February 28, 2019

Citrix Director

- Lorsque vous filtrez les machines par nom DNS, Citrix Director n'affiche aucune machine ou affiche des entrées en double des machines. Ce problème se produit lorsque la machine est ajoutée pour la première fois à la base de données de surveillance, mais qu'elle est ajoutée simultanément à partir de deux Delivery Controller différents. Par conséquent, deux entrées de machine sont créées. [LC4905]
- Une exception peut se produire lorsque vous, en tant qu'administrateur personnalisé, ne pouvez pas extraire le paramètre Remote PC du catalogue de machines. Le problème se produit lorsque vous avez l'autorisation de gérer le catalogue de machines, mais que l'étendue ne contient pas le catalogue particulier. [LC8170]
- Lorsque vous accédez à **Filtres** > **Sessions** dans Citrix Director et essayez de redimensionner le navigateur, le tableau entier peut être aligné incorrectement. [LC8624]
- Le fichier CSV devient inutilisable lorsque vous exportez des données à partir de Citrix Director. Ce problème peut se produire lorsque vous définissez des versions non anglaises de Microsoft Windows en tant que langue d'affichage de Director, car les virgules peuvent être utilisées à la fois comme séparateurs de valeur et comme séparateur décimal. [LC8625]
- Lorsque vous démarrez Citrix Director, le message d'erreur suivant s'affiche dans l'onglet **Infrastructure** :

  « Impossible de récupérer les données. Connexion perdue avec le serveur Web. Vérifiez votre connexion réseau et réessayez. » [LC8752]
- Les noms des sites Citrix Director sont tronqués lorsque plusieurs sites sont configurés. [LC9258]

Stratégie Citrix

- Lorsque vous ouvrez une deuxième instance de l'éditeur de stratégie de groupe (gpedit.msc), le nœud Stratégies Citrix ne s'ouvre pas et le message d'erreur suivant peut s'afficher :

  « Exception non gérée dans le code managé du composant logiciel enfichable. » [LC7600]
- Lorsque vous appliquez des stratégies Citrix via la console GPMC (Console de gestion des stratégies de groupe), les stratégies peuvent ne pas apparaître dans les paramètres de stratégie GPMC. Toutefois, lors de la modification de l'objet de stratégie de groupe (GPO), vous pouvez voir les stratégies et les paramètres sont activés. [LC8282]
- L'utilisation de Gestion de stratégie de groupe Citrix 3.1 pour ajouter le paramètre **Attributions d'imprimantes** à une **stratégie utilisateur** dans Active Directory peut entraîner un problème de redimensionnement de la fenêtre. La fenêtre peut commencer à se redimensionner automatiquement à l'horizontale après son ouverture jusqu'à ce qu'elle s'étende jusqu'au coin de

l'écran. Par conséquent, la modification de la stratégie peut être difficile car vous ne pouvez pas accéder à toutes les colonnes. [LC8684]

- Lorsque les fichiers du dossier de cache des stratégies locales (%ProgramData%/CitrixCseCache) sont définis sur Lecture seule, les paramètres de stratégie peuvent ne pas être appliqués correctement. [LC8750]
- Les tentatives de lancement d'applications App-V en mode Administration mono-utilisateur depuis des VDA peuvent échouer. Le problème se produit lorsque la valeur de la clé de Registre **ApplicationStartDetails** est vide ou si les détails de l'application sont manquants dans la clé de Registre. [LC8798]
- Les tentatives d'ajout de machines à un groupe de mise à disposition en utilisant le nom NETBIOS pour les associations d'utilisateur peuvent échouer. Au lieu de cela, le nom de domaine peut s'afficher. Le problème se produit lorsque le nom NETBIOS utilise l'adresse URL incorrecte. [LC9393]

Citrix Studio

- Lorsque vous essayez d'ajouter une application depuis le VDA Linux manuellement, le message d'erreur suivant peut s'afficher :

  « Value cannot be null while publishing the application. »

  Toutefois, l'application est ajoutée avec succès lorsque vous cliquez sur « OK » dans le message d'erreur qui s'affiche. [LC7910]
- Les tentatives de suppression d'applications d'un groupe de mise à disposition peuvent échouer lorsque les applications se trouvent dans le sous-dossier du noeud **Application** dans Citrix Studio. [LC8705]
- Les tentatives d'ajout de machines à un groupe de mise à disposition en utilisant le nom NETBIOS pour les associations d'utilisateur peuvent échouer. Au lieu de cela, le nom de domaine peut s'afficher. Le problème se produit lorsque le nom NETBIOS utilise l'adresse URL incorrecte. [LC9393]

Controller

- Des caractères superflus peuvent apparaître à la fin de « Nom d'affichage du service » et « Description du service » de certains services Citrix installés sur un système d'exploitation japonais. [LC5208]
- Lorsque vous tentez de récupérer des données pour des sessions à partir de Citrix Director, des entrées NULL apparaissent dans la base de données de surveillance. Par conséquent, certaines données ne sont pas affichées dans Citrix Director et le message d'erreur suivant s'affiche :

« Impossible de récupérer les données. » [LC6273]

- Lorsque vous essayez d'ajouter une application depuis le VDA Linux manuellement, le message d'erreur suivant peut s'afficher :

  « Value cannot be null while publishing the application. »

  Toutefois, l'application est ajoutée avec succès lorsque vous cliquez sur « OK » dans le message d'erreur qui s'affiche. [LC7910]

- Après la mise à niveau du Delivery Controller vers LTSR version 7.15, l'ancien disque de base créé après la mise à jour du catalogue de machines n'est pas supprimé de l'image de l'hyperviseur. [LC8637]
- Le Citrix Broker Service (Brokerservice.exe) peut se fermer de manière inattendue. Le problème se produit en raison du module défaillant, LicPolEng.dll. [LC8638]
- Lorsque vous provisionnez les machines virtuelles (VM) avec les privilèges VMware requis au minimum via Machine Creation Services, les tentatives de suppression des machines virtuelles peuvent échouer. Cet échec peut se produire même avec les autorisations minimales accordées pour VMware. [LC8868]
- Lorsque vous essayez de créer un catalogue de machines utilisant le stockage Premium, il est possible que l'option permettant de sélectionner la taille de la machine virtuelle de type E-Series ou L-Series ne soit pas disponible. [LC9052]
- Lorsqu'un utilisateur Active Directory auquel est affectée une préférence de zone est supprimé, les tentatives d'importation de la configuration du broker vers le broker secondaire peuvent échouer. L'opération d'importation peut également échouer après la mise à niveau de XenDesktop vers la dernière version. [LC9269]
- Les tentatives d'ajout de machines à un groupe de mise à disposition en utilisant le nom NETBIOS pour les associations d'utilisateur peuvent échouer. Au lieu de cela, le nom de domaine peut s'afficher. Le problème se produit lorsque le nom NETBIOS utilise l'adresse URL incorrecte. [LC9393]

Redirection HDX MediaStream Flash

- Si la redirection Flash HDX MediaStream est activée, lorsque vous reconnectez une session VDA avec Qumu.com, le contenu Flash peut ne pas être chargé dans Microsoft Internet Explorer. [LC9193]

Programme d'installation

- Les tentatives de modification du chemin du répertoire d'installation dans Delivery Controller risquent de ne pas fonctionner pour **XaXdProxy.msi**. [LC8691]

Linux VDA

- L'enregistrement d'un VDA Linux à l'aide du Delivery Controller peut échouer par intermittence. [LC7982]
- Citrix Director 7.13 qui s'exécute sur un serveur Red Hat Enterprise Linux 7.3 peut ne pas afficher les détails de la session de la machine. Le message d'erreur suivant s'affiche :

  « Impossible de récupérer les données. » [LC8204]
- Un VDA Linux peut s'enregistrer auprès du Delivery Controller et annuler l'enregistrement après un certain temps. [LC8205]
- Certaines applications tierces utilisées pour vérifier l'affichage de la session d'un VDA Linux peuvent ne pas afficher tous les pixels. [LC8419]
- Lorsqu'il existe plusieurs serveurs LDAP, les tentatives de lancement d'une application sur un VDA Linux peuvent échouer après la mise à jour des stratégies et l'expiration d'une session. [LC8444]
- Le processus ctxhdx peut se fermer de manière inattendue avec une erreur segfault lorsque la session est connectée à un VDA Linux. [LC8611]
- Lorsque vous utilisez la version Linux VDA 7.16 Early Access, l'agent Broker peut ne pas obtenir le nom de l'application. Cet échec oblige Director à afficher l'erreur **Agent requis**, après quoi le réenregistrement commence. [LC9243]

Profile Management

- Après le redémarrage du service Profile Management, Citrix Director peut ne pas afficher les informations de connexion et de personnalisation de l'utilisateur. [LC6942]

Provisioning Services

- Lors de l'utilisation d'un Provisioning Server avec les paramètres régionaux finlandais installés, les tentatives de création de machines virtuelles à l'aide de l'Assistant d'installation XenDesktop peuvent échouer et le message d'erreur suivant s'afficher :

  « The bdmCreated field is not formatted properly, the correct format is YYYY-MM-DD HH:MM. » [#LC7866]

- Lorsque Boot Device Manager (BDM) est configuré pour le processus DHCP Discover, Offer, Request and Acknowledge (DORA), le processus peut ne pas se terminer. Le problème se produit lorsque le relais DHCP envoie le paquet OFFER en tant que paquet UNICAST. [#LC8130]
- La relation de confiance de la machine cible Linux peut être perdue avec Active Directory, lorsque le mot de passe du compte de la machine cible expire. [#LC8331]
- Les machines cibles ne peuvent pas démarrer correctement et continuent donc à redémarrer. [#LC8358]
- Une machine cible faisant partie d'un groupe de mise à disposition ne démarre pas après une mise à niveau depuis une version précédente de PVS. [#LC8378]
- L'assistant d'installation XenDesktop peut tenter de se connecter à un hôte Hyper-V incorrect. Le problème se produit lorsqu'il existe plusieurs clusters gérés par le même serveur SCVMM (System Center Virtual Machine Manager). [#LC8415]
- La réponse de l'assistant de configuration et des opérations de Provisioning Services Console peut être lente ou la console peut expirer dans un environnement Active Directory. [#LC8692]
- Les machines cibles peuvent cesser de communiquer de manière aléatoire avec le serveur Provisioning Server lors de l'opération de lecture initiale à partir du Personal vDisk (étape d'E/S unique). [#LC8745]
- Lorsque vous essayez de copier et coller les propriétés de vDisk entre deux vDisks, il est possible que les propriétés ne soient pas collées sur le deuxième vDisk. [#LC8767]
- Cette amélioration est un rétroportage de fonctionnalités introduites dans Provisioning Services 7.17. Elle est incluse en réponse aux demandes des clients. Pour plus d'informations, voir Amélioration de la recherche de groupes Active Directory à plusieurs niveaux. [#LC9064, #LC9066]
- Stream Service peut se fermer de manière inattendue alors que Provisioning Server semble être en panne dans le nœud Serveurs. [#LC9138]
- Les machines cibles peuvent cesser de répondre. [#LC7911]
- Une machine cible UEFI (Unified Extensible Firmware Interface) peut rencontrer une exception fatale avec affichage d'un écran bleu, sur CVhdMp.sys avec le code d'arrêt 0x0000007E. Cette exception peut se produire lors du démarrage d'une machine cible UEFI à partir d'un vDisk configuré avec l'association de cartes réseau. [#LC8548]
- Les machines cibles peuvent cesser de répondre. [#LC8897]
- Microsoft Windows 10 v1709 peut rencontrer une exception fatale, affichant un écran bleu lorsqu'il est présent en mode privé. [#LC8979] Microsoft Windows 10 v1709 32 bits ne peut pas démarrer à partir d'un vDisk en mode image privée. [#LC8980]

- Les machines cibles exécutées sous Microsoft Windows 10 risquent de ne plus répondre au niveau de l'écran Préparation des périphériques lors du redémarrage. [#LC8844]
- Les machines cibles peuvent ne plus répondre à l'écran d'ouverture de session ou de démarrage Windows. [#LC9104]

StoreFront

- Lorsque le paramètre « Lancement automatique du bureau » est activé, l'option « Multiple launch prevention » peut ne pas fonctionner. Par conséquent, les demandes ultérieures de lancement de la même instance du bureau échouent. [LC7430]
- Après la mise à niveau de StoreFront 2.6 installé sur un lecteur autre que celui par défaut, les données d'abonnement aux applications des utilisateurs peuvent ne pas être conservées. [LC8046]
- Après avoir redémarré la console StoreFront MMC, la valeur de la case à cocher **Afficher Desktop Viewer** peut s'afficher de manière incorrecte. [LC8520]
- Si vous exécutez une commande **Set-STFWebReceiverSiteStyle** avec un fichier PNG (la transparence est prise en charge) pour personnaliser StoreFront, le fichier PNG est converti en un fichier JPEG. Le format de fichier JPEG peut perdre la prise en charge de la transparence. [LC8677]
- Si vous exécutez une commande **Set-STFWebReceiverApplicationShortcuts** pour définir les URL approuvées pour les raccourcis d'application dans les sites Citrix Receiver pour Web, une barre oblique (« / ») peut être ajoutée à la fin de l'URL. [LC8761]
- Lorsque vous utilisez la commande **Set-STFWebReceiverSiteStyle** pour personnaliser StoreFront, le style.css peut être modifié de manière incorrecte dans le dossier personnalisé. Par conséquent, la console StoreFront ne peut pas lire la personnalisation. [LC8776]
- Un échec d'authentification peut se produire sur les serveurs StoreFront. Le problème se produit en raison de l'insuffisance de ports dynamiques TCP. [LC8795]
- Les tentatives de modification du logo StoreFront à l'aide de la commande **Set-STFWebReceiverSiteStyle** peuvent échouer. [LC8994]
- Les tentatives de mise à niveau de StoreFront peuvent échouer lorsque des fichiers en lecture seule sont présents dans le répertoire de fichiers personnalisé de n'importe quelle instance de sites Citrix Receiver pour Web. [LC9252]

VDA pour OS de bureau

HDX 3D Pro

- Avec HDX 3D Pro et la résolution personnalisée activés sur un VDA qui s'exécute sur Microsoft Windows 10, un écran gris peut apparaître par intermittence lorsque vous vous connectez. [LC8417]

Redirection HDX MediaStream Flash

- Si la redirection Flash HDX MediaStream est activée, lorsque vous reconnectez une session VDA avec Qumu.com, le contenu Flash peut ne pas être chargé dans Microsoft Internet Explorer. [LC9193]

Redirection Windows Media HDX Mediastream

- Lorsque la redirection Windows Media HDX MediaStream est désactivée, les tentatives d'ouverture de certains formats de fichiers vidéo via le Lecteur Windows Media peuvent provoquer le basculement vertical de la vidéo en cours de lecture. [LC9194]

HDX RealTime

- RealTime Connector est installé. Lorsque vous utilisez des applications qui utilisent une webcam redirigée, telles que Skype Entreprise, la webcam qui est installée sur un VDA pour OS de bureau peut être redirigée et détectée lors du lancement initial d'une session. Toutefois, lorsque vous vous reconnectez à la session utilisateur, la webcam n'est plus détectée. Le problème se produit lorsque RealTime Media Engine n'est pas installé sur la machine utilisateur. [LC8793]

Clavier

- Lorsque vous démarrez une application sur un appareil Android et que vous êtes dans le champ de texte, le clavier peut ne pas apparaître automatiquement. En outre, vous devez toujours toucher le bouton du clavier pour l'ouverture ou la fermeture. [LC8936]

Impression

- Les tentatives d'impression sur les deux côtés du papier avec les paramètres d'imprimante dans Microsoft Word peuvent échouer. [LC7501]

- Les tentatives d'impression d'un document à partir d'une instance publiée de Microsoft Internet Explorer peuvent échouer. [LC8093]
- Avec le français comme langue d'affichage sur un VDA, les tentatives d'impression d'un document peuvent échouer. [LC8209]
- Une imprimante qui est redirigée à partir d'un périphérique utilisateur peut ne pas être redirigée lorsque vous vous reconnectez à la session. [LC8762]
- Les tentatives de redémarrage du service Citrix Print Manager (cpsvc.exe) peuvent échouer lorsque vous arrêtez le service Spouleur d'impression lors du lancement de la première session. [LC9192]

Session/Connexion

- Lors de la lecture d'un fichier à partir d'un lecteur client mappé, la longueur de l'ancien fichier mis en cache peut être renvoyée si la longueur du fichier a été modifiée en dehors de la session client. En outre, des caractères nuls sont insérés à la place de caractères supprimés.

  Pour activer le correctif, définissez la valeur de registre suivante sur 0 :

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\picadm\Parameters
  Nom : CacheTimeout
  Type : REG_DWORD
  Valeur : la valeur par défaut est de 60 secondes. Si CacheTimeOut est défini sur 0, la longueur du fichier est rechargée immédiatement et, si ce n'est pas le cas, elle est chargée après le délai défini. [LC6314]
- Une session s'exécutant sur un VDA pour OS de bureau peut ne plus répondre lorsque vous utilisez le mode graphique hérité. Lorsque le problème se produit, vous ne pourrez peut-être pas mettre à jour des éléments sur Desktop Viewer, mais Desktop Viewer n'est pas dans un état qui ne répond pas. En outre, après 30-60 minutes, la session qui avait cessé de répondre reprend. [LC7777]
- Lorsque vous lancez une application avec l'attente de session activée, la session peut se déconnecter après l'apparition de l'application. [LC8245]
- Lorsque vous essayez de démarrer un VDA pour OS de bureau, le bureau peut démarrer puis disparaître après quelques secondes. [LC8373]
- L'Explorateur Windows peut se fermer de manière inattendue dans l'un des cas suivants :
  - Lorsque vous sélectionnez un grand nombre de fichiers dont le nom contient plus de 260 caractères, puis l'option Envoyer à > Destinataire de télécopie.
  - Lorsque vous tentez d'ouvrir des applications tierces.
  - Lorsque vous tentez de combiner des fichiers à l'aide de Nitro PDF. [LC8423]

- Les modifications que vous apportez à Paramètres système avancés sous Effets visuels s'appliquent à la session VDA pour OS de bureau en cours, mais risquent de ne pas être conservés pour les sessions ultérieures. Pour que ces modifications soient conservées, définissez la clé de registre suivante :

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix;
  Nom : EnableVisualEffect;
  Type : DWORD;
  Valeur : 1 [LC8049, LC8658]

- Après la déconnexion d'une session, monitor1 peut s'afficher de manière incorrecte en tant que moniteur principal lors de la prochaine connexion locale. Ce problème peut se produire lorsque vous vous connectez localement à un VDA Remote PC Access dans un environnement à plusieurs moniteurs et configurez monitor2 comme moniteur principal, vous connectez via une machine utilisateur, puis déconnectez une session à l'aide de Desktop Viewer. [LC8675]
- Lorsque vous essayez de démarrer une application publiée qui s'exécute sur Microsoft Windows Server 2012 ou 2016, vous pouvez être verrouillé. [LC8681]
- Lorsque vous démarrez une application dans un environnement à plusieurs moniteurs, une bannière d'ouverture de session peut apparaître et englober les deux moniteurs. Lorsque vous utilisez un seul moniteur, la fenêtre de la bannière d'ouverture de session s'affiche en plein écran. [LC8741]
- Avec Local App Access activé, lorsque vous essayez d'ouvrir des applications sur les bureaux publiés qui s'exécutent sur Microsoft Windows 10, les applications ne peuvent pas être réduites. [LC8813]
- Le logiciel DLP peut ne pas réussir à analyser les fichiers avec le lien UNC. [LC8893]
- Après le démarrage d'une application publiée, la touche Verr Num ne fonctionne pas. Le problème se produit lorsque le voyant de la touche Verr Num est visible sur la machine utilisateur, mais les chiffres ne fonctionnent pas dans une session utilisateur. Le problème peut se produire lorsque la mise à jour du voyant demandée par le client est antérieure à l'initialisation par le bureau distant nouvellement créé de l'état de son voyant. Lorsque cela se produit, la WinsStation peut ne pas mettre à jour l'état de son voyant et l'état du voyant n'est pas synchronisé entre le point de terminaison et le VDA. [LC8921]
- Les tentatives de démarrage d'applications et de bureaux peuvent échouer. Ce problème se produit lorsque le VDA pour OS de serveur cesse de répondre.

  Pour activer cette correction, définissez la clé de registre suivante :

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard;
  Nom : EnableSCardHookVcResponseTimeout;

Type : DWORD;
Valeur : 1 [LC8969]

- Les tentatives d'ouverture d'applications hébergées par VM peuvent échouer. [LC9001]
- Les tentatives de reconnexion à une session peuvent échouer. [LC9040]
- Lorsque vous utilisez la commande **WFQuerySessionInformation** du SDK WFAPI dans une session pour récupérer les informations de version du VDA installé, la commande peut ne pas fonctionner. [LC9041]
- Après la mise à niveau de XenApp et XenDesktop de la version 7.14 à la version 7.15, les tentatives de basculement entre les onglets d'une application publiée peuvent entraîner l'absence de réponse de l'application. En outre, si vous redimensionnez la fenêtre transparente sur une taille plus petite, puis développez la fenêtre, il faut un certain temps pour peindre tous les éléments dans la fenêtre. [LC9078]
- Une application publiée peut se fermer par intermittence immédiatement après le démarrage de l'application. [LC9167]
- Lorsque vous vous reconnectez à une application transparente dans une suite Millennium avec une résolution d'écran différente de la connexion initiale, l'application risque de ne pas être correctement redimensionnée. Par conséquent, la fenêtre peut être tronquée. [LC9214]
- Les tentatives de connexion à un bureau publié Windows 10 version 1709 via une machine utilisateur peuvent entraîner un écran gris. Lorsque vous tentez de vous connecter via la console de l'hyperviseur à un bureau publié, un écran noir avec une roue tournante apparaît. Cependant, la connexion via un RDP à un bureau publié fonctionne correctement. [LC9215]
- Les tentatives de démarrage d'applications à partir de Citrix Receiver pour Mac peuvent échouer. Le problème se produit lorsque la licence client (LicenseRequestClientLicense) ne peut pas être récupérée. [LC9286]
- Lorsque HDX 3D Pro est activé, les tentatives de démarrage d'un XenDesktop peuvent échouer par intermittence. Le problème se produit en cas d'échec du processeur graphique. [LC9343]
- L'affichage d'une session utilisateur sur une session Bureau à distance non gérée peut être incorrect avec le Smooth Roaming. [LC9471]

Cartes à puce

- Lorsque vous utilisez une carte à puce, certaines applications tierces peuvent cesser de répondre et ne pas afficher l'invite du code PIN. [LC8805]

Exceptions système

- Les serveurs peuvent rencontrer une exception fatale, affichant un écran bleu, sur picadm.sys avec le code bugcheck 0x22. [LC6177]
- Les serveurs peuvent rencontrer une exception fatale, affichant un écran bleu, sur picadm.sys avec le code d'erreur 0x00000050 (PAGE_FAULT_IN_NONPAGED_AREA). [LC6985]
- Les serveurs peuvent rencontrer une exception fatale, affichant un écran bleu, sur picadm.sys avec le code bugcheck 0x22. [LC7574]
- Les serveurs peuvent rencontrer une exception fatale sur vdtw30.dll et afficher un écran bleu avec le code d'arrêt SYSTEM_SERVICE_EXCEPTION (3b). [LC8087]
- Les serveurs peuvent rencontrer une exception fatale, affichant un écran bleu, sous pdcrypt2.sys avec le code bugcheck 0x3B. Le problème se produit lors du lancement d'un VDA. [LC8328]
- Si le codage matériel HDX 3D Pro et GPU est activé, lors de l'utilisation des GPU NVIDIA, le logiciel graphique Citrix (Ctxgfx.exe) peut se fermer de façon inattendue. Le problème se produit lors de l'utilisation d'écrans haute résolution. LC8435]
- Le VDA pour OS de serveur peut rencontrer une exception fatale sur picadm.sys et afficher un écran bleu. [LC8708]
- Les VDA peuvent rencontrer une exception fatale sur picadm.sys et afficher un écran bleu, avec le code bugcheck 0x22. [LC8749]
- Lorsque vous vous connectez pour la première fois après le redémarrage du VDA, une exception de violation d'accès inattendue peut se produire. Le graphique logiciel Citrix (Ctxgfx.exe) se ferme de façon inattendue. En conséquence, l'image et le texte apparaissant dans le VDA peuvent être flous. [LC9005]
- L'Explorateur Windows peut se fermer de manière inattendue dans l'un des cas suivants :
  - Lorsque vous sélectionnez un grand nombre de fichiers dont le nom contient plus de 260 caractères, puis l'option **Envoyer à** > **Destinataire de télécopie**.
  - Lorsque vous tentez d'ouvrir des applications tierces.
  - Lorsque vous tentez de combiner des fichiers à l'aide de Nitro PDF. [LC9076]

Expérience utilisateur

- Lorsque vous copiez le contenu d'une application qui s'exécute sur un client et que vous le collez dans une application dans une session utilisateur, ce contenu peut ne pas être collé. En outre, le bouton **Coller** peut être désactivé. [LC8516]

- L'écran peut ne pas s'actualiser avec l'invite d'ouverture de session après une tentative de connexion à une session précédemment verrouillée. [LC8774]

Interface utilisateur

- Le papier peint du bureau s'affiche même après avoir défini la stratégie « Papier peint du bureau » sur « Interdit ». [LC8398]

Divers

- Cette correction apporte des améliorations mineures en termes de performances et de qualité pour Enlightened Data Transport (EDT). [LC9278]

VDA pour OS de serveur

Redirection Windows Media HDX Mediastream

- Lorsque la redirection Windows Media HDX MediaStream est désactivée, les tentatives d'ouverture de certains formats de fichiers vidéo via le Lecteur Windows Media peuvent provoquer le basculement vertical de la vidéo en cours de lecture. [LC9194]

HDX RealTime

- RealTime Connector est installé. Lorsque vous utilisez des applications qui utilisent une webcam redirigée, telles que Skype Entreprise, la webcam qui est installée sur un VDA pour OS de bureau peut être redirigée et détectée lors du lancement initial d'une session. Toutefois, lorsque vous vous reconnectez à la session utilisateur, la webcam n'est plus détectée. Le problème se produit lorsque RealTime Media Engine n'est pas installé sur la machine utilisateur. [LC8793]

Clavier

- Lorsque vous démarrez une application sur un appareil Android et que vous êtes dans le champ de texte, le clavier peut ne pas apparaître automatiquement. En outre, vous devez toujours toucher le bouton du clavier pour l'ouverture ou la fermeture. [LC8936]

Impression

- Les tentatives d'impression sur les deux côtés du papier avec les paramètres d'imprimante dans Microsoft Word peuvent échouer. [LC7501]
- Les tentatives d'impression d'un document à partir d'une instance publiée de Microsoft Internet Explorer peuvent échouer. [LC8093]
- Avec le français comme langue d'affichage sur un VDA, les tentatives d'impression d'un document peuvent échouer. [LC8209]
- Les tentatives de redémarrage du service Citrix Print Manager (cpsvc.exe) peuvent échouer lorsque vous arrêtez le service Spouleur d'impression lors du lancement de la première session. [LC9192]

Administration de serveur/site

- Citrix Stack Control Service (SCService64.exe) peut se fermer de manière inattendue lorsque le VDA vérifie l'appartenance à un groupe de l'utilisateur lorsqu'il existe plusieurs groupes avec le même nom dans plusieurs domaines. Le problème se produit lorsque la chaîne « DnsDomainName » est vide dans la structure DS_DOMAIN_TRUSTSW. [LC8484]

Session/Connexion

- Le message d'avertissement suivant peut s'afficher dans le journal d'événements système lors du lancement du VDA XenApp 7.6 Long Term Service Release Cumulative Update 2 pour OS de serveur ou les versions précédentes :

  « Une tentative de connexion au service SemsService a échoué avec le code d'erreur 0x2. » [LC6311]

- Lors de la lecture d'un fichier à partir d'un lecteur client mappé, la longueur de l'ancien fichier mis en cache peut être renvoyée si la longueur du fichier a été modifiée en dehors de la session client. En outre, des caractères nuls sont insérés à la place de caractères supprimés.

  Pour activer le correctif, définissez la valeur de registre suivante sur 0 :

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\picadm\Parameters
  Nom : CacheTimeout
  Type : REG_DWORD
  Valeur : la valeur par défaut est de 60 secondes. Si CacheTimeOut est défini sur 0, la longueur du fichier est rechargée immédiatement et, si ce n'est pas le cas, elle est chargée après le délai défini. [LC6314]

- Après le retrait d'un ordinateur portable de la station d'accueil, le partage de session peut échouer. Le problème se produit lorsque le VDA se réinscrit auprès du Delivery Controller alors qu'une notification de panne est déclenchée pendant la reconnexion automatique du client. [LC7450]
- Une session s'exécutant sur un VDA pour OS de bureau peut ne plus répondre lorsque vous utilisez le mode graphique hérité. Lorsque le problème se produit, vous ne pourrez peut-être pas mettre à jour des éléments sur Desktop Viewer, mais Desktop Viewer n'est pas dans un état qui ne répond pas. En outre, après 30-60 minutes, la session qui avait cessé de répondre reprend. [LC7777]
- Après la fermeture d'une application publiée avec un client App-V installé sur le VDA et les paramètres de configuration "EnablePubilishingRefreshUI" et "Session Lingering" activés dans la session, une fenêtre noire peut rester ouverte sur un appareil iOS. Le problème se produit lorsque la session est à l'état persistant. [LC8080]
- Lorsque vous lancez une application avec l'attente de session activée, la session peut se déconnecter après l'apparition de l'application. [LC8245]
- Les serveurs peuvent cesser de répondre sur RPM.dll et le message d'erreur suivant s'affiche :

  « ID d'événement, picadm : Dépassement du délai d'attente d'un message de réponse du client » [#LC8339]
- L'Explorateur Windows peut se fermer de manière inattendue dans l'un des cas suivants :
  - Lorsque vous sélectionnez un grand nombre de fichiers dont le nom contient plus de 260 caractères, puis l'option Envoyer à > Destinataire de télécopie.
  - Lorsque vous tentez d'ouvrir des applications tierces.
  - Lorsque vous tentez de combiner des fichiers à l'aide de Nitro PDF. [LC8423]
- Citrix Director peut signaler plusieurs échecs de connexion. Le problème se produit lorsque l'expansion de groupes pour contrôler la visibilité limitée d'une application est utilisée pour chaque utilisateur. Ce processus d'expansion prend beaucoup de temps et peut être observé dans des réseaux de grande taille avec de nombreux groupes couvrant plusieurs domaines. [LC8652]
- Les ports COM peuvent ne pas correspondre dans la version 7.15 des VDA. [LC8656]
- Lorsque vous essayez de démarrer une application publiée qui s'exécute sur Microsoft Windows Server 2012 ou 2016, vous pouvez être verrouillé. [LC8681]
- Lorsque vous démarrez une application dans un environnement à plusieurs moniteurs, une bannière d'ouverture de session peut apparaître et englober les deux moniteurs. Lorsque vous utilisez un seul moniteur, la fenêtre de la bannière d'ouverture de session s'affiche en plein écran. [LC8741]

- Avec Local App Access activé, lorsque vous essayez d'ouvrir des applications sur les bureaux publiés qui s'exécutent sur Microsoft Windows 10, les applications ne peuvent pas être réduites. [LC8813]
- Lorsque vous connectez un périphérique utilisateur à un VDA, le bureau peut ne pas s'afficher. Au lieu de cela, un écran gris apparaît sur le bureau. [LC8821]
- Le logiciel DLP peut ne pas réussir à analyser les fichiers avec le lien UNC. [LC8893]
- Après le démarrage d'une application publiée, la touche Verr Num ne fonctionne pas. Le problème se produit lorsque le voyant de la touche Verr Num est visible sur la machine utilisateur, mais les chiffres ne fonctionnent pas dans une session utilisateur. Le problème peut se produire lorsque la mise à jour du voyant demandée par le client est antérieure à l'initialisation par le bureau distant nouvellement créé de l'état de son voyant. Lorsque cela se produit, la WinsStation peut ne pas mettre à jour l'état de son voyant et l'état du voyant n'est pas synchronisé entre le point de terminaison et le VDA. [LC8921]
- Les tentatives de démarrage d'applications et de bureaux peuvent échouer. Ce problème se produit lorsque le VDA pour OS de serveur cesse de répondre.

  Pour activer cette correction, définissez la clé de registre suivante :

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard;
  Nom : EnableSCardHookVcResponseTimeout;
  Type : DWORD;
  Valeur : 1 [LC8969]
- Les tentatives d'ouverture d'applications hébergées par VM peuvent échouer. [LC9001]
- Lorsque vous utilisez la commande **WFQuerySessionInformation** du SDK WFAPI dans une session pour récupérer les informations de version du VDA installé, la commande peut ne pas fonctionner. [LC9041]
- Après la mise à niveau de XenApp et XenDesktop de la version 7.14 à la version 7.15, les tentatives de basculement entre les onglets d'une application publiée peuvent entraîner l'absence de réponse de l'application. En outre, si vous redimensionnez la fenêtre transparente sur une taille plus petite, puis développez la fenêtre, il faut un certain temps pour peindre tous les éléments dans la fenêtre. [LC9078]
- Une application publiée peut se fermer par intermittence immédiatement après le démarrage de l'application. [LC9167]
- Lorsque vous vous reconnectez à une application transparente dans une suite Millennium avec une résolution d'écran différente de la connexion initiale, l'application risque de ne pas être correctement redimensionnée. Par conséquent, la fenêtre peut être tronquée. [LC9214]
- Les tentatives de démarrage d'applications à partir de Citrix Receiver pour Mac peuvent

échouer. Le problème se produit lorsque la licence client (LicenseRequestClientLicense) ne peut pas être récupérée. [LC9286]

Cartes à puce

- Lorsque vous utilisez une carte à puce, certaines applications tierces peuvent cesser de répondre et ne pas afficher l'invite du code PIN. [LC8805]

Exceptions système

- Les serveurs peuvent rencontrer une exception fatale, affichant un écran bleu, sur picadm.sys avec le code bugcheck 0x22. [LC6177]
- Les serveurs peuvent rencontrer une exception fatale, affichant un écran bleu, sur picadm.sys avec le code d'erreur 0x00000050 (PAGE_FAULT_IN_NONPAGED_AREA). [LC6985]
- Les serveurs peuvent rencontrer une exception fatale, affichant un écran bleu, sur picadm.sys avec le code bugcheck 0x22. [LC7574]
- Le processus Service Host (Svchost.exe) peut rencontrer une violation d'accès et se fermer de manière inattendue. Le problème se produit en raison du module défaillant icaendpoint.dll. [LC7694]
- Les serveurs peuvent rencontrer une exception fatale sur vdtw30.dll et afficher un écran bleu avec le code d'arrêt SYSTEM_SERVICE_EXCEPTION (3b). [LC8087]
- Les serveurs peuvent rencontrer une exception fatale, affichant un écran bleu, sous pdcrypt2.sys avec le code bugcheck 0x3B. Le problème se produit lors du lancement d'un VDA. [LC8328]
- Si le codage matériel HDX 3D Pro et GPU est activé, lors de l'utilisation des GPU NVIDIA, le logiciel graphique Citrix (Ctxgfx.exe) peut se fermer de façon inattendue. Le problème se produit lors de l'utilisation d'écrans haute résolution. [LC8435]
- Les serveurs peuvent rencontrer une exception fatale, affichant un écran bleu, sous icardd.dll avec le code bugcheck 0x0000003B. [LC8492]
- Le VDA pour OS de serveur peut rencontrer une exception fatale sur picadm.sys et afficher un écran bleu. [LC8708]
- Les serveurs peuvent rencontrer une exception fatale, affichant un écran bleu, sous icardd.dll avec le code bugcheck 0x0000003B. [LC8732]
- Les VDA peuvent rencontrer une exception fatale sur picadm.sys et afficher un écran bleu, avec le code bugcheck 0x22. [LC8749]

- Lorsque vous vous connectez pour la première fois après le redémarrage du VDA, une exception de violation d'accès inattendue peut se produire. Le graphique logiciel Citrix (Ctxgfx.exe) se ferme de façon inattendue. En conséquence, l'image et le texte apparaissant dans le VDA peuvent être flous. [LC9005]
- L'Explorateur Windows peut se fermer de manière inattendue dans l'un des cas suivants :
  - Lorsque vous sélectionnez un grand nombre de fichiers dont le nom contient plus de 260 caractères, puis l'option **Envoyer à** > **Destinataire de télécopie**.
  - Lorsque vous tentez d'ouvrir des applications tierces.
  - Lorsque vous tentez de combiner des fichiers à l'aide de Nitro PDF. [LC9076]

Expérience utilisateur

- Lorsque vous copiez le contenu d'une application qui s'exécute sur un client et que vous le collez dans une application dans une session utilisateur, ce contenu peut ne pas être collé. En outre, le bouton **Coller** peut être désactivé. [LC8516]
- Sur le VDA pour OS de serveur, le curseur de la souris peut disparaître de la session. Ce problème se produit lorsque le curseur se transforme en curseur de **sélection de texte** et que la couleur d'arrière-plan est la même que la couleur du curseur de **sélection de texte**. La couleur d'arrière-plan par défaut dans Microsoft Windows pour les zones modifiables est le blanc, et la couleur du curseur de **sélection de texte** par défaut est également blanche. Par conséquent, le curseur peut ne plus être visible. [LC8807]
- Microsoft Windows peut continuer à conserver le champ de mot de passe modifiable lors de l'ouverture de session même après l'envoi des informations d'identification correctes. [LC9407]

Interface utilisateur

- Le papier peint du bureau s'affiche même après avoir défini la stratégie « Papier peint du bureau » sur « Interdit ». [LC8398]

Divers

- Certaines applications tierces utilisées pour vérifier l'affichage de la session d'un VDA Linux peuvent ne pas afficher tous les pixels. [LC8419]
- Les clés de Registre RunOnce peuvent ne pas être implémentées correctement. [LC9260]
- Cette correction apporte des améliorations mineures en termes de performances et de qualité pour Enlightened Data Transport (EDT). [LC9278]

Composants de bureau virtuel - Autre

- L'attribut LastPasswordset sur Active Directory peut ne pas être mis à jour correctement lors de l'utilisation de VDA version 7.15 LTSR. [LC8387]
- Après la mise à niveau du Delivery Controller vers la version 7.15, les sessions actives pour utilisateurs anonymes indiquent qu'une connexion est en cours. Cette situation entraîne un index de chargement incorrect pour le VDA. [LC8771]
- Les applications démarrées peuvent ne pas apparaître dans le Gestionnaire d'activités de Citrix Director dans un scénario double hop. [LC8985]
- L'état de l'enregistrement entre le Delivery Controller et le VDA peut être incohérent, ce qui entraîne le réenregistrement lors du lancement du VDA. [LC9216]

Divers

Lorsque le service de télémétrie Citrix est désactivé ou arrêté et que vous utilisez un metainstaller pour mettre à niveau XenApp et XenDesktop 7.15 LTSR vers la mise à jour cumulative 1 (CU1), le message d'avertissement suivant peut s'afficher :

« Nous ne pouvons pas démarrer le service Citrix qui vous permet de vous inscrire à Call Home. Voir CTX218094 pour obtenir des conseils. » [LCM-3642]

Mise à jour cumulative 1 (CU1)

February 28, 2019

À propos de cette version

La mise à jour cumulative 1 (CU1) de XenApp et XenDesktop 7.15 LTSR résout plus de 80 problèmes signalés depuis la publication initiale de la version 7.15 LTSR.

7.15 LTSR (informations générales)

Problèmes résolus depuis XenApp et XenDesktop 7.15 LTSR (version initiale)

Problèmes connus dans cette version

Avant de procéder à la mise à niveau de 7.6 LTSR CU5

Le principal avantage de la mise à niveau de 7.6 LTSR CU5 vers 7.15 LTSR CU1 est que la version 7.15 LTSR de base contient beaucoup plus de fonctionnalités que la version de base 7.6 LTSR. Cependant,

si vous envisagez de procéder à cette mise à niveau, sachez qu'un petit sous-ensemble de correctifs inclus dans 7.6 LTSR CU5 n'est pas présent dans 7.15 LTSR CU1. C'est parce que 7.15 LTSR CU1 a été publié avant 7.6 LTSR CU5. Pour une liste des correctifs applicables à 7.15 mais non inclus dans 7.15 LTSR CU1, consultez la section Liste des correctifs présents dans 7.6 LTSR CU5 mais pas dans 7.15 LTSR CU1. Si votre déploiement dépend de correctifs spécifiques inclus dans 7.6 LTSR CU5, Citrix vous recommande de consulter cette liste avant de procéder à la mise à niveau.

Nouveaux déploiements

Comment effectuer un nouveau déploiement CU1 ?

Vous pouvez configurer un nouvel environnement XenApp et XenDesktop basé sur CU1, à l'aide du metainstaller CU1. Avant d'effectuer cette configuration, nous vous recommandons de vous familiariser avec le produit :

Consultez la section XenApp et XenDesktop 7.15 LTSR (version initiale) et prêtez une attention particulière aux sections Vue d'ensemble technique, Installer et configurer et Sécurité avant de commencer à planifier votre déploiement. Assurez-vous que votre installation correspond à la configuration système requise pour tous les composants.

Déploiements existants

Que dois-je mettre à jour ?

CU1 fournit des mises à jour pour 13 composants de base de 7.15 LTSR. Rappel : Citrix vous recommande de mettre à niveau tous les composants LTSR de votre déploiement vers CU1. Par exemple : si Provisioning Services fait partie de votre déploiement LTSR, mettez à jour les composants Provisioning Services vers CU1. Si Provisioning Services ne fait pas partie de votre déploiement, vous n'avez pas besoin de l'installer ni de le mettre à jour.

Composants de base CU1 XenApp et XenDesktop 7.15 LTSR

Composants LTSR 7.15 CU1 standard	Version	Remarques
VDA pour OS de bureau	7.15.1000	
VDA pour OS de serveur	7.15.1000	
Delivery Controller	7.15.1000	
Citrix Studio	7.15.1000	
Citrix Director	7.15.1000	

Composants LTSR 7.15 CU1 standard	Version	Remarques
Expérience Gestion des stratégies de groupe	3.1.1000	
StoreFront	3.12.1000	
Provisioning Services	7.15.1	
Serveur d'impression universelle	7.15.1000	
Enregistrement de session	7.15.1000	Édition Platinum uniquement
Linux VDA	7.15.1000	Consultez la documentation VDA Linux pour en savoir plus sur les plates-formes prises en charge
Profile Management	7.15.1000	
Service d'authentification fédérée	7.15.1000	

Composants compatibles CU1 XenApp et XenDesktop 7.15 LTSR

Les composants suivants, dans les versions indiquées ci-dessous, sont compatibles avec les environnements LTSR. Ils ne bénéficient pas des avantages du programme LTSR (cycle de vie prolongé et mises à jour cumulatives contenant uniquement des corrections). Citrix peut vous demander de mettre à niveau vers une version plus récente de ces composants dans vos environnements 7.15 LTSR :

Plates-formes et composants compatibles avec LTSR 7.15	Version
AppDNA	7.16
Citrix SCOM Management Pack pour Serveur de licences	1.2
Citrix SCOM Management Pack pour Provisioning Services	1.19
Citrix SCOM Management Pack pour StoreFront	1.13
Citrix SCOM Management Pack pour XenApp et XenDesktop	3.14
Pack d'optimisation HDX RealTime	2.2.100

Plates-formes et composants compatibles avec LTSR 7.15	Version
Serveur de licences	11.14.0.1 Build 22103
Workspace Environment Management	4.4
Application Layering	4.6
Réinitialisation en libre-service des mots de passe	1.1

Versions Citrix Receiver compatibles

Pour faciliter la maintenance et pour garantir des performances optimales, Citrix vous recommande de mettre à niveau vers la dernière version de Citrix Receiver dès qu'elle est disponible. Les dernières versions sont disponibles au téléchargement sur téléchargements. À des fins de commodité, pensez à vous inscrire au flux RSS Citrix Receiver pour être notifié lorsqu'une nouvelle version de Citrix Receiver est disponible.

Citrix Receiver ne peut pas bénéficier des avantages du programme LTSR de XenApp et XenDesktop (cycle de vie prolongé et mises à jour cumulatives contenant uniquement des corrections). Citrix peut vous demander de mettre à niveau vers une version plus récente de Citrix Receiver dans vos environnements CU1 7.15 LTSR. Pour Citrix Receiver pour Windows, Citrix a annoncé un programme LTSR spécial. Pour de plus amples informations sur ce programme, consultez la page Étapes du cycle de vie de Citrix Receiver.

Plus spécifiquement, 7.15 LTSR CU1 prend en charge les versions suivantes de Citrix Receiver et toutes les versions ultérieures.

Version Citrix Receiver compatible avec LTSR

Version Citrix Receiver compatible avec LTSR	Version
Citrix Receiver pour Android	3.12.3 ou version ultérieure
Citrix Receiver pour Chrome	2.5.2 ou version ultérieure
Citrix Receiver pour HTML5	2.5.2 ou version ultérieure
Citrix Receiver pour iOS	7.3.1 ou version ultérieure
Citrix Receiver pour Linux	13.7 ou version ultérieure
Citrix Receiver pour Mac	12.7 ou version ultérieure
Citrix Receiver pour la plateforme Windows universelle (UWP)	1.0.5 ou version ultérieure

Version Citrix Receiver compatible avec LTSR	Version
Citrix Receiver pour Windows	4.9 ou version ultérieure

Exclusions notables pour XenApp et XenDesktop 7.15 LTSR

Les fonctionnalités, plates-formes et composants suivants ne bénéficient pas des avantages et des étapes de cycle de vie du programme 7.15 LTSR. Plus précisément, le cycle de vie prolongé et les mises à jour cumulatives contenant uniquement des corrections sont exclus. Les mises à jour des fonctionnalités et composants exclus seront disponibles au travers des versions régulières.

Fonctions exclues
Framehawk
Intégration de StoreFront Citrix Online

Composants exclus
Personal vDisk : exclu pour les machines Windows 10 ; •Pour les machines Windows 7, prise en charge LTSR limitée jusqu'au 14 janvier 2020 (exigences de CU s'appliquent)
AppDisks

Plates-formes Windows exclues *
Windows 2008 32bits (pour le serveur d'impression universelle)

*Citrix se réserve le droit de mettre à jour la prise en charge des plates-formes en fonction des étapes du cycle de vie des fournisseurs tiers.

Installer et mettre à niveau les outils d'analyse

Lorsque vous utilisez le programme d'installation du produit complet pour déployer et mettre à niveau les composants XenApp ou XenDesktop, des informations anonymes sur le processus d'installation sont collectées et stockées sur la machine sur laquelle vous installez/mettez à niveau le composant. Ces données sont utilisées pour aider Citrix à améliorer l'expérience de ses clients

avec l'installation. Pour plus d'informations, veuillez consulter l'article https://more.citrix.com/XD-INSTALLER.

Migration XenApp 6.5

Le processus de migration XenApp 6.5 vous aide à effectuer une transition rapidement et efficacement depuis une batterie XenApp 6.5 vers un site exécutant XenApp 7.15 LTSR CU1. Ceci est utile dans les déploiements contenant un grand nombre d'applications et de stratégies de groupe Citrix : réduisant le risque d'introduction d'erreurs par inadvertance lors du déplacement manuel des applications et des stratégies de groupe Citrix vers le nouveau site XenApp.

Après avoir installé les composants principaux XenApp 7.15 LTSR CU1 et créé un site, le processus de migration suit cette séquence :

- Exécutez le programme d'installation de XenApp 7.15 CU1 sur chaque tâche XenApp 6.5, qui effectue une mise à niveau automatique vers un nouveau Virtual Delivery Agent pour OS de serveur à utiliser dans le nouveau site.
- Exécutez les applets de commande d'exportation PowerShell sur un Controller XenApp 6.5, qui permet d'exporter les paramètres de stratégie et d'application Citrix vers des fichiers XML.
- Modifiez les fichiers XML, le cas échéant, pour affiner les éléments que vous voulez importer dans le nouveau site. En personnalisant les fichiers, vous pouvez importer les paramètres de stratégie et d'application dans votre site XenApp 7.15 LTSR CU1 par étape : certaines maintenant et d'autres ultérieurement.
- Exécutez les applets de commande d'importation PowerShell sur le nouveau Controller XenApp 7.15 CU1, qui importe les paramètres depuis les fichiers XML vers le nouveau site XenApp.

Reconfigurez le nouveau site si nécessaire, puis testez-le.

Pour plus d'informations, voir Migrer XenApp 6.x.

Liste des correctifs présents dans 7.6 LTSR CU5 mais pas dans 7.15 LTSR CU1

Si vous envisagez cette mise à niveau de 7.6 LTSR CU5 vers 7.15 LTSR CU1, sachez qu'un petit sous-ensemble de correctifs inclus dans 7.6 LTSR CU5 n'est pas présent dans 7.15 LTSR CU1. Si votre déploiement dépend de correctifs spécifiques inclus dans 7.6 LTSR CU5, Citrix vous recommande de consulter cette liste avant de procéder à la mise à niveau.

- LC6311
- LC6985
- LC7430
- LC7450
- LC7574

- LC7600
- LC7777
- LC7911
- LC8046
- LC8080
- LC8130
- LC8170
- LC8281
- LC8339
- LC8492
- LC8732
- LC8750
- LC8774

Problèmes résolus

February 28, 2019

La mise à jour cumulative 1 (CU1) de XenApp et XenDesktop 7.15 LTSR résout plus de 80 problèmes signalés depuis la publication initiale de la version 7.15 LTSR :

Citrix Director

- Lorsque vous ouvrez la console Director et que vous recherchez des utilisateurs pour la première fois, la barre de chargement n'apparaît pas. Dans les recherches suivantes, la barre apparaît comme prévu. [LC8190]

Stratégie Citrix

- Les tentatives d'ajout d'une nouvelle règle de redirection USB à une stratégie utilisateur dans Active Directory peuvent échouer. Le problème se produit lorsque la barre de défilement n'est pas disponible. [LC8112]
- Lorsque vous tentez de gérer la stratégie Attributions d'imprimantes, les problèmes suivants peuvent se produire :
  - L'exception « InvalidCastException » se produit lors de l'ajout ou de la modification d'une stratégie d'attributions d'imprimantes.
  - L'exception « InvalidOperationException » se produit lors de l'ajout d'une nouvelle imprimante de session.

  - Les tentatives de suppression d'une imprimante de session à partir de la stratégie d'attribution d'imprimantes échouent. Ce problème se produit lorsque l'option « Supprimer » est désactivée.
  - Lorsque vous arrêtez de taper dans la zone de recherche de la stratégie Attributions des imprimantes, l'action de recherche ne démarre pas.
  - Les cases à cocher des paramètres de remplacement d'imprimante de session (qualité d'impression, taille de papier, échelle et option TrueType) sont toujours sélectionnées, même si elles ont été désactivées précédemment. [LC8146]

Citrix Studio

- Lorsque vous essayez d'ajouter des machines attribuées à des utilisateurs à un groupe de mise à disposition, les machines non attribuées peuvent être affichées dans la page « Allocation de Machine ». [LC6755]
- Les tentatives d'accès à des catalogues de machines dans Citrix Studio peuvent entraîner la fermeture inattendue de Citrix Studio et l'exception suivante se produit :

  « ID d'erreur : XDDS: ABB14FD9 » [LC7961]
- Le texte de l'option « Utiliser le stockage local de l'hyperviseur » dans l'assistant « Ajouter une connexion et des ressources » exécuté sur une version non anglaise du système d'exploitation Windows peut être tronqué. [LC8041]
- Après la mise à niveau de Citrix Studio vers la version 7.14.1, la colonne « Utilisé par » (faisant référence au groupe de mise à disposition utilisant l'application) pour des packages App-V existants peut être vide. [LC8075]
- Lorsque vous cliquez sur le lien hypertexte d'un groupe de mise à disposition dans Citrix Studio, il est possible que vous ne soyez pas redirigé vers le nœud du groupe de mise à disposition sélectionné. [LC8095]
- Lorsque vous tentez de gérer la stratégie Attributions d'imprimantes, les problèmes suivants peuvent se produire :
  - L'exception « InvalidCastException » se produit lors de l'ajout ou de la modification d'une stratégie d'attributions d'imprimantes.
  - L'exception « InvalidOperationException » se produit lors de l'ajout d'une nouvelle imprimante de session.
  - Les tentatives de suppression d'une imprimante de session à partir de la stratégie d'attribution d'imprimantes échouent. Ce problème se produit lorsque l'option « Supprimer » est désactivée.
  - Lorsque vous arrêtez de taper dans la zone de recherche de la stratégie Attributions des imprimantes, l'action de recherche ne démarre pas.

  - Les cases à cocher des paramètres de remplacement d'imprimante de session (qualité d'impression, taille de papier, échelle et option TrueType) sont toujours sélectionnées, même si elles ont été désactivées précédemment. [LC8146]

- Après la mise à niveau du Delivery Controller vers la version 7.15, les tentatives de lancement de Citrix Studio sur le Delivery Controller peuvent échouer et le message d'erreur suivant s'affiche :

  « MissingMandatoryParameter,Citrix.Licensing.Admin.SDK.Commands.GetLicAlertsCommand »
  [LC8396]

- Lorsque vous sélectionnez le nœud Groupes de mise à disposition dans Citrix Studio, puis sélectionnez l'onglet Applications, le lien hypertexte dans l'onglet applications peut ne pas fonctionner. [LC8555]

Controller

- Si un groupe de mise à disposition contient au moins un VDA en mode de maintenance, vous ne pourrez peut-être pas sélectionner le groupe de mise à disposition pour lancer des applications publiées. [LC6943]
- Après la mise à jour d'un catalogue de machines créé à l'aide de MCS (Machine Creation Services), les machines virtuelles hébergées sur vSAN 6 ou versions ultérieures risquent de ne pas démarrer. Le message d'erreur suivant s'affiche dans la console VMware :

  « A general system error occurred: PBM error occurred during PreProcessReconfigureSpec: pbm.fault.PBMFault; Error when trying to run pre-provision validation; Invalid entity. » [LC7860]

- Les tentatives d'accès à des catalogues de machines dans Citrix Studio peuvent entraîner la fermeture inattendue de Citrix Studio et l'exception suivante se produit :

  « ID d'erreur : XDDS: ABB14FD9 » [LC7961]

- Citrix Director peut afficher un nombre incorrect de sessions déconnectées au début de chaque heure. [LC8006]
- La stratégie « AllowRestart » des sessions sur OS de serveur ne vous autorise pas à fermer les sessions des sessions déconnectées. Lorsque vous redémarrez une session déconnectée, la session est reconnectée à la session précédente au lieu de démarrer une nouvelle session. [LC8090]
- Lorsque vous tentez de gérer la stratégie Attributions d'imprimantes, les problèmes suivants peuvent se produire :
  - L'exception « InvalidCastException » se produit lors de l'ajout ou de la modification d'une stratégie d'attributions d'imprimantes.

  - L'exception « InvalidOperationException » se produit lors de l'ajout d'une nouvelle imprimante de session.
  - Les tentatives de suppression d'une imprimante de session à partir de la stratégie d'attribution d'imprimantes échouent. Ce problème se produit lorsque l'option « Supprimer » est désactivée.
  - Lorsque vous arrêtez de taper dans la zone de recherche de la stratégie Attributions des imprimantes, l'action de recherche ne démarre pas.
  - Les cases à cocher des paramètres de remplacement d'imprimante de session (qualité d'impression, taille de papier, échelle et option TrueType) sont toujours sélectionnées, même si elles ont été désactivées précédemment. [LC8146]

- Le service de surveillance peut ne pas réussir à insérer les données de la nouvelle session dans la base de données de surveillance. [LC8191]
- Le panneau Durée de connexion par utilisateur sous **Director** > **Tendances** > **Performances d'ouverture de session** peut afficher uniquement des enregistrements partiels sur les ouvertures de session. [LC8265]
- Après la mise à niveau du Delivery Controller vers la version 7.15, les tentatives de lancement de Citrix Studio sur le Delivery Controller peuvent échouer et le message d'erreur suivant s'affiche :

  « MissingMandatoryParameter,Citrix.Licensing.Admin.SDK.Commands.GetLicAlertsCommand »
  [LC8396]
- Dans un environnement XenApp et XenDesktop de grande taille, la procédure stockée de nettoyage de base de données de contrôle ne fonctionne pas correctement si la base de données de contrôle est volumineuse. [LC8770]

Redirection HDX MediaStream Flash

- Avec la redirection Flash HDX MediaStream activée, les vidéos Flash peuvent ne pas parvenir à s'afficher correctement sur MSN.com et News.com. [LC6823]

Linux VDA

- Un VDA Linux peut s'enregistrer auprès du Delivery Controller et annuler l'enregistrement après un certain temps. [LC8205]
- Certaines applications tierces utilisées pour vérifier l'affichage de la session d'un VDA Linux peuvent ne pas afficher tous les pixels. [LC8419]

- Lorsqu'il existe plusieurs serveurs LDAP, les tentatives de lancement d'une application sur un VDA Linux peuvent échouer après la mise à jour des stratégies et l'expiration d'une session. [LC8444]

Profile Management

- Profile Management peut entraîner l'affichage d'un écran noir lorsque vous tentez de lancer une session Microsoft Windows 10. Avec cette correction, vous devez configurer la stratégie « Répertoires à synchroniser » et ajouter le dossier « *AppData\Local\Microsoft\Windows\Caches*. » [LC7596]
- Lorsque vous ouvrez une session à partir d'un VDA exécuté sur Microsoft Windows 10, le fichier ntuser.dat peut être en cours d'utilisation et ne pas être copié dans le magasin Profile Management. Par conséquent, les modifications apportées à la clé de Registre « HKEY_CURRENT_USER » sont perdues. [LC8068]
- Avec la stratégie « Supprimer les profils mis en cache localement à la fermeture de session » activée et le paramètre « Délai avant la suppression des profils en cache » défini sur deux minutes, si l'utilisateur tente de se déconnecter et se connecter à une session dans les deux minutes avec le même compte utilisateur, un nouveau profil local peut être créé. [LC8388]

Provisioning Services

StoreFront

- Lorsque « TWIMode » est défini sur « Désactivé » pour certaines applications, toutes les applications sont lancées en mode fenêtré lors de l'utilisation de Citrix Receiver pour Chrome. [LC7558]
- Lorsqu'il y a deux ou plusieurs magasins dans StoreFront, le fait de cliquer sur « Configurer les paramètres d'accès distant » dans le premier ou le second magasin peut dupliquer le nom de ce magasin sur le magasin le plus récemment ajouté. [LC8089]
- Lorsque vous configurez des magasins avec authentification partagée dans StoreFront, les tentatives d'association d'un nouveau boîtier NetScaler Gateway à un magasin peuvent entraîner la suppression des boîtiers NetScaler Gateway existants qui sont déjà associés. Lorsque vous essayez de vous connecter aux magasins, le message d'erreur suivant s'affiche :

  « Votre ouverture de session a expiré. Rouvrez une session pour continuer. »

  En outre, la console StoreFront affiche les noms des magasins en double. [LC8219]
- Lors de l'importation d'un magasin avec la configuration HTML5 à l'aide de la commande PowerShell « Import-STFConfiguration », l'importation peut se terminer avec succès. Toutefois, les

tentatives de lancement d'une application à l'aide de Citrix Receiver pour HTML5 échouent. [LC8290]

- Le serveur StoreFront peut afficher des entrées null pour les sites Receiver pour Web dans la console. Le problème se produit lorsque le nom du magasin commence par le texte « discovery » dans l'URL. [LC8320]
- Avec le service de journalisation de W3C activé, les tentatives de modification de la configuration de StoreFront peuvent échouer et le message d'erreur suivant s'affiche :

  « Une erreur s'est produite lors de l'enregistrement de vos modifications. » [LC8370]
- Lorsque le regroupement de sockets est activé et que la connectivité de base de données du site est incohérente, les sockets dans StoreFront risquent d'être épuisés lorsque vous vous connectez et que vous vous déconnectez continuellement. [LC8514]

VDA pour OS de bureau

Redirection HDX MediaStream Flash

- Avec la redirection Flash HDX MediaStream activée, les vidéos Flash peuvent ne pas parvenir à s'afficher correctement sur MSN.com et News.com. [LC6823]
- Les tentatives d'enregistrement de fichiers Microsoft Office tels que les feuilles de calcul Microsoft Excel qui s'exécutent dans une session avec applications transparentes HDX activées peuvent entraîner la fermeture inattendue des fichiers. [LC8572]

HDX Plug and Play

- Les périphériques USB qui indiquent le même numéro de série pour plusieurs périphériques tels que Syn-Tech ProKee V2 peuvent ne pas être redirigés vers une session VDA. La trace CDF suivante s'affiche :

  « Impossible d'attribuer l'ID de l'instance, erreur 0xc000000d ». [LC8264]

Impression

- Les tentatives de lancement d'une application publiée peuvent échouer lorsque l'application attend un objet mutex dans le Citrix Print Manager Service (cpsvc.exe). [LC6829]
- Le Citrix Print Manager Service (cpsvc.exe) peut s'arrêter de façon inattendue. [LC7535]
- Lorsque vous passez d'une session à une autre entre les clients, les imprimantes de session ne peuvent pas être supprimées. Par exemple, lorsque vous configurez la stratégie « Attributions

d'imprimantes » – imprimante A pour le client A et imprimante B pour le client B, l'imprimante A peut ne pas être supprimée lorsque vous passez du client A au client B. [LC8077]

Administration de serveur/site

- Sur un VDA 7.12 ou version ultérieure, lorsque vous tentez de supprimer l'affichage de la barre de langue dans une session transparente en définissant le drapeau de session transparente sur « 0x00040000 » (désactive l'agent de barre de langue) sous la clé de Registre HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ Control\Citrix\wfshell\TWI, la langue n'est plus masquée. [LC8349]

Session/Connexion

- Lorsque Local App Access est activé, l'utilisation de la politique d'affichage d'un avertissement d'ouverture de session interactive peut entraîner l'affichage d'un écran noir ou gris pendant 45 secondes. [LC6518]
- Les tentatives de reconnexion à une application peuvent échouer. Le problème se produisait lorsque l'une des applications déconnectées ne répondait plus lorsque la session était déconnectée initialement. [LC6550]
- Lorsque vous verrouillez une session avec deux moniteurs à l'aide de HDX 3D Pro, seul le moniteur principal est verrouillé. [LC7767]
- Lorsque vous établissez un appel vidéo Skype Entreprise, une bordure de fenêtre bleue peut s'afficher après intersection avec la fenêtre d'une application tierce. [LC7773]
- Lorsque Local App Access est activé, l'utilisation de la stratégie d'affichage d'un avertissement d'ouverture de session interactive peut entraîner l'affichage d'un écran noir ou gris. [LC7798]
- Certaines applications publiées peuvent ne pas couvrir l'écran entier lorsqu'elles sont agrandies. [LC7854]
- Lors d'une opération d'insertion entre deux feuilles de calcul Microsoft Excel 2010 s'exécutant sur un VDA version 7.9, la fenêtre Excel peut cesser de répondre. [LC7912]
- Dans certains scénarios, les applications transparentes peuvent ne pas s'afficher en mode transparent ou certaines fonctionnalités peuvent ne pas fonctionner. [LC8030]
- Avec HDX 3D Pro activé sur un VDA et la stratégie « Contenu du message pour les utilisateurs essayant de se connecter » activée lorsque l'écran d'ouverture de session s'affiche, les tentatives de lancement d'un bureau publié peuvent échouer et un écran gris s'affiche.

  Pour activer cette correction, définissez la clé de registre suivante :

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDX3D\BitmapRemotingConfig
Nom : HKLM_DisableMontereyFBCOnInit
Valeur : DWORD
Type : 1 pour activer [LC8082]

- Lorsque Local App Access est activé, l'utilisation de la stratégie d'affichage d'un avertissement d'ouverture de session interactive peut entraîner l'affichage d'un écran gris lors de la connexion à un VDA. [LC8136]
- Lorsque vous utilisez des applications qui utilisent une webcam redirigée, telles que Skype Entreprise ou un lecteur multimédia VLC, la webcam peut être redirigée et détectée lors du lancement initial d'une session. Toutefois, lorsque vous vous reconnectez à la session utilisateur, la webcam n'est plus détectée. Au lieu de cela, un écran gris apparaît à la place de l'aperçu vidéo. [LC8588]

Cartes à puce

- Lorsque vous vous connectez à une session à l'aide d'une carte à puce, la session peut cesser de répondre jusqu'à ce que vous déconnectiez et reconnectiez à la session. [#LC8036]

Exceptions système

- Le processus wfshell.exe peut se fermer de manière inattendue, pointant vers le module de regroupement de la barre des tâches. [LC6968]
- Lorsque la stratégie de redirection USB est activée, les VDA peuvent rencontrer une exception fatale et afficher un écran bleu avec le code bugcheck SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e). [LC7999]
- Les VDA peuvent rencontrer une exception fatale et afficher un écran bleu avec le code bugcheck 0x7E. Le problème se produit lorsque vous quittez une session VDA qui a été inactive pendant un certain temps. [LC8045]
- Les serveurs peuvent rencontrer une exception fatale et afficher un écran bleu sous picavc.sys avec le code bugcheck SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e). [LC8063]

Expérience utilisateur

- Lors de la reconnexion à une session d'application transparente, les fenêtres d'application peuvent ne pas s'afficher correctement du côté client. Au lieu de cela, les graphiques de session sont dessinés dans un petit rectangle du côté client. [LC7857]

- Le lecteur Windows Media peut afficher les fichiers au format Microsoft AVI (.avi) inversés verticalement. [LC8308]
- Lorsqu'une application publiée est agrandie sur l'écran d'un troisième moniteur, l'application peut ne pas couvrir tout l'écran. Au lieu de cela, un cadre noir s'affiche. [LC8472]
- Les applications transparentes hébergées sur le VDA 7.15 peuvent afficher un cadre gris ou noir en arrière-plan lors du déplacement de la fenêtre de l'application. [LC8551]

Interface utilisateur

- Si vous ouvrez une feuille de calcul avec plusieurs classeurs dans Excel 2010, la barre des tâches affiche uniquement le classeur le plus récent. [LC7557]

VDA pour OS de serveur

Redirection HDX MediaStream Flash

- Les tentatives d'enregistrement de fichiers Microsoft Office tels que les feuilles de calcul Microsoft Excel qui s'exécutent dans une session avec applications transparentes HDX activées peuvent entraîner la fermeture inattendue des fichiers. [LC8572]

HDX Plug and Play

- Les périphériques USB qui indiquent le même numéro de série pour plusieurs périphériques tels que Syn-Tech ProKee V2 peuvent ne pas être redirigés vers une session VDA. La trace CDF suivante s'affiche :

  « Impossible d'attribuer l'ID de l'instance, erreur 0xc000000d ». [LC8264]

Impression

- Les tentatives de lancement d'une application publiée peuvent échouer lorsque l'application attend un objet mutex dans le Citrix Print Manager Service (cpsvc.exe). [LC6829]
- Le Citrix Print Manager Service (cpsvc.exe) peut s'arrêter de façon inattendue. [LC7535]
- Lorsque vous passez d'une session à une autre entre les clients, les imprimantes de session ne peuvent pas être supprimées. Par exemple, lorsque vous configurez la stratégie « Attributions d'imprimantes » – imprimante A pour le client A et imprimante B pour le client B, l'imprimante A peut ne pas être supprimée lorsque vous passez du client A au client B.[LC8077]

Administration de serveur/site

- Sur un VDA 7.12 ou version ultérieure, lorsque vous tentez de supprimer l'affichage de la barre de langue dans une session transparente en définissant le drapeau de session transparente sur « 0x00040000 » (désactive l'agent de barre de langue) sous la clé de Registre HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ Control\Citrix\wfshell\TWI, la langue n'est plus masquée. [#LC8349]

Session/Connexion

- Les tentatives de reconnexion à une application peuvent échouer. Le problème se produisait lorsque l'une des applications déconnectées ne répondait plus lorsque la session était déconnectée initialement. [LC6550]
- Lorsque vous cliquez sur « Annuler » sur la barre de progression de lancement d'une session, des informations de session incorrectes peuvent rester sur le Delivery Controller. Par conséquent, la session actuelle n'est pas créée sur le VDA, et vous ne pourrez peut-être pas démarrer une nouvelle session. [LC6779]
- Le microphone peut être redirigé par intermittence dans la session utilisateur même après la définition de la valeur de stratégie « Redirection du microphone Client » sur « Interdit ».

  Cette correction résout le problème. Toutefois, si vous continuez à observer ce problème, appliquez la clé de Registre suivante sur la machine avec le microphone :

  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\ica-tcp\AudioConfig
    Nom : MaxPolicyAge
    Type : DWORD
    Valeur : durée maximale (en secondes) autorisée entre la dernière évaluation de stratégie et l'heure d'activation du point de terminaison. La durée par défaut est de 30 secondes.
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\ica-tcp\AudioConfig
    Nom : PolicyTimeout
    Type : DWORD
    Valeur : durée maximale (en millisecondes) pendant laquelle le système attend une réponse des stratégies pour déterminer que les stratégies ne sont pas à jour. La durée par défaut est de 4000 millisecondes. Lorsque la durée est dépassée, le système lit les stratégies et continue l'initialisation. Si vous définissez cette valeur sur (0), la vérification des stratégies Active Directory est ignorée et les stratégies sont traitées immédiatement. [LC7495]

- Lorsque vous établissez un appel vidéo Skype Entreprise, une bordure de fenêtre bleue peut s'afficher après intersection avec la fenêtre d'une application tierce. [LC7773]
- Certaines applications publiées peuvent ne pas couvrir l'écran entier lorsqu'elles sont agrandies. [LC7854]
- Après la mise à niveau vers la version 7.13, 7.14 ou 7.15 d'un VDA lors de l'utilisation d'un vGPU, une zone noire peut apparaître dans les applications ou bureaux publiés exécutés sur le système d'exploitation Microsoft Windows Server. [LC7875]
- Lors d'une opération d'insertion entre deux feuilles de calcul Microsoft Excel 2010 s'exécutant sur un VDA version 7.9, la fenêtre Excel peut cesser de répondre. [LC7912]
- Dans certains scénarios, les applications transparentes peuvent ne pas s'afficher en mode transparent ou certaines fonctionnalités peuvent ne pas fonctionner. [LC8030]
- Lorsque Local App Access est activé, l'utilisation de la stratégie d'affichage d'un avertissement d'ouverture de session interactive peut entraîner l'affichage d'un écran gris lors de la connexion à un VDA. [LC8136]
- Les VDA pour OS de serveur peuvent se réinscrire par intermittence lorsqu'une notification de panne est envoyée aux Delivery Controller. [LC8228]
- Lorsque vous utilisez des applications qui utilisent une webcam redirigée, telles que Skype Entreprise ou un lecteur multimédia VLC, la webcam peut être redirigée et détectée lors du lancement initial d'une session. Toutefois, lorsque vous vous reconnectez à la session utilisateur, la webcam n'est plus détectée. Au lieu de cela, un écran gris apparaît à la place de l'aperçu vidéo. [LC8588]

Cartes à puce

- Lorsque vous vous connectez à une session à l'aide d'une carte à puce, la session peut cesser de répondre jusqu'à ce que vous déconnectiez et reconnectiez à la session. [LC8036]

Exceptions système

- Le processus wfshell.exe peut se fermer de manière inattendue, pointant vers le module de regroupement de la barre des tâches. [LC6968]
- Windows Shell Experience Host peut se fermer de manière inattendue lorsque vous cliquez sur le contrôle de volume dans la barre des tâches. [LC7000]
- Le processus Service Host (Svchost.exe) peut rencontrer une violation d'accès et se fermer de manière inattendue. Le problème se produit en raison du module défaillant icaendpoint.dll. [LC7900]

- Lorsque la stratégie de redirection USB est activée, les VDA peuvent rencontrer une exception fatale et afficher un écran bleu avec le code bugcheck SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e). [LC7999]
- Les serveurs peuvent rencontrer une exception fatale et afficher un écran bleu sous picavc.sys avec le code bugcheck SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e). [LC8063]

Expérience utilisateur

- Lors de la reconnexion à une session d'application transparente, les fenêtres d'application peuvent ne pas s'afficher correctement du côté client. Au lieu de cela, les graphiques de session sont dessinés dans un petit rectangle du côté client. [LC7857]
- Le lecteur Windows Media peut afficher les fichiers au format Microsoft AVI (.avi) inversés verticalement. [LC8308]
- Lorsqu'une application publiée est agrandie sur l'écran d'un troisième moniteur, l'application peut ne pas couvrir tout l'écran. Au lieu de cela, un cadre noir s'affiche. [LC8472]
- Les applications transparentes hébergées sur le VDA 7.15 peuvent afficher un cadre gris ou noir en arrière-plan lors du déplacement de la fenêtre de l'application. [LC8551]

Interface utilisateur

- Lors de l'utilisation du Centre de connexion pour fermer la session depuis une session transparente comportant des données non enregistrées, une fenêtre noire s'affiche avec le message suivant :

  « Les programmes doivent toujours se fermer » avec les deux options « Forcer la fermeture de session » ou « Annuler ». L'option « Annuler » ne fonctionne pas.

  Après l'installation de cette correction, l'option Annuler fonctionne comme prévu. [LC6075]
- Si vous ouvrez une feuille de calcul avec plusieurs classeurs dans Excel 2010, la barre des tâches affiche uniquement le classeur le plus récent. [LC7557]
- L'écran de fermeture de session peut ne pas s'afficher lorsque vous essayez de fermer une session de bureau Microsoft Windows Server 2008 R2. Vous pourrez peut-être fermer la session, mais la session apparaît comme si elle s'était déconnectée de manière inattendue. [LC8016]

Composants de bureau virtuel - Autre

- Citrix Director peut afficher un nombre incorrect de sessions déconnectées au début de chaque heure. [LC8006]

- Le service de surveillance peut ne pas réussir à insérer les données de la nouvelle session dans la base de données de surveillance. [LC8191]
- Le panneau Durée de connexion par utilisateur sous **Director** > **Tendances** > **Performances d'ouverture de session** peut afficher uniquement des enregistrements partiels sur les ouvertures de session. [LC8265]
- Le client SCCM (System Center Configuration Manager) peut se fermer de manière inattendue après la mise à niveau de Microsoft Windows 10 de la Build 1511 vers la Build 1703 avec un VDA installé dessus. [LC8632]
- Le réarmement de Microsoft Office 2016 peut être interrompu sur Microsoft Windows 10 lors de l'utilisation de Machine Creation Services (MCS). [LC8680]
- Dans un environnement XenApp et XenDesktop de grande taille, la procédure stockée de nettoyage de base de données de contrôle ne fonctionne pas correctement si la base de données de contrôle est volumineuse. [LC8770]

7.15 LTSR (version initiale)

February 28, 2019

À propos de cette version

La version 7.15 Long Term Service Release (LTSR) de XenApp et XenDesktop comprend les nouvelles versions des VDA Windows et les nouvelles versions de plusieurs composants principaux de XenApp et XenDesktop.
Vous pouvez :

- **Installer ou mettre à niveau un site XenApp ou XenDesktop**

Utilisez le fichier ISO de cette version pour installer ou mettre à niveau tous les composants principaux et les VDA. L'installation ou la mise à niveau vers la version la plus récente vous permet d'utiliser toutes les fonctionnalités les plus récentes.

- **Installer ou mettre à niveau des VDA dans un site existant**

Si vous disposez d'un déploiement XenApp ou XenDesktop, et que vous n'êtes pas prêt à mettre à niveau les composants principaux, vous pouvez toujours utiliser plusieurs des dernières fonctionnalités HDX en installant (ou en effectuant une mise à niveau vers) un nouveau VDA. Mettre à niveau les VDA uniquement est souvent utile lorsque vous voulez tester les améliorations dans un environnement de non production.

Pour obtenir des instructions, veuillez consulter Préparer l'installation ou Mettre un déploiement à niveau.

Les pages de téléchargement XenApp et XenDesktop pour cette version incluent également les versions mises à jour des logiciels suivants. Pour obtenir des informations sur les fonctionnalités et des instructions d'installation, consultez la documentation du composant.

StoreFront

AppDNA

Citrix SCOM Management Pack pour XenApp et XenDesktop

Pour obtenir un aperçu des fonctionnalités qui ont été ajoutées depuis la version 7.6 LTSR de XenApp et XenDesktop, reportez-vous à Comparaison des fonctionnalités de XenApp et XenDesktop LTSR 7.15.

Cette version comprend également les fonctionnalités nouvelles, modifiées et améliorées suivantes depuis XenApp et XenDesktop 7.14.1.

Installation de VDA sur les machines sans Microsoft Media Foundation

La plupart des éditions Windows prises en charge sont fournies avec Microsoft Media Foundation. Si la machine sur laquelle vous installez un VDA n'est pas dotée de Media Foundation (éditions N par exemple), plusieurs fonctionnalités multimédia ne seront pas installées et ne fonctionneront pas. Vous pouvez accepter cette limitation, ou mettre fin à l'installation du VDA et la redémarrer plus tard, après l'installation de Media Foundation. Dans l'interface graphique, ce choix est proposé dans un message. Dans la ligne de commande, vous pouvez utiliser l'option /no_mediafoundation_ack pour confirmer la limitation.

Mise à niveau d'une tâche XenApp 6.5 vers un nouveau VDA

Après la migration d'une batterie XenApp 6.5, vous pouvez mettre à niveau une tâche XenApp 6.5 vers un nouveau VDA. Précédemment, l'exécution du programme d'installation de XenApp et XenDesktop sur le serveur de tâches supprimait automatiquement le logiciel XenApp 6.5 et installait le nouveau VDA. Maintenant, vous supprimez d'abord HRP7 et le logiciel XenApp 6.5 du serveur, à l'aide de processus distincts. Ensuite, vous installez le nouveau VDA. Pour plus de détails, voir Mettre à niveau une tâche XenApp 6.5 vers un nouveau VDA.

MCS prend en charge les VM de génération 2

Lorsque vous utilisez Microsoft System Center Virtual Machine Manager pour fournir des machines virtuelles, vous pouvez maintenant utiliser Machine Creation Services (MCS) pour provisionner des machines virtuelles de génération 2.

Cache d'hôte local

Lors d'une nouvelle installation de XenApp et XenDesktop, le cache d'hôte local est activé par défaut. La location de connexion est désactivée par défaut.

Après une mise à niveau, le paramètre de cache d'hôte local est inchangé. Par exemple, si le cache d'hôte local a été activé dans la version antérieure, il reste activé dans la version mise à niveau. Si le cache d'hôte local a été désactivé (ou qu'il n'est pas pris en charge) dans la version antérieure, il reste désactivé dans la version mise à niveau.

Director

Détection des défaillances applicatives Director ajoute à la vue Tendances l'onglet **Échecs applicatifs** pour afficher l'historique des échecs associés aux applications publiées. Vous pouvez voir les échecs et les erreurs qui se sont produits lors du lancement ou de l'exécution d'une application ou d'un processus sélectionné(e) pour une période de temps sélectionnée. Ces informations vous permettent de comprendre et de résoudre les problèmes spécifiques à l'application. Pour plus d'informations, consultez la section Détection des défaillances applicatives dans Résolution des problèmes d'applications.

Par défaut, les échecs d'applications hébergées sur des VDA avec OS de serveur sont détectés. Vous pouvez modifier les paramètres de détection dans les stratégies de groupe de surveillance : Activer la détection des défaillances applicatives et Activer la détection des défaillances applicatives sur les VDA d'OS de bureau et Liste des applications exclues de la détection des défaillances. Pour de plus amples informations, consultez la section Stratégies pour la détection des défaillances applicatives dans Paramètres de stratégie Surveillance.

Cette fonctionnalité requiert la version 7.15 ou ultérieure de Delivery Controller et de VDA. Les VDA avec OS de bureau Windows Vista ou version ultérieure et les VDA avec OS de serveur Windows Server 2008 ou version ultérieure sont pris en charge.

Virtual Delivery Agent (VDA) 7.15

Après la mise à niveau de vos VDA depuis 7.9, 7.11, 7.12, 7.13 ou 7.14, vous n'avez pas besoin de mettre à jour le niveau fonctionnel du catalogue de machines. La valeur par défaut (7.9 (ou ultérieure)) reste le niveau fonctionnel actuel. Pour de plus amples informations, consultez la section Versions VDA et niveaux fonctionnels.

Enregistrement de session 7.15

Équilibrage de charge pour l'enregistrement de session : cette fonctionnalité expérimentale, présente dans XenApp et XenDesktop 7.14, n'est pas incluse dans cette version.

Nouveaux déploiements

Comment effectuer un nouveau déploiement 7.15 LTSR ?

Vous pouvez configurer un nouvel environnement XenApp ou XenDesktop à l'aide du metainstaller 7.15 LTSR.* Avant de procéder, nous vous recommandons de vous familiariser avec le produit :

Consultez la documentation XenApp et XenDesktop 7.15 Long Term Service Release et prêtez une attention particulière aux sections Vue d'ensemble technique, Installer et configurer et Sécurité avant de commencer à planifier votre déploiement. Assurez-vous que votre installation correspond à la configuration système requise pour tous les composants. Suivez les instructions de déploiement de la section Installer et configurer.

* Remarque : Provisioning Services et Enregistrement de session sont disponibles sous forme de téléchargements et de programmes d'installation distincts

Déploiements existants

Que dois-je mettre à jour ?

XenApp et XenDesktop 7.15 LTSR fournit des mises à jour de tous les composants de base de 7.6 LTSR. Rappel : Citrix vous recommande de mettre à niveau tous les composants LTSR de votre déploiement vers 7.15 LTSR. Par exemple : si Provisioning Services fait partie de votre déploiement LTSR, mettez à jour le composant Provisioning Services. Si Provisioning Services ne fait pas partie de votre déploiement, vous n'avez pas besoin de l'installer ni de le mettre à jour.

Depuis la version 7.6 LTSR initiale, nous avons ajouté un metainstaller qui vous permet de mettre à jour les composants existants de votre environnement LTSR à partir d'une interface unifiée. Suivez les instructions de mise à niveau pour utiliser le metainstaller afin de mettre à jour les composants LTSR de votre déploiement.

Composants de base XenApp et XenDesktop 7.15 LTSR

Composants LTSR 7.15 standard	Version	Remarques
VDA pour OS de bureau	7.15	

Composants LTSR 7.15 standard	Version	Remarques
VDA pour OS de serveur	7.15	
Delivery Controller	7.15	
Citrix Studio	7.15	
Citrix Director	7.15	
Expérience Gestion des stratégies de groupe	3.1	
StoreFront	3.12	
Provisioning Services	7.15	
Serveur d'impression universelle	7.15	
Enregistrement de session	7.15	Édition Platinum uniquement
Linux VDA	7.15	Consultez la documentation VDA Linux pour en savoir plus sur les plates-formes prises en charge
Profile Management	7.15	
Service d'authentification fédérée	7.15	

Composants compatibles XenApp et XenDesktop 7.15 LTSR

Les composants suivants, dans les versions indiquées ci-dessous, sont compatibles avec les environnements LTSR. Ils ne bénéficient pas des avantages du programme LTSR (cycle de vie prolongé et mises à jour cumulatives contenant uniquement des corrections). Citrix peut vous demander de mettre à niveau vers une version plus récente de ces composants dans vos environnements 7.15 LTSR :

Plates-formes et composants compatibles avec LTSR 7.15	Version
AppDNA	7.15
Citrix SCOM Management Pack pour Serveur de licences	1.2
Citrix SCOM Management Pack pour Provisioning Services	1.19

Plates-formes et composants compatibles avec LTSR 7.15	Version
Citrix SCOM Management Pack pour StoreFront	1.12
Citrix SCOM Management Pack pour XenApp et XenDesktop	3.13
Pack d'optimisation HDX RealTime	2.3
Serveur de licences	11.14.0 Build 21103
Workspace Environment Management	4.4
Application Layering	4.3
Réinitialisation en libre-service des mots de passe	1.1

Versions Citrix Receiver compatibles

Pour faciliter la maintenance et pour garantir des performances optimales, Citrix vous recommande de mettre à niveau vers la dernière version de Citrix Receiver dès qu'elle est disponible. Les dernières versions sont disponibles au téléchargement sur https://www.citrix.com/downloads/citrix-receiver.html. À des fins de commodité, pensez à vous inscrire au flux RSS Citrix Receiver pour être notifié lorsqu'une nouvelle version de Citrix Receiver est disponible.

Veuillez noter que Citrix Receiver ne peut pas bénéficier des avantages du programme LTSR de XenApp et XenDesktop (cycle de vie prolongé et mises à jour cumulatives contenant uniquement des corrections). Citrix peut vous demander de mettre à niveau vers une version plus récente de Citrix Receiver dans vos environnements 7.15 LTSR. Dans le cas de Citrix Receiver pour Windows, Citrix a annoncé un programme LTSR spécial. Pour de plus amples informations sur ce programme, consultez la page Étapes du cycle de vie de Citrix Receiver.

Plus spécifiquement, 7.15 LTSR prend en charge les versions suivantes de Citrix Receiver et toutes les versions ultérieures.

Version Citrix Receiver compatible avec LTSR	Version
Citrix Receiver pour Android	3.11.1 ou version ultérieure
Citrix Receiver pour Chrome	2.4 ou version ultérieure
Citrix Receiver pour HTML5	2.4 ou version ultérieure
Citrix Receiver pour iOS	7.2 ou version ultérieure
Citrix Receiver pour Linux	13.5 ou version ultérieure

Version Citrix Receiver compatible avec LTSR	Version
Citrix Receiver pour Mac	12.5 ou version ultérieure
Citrix Receiver pour la plateforme Windows universelle (UWP)	1.0.5 ou version ultérieure
Citrix Receiver pour Windows	4.9 ou version ultérieure

Exclusions notables pour XenApp et XenDesktop 7.15 LTSR

Les fonctionnalités, plates-formes et composants suivants ne bénéficient pas des avantages et des étapes de cycle de vie du programme 7.15 LTSR. Plus précisément, le cycle de vie prolongé et les mises à jour cumulatives contenant uniquement des corrections sont exclus. Les mises à jour des fonctionnalités et composants exclus seront disponibles au travers des versions régulières.

Fonctions exclues
Framehawk
Intégration de StoreFront Citrix Online

Composants exclus
Personal vDisk : exclu pour les machines Windows 10 ; Personal vDisk : exclu pour les machines Windows 10 ;
AppDisks

Plates-formes Windows exclues *
Windows 2008 32bits (pour le serveur d'impression universelle)

* Citrix se réserve le droit de mettre à jour la prise en charge des plates-formes en fonction des étapes du cycle de vie des fournisseurs tiers.

Lorsque vous utilisez le programme d'installation du produit complet pour déployer et mettre à niveau les composants XenApp ou XenDesktop, des informations anonymes sur le processus d'installation sont collectées et stockées sur la machine sur laquelle vous installez/mettez à niveau le composant. Ces données sont utilisées pour aider Citrix à améliorer l'expérience de ses clients

avec l'installation. Pour plus d'informations, veuillez consulter l'article https://more.citrix.com/XD-INSTALLER.

Migration XenApp 6.5

Le processus de migration XenApp 6.5 vous aide à effectuer une transition rapidement et efficacement depuis une batterie XenApp 6.5 vers un site exécutant XenApp 7.15 LTSR (ou une version ultérieure prise en charge). Ceci est utile dans les déploiements contenant un grand nombre d'applications et de stratégies de groupe Citrix : réduisant le risque d'introduction d'erreurs par inadvertance lors du déplacement manuel des applications et des stratégies de groupe Citrix vers le nouveau site XenApp.

Après avoir installé les composants principaux XenApp 7.15 LTSR et créé un site, le processus de migration suit cette séquence :

- Exécutez le programme d'installation de XenApp 7.15 sur chaque tâche XenApp 6.5, qui effectue une mise à niveau automatique vers un nouveau Virtual Delivery Agent pour OS de serveur à utiliser dans le nouveau site.
- Exécutez les applets de commande d'exportation PowerShell sur un Controller XenApp 6.5, qui permet d'exporter les paramètres de stratégie et d'application Citrix vers des fichiers XML.
- Modifiez les fichiers XML, le cas échéant, pour affiner les éléments que vous voulez importer dans le nouveau site. En personnalisant les fichiers, vous pouvez importer les paramètres de stratégie et d'application dans votre site XenApp 7.15 LTSR par étape : certaines maintenant et d'autres ultérieurement.
- Exécutez les applets de commande d'importation PowerShell sur le nouveau Controller XenApp 7.15, qui importe les paramètres depuis les fichiers XML vers le nouveau site XenApp.

Reconfigurez le nouveau site si nécessaire, puis testez-le.

Pour plus d'informations, voir Migrer XenApp 6.x.

Problèmes résolus

February 28, 2019

Les problèmes suivants ont été résolus depuis la version 7.14.1 :

Problèmes résolus depuis 7.14.1

Problèmes résolus depuis 7.6 LTSR CU4

Problèmes résolus depuis 7.14.1

AppDNA

Citrix Director

- Lorsque vous accédez à l'onglet **Tendances** > **Échecs** > **Connexion** dans Citrix Director, le message d'erreur suivant peut s'afficher :

  « Erreur inattendue. Vérifiez votre connexion réseau ou consultez les journaux d'événements du serveur Director pour plus d'informations. » [LC7755]

- Les tentatives d'affichage des informations de stratégie pour certaines sessions dans Citrix Director peuvent échouer et le message d'erreur suivant s'affiche :

  « Impossible de récupérer les données » [LC8207]

Stratégie Citrix

- Des objets de stratégie de groupe qui contiennent des paramètres Citrix et Microsoft ne peuvent pas être appliqués. Ce problème se produit lorsque l'unité d'extension de la liste contient plusieurs GUID. [LC7533]

Citrix Studio

- Les tentatives d'ajout de comptes d'ordinateur à des catalogues de machines, nouveaux ou existants, peuvent échouer lors de l'utilisation du mode GUI au lieu de commandes PowerShell. Le problème se produit lorsque l'outil de recherche de répertoire ne lie pas l'objet correct lors de la recherche du nom NetBIOS.

  Par exemple, si le nom de domaine est xyz.ad.airxyz.aa et le nom NetBIOS est xyz-Ad, le nom NetBIOS est accepté en tant que xyz au lieu de xyz-Ad lors de l'utilisation du mode GUI. Par conséquent, le compte de machine ne peut pas être ajouté pour les comptes d'ordinateur existants et nouveaux. [LC6679]

- Après la mise à niveau de Citrix Delivery Controller vers la version 7.12, les tentatives d'ajout de machines depuis Citrix Provisioning Services (PVS) à un catalogue peuvent échouer dans un environnement multi-domaine. Le problème se produit lorsque PVS ne renvoie pas le nom de domaine avec le nom de l'appareil. Lorsque Citrix Studio recherche le nom du compte dans le domaine local, le compte est introuvable. [LC6818]

- Les tentatives de publication d'applications App-V peuvent échouer. [LC7421]

- Lorsqu'un administrateur tente d'ajouter une application App-V à partir d'un groupe d'isolement au groupe de mise à disposition ou tente de créer un groupe d'isolement, le message d'erreur suivant peut s'afficher dans Citrix Studio :

  « Une erreur indéterminée s'est produite. » [LC7594]

- Les tentatives d'ajout de machines à un groupe de mise à disposition en utilisant le nom « NETBIOS » pour l'association d'utilisateur peuvent échouer. Au lieu de cela, le nom de domaine peut s'afficher. Le problème se produit lorsque le nom NETBIOS utilise l'adresse URL incorrecte. [LC7830]

Controller

- Après la mise à niveau de Citrix Delivery Controller vers la version 7.12, les tentatives d'ajout de machines depuis Citrix Provisioning Services (PVS) à un catalogue peuvent échouer dans un environnement multi-domaine. Le problème se produit lorsque PVS ne renvoie pas le nom de domaine avec le nom de l'appareil. Lorsque Citrix Studio recherche le nom du compte dans le domaine local, le compte est introuvable. [LC6818]
- Les tentatives d'ajout de machines à un catalogue Machine Creation Services existant peuvent ne pas respecter la méthode round robin sélectionnée pour les stockages multiples afin d'accepter les nouvelles machines. [LC7456]
- Les tentatives par des administrateurs personnalisés de créer un groupe d'isolement peuvent échouer et le message d'erreur suivant s'afficher :

  « Vous ne disposez pas des autorisations requises pour traiter cette demande. Pour de plus amples informations, contactez l'administrateur de votre site XenDesktop. » [LC7563]

- Lorsqu'un administrateur tente d'ajouter une application App-V à partir d'un groupe d'isolement au groupe de mise à disposition ou tente de créer un groupe d'isolement, le message d'erreur suivant peut s'afficher dans Citrix Studio :

  « Une erreur indéterminée s'est produite. » [LC7594]

- Les tentatives de désactivation de TLSv1.0 sur Citrix Delivery Controller peuvent entraîner la perte de la communication avec l'hyperviseur vCenter VMware. [LC7686]
- Les tentatives d'ajout de machines à un groupe de mise à disposition en utilisant le nom « NETBIOS » pour l'association d'utilisateur peuvent échouer. Au lieu de cela, le nom de domaine peut s'afficher. Le problème se produit lorsque le nom NETBIOS utilise l'adresse URL incorrecte. [LC7830]

Pack d'optimisation HDX RealTime

Profile Management

- Lorsque vous tentez d'ouvrir des fichiers dans un profil alors que Streaming des profils est activé, le fichier peut paraître vide après l'ouverture de session. [LC6996]
- Les serveurs peuvent rencontrer une exception fatale, affichant un écran bleu, sous upmjit.sys avec le code bugcheck 0x135. [LC7841][]
- UserProfileManager.exe peut se fermer de manière inattendue lorsque vous ouvrez une session sur un VDA. [LC7952][]

StoreFront

- Les tentatives de reconnexion à des sessions déconnectées peuvent échouer dans un déploiement d'agrégation multisite. Par conséquent, une seconde instance de la même ressource peut s'afficher. [LC7453][]
- Lorsqu'une partie de la source d'une application agrégée est désactivée, l'application peut être masquée de manière inattendue pour l'utilisateur final. [LC7675][]
- Les tentatives de désactivation de l'option « Compte en libre-service » dans StoreFront peuvent ne pas prendre effet, même si l'option apparaît comme désactivée. [LC7744][]
- Les tentatives de suppression d'authentifications partagées de magasins dans StoreFront peuvent entraîner l'affichage du message d'erreur suivant lors de l'enregistrement des modifications :

  « Une erreur s'est produite lors de l'enregistrement de vos modifications. » [LC7781]

Serveur d'impression universelle

Redirection de

- Le service de spouleur d'impression peut cesser de répondre et par conséquent, l'impression universelle ne fonctionne pas. Le problème se produit lorsqu'un délai d'expiration est atteint lors de l'attente d'une réponse de transaction du service de spouleur. [LC5209]
- Lorsque vous utilisez Profile Management, les modifications apportées aux imprimantes de serveur d'impression universelle Citrix (ajout, suppression, changement de nom) dans une session sur un serveur peuvent ne pas être correctement reflétées dans les prochaines sessions sur un autre serveur. [LC7645]

Serveur

- Les tentatives d'impression d'un document peuvent échouer et le message d'erreur suivant s'affiche :

  « Impossible d'imprimer : problème de configuration d'imprimante. » [LC6825]

- Lorsque vous utilisez certaines imprimantes, Microsoft Notepad peut afficher le message « Descripteur non valide » et ne pas parvenir à imprimer. Ce problème se produit si « Utiliser uniquement les pilotes spécifiques au modèle de l'imprimante » est configuré dans la stratégie Citrix « Utilisation du pilote d'impression universelle » et si « Activé avec aucun retour à l'impression distante native de Windows » est configuré dans la stratégie Citrix « Activer le serveur d'impression universelle ». [LC7623]

VDA pour OS de bureau

Installation, désinstallation, mise à niveau

- Après la mise à niveau du VDA de la version 5.6.400 à la version 7.9, lorsque le VDA est redémarré, les pilotes miroirs installés par la version précédente peuvent rester. [LC6295]
- Certaines classes WMI peuvent être renommées après l'installation de la version 7.12 ou 7.13 du VDA sur une version non anglaise du système d'exploitation Microsoft Windows. [LC7555]
- Certaines classes WMI peuvent être renommées après l'installation de la version 7.12 ou 7.13 du VDA sur une version non anglaise du système d'exploitation Microsoft Windows. [LC7587]

Impression

- Citrix Print Manager Service (cpsvc.exe) peut cesser de répondre et se fermer de manière inattendue lorsque de nouveaux utilisateurs ouvrent une session. [LC6933]
- Après la mise à niveau du VDA de la version 7.9 à la version 7.12 ou ultérieure, les tentatives d'impression à partir de Microsoft Internet Explorer en utilisant le pilote d'impression universel Citrix peuvent imprimer uniquement vers le magasin 1 au lieu d'imprimer vers le magasin qui est sélectionné. [LC7463]

Session/Connexion

- Lorsque plusieurs webcams du même modèle sont installées sur le VDA pour OS de bureau, seule la webcam la plus récente peut être reconnue par la session et mappée. [LC5008]

- Un lecteur client amovible peut ne pas être renvoyé par le WFAPI SDK sur le VDA pour OS de bureau. [LC6877]
- Les positions des fenêtres peuvent ne pas être conservées lorsque vous vous reconnectez à une session de bureau publié et que vous utilisez plusieurs moniteurs. [LC7644]
- Lorsque vous basculez des sessions entre plusieurs moniteurs en mode plein écran avec le mode graphique d'ancienne génération activé et sans Desktop Viewer configuré, seul un moniteur peut sembler exécuté la session. [LC7907]

Cartes à puce

- Parfois, le retrait d'un lecteur de carte à puce peut ne pas déclencher le verrouillage de la session utilisateur, même si le retrait de carte à puce est configuré pour verrouiller la session utilisateur. [LC7411]

Exceptions système

- Les VDA peuvent rencontrer une exception fatale, affichant un écran bleu, sous vd3dk.sys avec le code bugcheck 0X00000050. [LC6833]
- Les VDA peuvent rencontrer une exception fatale, affichant un écran bleu, sous picadm.sys avec le code bugcheck 0x7F lors de l'arrêt d'une session. [LC7545]
- Le processus Service Host (Svchost.exe) peut rencontrer une violation d'accès et se fermer de manière inattendue. Le problème se produit en raison du module défaillant scardhook64.dll. [LC7580]
- Des exceptions fatales peuvent se produire sur les serveurs, qui affichent alors un écran bleu sur vdtw30.dll avec le code d'arrêt 0xc0000006. [LC7608]
- Les VDA peuvent rencontrer une exception fatale, affichant un écran bleu, sous tdica.sys avec un code bugcheck. [LC7632]
- Cette correction résout un problème de mémoire avec le fichier wdica.sys qui peut entraîner la fermeture inattendue de serveurs. [LC7666]

Expérience utilisateur

- Cette correction améliore la prise en charge des sons diffusés pendant une courte période lors de l'utilisation de l'audio haute qualité.

  Remarque :

  – Ce correctif ne prend pas effet dans les sessions s'exécutant sur Windows Server 2008 R2.

  - Pour que cette correction fonctionne, vous devez utiliser Citrix Receiver 4.4 pour Windows Long Term Service Release (LTSR) CU5 ou version ultérieure et la version VDA de XenApp et XenDesktop 7.6 LTSR CU4 ou version ultérieure. [LC5842]

- Lors d'une opération d'insertion entre deux feuilles de calcul Microsoft Excel 2010 s'exécutant sur un VDA version 7.9, la fenêtre Excel peut cesser de répondre. [LC7481]
- Dans un environnement multi-écrans, définissez le moniteur externe comme l'« affichage principal » de Windows et placez-le à droite de l'ordinateur portable secondaire ou de l'écran de la tablette dans les paramètres d'affichage du panneau de configuration. Lorsque vous démarrez une application publiée qui s'affiche sur le moniteur externe et que vous déplacez cette application vers l'écran de la tablette ou un ordinateur portable qui est connecté au moniteur externe, l'application publiée peut devenir noire si vous ouvrez ou fermez le capot de la tablette ou d'un ordinateur portable.

  Pour activer cette correction, définissez l'entrée de registre suivante sur le VDA :

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Ica\Thinwire Nom : EnableDrvTw2NotifyMonitorOrigin Type : REG_DWORD Valeur : 1 (pour activer) et 0 (pour désactiver ; 0 est la valeur par défaut). Par défaut, la valeur de registre est manquante. [LC7760]

Interface utilisateur

- Les icônes de raccourci d'URL peuvent être vides lors de l'utilisation d'un bureau tactile.[#LC6663]
- Si vous ouvrez une feuille de calcul avec plusieurs classeurs dans Excel 2010, la barre des tâches affiche uniquement le classeur le plus récent. [LC7557]

VDA pour OS de serveur

Installation, désinstallation, mise à niveau

- Certaines classes WMI peuvent être renommées après l'installation de la version 7.12 ou 7.13 du VDA sur une version non anglaise du système d'exploitation Microsoft Windows. [LC7555]
- Certaines classes WMI peuvent être renommées après l'installation de la version 7.12 ou 7.13 du VDA sur une version non anglaise du système d'exploitation Microsoft Windows. [LC7587]

Impression

- Citrix Print Manager Service (cpsvc.exe) peut cesser de répondre et se fermer de manière inattendue lorsque de nouveaux utilisateurs ouvrent une session. [LC6933]

- Après la mise à niveau du VDA de la version 7.9 à la version 7.12 ou ultérieure, les tentatives d'impression à partir de Microsoft Internet Explorer en utilisant le pilote d'impression universel Citrix peuvent imprimer uniquement vers le magasin 1 au lieu d'imprimer vers le magasin qui est sélectionné. [LC7463]

Administration de serveur/site

- Le message d'erreur suivant peut s'afficher pour les utilisateurs du domaine enfant lors du lancement d'une application via l'Interface Web ou StoreFront :

  « Vous ne détenez pas les droits d'accès à cette application publiée. » [LC7566]

Session/Connexion

- Lorsque plusieurs webcams du même modèle sont installées sur le VDA pour OS de bureau, seule la webcam la plus récente peut être reconnue par la session et mappée. [LC5008]
- Les tentatives de reconnexion à une session peuvent échouer par intermittence. Lorsque cela se produit, l'état des VDA pour OS de serveur affiche « Initialisation ». Le problème se produit lorsque le VDA est enregistré à nouveau avec un Delivery Controller. [LC6647]
- Les sessions actives peuvent être déconnectées sur les serveurs XenApp lorsque le Delivery Controller perd la connectivité. Le problème se produit lorsque les VDA ne parviennent pas à suivre l'état des sessions qui passent de l'état de « pré-lancement » à l'état « actif » correctement. Par conséquent, lorsque le Delivery Controller est redémarré, il tente d'effacer les ressources des VDA, et les sessions dans l'état de pré-lancement sont déconnectées ou fermées alors que les applications sont en cours d'utilisation. [LC6819]
- Lorsque vous lancez une application publiée sur Microsoft Windows Server 2016, un écran noir peut s'afficher pendant quelques secondes avant que l'application ne devienne visible. [LC7947]

Exceptions système

- Les VDA peuvent rencontrer une exception fatale, affichant un écran bleu, sous picadm.sys avec le code bugcheck 0x7F lors de l'arrêt d'une session. [LC7545]
- Le processus Service Host (Svchost.exe) peut rencontrer une violation d'accès et se fermer de manière inattendue. Le problème se produit en raison du module défaillant scardhook64.dll. [LC7580]
- Des exceptions fatales peuvent se produire sur les serveurs, qui affichent alors un écran bleu sur vdtw30.dll avec le code d'arrêt 0xc0000006. [LC7608]

- Les VDA peuvent rencontrer une exception fatale, affichant un écran bleu, sous tdica.sys avec un code bugcheck. [LC7632]
- Cette correction résout un problème de mémoire avec le fichier wdica.sys qui peut entraîner la fermeture inattendue de serveurs. [LC7666]

Expérience utilisateur

- Cette correction améliore la prise en charge des sons diffusés pendant une courte période lors de l'utilisation de l'audio haute qualité.

  Remarque :

  - Ce correctif ne prend pas effet dans les sessions s'exécutant sur Windows Server 2008 R2.
  - Pour que cette correction fonctionne, vous devez utiliser Citrix Receiver 4.4 pour Windows Long Term Service Release (LTSR) CU5 ou version ultérieure et la version VDA de XenApp et XenDesktop 7.6 LTSR CU4 ou version ultérieure. [LC5842]
- Lors d'une opération d'insertion entre deux feuilles de calcul Microsoft Excel 2010 s'exécutant sur un VDA version 7.9, la fenêtre Excel peut cesser de répondre. [LC7481]
- Dans un environnement multi-écrans, définissez le moniteur externe comme l'« affichage principal » de Windows et placez-le à droite de l'ordinateur portable secondaire ou de l'écran de la tablette dans les paramètres d'affichage du panneau de configuration. Lorsque vous démarrez une application publiée qui s'affiche sur le moniteur externe et que vous déplacez cette application vers l'écran de la tablette ou un ordinateur portable qui est connecté au moniteur externe, l'application publiée peut devenir noire si vous ouvrez ou fermez le capot de la tablette ou d'un ordinateur portable.

  Pour activer cette correction, définissez l'entrée de registre suivante sur le VDA :

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Ica\Thinwire Nom : EnableDrvTw2NotifyMonitorOrigin Type : REG_DWORD Valeur : 1 (pour activer) et 0 (pour désactiver ; 0 est la valeur par défaut). Par défaut, la valeur de registre est manquante. [LC7760]

Interface utilisateur

- Les icônes de raccourci d'URL peuvent être vides lors de l'utilisation d'un bureau tactile. [LC6663]
- Si vous ouvrez une feuille de calcul avec plusieurs classeurs dans Excel 2010, la barre des tâches affiche uniquement le classeur le plus récent. [LC7557]

Composants de bureau virtuel - Autre

- Les tentatives de publication d'applications App-V peuvent échouer. [LC7421]
- Les tentatives de lancement d'applications App-V en mode Administration unique peuvent échouer. Le problème se produit lorsque le nom de l'application contient des caractères spéciaux. [LC7897]

Problèmes résolus depuis 7.6 LTSR CU4

Citrix Director

- Citrix Director avec authentification intégrée Windows (WIA) risque de ne pas fonctionner avec une configuration de délégation Kerberos contrainte. [LC5196]
- Une erreur « Système non disponible » se produit après une tentative de connexion sur Citrix Director. [LC5385]
- Citrix Director peut ne pas afficher les détails de la session. Le problème se produit lors de l'utilisation de contenu publié comme type d'application. [LC6577]

Stratégie Citrix

- Le traitement de la stratégie Citrix peut cesser de répondre, ce qui entraîne l'absence de réponse des sessions utilisateur. Lorsque cela se produit, les requêtes de connexion auprès de Receiver et de Bureau à distance (RDP) échouent. [LA4969]
- Sur les systèmes avec correctif LC1987 (GPCSExt170W2K8R2X64006 ou son remplacement) installé, les stratégies Active Directory (AD) qui contiennent des paramètres Citrix et Microsoft peuvent ne pas être appliquées.

  Remarque : cette correction résout le problème pour les stratégies Active Directory que vous créez après l'installation de cette mise à jour. Il résout également le problème pour les stratégies *existantes* lorsque les paramètres Citrix ont été configurés avant les paramètres Microsoft. Il ne résout pas le problème pour les stratégies AD existantes lorsque les paramètres Microsoft ont été configurés *avant* les paramètres Citrix. Pour ces stratégies Active Directory, vous devez ouvrir les stratégies affectées et enregistrer les paramètres Citrix. [LC2121]
- Avec cette amélioration, le service Citrix Group Policy Engine génère des messages de journal d'événements supplémentaires lors du traitement des stratégies Citrix. [LC3664]
- Lors de la mise à niveau de la version 7.6 vers la version 7.8 ou 7.9, certains jeux de couleurs dans Citrix Studio peuvent être trop sombres pour que le texte s'affiche correctement. [LC5690]

- Après avoir installé le Service d'authentification fédérée de Citrix, les tentatives de configuration des **listes de contrôle d'accès de sécurité** sur le serveur StoreFront sous **User Rules** peuvent entraîner le blocage de la fenêtre Configuration. [LC5788]
- La consommation de processeur et de mémoire de Microsoft Excel peut connaître une forte hausse lors de l'ouverture d'un fichier avec l'extension de fichier XLSM avec des macros. Par conséquent, les tentatives d'ouverture du fichier échouent. [LC6142]
- Des objets de stratégie de groupe qui contiennent des paramètres Citrix et Microsoft ne peuvent pas être appliqués. Ce problème se produit lorsque l'unité d'extension de la liste contient plusieurs GUID. [LC7533]

Citrix Studio

- Lorsque plusieurs utilisateurs créent des stratégies dans plusieurs sessions Studio, la dernière stratégie créée écrase la stratégie précédente lorsque Citrix Studio est actualisé. [LA5533]
- Citrix Studio ne reconnaît pas la licence XenDesktop App Edition et le message d'erreur suivant s'affiche :

  « Impossible de trouver une licence valide
  Aucune licence appropriée n'est disponible. Vérifiez que l'adresse du serveur de licences et que l'édition et le modèle du produit sont corrects. » [LC0822]
- Lorsque vous essayez d'ajouter des utilisateurs inter-domaines à un groupe de mise à disposition, Citrix Studio résout leur domaine sur le compte de domaine local. [LC1886
- Les tentatives de publication d'une application dans Citrix Studio 7.7 à l'aide d'arguments de ligne de commande qui contiennent des guillemets (") peuvent entraîner un message d'erreur. [LC4525]
- Citrix Studio peut offrir l'option de restauration du catalogue, même si aucune mise à jour du catalogue n'a été effectuée. Activer cette option entraîne une exception. [LC4791]
- Les tentatives d'ajout de machines à un catalogue de machines à partir de Citrix Studio peuvent échouer et un message d'erreur s'afficher. Ce problème ne se produit pas lorsque vous ajoutez des machines à l'aide de l'assistant d'installation de XenDesktop. [LC5030]
- Si deux applications ont le même ApplicationID, lorsque les applications App-V sont actualisées, Citrix Studio peut définir le nom du pack App-V de manière incorrecte. [LC5261]
- Lorsqu'un Delivery Controller est déconnecté ou devient indisponible pour toute autre raison, Citrix Studio peut fonctionner lentement. [LC5335]
- Après la mise à niveau vers XenApp ou XenDesktop 7.7 depuis la version 7.6, une invite à mettre à niveau peut parfois s'afficher dans Citrix Studio. [LC5478]

- Lorsque vous fermez et essayez de rouvrir une instance de la version 7.9 de Citrix Studio qui est configurée avec des serveurs App-V contenant plusieurs packages, Studio reste dans un état de développement et ne parvient pas à s'ouvrir. [LC5643]
- En utilisant Citrix Studio, vous pouvez ajouter un seul serveur App-V à un site. Pour ajouter des serveurs App-V supplémentaires au site, vous devez utiliser PowerShell. [LC5767]
- Après la mise à niveau de Citrix Studio de 7.8 vers 7.9, les applications que vous ajoutez après la mise à niveau s'affichent sans nom de package ou de version. [LC5958]
- L'ajout d'une application via le nœud Applications dans Citrix Studio peut entraîner une erreur, l'application n'est pas ajoutée. Pour contourner le problème, utilisez le nœud Groupe de mise à disposition pour ajouter des applications. [LC5975]
- Lors de la tentative de création d'un nouveau site XenDesktop à l'aide de Citrix Studio, pointant vers l'écouteur AlwaysOn SQL, le message d'erreur suivant peut s'afficher :

  « Impossible de contacter le serveur réplica <nomserveur>. Vérifiez l'état de la base de données sur le serveur SQL. Assurez-vous que le serveur de base de données autorise les connexions distantes et que le pare-feu ne bloque pas les connexions. » [LC6010]
- Si vous supprimez un package App-V publié existant de Citrix Studio et que vous essayez d'ajouter une version différente du même package App-V avec le même nom et le même emplacement de publication au groupe de mise à disposition, le package peut s'afficher avec un point d'exclamation rouge et le message d'erreur suivant s'affiche :

  « Impossible de charger les données d'application pour l'application « NOM APPLICATION » » [LC6254]
- Les tentatives d'ajout d'un Delivery Controller dans une configuration de base de données en miroir à l'aide de l'option d'ajout d'un contrôleur supplémentaire de Citrix Studio et de la commande PowerShell « Add-XDController » peuvent échouer. [LC6563]
- Les tentatives d'ajout de comptes d'ordinateur à des catalogues de machines, nouveaux ou existants, peuvent échouer lors de l'utilisation du mode GUI au lieu de commandes PowerShell. Le problème se produit lorsque l'outil de recherche de répertoire ne lie pas l'objet correct lors de la recherche du nom NetBIOS.

  Par exemple, si le nom de domaine est xyz.ad.airxyz.aa et le nom NetBIOS est xyz-Ad, le nom NetBIOS est accepté en tant que xyz au lieu de xyz-Ad lors de l'utilisation du mode GUI. Par conséquent, le compte de machine ne peut pas être ajouté pour les comptes d'ordinateur existants et nouveaux. [LC6679]
- Après la mise à niveau de Citrix Delivery Controller vers la version 7.12, les tentatives d'ajout de machines depuis Citrix Provisioning Services (PVS) à un catalogue peuvent échouer dans un environnement multi-domaine. Le problème se produit lorsque PVS ne renvoie pas le nom de

domaine avec le nom de l'appareil. Lorsque Citrix Studio recherche le nom du compte dans le domaine local, le compte est introuvable. [LC6818]

- Lors de la mise à niveau d'un site XenApp, le modèle de licence peut passer de XenApp à XenDesktop de façon inattendue. [LC6981]
- La commande « Start-Transcript » peut échouer pour « Get-XDSite » et d'autres commandes PoSH administratives de haut niveau XenDesktop lorsqu'elle est exécutée dans PowerShell 5. [LC7006]
- Lorsqu'un administrateur tente d'ajouter une application App-V à partir d'un groupe d'isolement au groupe de mise à disposition ou tente de créer un groupe d'isolement, le message d'erreur suivant peut s'afficher dans Citrix Studio :

  « Une erreur indéterminée s'est produite. » [LC7594]
- Les tentatives d'ajout de machines à un groupe de mise à disposition en utilisant le nom « NETBIOS » pour l'association d'utilisateur peuvent échouer. Au lieu de cela, le nom de domaine peut s'afficher. Le problème se produit lorsque le nom NETBIOS utilise l'adresse URL incorrecte. [LC7830]

Controller

- Le déploiement de machines virtuelles à l'aide de Machine Creation Services dans Citrix Studio échoue, affichant le message d'erreur suivant :

  « ID d'erreur: XDDS: 0F7CB924. » [LC4930]
- Lorsque les utilisateurs tentent de supprimer le catalogue regroupé créé sur XenServer, puis exécutent la mise à jour du catalogue, les disques de base ne sont pas supprimés du stockage et le nombre de disques de base peut augmenter. [LC0577]
- La fiabilité de session ne peut pas être désactivée à l'aide d'un objet de stratégie de groupe (GPO) Active Directory ou via Citrix Studio sur les sessions VDA 7.x qui démarrent à l'aide de XenDesktop 5.6 Desktop Delivery Controller (DDC). [LC0878]
- Lors de la création d'une nouvelle machine regroupée à l'aide de Machine Creation Services à partir d'une image principale avec des paramètres VMX et nvram personnalisés, les paramètres ne sont pas copiés vers les nouvelles machines virtuelles. [LC0967]
- La tâche PrepareSession qui est exécutée par Broker Service peut expirer lorsqu'elle est utilisée dans des environnements XenDesktop 5.6, ce qui entraîne l'échec de StoreFront. [LC1055]
- Ce correctif résout un problème de synchronisation qui peut se produire lorsque l'hyperviseur est congestionné pendant le formatage d'un volume de disque PvD lors de la création initiale de la machine. [LC3275]

- La création de machines virtuelles avec Machine Creation Services à l'aide de stockage VMware vSphere 6.0 et vSAN 6 peut échouer. [LC4563]
- La réponse WaitForTask entraîne l'exception VimApi.MissingProperty qui n'autorise pas la mise à jour des catalogues de machines. [LC4573]
- Les tentatives d'ajout de machines à un catalogue de machines à partir de Citrix Studio peuvent échouer et un message d'erreur s'afficher. Ce problème ne se produit pas lorsque vous ajoutez des machines à l'aide de l'assistant d'installation de XenDesktop. [LC5030]
- Après la mise à niveau du VDA vers la version 7.8, les tentatives de mise à jour d'inventaire peuvent échouer et le message d'erreur suivant s'afficher :

  « Échec de la mise à jour de l'inventaire avec le message 'Une erreur interne s'est produite Code d'erreur 0x2'. » [LC5051]
- Des caractères superflus peuvent apparaître à la fin de « Nom d'affichage du service » et « Description du service » de certains services Citrix installés sur un système d'exploitation japonais. [LC5208]
- Si deux applications ont le même ApplicationID, lorsque les applications App-V sont actualisées, Citrix Studio peut définir le nom du pack App-V de manière incorrecte. [LC5261]
- Après la mise à niveau vers XenApp ou XenDesktop 7.7 depuis la version 7.6, une invite à mettre à niveau peut parfois s'afficher dans Citrix Studio. [LC5478]
- Une esperluette (&) dans le titre d'une application entraîne la corruption de XML StoreFront et aucune application ou icône ne s'affiche. [LC5505]
- Lorsque vous fermez et essayez de rouvrir une instance de la version 7.9 de Citrix Studio qui est configurée avec des serveurs App-V contenant plusieurs packages, Studio reste dans un état de développement et ne parvient pas à s'ouvrir. [LC5643]
- Après la mise à niveau vers XenDesktop 7.9, l'ouverture de session peut parfois échouer car le broker NetScaler n'envoie pas les informations d'identification correctement. [LC5753]
- En utilisant Citrix Studio, vous pouvez ajouter un seul serveur App-V à un site. Pour ajouter des serveurs App-V supplémentaires au site, vous devez utiliser PowerShell. [LC5767]
- Après avoir installé le Service d'authentification fédérée de Citrix, les tentatives de configuration des **listes de contrôle d'accès de sécurité** sur le serveur StoreFront sous **User Rules** peuvent entraîner le blocage de la fenêtre Configuration. [LC5788]
- Modifier le port SDK des services Flexcast Management Architecture tels qu'Analytics, Broker, Log, etc. entraîne une connexion incorrecte de Citrix Studio. [LC6005]
- Lors de la tentative de création d'un nouveau site XenDesktop à l'aide de Citrix Studio, pointant vers l'écouteur AlwaysOn SQL, le message d'erreur suivant peut s'afficher :

« Impossible de contacter le serveur réplica <nomserveur>. Vérifiez l'état de la base de données sur le serveur SQL. Assurez-vous que le serveur de base de données autorise les connexions distantes et que le pare-feu ne bloque pas les connexions. » [LC6010]

- Citrix Director peut afficher un certain nombre de machines non enregistrées dans le tableau de bord qui ne correspondent pas au rapport sur la page Tendances. [LC6184]
- Le service de surveillance ne réussit pas à insérer les données de la nouvelle session dans la base de données de surveillance lorsque la stratégie Indice de calculateur de charge est activée. De ce fait, il est possible que les informations relatives aux sessions, telles que la durée d'ouverture de session, le nombre de sessions actives, etc, affichées par Citrix Director ne soient pas à jour. Lorsque le problème se produit dans Citrix Director, il est causé par un problème dans le Delivery Controller. La version actuelle du Controller résout le problème. [LC6241]
- Les tentatives de suppression d'une unité d'hébergement peuvent provoquer l'échec de la réplication des AppDisks sur toute autre unité d'hébergement. Par conséquent, les machines dans le groupe de mise à disposition avec les AppDisks ne démarrent pas. [LC6433]
- Après avoir redémarré le service de surveillance de Citrix (Citrix Monitoring Service) ou le Citrix Delivery Controller, l'ID d'événement 1013 peut s'afficher :

  « Échec de la maintenance initiale de la base de données avec : System.NullReferenceException : référence d'objet non défini sur une instance d'un objet. »

  Ce problème se produit lors de l'arrêt du service de surveillance de Citrix. [LC6438]
- Les tentatives d'utilisation de certaines applications tierces telles que RayStation sur un Citrix Delivery Controller peuvent échouer et le message d'erreur suivant s'affiche :

  « The communication object, System.ServiceModel.Channels.ServiceChannel, cannot be used for communication because it is in the Faulted state. » [LC6552]
- Les tentatives d'ajout d'un Delivery Controller dans une configuration de base de données en miroir à l'aide de l'option d'ajout d'un contrôleur supplémentaire de Citrix Studio et de la commande PowerShell « Add-XDController » peuvent échouer. [LC6563]
- Les tentatives de suppression de catalogues MCS sur des VMware VSAN peuvent échouer. [LC6691]
- La consommation de mémoire du Monitoring Service peut enregistrer une hausse, ce qui entraîne une absence de réponse des serveurs. [LC6705]
- Après la mise à niveau de Citrix Studio à partir de versions précédentes ou lorsque vous effectuez une nouvelle installation de la version Citrix Studio 7.12, Citrix Studio peut se trouver coincé dans une boucle de mise à niveau obligatoire à cause du Delivery Controller. [LC6737]
- Lors de l'utilisation de la version 7.12 de Machine Creation Services pour créer des VM, l'installation de XenTools échoue, ce qui empêche l'arrêt correct des VM. [LC6769]

- Après la mise à niveau de Citrix Delivery Controller vers la version 7.12, les tentatives d'ajout de machines depuis Citrix Provisioning Services (PVS) à un catalogue peuvent échouer dans un environnement multi-domaine. Le problème se produit lorsque PVS ne renvoie pas le nom de domaine avec le nom de l'appareil. Lorsque Citrix Studio recherche le nom du compte dans le domaine local, le compte est introuvable. [#LC6818]
- Les autorisations de publier des packages App-V peuvent être refusées pour les administrateurs qui n'ont pas d'autorisation complète avec l'exception suivante :

  « Citrix.Console.Models.Exceptions.PermissionDeniedException : Vous ne disposez pas des autorisations nécessaires pour réaliser cette opération. » [LC6897]
- Le processus HighAvailabilityService.exe peut consommer beaucoup de mémoire. [LC6918]
- Lors de la mise à niveau d'un site XenApp, le modèle de licence peut passer de XenApp à XenDesktop de façon inattendue. [LC6981]
- La commande « Start-Transcript » peut échouer pour « Get-XDSite » et d'autres commandes PoSH administratives de haut niveau XenDesktop lorsqu'elle est exécutée dans PowerShell 5. [LC7006]
- Ce correctif résout un problème de mémoire dans Citrix Host Service. [LC7516]
- Les tentatives par des administrateurs personnalisés de créer un groupe d'isolement peuvent échouer et le message d'erreur suivant s'afficher :

  « Vous ne disposez pas des autorisations requises pour traiter cette demande. Pour de plus amples informations, contactez l'administrateur de votre site XenDesktop. » [LC7563]
- Lorsqu'un administrateur tente d'ajouter une application App-V à partir d'un groupe d'isolement au groupe de mise à disposition ou tente de créer un groupe d'isolement, le message d'erreur suivant peut s'afficher dans Citrix Studio :

  « Une erreur indéterminée s'est produite. » [LC7594]
- Les tentatives d'installation du VDA sur Microsoft Windows Server peuvent échouer lorsque le service de rôle de Microsoft Remote Desktop Session Host est déjà installé. [LC7680]
- Les tentatives de désactivation de TLSv1.0 sur Citrix Delivery Controller peuvent entraîner la perte de la communication avec l'hyperviseur vCenter VMware. [LC7686]
- Les tentatives d'ajout de machines à un groupe de mise à disposition en utilisant le nom « NETBIOS » pour l'association d'utilisateur peuvent échouer. Au lieu de cela, le nom de domaine peut s'afficher. Le problème se produit lorsque le nom NETBIOS utilise l'adresse URL incorrecte. [LC7830]

Licences

- Le serveur de licences peut faire échouer l'analyse de conformité PCI (Payment Card Industry) pour détournement de clic car le type d'en-tête « X-Frame-Options » n'est pas défini. [LC1983]
- Les tentatives d'ajout d'un groupe de domaine dont le nom contient plus de 32 caractères peuvent échouer. [LC1986]
- Si le nom de domaine NetBios contient une esperluette (&), les tentatives d'ouverture de l'onglet Licences dans Studio peuvent échouer avec le message d'erreur suivant :

  « Serveur de licences Citrix indisponible » [LC2728]

Profile Management

- Les tentatives par certaines applications tierces de renommer ou de déplacer des fichiers durant l'ouverture ou la fermeture de session peuvent échouer. À titre d'exemple, si le profil local contient les fichiers fichier0, fichier1 et fichier2, toute tentative visant à renommer fichier2 pour fichier3, fichier1 pour fichier2 et fichier0 pour fichier1 peut échouer durant le processus de fermeture de session si fichier2 existe déjà sur la zone d'attente ou le magasin de l'utilisateur. [LC0465]
- Lorsque les utilisateurs ferment leur session, le service Profile Management (UserProfileManager.exe) échoue parfois. [LC0625]
- Le panneau « Durée d'ouverture de session » dans le compteur Analyseur des performances (Perfmon) peut enregistrer les données d'ouvertures de session utilisateur qui ne sont pas gérées par Profile Management. [LC0779]
- Il se peut que Profile Management ne synchronise pas les fichiers avec le magasin de l'utilisateur après un certain laps de temps. [LC1338]
- Après activation des options de journalisation suivantes, aucune information de débogage n'est enregistrée dans le fichier journal :
  - Stratégie : Actions Active Directory
  - Stratégie : Valeurs de stratégie à l'ouverture et fermeture de session
  - Stratégie : Différences de registre à la fermeture de session [LC2003]
- Si un utilisateur active la gestion des profils comme décrit dans l'article https://support.microsoft.com/en-us/kb/2890783, la migration de Profile Management peut échouer pour les raisons suivantes :
  - Le profil itinérant Microsoft est créé avec l'extension « V4 ».
  - Le profil UPM n'était pas migré et était créé à partir du modèle « Utilisateur par défaut ». [LC2427]

- Après la réinitialisation du profil utilisateur dans Desktop Director, la redirection de dossiers ne fonctionne pas lorsque les utilisateurs ouvrent une session pour la première fois. Elle fonctionne lors de l'ouverture de session suivante. [LC2602]
- Le service Profile Management (UserProfileManager.exe) peut se fermer de manière inattendue. [LC2979]
- Après application de la correction LC0625, le service Profile Management (UserProfileManager.exe) peut se fermer de manière inattendue. [LC3058]
- Sur Windows 8.1, les tentatives de téléchargement de fichiers à l'aide d'Internet Explorer 11 échouent si le mode protégé amélioré (EPM) est activé. [LC3464]
- Les fichiers peuvent être verrouillés dans Profile Management durant le processus de fermeture de session avec le message d'erreur suivant :

  « Le processus ne peut pas accéder au fichier car ce fichier est verrouillé par un autre processus. »

  Les tentatives de suppression de fichiers verrouillés par Profile Management peuvent échouer tant que les fichiers ne sont pas déverrouillés. [LC3532]
- Profile Management peut se fermer de manière inattendue alors que la machine est en cours de fermeture. [LC3626]
- Les serveurs XenApp peuvent cesser de répondre dans la batterie tant que le serveur n'a pas été redémarré. [LC4318]
- Lors de la tentative de connexion à un serveur XenApp 7.7 à l'aide de RDP, il est possible que le serveur cesse de répondre sur l'écran de bienvenue. [LC5169]
- Après la mise à niveau d'un VDA de la version 7.6.1000 ou antérieure vers la version 7.7 ou supérieure, les tentatives de suppression, de réparation ou de réinstallation de Profile Management ou du VDA peuvent échouer. [LC5207]
- Lors de la fermeture de session, Profile Management verrouille parfois les fichier/dossiers sur le serveur, par conséquent le lancement d'applications échoue. Les profils mis en cache localement ne sont pas également supprimés. [LC5266]
- Profile Management verrouille parfois les fichiers dans les profils utilisateur. Lorsque cela se produit, les utilisateurs reçoivent un profil temporaire lors de la tentative de reconnexion jusqu'à ce que leur profil soit déverrouillé. [LC5278]
- Il est possible que les profils mis en cache localement ne soient pas effacés lorsque les utilisateurs ferment leurs sessions. [LC5470]
- Lorsque le serveur de licences est hors connexion, les fichiers qui utilisent la redirection des dossiers utilisateur sur le serveur sont perdus. [LC5595]

- Les fichiers des utilisateurs sont perdus lorsque la période d'essai de la licence expire et qu'elle n'est pas renouvelée. [LC5775]
- Profile Management peut afficher un indicateur « NetworkDetection » par erreur indiquant que le réseau est peut-être perdu. Cette correction introduit une vérification supplémentaire pour s'assurer que le réseau n'est pas disponible plutôt que temporairement indisponible. [LC5943]
- Parfois, l'écran d'ouverture de session utilisateur cesse de répondre sur Windows Server 2012 R2. [LC6149]
- Les tentatives de migration de profils itinérants dans Profile Management peuvent échouer. Le problème se produit lorsqu'un numéro incorrect de version est ajouté au profil. [LC6150]
- Les icônes des applications peuvent être grisées lorsque vous tentez de copier les icônes provenant du magasin du profil utilisateur de Profile Management via une connexion WAN. [LC6152]
- Les associations de type de fichier peuvent ne pas se déplacer dans les sessions activées par Profile Management s'exécutant sur Microsoft Windows 10 et Windows Server 2016. [LC6736]
- Lorsque la stratégie Supprimer le cache local à la fermeture de session est activée sur Microsoft Windows 10 ou Windows Server 2016, le fichier NTUSER.DAT peut ne pas être supprimé à la fermeture de session, ce qui entraîne la création d'un autre profil local à la prochaine ouverture de session. [LC6765]
- Lors de l'utilisation de Profile Management sur Microsoft Windows Server 2016 et si usrclass.dat est inclus, le menu Démarrer peut ne pas fonctionner. [LC6914]
- Lorsque vous tentez d'ouvrir des fichiers dans un profil alors que Streaming des profils est activé, le fichier peut paraître vide après l'ouverture de session. [LC6996]
- Profile Management peut entraîner l'affichage d'un écran noir lorsque vous tentez de lancer une session Microsoft Windows 10. Avec cette correction, vous devez configurer la stratégie « Répertoires à synchroniser » et ajouter le dossier « *AppData\Local\Microsoft\Windows\Caches*. » [LC7596]

Provisioning Services

Problèmes liés à la console

- Grâce à cette correction, les options « Schedule the next vDisk update to occur on » et « Apply vDisk updates as soon as they are directed by the server » ne sont plus disponibles pour Provisioning Services. [LA4166]
- Les tentatives de création de machines virtuelles à l'aide de l'assistant d'installation de XenDesktop peuvent échouer dans un environnement Microsoft System Center Virtual Machine Manager

(SCVMM) autre que l'anglais. [LC5451]

- Les tentatives de création d'une image ISO avec le script PowerShell New-BootDeviceManager peuvent échouer et le message d'erreur suivant s'affiche : « ISOFileName must be called with the name of the new ISO file to create. » [LC5559]
- Lorsque vous utilisez un volume de stockage en cluster, l'Assistant Streamed VM Setup ne reconnaît pas la sélection de volume et peut créer les machines cibles dans des volumes aléatoires. [LC5890]
- Les tentatives de fermeture de la Console Provisioning Services après avoir exécuté l'Assistant XenDesktop Setup wizard ou l'Assistant Streamed VM Setup peuvent entraîner une exception. [LC6048]
- Après la mise à niveau vers PVS 7.11 à partir de la version 7.6, il est possible que les utilisateurs d'autres domaines puissent ne pas ouvrir de session sur la console. [LC6216]
  []
- Expiration du délai de communication avec le serveur. Dans certains cas, les délais de connexion peuvent être très longs (par exemple, supérieurs à 2 minutes). Cela peut entraîner des problèmes d'expiration du serveur entre le SoapServer et la console PVS. Par défaut, le délai d'expiration de telles connexions est de 2 minutes. Toutefois, vous pouvez augmenter cette valeur en modifiant la valeur de Registre HOTKEY_LOCAL_MACHINE\Software\Citrix\ProvisioningServices ConnectionTimeout=<délai d'expiration en secondes>. Si la durée d'ouverture de session est supérieure à environ 4 minutes, les utilisateurs rencontreront également des problèmes d'expiration depuis la console MMC Microsoft contenant la console PVS (ces délais d'expiration peuvent être ignorés).

  Ce problème est notamment causé par des domaines inaccessibles dans Active Directory, car un délai de 30 secondes est appliqué à chaque tentative de connexion à un domaine inaccessible. Le délai peut rapidement s'élever à plusieurs minutes si plusieurs domaines sont inaccessibles. En général, les domaines inaccessibles sont créés par l'ajout d'un domaine test ou expérimental à Active Directory, puis sa suppression plus tard. Bien que le domaine soit supprimé, il est toujours signalé par Active Directory lors de l'énumération des domaines ou groupes d'autorisation.

  Les domaines inaccessibles peuvent également être causés par l'arrêt et la déconnexion temporaires d'un contrôleur de domaine du réseau, donc tous les domaines inaccessibles ne doivent être placés sur liste noire.

  Le meilleur moyen de déterminer s'il existe des domaines inaccessibles consiste à examiner la trace CDF du module PVS_DLL_ADSUPPORT et à rechercher les erreurs « Unreachable Domain » et « Server Referral ». Si ces erreurs sont présentes, vérifiez les domaines pour vous assurer qu'ils ne sont plus utilisés et, dans ce cas, ajoutez ces noms de domaine à la liste noire.

La liste noire est un fichier au format JSON appelé « %ProgramData\Citrix\Provisioning Services\blacklist.json ». Par exemple :

```
{


"Domains":

[

"sub.xs.local",

"sb.xs.local"

]

 }
```

Où les deux domaines **sub.xs.local** et **sb.xs.local** seront exclus de l'énumération de domaines et de groupes. Une fois que le fichier est mis à jour, vous devez redémarrer le SoapServer et les consoles en cours d'exécution afin de charger les valeurs mises à jour. [LC6249]

- Après la configuration de la Console Provisioning Services Console, les noms d'étiquette peuvent être absents dans les propriétés de la machine cible. [LC6864]

Problèmes liés au serveur

- Dans les déploiements VMware ESX, l'assistant XenDesktop Setup Wizard peut renvoyer une exception, ce qui empêche les utilisateurs de configurer correctement les modèles et les machines. [LA2499]
- Deux serveurs PVS peuvent ne pas être en mesure de voir l'état de réplication d'un vDisk sur l'autre serveur, mais chaque serveur indique l'état de ses propres vDisks correctement. [LC4317]
- Le service PXE Citrix peut ignorer les entrées dans le fichier BOOTPTAB. [#LC4600]
- Lors de l'utilisation d'une partition BDM, les machines cibles exécutées sur VMware n'essayent pas de se connecter à tous les serveurs figurant dans la liste si le serveur en haut de la liste est injoignable. [LC4736]
- Les tentatives de création de machines virtuelles à l'aide de l'assistant d'installation de XenDesktop peuvent échouer dans un environnement Microsoft System Center Virtual Machine Manager (SCVMM) autre que l'anglais. [LC5451]
- Si les partitions d'un disque dur ne sont pas toutes clonées, les partitions finales qui sont en cours de clonage peuvent échouer. [LC5452]

- Lors de l'exécution de l'état de la réplication pour deux serveurs PVS à partir de la console PVS, l'état des deux serveurs est incomplet. [LC5700]
- Lorsque vous utilisez un volume de stockage en cluster, l'Assistant Streamed VM Setup ne reconnaît pas la sélection de volume et peut créer les machines cibles dans des volumes aléatoires. [LC5890]
- Après la mise à niveau vers PVS 7.11 à partir de la version 7.6, il est possible que les utilisateurs d'autres domaines puissent ne pas ouvrir de session sur la console. []
- Expiration du délai de communication avec le serveur. Dans certains cas, les délais de connexion peuvent être très longs (par exemple, supérieurs à 2 minutes). Cela peut entraîner des problèmes d'expiration du serveur entre le SoapServer et la console PVS. Par défaut, le délai d'expiration de telles connexions est de 2 minutes. Toutefois, vous pouvez augmenter cette valeur en modifiant la valeur de Registre HOTKEY_LOCAL_MACHINE\Software\Citrix\ProvisioningServices ConnectionTimeout=<délai d'expiration en secondes>. Si la durée d'ouverture de session est supérieure à environ 4 minutes, les utilisateurs rencontreront également des problèmes d'expiration depuis la console MMC Microsoft contenant la console PVS (ces délais d'expiration peuvent être ignorés).

  Ce problème est notamment causé par des domaines inaccessibles dans Active Directory, car un délai de 30 secondes est appliqué à chaque tentative de connexion à un domaine inaccessible. Le délai peut rapidement s'élever à plusieurs minutes si plusieurs domaines sont inaccessibles. En général, les domaines inaccessibles sont créés par l'ajout d'un domaine test ou expérimental à Active Directory, puis sa suppression plus tard. Bien que le domaine soit supprimé, il est toujours signalé par Active Directory lors de l'énumération des domaines ou groupes d'autorisation.

  Les domaines inaccessibles peuvent également être causés par l'arrêt et la déconnexion temporaires d'un contrôleur de domaine du réseau, donc tous les domaines inaccessibles ne doivent être placés sur liste noire.

  Le meilleur moyen de déterminer s'il existe des domaines inaccessibles consiste à examiner la trace CDF du module PVS_DLL_ADSUPPORT et à rechercher les erreurs « Unreachable Domain » et « Server Referral ». Si ces erreurs sont présentes, vérifiez les domaines pour vous assurer qu'ils ne sont plus utilisés et, dans ce cas, ajoutez ces noms de domaine à la liste noire.

  La liste noire est un fichier au format JSON appelé « %ProgramData\Citrix\Provisioning Services\blacklist.json ». Par exemple :

```
1  {
2
3
4  "Domains":
5
```



```
6   [
7
8   "sub.xs.local",
9
10  "sb.xs.local"
11
12  ]
13
14   }
```

Où les deux domaines **sub.xs.local** et **sb.xs.local** seront exclus de l'énumération de domaines et de groupes. Une fois que le fichier est mis à jour, vous devez redémarrer le SoapServer et les consoles en cours d'exécution afin de charger les valeurs mises à jour. [LC6249]

Problèmes liés aux machines cibles

- La fonctionnalité de mise à jour automatique de la machine cible Provisioning Services génère le message d'erreur d'application suivant (Event ID: 0) dans l'Observateur d'événements de la cible si la mise à jour n'est pas disponible.
  « No update server found. Stopping client service. » [LC0450]
- Le logiciel de la machine cible ne reconnaît pas le lecteur AppDisk et utilise le lecteur du AppDisk pour l'écriture sur le cache, ce qui peut entraîner des conflits. [LC5409]
- Lorsque vous configurez un vDisk pour utiliser « Write Cache on RAM » et que vous définissez la taille de cache RAM sur 4096 Mo ou 4097 Mo, le démarrage à partir d'une machine virtuelle Hyper-V de deuxième-2 peut entraîner une exception fatale sur les machines cibles, qui affichent un écran bleu. [LC6707]

StoreFront

- Si l'administrateur modifie le paramètre de stratégie de groupe, MaxPasswordAge, le service de domaine par défaut StoreFront ne recharge pas la nouvelle valeur. Dans StoreFront, il est possible qu'un « nombre de jours avant expiration du mot de passe » incorrect s'affiche.

  Remarque : ce problème est résolu, toutefois il faut parfois jusqu'à une heure pour que la nouvelle valeur soit chargée. [DNA-41380]
- Avec StoreFront 3.5 installé, la couleur des dossiers dans la vue Catégories peut ne plus utiliser la couleur personnalisée définie dans la console de gestion StoreFront. La couleur par défaut est utilisée. [LC5001]

- StoreFront peut se fermer de manière inattendue lors de la gestion de sites Citrix Receiver pour Web. Le problème se produit lorsque le fichier style.css est personnalisé pour Citrix Receiver pour Web. [LC5589]
- L'activation du Service d'authentification fédérée sur StoreFront peut entraîner des erreurs d'ouverture de session. [LC5708]
- Même si Citrix Receiver pour HTML5 est activé dans Citrix StoreFront, la console StoreFront peut s'afficher « Non utilisé » au lieu d'afficher la version HTML. [LC6626]
- Lorsque vous sélectionnez un site configuré lors de la configuration de XenDesktop, il se peut qu'un magasin par défaut qui utilise le service d'authentification par défaut soit créé dans StoreFront. Si vous supprimez ce magasin, les utilisateurs de Citrix Receiver pour Windows ne peuvent pas ajouter d'autres magasins et le message d'erreur suivant peut s'afficher :

  « Une erreur de protocole s'est produite lors de la communication avec le service d'authentification ». [LC6664]
- Si vous configurez la réinitialisation en libre-service des mots de passe (SSPR) pour un magasin spécifique dans la console StoreFront, la configuration s'applique à tous les magasins et pas seulement au magasin spécifique que vous avez sélectionné. [LC6987]
- Les tentatives de reconnexion à des sessions déconnectées peuvent échouer dans un déploiement d'agrégation multisite. Par conséquent, une seconde instance de la même ressource peut s'afficher. []
- Lorsque l'une des sources d'une application agrégée est désactivée, l'application peut être masquée. []
- Les tentatives de désactivation de l'option « Compte en libre-service » dans StoreFront peuvent ne pas prendre effet, même si l'option apparaît comme désactivée. []
- Les tentatives de suppression d'authentifications partagées de magasins dans StoreFront peuvent entraîner l'affichage du message d'erreur suivant lors de l'enregistrement des modifications :

  « Une erreur s'est produite lors de l'enregistrement de vos modifications. » [LC7781]

Serveur d'impression universelle

Redirection de

- Lorsque vous utilisez Profile Management, les modifications apportées aux imprimantes de serveur d'impression universelle Citrix (ajout, suppression, changement de nom) dans une session sur un serveur peuvent ne pas être correctement reflétées dans les prochaines sessions sur un autre serveur. [LC7645]

Serveur

- Les tentatives d'impression à partir de Microsoft Internet Explorer peuvent échouer avec le message d'erreur suivant lors de l'utilisation du pilote d'impression universel Citrix :

  « Erreur interne. Internet Explorer ne peut pas imprimer ce document. » [LC4735]

- Les tentatives d'impression d'un document peuvent échouer et le message d'erreur suivant s'affiche :

  « Impossible d'imprimer : problème de configuration d'imprimante. » [LC6825]

- Lorsque vous utilisez certaines imprimantes, Microsoft Notepad peut afficher le message « Descripteur non valide » et ne pas parvenir à imprimer. Ce problème se produit si « Utiliser uniquement les pilotes spécifiques au modèle de l'imprimante » est configuré dans la stratégie Citrix « Utilisation du pilote d'impression universelle » et si « Activé avec aucun retour à l'impression distante native de Windows » est configuré dans la stratégie Citrix « Activer le serveur d'impression universelle ». [LC7623]

VDA pour OS de bureau

Redirection de contenu

- La tentative de capture d'images à l'aide de DirectShow échoue, ce qui entraîne la fermeture inattendue de l'application. [LC6667]

HDX Broadcast

- Les périphériques audio HDX peuvent être désactivés de manière aléatoire lorsque vous démarrez une session. [LC5281]

Installation, désinstallation, mise à niveau

- Après la mise à niveau du VDA de la version 5.6.400 à la version 7.9, lorsque le VDA est redémarré, les pilotes miroirs installés par la version précédente peuvent rester. [LC6295]
- Lors de la mise à niveau de VDA version 5.6 vers 7.x, un pilote vidéo d'ancienne génération incorrect peut être installé. [LC6363]
- Lors de l'utilisation de la version 7.12 de Machine Creation Services pour créer des VM, l'installation de XenTools échoue, ce qui empêche l'arrêt correct des VM. [LC6769]
- Certaines classes WMI peuvent être renommées après l'installation de la version 7.12 ou 7.13 du VDA sur une version non anglaise du système d'exploitation Microsoft Windows. [LC7555]

- Certaines classes WMI peuvent être renommées après l'installation de la version 7.12 ou 7.13 du VDA sur une version non anglaise du système d'exploitation Microsoft Windows. [LC7587

Clavier

- Citrix Receiver pour Linux peut ne pas prendre en charge les cartes d'identité espagnoles DNIe. [LC6547]
- Lorsque HDX 3D Pro est activé sur un VDA, les raccourcis « Alt + p » et « Alt + s » peuvent ne pas fonctionner. [LC6826]

Impression

- Lorsque vous essayez d'imprimer plusieurs copies d'un document, il se peut qu'une seule copie s'imprime. Ce problème se produit si « Utiliser uniquement les pilotes spécifiques au modèle de l'imprimante » est configuré dans la stratégie Citrix « Utilisation du pilote d'impression universelle » et si « Activé avec aucun retour à l'impression distante native de Windows » est configuré dans la stratégie Citrix « Activer le serveur d'impression universelle ». [LC6023]
- Citrix Print Manager Service (cpsvc.exe) peut cesser de répondre et se fermer de manière inattendue lorsque de nouveaux utilisateurs ouvrent une session. [LC6933]
- Après la mise à niveau du VDA de la version 7.9 à la version 7.12 ou ultérieure, les tentatives d'impression à partir de Microsoft Internet Explorer en utilisant le pilote d'impression universel Citrix peuvent imprimer uniquement vers le magasin 1 au lieu d'imprimer vers le magasin qui est sélectionné. [LC7463]

Administration de serveur/site

- Les modifications que vous apportez à « Paramètres système avancés » sous « Effets visuels » s'appliquent à la session VDA pour OS de bureau en cours, mais risquent de ne pas être conservés pour les sessions ultérieures. Pour que ces modifications soient conservées, définissez la clé de registre suivante :

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix
  Nom : EnableVisualEffect
  Type : DWORD
  Valeur : 1 [LC8049]

Session/Connexion

- La stratégie Règles de redirection des périphériques USB clients peut ne pas s'appliquer. Le problème se produit lorsque le nombre de caractères saisis par l'utilisateur dans la stratégie dépasse 1002. [LC1144]
- Les tentatives de reconnexion à une session VDA après une interruption du réseau peuvent échouer. Le problème se produit après la mise à niveau de VDA vers la version 7.8. [LC5040]
- Lorsque Framehawk est activé, le bouton de défilement d'une souris peut ne pas effectuer d'action dans une session de VDA XenDesktop 7.8. La correction côté VDA correspondante est disponible dans XenDesktop 7.9. [LC5302]
- Un VDA peut rencontrer une exception fatale de type 0x50 (Page_Fault_In_NonPaged_Area) sur le pilote d'affichage Citrix vdodk.sys. [LC5074]
- Lorsque le AppDisk est connecté à une machine virtuelle qui est exécutée sur une version non anglaise du système d'exploitation Microsoft Windows, une invite « Redémarrer maintenant ou redémarrer plus tard » peut s'afficher. Avec cette correction, l'invite disparaît. [LC5403]
- Après la reconnexion à une session comportant plusieurs moniteurs, les écrans deviennent noirs et les paramètres personnalisés reviennent sur leurs valeurs par défaut. [LC5556]
- Après la mise à niveau d'un VDA à partir de la version 7.6.300 vers la version 7.8, la synchronisation du Presse-papiers peut cesser de fonctionner. [LC5699]
- Lorsque Framehawk est activé, le bouton de défilement d'une souris peut ne pas effectuer d'action dans une session de VDA XenDesktop 7.9. [LC5779]
- Une fois configuré pour les services d'authentification fédérée, un VDA peut cesser d'accepter les connexions, et cesser de répondre à l'écran de bienvenue, jusqu'à ce qu'il soit redémarré. [LC5978]
- Il est possible que Citrix Receiver ne dépasse pas l'étape « Connection Established. Negotiate Capabilities » lors du lancement d'une application. [LC6021]
- Les modifications que vous apportez à « Paramètres système avancés » sous « Effets visuels » s'appliquent à la session VDA en cours, mais risquent de ne pas être conservés pour les sessions ultérieures. Pour que ces modifications soient conservées, vous devez définir la clé de registre suivante :

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix
  Nom : EnableVisualEffect
  Type : DWORD
  Valeur : 0 [LC6163]
- Les tentatives de déconnexion d'une session RemotePC sur un appareil tactile peuvent entraîner un écran noir qui ne peut pas être résolu. [LC6384]

- Citrix Receiver pour Linux peut ne pas prendre en charge les cartes d'identité espagnoles DNIe. [LC6547]
- Lors du verrouillage d'une session Remote PC avec SecureDoc installé sur Windows 10, l'écran de verrouillage s'affiche pendant deux minutes. Durant cette période, vous ne pouvez pas interagir avec la session. [LC6668]
- Lorsque vous vous déconnectez et vous reconnectez à une session Citrix Receiver pour Mac plusieurs fois lors de la lecture, l'audio peut ne pas fonctionner. [LC6678]
- Un lecteur client amovible peut ne pas être renvoyé par le WFAPI SDK sur le VDA pour OS de bureau. [LC6877]
- Un écran gris peut s'afficher lors de l'utilisation d'un mode graphique d'ancienne génération sur un VDA Windows 7 XenDesktop 7.13. [LC7477]
- Lorsque vous basculez des sessions entre plusieurs moniteurs en mode plein écran avec le mode graphique d'ancienne génération activé et sans Desktop Viewer configuré, seul un moniteur peut sembler exécuté la session. [LC7907]

Exceptions système

- Le VDA pour OS de serveur peut rencontrer une exception fatale sur TDICA.sys, affichant un écran bleu. [LC6898]
- Des exceptions fatales peuvent se produire sur les serveurs, qui affichent alors un écran bleu sur vdtw30.dll avec le code d'arrêt 0xc0000006. [LC7608]
- Les VDA peuvent rencontrer une exception fatale, affichant un écran bleu, sous tdica.sys avec un code bugcheck. [LC7632]
- Cette correction résout un problème de mémoire avec le fichier wdica.sys qui peut entraîner la fermeture inattendue de serveurs. [LC7666]

Cartes à puce

- Lors du basculement entre des sessions utilisateur et des sessions de bureau à distance Microsoft, les applications recourant à une carte à puce en cours de session, telles que Microsoft Outlook et Microsoft Word, peuvent ne pas être en mesure d'utiliser les cartes à puce. Par conséquent, différents messages d'erreur peuvent s'afficher. De plus, un test de la prise en charge des cartes à puce en session avec « CertUtil/scinfo » dans une fenêtre de commande peut entraîner le message d'erreur suivant :

  « Le gestionnaire de ressources de la carte à puce Microsoft n'est pas en cours d'exécution. » [LC5839]

- L'authentification unique avec carte à puce peut échouer par intermittence. [LC6147]

Expérience utilisateur

- Si vous ouvrez une feuille de calcul avec plusieurs classeurs dans Excel 2010, la barre des tâches affiche uniquement le classeur le plus récent. [LC5370]
- Seul le coin supérieur gauche de l'écran s'affiche lors de l'utilisation du mode graphique d'ancienne génération sur un VDA XenDesktop 7.11 Windows 7. [LC6532]
- Lors d'une opération d'insertion entre deux feuilles de calcul Microsoft Excel 2010 s'exécutant sur un VDA version 7.9, la fenêtre Excel peut cesser de répondre. [LC7481]

Interface utilisateur

- Lors de l'utilisation du Centre de connexion pour fermer la session depuis une session transparente comportant des données non enregistrées, une fenêtre noire s'affiche avec le message suivant :

  « Les programmes doivent toujours se fermer » avec les deux options « Forcer la fermeture de session » ou « Annuler ». L'option « Annuler » ne fonctionne pas.

  Après l'installation de cette correction, l'option Annuler fonctionne comme prévu. [LC6075]
- Lorsque la stratégie « Affichage automatique du clavier » est activée et que la stratégie « Démarrer un bureau tactile » est interdite, le démarrage d'un bureau publié à partir d'un iPad peut entraîner l'affichage 80 % dans la visionneuse de documents. Lorsque vous fermez certaines applications sur le bureau, la visionneuse de documents peut s'afficher à 100 %. [LC6460]
- Si vous ouvrez une feuille de calcul avec plusieurs classeurs dans Excel 2010, la barre des tâches affiche uniquement le classeur le plus récent. [LC7557]

VDA pour OS de serveur

Redirection de contenu

- La tentative de capture d'images à l'aide de DirectShow échoue, ce qui entraîne la fermeture inattendue de l'application. [LC6667]

Installation, désinstallation, mise à niveau

- Après la mise à niveau de VDA 7.11 pour OS de bureau vers VDA 7.12 pour OS de bureau, le message d'erreur suivant peut s'afficher lors du lancement de certaines applications.

« wfapi.dll est manquant. » [LC6874]

- Certaines classes WMI peuvent être renommées après l'installation de la version 7.12 ou 7.13 du VDA sur une version non anglaise du système d'exploitation Microsoft Windows. [LC7555]
- Certaines classes WMI peuvent être renommées après l'installation de la version 7.12 ou 7.13 du VDA sur une version non anglaise du système d'exploitation Microsoft Windows. [LC7587]

Impression

- Citrix Print Manager se ferme de manière inattendue lors de la tentative de mappage d'une imprimante réseau à l'aide de la commande CreateClientPrinter. [LC4685]
- Lorsque vous essayez d'imprimer plusieurs copies d'un document, il se peut qu'une seule copie s'imprime. Ce problème se produit si « Utiliser uniquement les pilotes spécifiques au modèle de l'imprimante » est configuré dans la stratégie Citrix « Utilisation du pilote d'impression universelle » et si « Activé avec aucun retour à l'impression distante native de Windows » est configuré dans la stratégie Citrix « Activer le serveur d'impression universelle ». [LC6023]
- Citrix Print Manager Service (cpsvc.exe) peut cesser de répondre et se fermer de manière inattendue lorsque de nouveaux utilisateurs ouvrent une session. [LC6933]
- Après la mise à niveau du VDA de la version 7.9 à la version 7.12 ou ultérieure, les tentatives d'impression à partir de Microsoft Internet Explorer en utilisant le pilote d'impression universel Citrix peuvent imprimer uniquement vers le magasin 1 au lieu d'imprimer vers le magasin qui est sélectionné. [LC7463]

Administration de serveur/site

- Si les utilisateurs basculent entre des sessions se trouvant sur des sous-réseaux différents, la liste des imprimantes contient des imprimantes provenant des deux sous-réseaux, plutôt que du sous-réseau auquel les utilisateurs sont actuellement connectés. [LC2308]
- Le message d'erreur suivant peut s'afficher pour les utilisateurs du domaine enfant lors du lancement d'une application via l'Interface Web :

  « Vous ne détenez pas les droits d'accès à cette application publiée. » [LC7566]
- Les modifications que vous apportez à « Paramètres système avancés » sous « Effets visuels » s'appliquent à la session VDA pour OS de bureau en cours, mais risquent de ne pas être conservés pour les sessions ultérieures. Pour que ces modifications soient conservées, définissez la clé de registre suivante :

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix
  Nom : EnableVisualEffect

Type : DWORD
Valeur : 1 [LC8049]

Session/Connexion

- Sur les systèmes avec correctif LC2702 (inclus dans Hotfix Rollup Pack 6), les applications peuvent ne pas s'enregistrer sur les lecteurs clients mappés et générer des fichiers endommagés. [LC3976]
- Le lancement d'un processus avec WinDbg.exe peut échouer lorsque Streaming Profiler ou Offline Plug-in est installé. Ce problème se produit car RadeAPHook accroche le paramètre de HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\<*nom du processus*> et HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\<*nom du processus*>.

  Pour appliquer la modification, créez la clé de registre suivante :

- *Pour Windows 32 bits :*
  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\StreamingHook
  Nom : EnableReadImageFileExecOptionsExclusionList
  Type : Reg_SZ
  Valeur : < *liste d'exécutables à exclure du hooking pour le paramètre Image File Execution Options, séparés par des virgules sans espaces. Par exemple, windbg.exe,application_1.exe.*>
- *Pour applications 32 bits sous Windows 64 bits : *
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\StreamingHook
  Nom : EnableReadImageFileExecOptionsExclusionList
  Type : Reg_SZ
  Valeur : < liste d'exécutables à exclure du hooking pour le paramètre Image File Execution Options, séparés par des virgules sans espaces. Par exemple, windbg.exe,application_1.exe.>

  *[LC4750]
- Lors du démarrage d'une nouvelle session, les tentatives par Citrix Audio Redirection Service de connexion à une session de canal virtuel qui contient des informations non valides risquent d'échouer. [LC5024]
- Lorsque Framehawk est activé, le bouton de défilement d'une souris peut ne pas effectuer d'action dans une session de VDA XenDesktop 7.8. La correction côté VDA correspondante est disponible dans XenDesktop 7.9. [LC5302]
- Après la mise à niveau d'un VDA à partir de la version 7.6.300 vers la version 7.8, la synchronisation du Presse-papiers peut cesser de fonctionner. [LC5699]
- Lorsque Framehawk est activé, le bouton de défilement d'une souris peut ne pas effectuer d'action dans une session de VDA XenDesktop 7.9. [LC5779]

- Une fois configuré pour les services d'authentification fédérée, un VDA peut cesser d'accepter les connexions, et cesser de répondre à l'écran de bienvenue, jusqu'à ce qu'il soit redémarré. [LC5978]
- Les modifications que vous apportez à « Paramètres système avancés » sous « Effets visuels » s'appliquent à la session VDA en cours, mais risquent de ne pas être conservés pour les sessions ultérieures. Pour que ces modifications soient conservées, vous devez définir la clé de registre suivante :

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix
  Nom : EnableVisualEffect
  Type : DWORD
  Valeur : 0[LC6163]
- Le message d'avertissement suivant peut s'afficher dans le journal d'événements système lors du lancement du VDA XenApp 7.6 Long Term Service Release Cumulative Update 2 pour OS de serveur ou les versions précédentes :

  « Une tentative de connexion au service SemsService a échoué avec le code d'erreur 0x2. » [LC6311]
- Une session XenApp non opérationnelle peut être créée lorsqu'une session Bureau à distance reprend une session de console sur un VDA pour OS de serveur. [LC6617]
- Les tentatives de reconnexion à une session peuvent échouer par intermittence. Lorsque cela se produit, l'état des VDA pour OS de serveur affiche « Initialisation ». Le problème se produit lorsque le VDA est enregistré à nouveau avec un Delivery Controller. [LC6647]
- Lors du verrouillage d'une session Remote PC avec SecureDoc installé sur Windows 10, l'écran de verrouillage s'affiche pendant deux minutes. Durant cette période, vous ne pouvez pas interagir avec la session. [LC6668]
- Lorsque vous vous déconnectez et vous reconnectez à une session Citrix Receiver pour Mac plusieurs fois lors de la lecture, l'audio peut ne pas fonctionner. [LC6678]
- Lorsque vous lancez une application publiée sur Microsoft Windows Server 2016, un écran noir peut s'afficher pendant quelques secondes avant que l'application ne devienne visible. [LC7947]

Cartes à puce

- Lors du basculement entre des sessions utilisateur et des sessions de bureau à distance Microsoft, les applications recourant à une carte à puce en cours de session, telles que Microsoft Outlook et Microsoft Word, peuvent ne pas être en mesure d'utiliser les cartes à puce. Par conséquent, différents messages d'erreur peuvent s'afficher. De plus, un test de la prise en charge

des cartes à puce en session avec « CertUtil/scinfo » dans une fenêtre de commande peut entraîner le message d'erreur suivant :

« Le gestionnaire de ressources de la carte à puce Microsoft n'est pas en cours d'exécution. » [LC5839]

Exceptions système

- Le VDA pour OS de serveur peut rencontrer une exception fatale sur TDICA.sys, affichant un écran bleu. [LC6898]
- Des exceptions fatales peuvent se produire sur les serveurs, qui affichent alors un écran bleu sur vdtw30.dll avec le code d'arrêt 0xc0000006. [LC7608]
- Les VDA peuvent rencontrer une exception fatale, affichant un écran bleu, sous tdica.sys avec un code bugcheck. [LC7632]
- Cette correction résout un problème de mémoire avec le fichier wdica.sys qui peut entraîner la fermeture inattendue de serveurs. [LC7666]

Expérience utilisateur

- Si vous ouvrez une feuille de calcul avec plusieurs classeurs dans Excel 2010, la barre des tâches affiche uniquement le classeur le plus récent. [LC5370]
- Lors d'une opération d'insertion entre deux feuilles de calcul Microsoft Excel 2010 s'exécutant sur un VDA version 7.9, la fenêtre Excel peut cesser de répondre. [LC7481]

Interface utilisateur

- Lors de l'utilisation du Centre de connexion pour fermer la session depuis une session transparente comportant des données non enregistrées, une fenêtre noire s'affiche avec le message suivant :

  « Les programmes doivent toujours se fermer » avec les deux options « Forcer la fermeture de session » ou « Annuler ». L'option « Annuler » ne fonctionne pas.

  Après l'installation de cette correction, l'option Annuler fonctionne comme prévu. [LC6075]
- Lorsque la stratégie « Affichage automatique du clavier » est activée et que la stratégie « Démarrer un bureau tactile » est interdite, le démarrage d'un bureau publié à partir d'un iPad peut entraîner l'affichage 80 % dans la visionneuse de documents. Lorsque vous fermez certaines applications sur le bureau, la visionneuse de documents peut s'afficher à 100 %. [LC6460]

- Si vous ouvrez une feuille de calcul avec plusieurs classeurs dans Excel 2010, la barre des tâches affiche uniquement le classeur le plus récent. [LC7557]

Composants de bureau virtuel - Autre

- Le type de session de la session d'application hébergée par une machine virtuelle d'un utilisateur peut passer de « Application » à « Bureau » de façon inattendue. En conséquence, les tentatives de reconnexion à une application échouent. [LC5461]
- Lors du lancement d'un package App-V à l'aide de l'infrastructure Microsoft App-V 5.0 intégrée avec XenDesktop, le package App-V peut ne pas réussir à se synchroniser et l'exception suivante se produit :

  Impossible de démarrer <nom_application> [LC5483]
- Les tentatives de chargement d'une application App-V via le réseau peuvent entraîner le message d'erreur suivant :

  « Index hors plage. Il doit s'agir d'une valeur non négative et inférieure à la taille de la collection. » [LC5828]
- Après la mise à niveau à partir de la version 7.7 de XenApp vers la version 7.8, les tentatives de lancement d'applications App-V peuvent échouer. Le problème se produit lorsque la valeur booléenne « TargetIn » est définie sur « 0 » au lieu de « 1 ». Par ailleurs, la définition manuelle de la valeur peut n'avoir aucun effet. Lorsque vous actualisez l'application, elle peut revenir à la valeur précédente. [LC5861]
- Lorsque vous ajoutez un package App-V qui contient plusieurs applications à Citrix Studio et publiez toutes les applications du package, il se peut que seule la première application démarre dans la session utilisateur. [LC5863]
- L'application App-V peut être lancée uniquement par un seul utilisateur. Les tentatives par un autre utilisateur de démarrer la même application sur le même serveur peuvent échouer. [LC6414]
- Les applications séquencées par App-V peuvent ne pas être contenues dans le package App-V même si elles sont référencées par le package (InTarget = False.). Par conséquent, le lancement de l'application ne s'applique pas à des groupes de connexion dépendants qui sont requis pour que l'application fonctionne correctement. [LC6534]
- Après la mise à niveau de XenApp/XenDesktop 7.11 vers 7.12, les programmes de redémarrage des groupes de mise à disposition existants ne sont pas appliqués. [LC6766]
- Les tentatives de lancement d'applications App-V à partir d'un lecteur mappé peuvent échouer. [LC6961]

- Les tentatives de publication d'applications App-V peuvent échouer.

  [LC7421]

- Les tentatives de création de catalogues de machines peuvent échouer lorsque Microsoft Message Queuing est installé sur l'image principale du VDA et le message d'erreur suivant s'afficher dans Citrix Studio :

  « Image Preparation did not complete. Status 'NotSet » [LC7528]

- Les tentatives de lancement d'applications App-V en mode Administration unique peuvent échouer. Le problème se produit lorsque le nom de l'application contient des caractères spéciaux. [LC7897]

Autres problèmes résolus

- Les stratégies de groupe dans Citrix Studio sont manquantes si la stratégie UPM - Software\Microsoft\Speech_OneCore sous Profile Management > Registre > Exclusions par défaut a été configurée avant la mise à niveau des Delivery Controller de 7.11 vers 7.14, de 7.12 vers 7.14, ou de 7.13 vers 7.14. [UPM-538]
- Les tentatives d'installation d'Enregistrement de session version 7.14 (ou de mise à niveau vers cette version) à l'aide du programme d'installation du produit complet de XenApp et XenDesktop échouent sur Windows Server 2008 et le message d'erreur suivant s'affiche : « Queuing Microsoft Message a échoué ». [SRT-1782]
- Après la mise à niveau des Controller, l'état d'alimentation d'un VDA peut indiquer « Inconnu ». [DNA-37756]

Problèmes connus

February 28, 2019

Les problèmes connus décrits dans les sections 7.15, CU1 et CU2 de cet article sont toujours présents dans CU3 à moins qu'ils ne soient inclus dans la liste des problèmes résolus.

Problèmes connus dans la mise à jour cumulative 3

- Pour obtenir une liste des problèmes connus de Citrix liés à la mise à jour Windows du 10 octobre 2018 (v1809), voir l'article du Centre de connaissances CTX234973.

- Dans un environnement AWS, les restaurations de VDA de serveur vers une image ou un instantané XenApp et XenDesktop 7.15 LTSR CU2 peuvent échouer. Pour résoudre ce problème, étendez le délai d'expiration de restauration à une valeur de 30 minutes avec l'applet de commande PowerShell suivante :

  Set-ProvServiceConfigurationData –Name ImageManagemntPrep_preparationTimeout –Value 30 [LCM-4364]

- Après la mise à niveau vers XenApp et XenDesktop 7.15 LTSR CU3, un échec de mise à niveau de site peut se produire lorsque le serveur de licences du site n'est pas mis à jour vers la version qui est publiée dans le cadre de CU3. Le programme d'installation du produit n'affiche pas de notification pendant la mise à niveau. [LCM-5467]

- Après avoir exécuté l'assistant XenDesktop, le catalogue de machines dans Studio est vide et l'adresse IP de streaming s'affiche à la place de l'adresse IP de gestion, ce qui est incorrect. Pour utiliser l'adresse IP de gestion, définissez la clé de registre suivante :

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ProvisioningServices
Nom : UseManagementIpInCatalog
Type : DWORD
Valeur : 1

[LD0125]

Problèmes connus dans la mise à jour cumulative 2

- Sur les VDA Windows 2016, les utilisateurs se connectant avec des cartes à puce peuvent ne pas être en mesure de voir tous les utilisateurs disponibles à la connexion. Le problème est causé par la taille par défaut de la fenêtre d'ouverture de session, qui est 600x520. Pour plus d'informations sur une solution de contournement, consultez l'article CTX204070 du centre de connaissances. [LCM-3951]

- Pour obtenir la liste des problèmes connus avec Windows 10 Redstone 4 (versions Insider Preview), consultez l'article CTX231942 du centre de connaissances.

- Après la mise à niveau de Citrix Studio vers la mise à jour cumulative 2 de la version 7.15, il est possible que les stratégies ne soient pas localisées. Pour plus d'informations, consultez l'article CTX234711 du centre de connaissances. [LC9613]

- Les sessions 7.15 LTSR CU2 peuvent être lancées en tant qu'écran noir. Le problème se produit avec les sessions exécutées sur XenApp et XenDesktop 7.15 LTSR CU2 et les VDA 7.17 lorsque Profile Management est activé. Pour plus d'informations sur une solution de contournement, consultez l'article CTX235100 du centre de connaissances. [LC9648]

Problèmes connus dans la mise à jour cumulative 1

- La console de gestion StoreFront ne s'ouvre pas après une mise à niveau vers StoreFront 3.12.1000 (XenApp et XenDesktop 7.15 LTSR CU1) à partir de StoreFront 3.12 (XenApp et XenDesktop 7.15 LTSR), ou après une installation de StoreFront 3.12.1000. La console de gestion StoreFront affiche l'erreur « MMC n'a pas pu créer le composant logiciel enfichable. Le composant logiciel enfichable n'a peut-être pas été installé correctement. » Pour contourner ce problème, suivez les étapes décrites dans CTX233206. [LC8935]
- Lors de l'installation d'un pilote signé avec un certificat SHA-256 sur une machine Windows 7 ou Windows Server 2008 R2, un message Microsoft WHQL (Windows Hardware Quality Labs) peut apparaître. Pour résoudre le problème, installez les correctifs Microsoft suivants sur la machine :
  - Windows 7 (un correctif) : Correctif Microsoft
  - Windows Server 2008 R2 (deux correctifs) : correctif 1 et correctif 2 [LCM-2836]
- Lorsque le service de télémétrie Citrix est désactivé ou arrêté et que vous utilisez un metainstaller pour mettre à niveau XenApp et XenDesktop 7.15 LTSR vers la mise à jour cumulative 1 (CU1), le message d'avertissement suivant peut s'afficher :
  « Nous ne pouvons pas démarrer le service Citrix qui vous permet de vous inscrire auprès de Call Home. Voir CTX218094 pour obtenir des conseils. » [LCM-3642]
- Profile Management peut entraîner l'affichage d'un écran noir lorsque vous tentez de lancer une session Microsoft Windows 10. Avec cette correction, vous devez configurer la stratégie « Répertoires à synchroniser » et ajouter le dossier « *AppData\Local\Microsoft\Windows\Caches*. » Pour plus d'informations sur une solution de contournement, consultez l'article CTX234144 du centre de connaissances. [LC9030]

Problèmes connus dans 7.15 LTSR (version initiale)

La version 7.15 LTSR de XenApp et de XenDesktop contient les problèmes suivants :

App-V

- Dans Studio, lors de la suppression d'une ou de plusieurs applications App-V à partir du nœud Applications, ou à partir d'un groupe de mise à disposition sélectionné, le message « Une erreur inconnue s'est produite » s'affiche. Vous pouvez ignorer le message ; les applications sont supprimées. [DNA-29702]
- Vous ne pouvez pas supprimer une application App-V d'un groupe de mise à disposition si un processus enfant a été lancé pour cette application, mais n'a pas réussi à se fermer lors de la fermeture de l'application. Le message d'erreur indique que l'application est en cours d'utilisation.

Pour déterminer le nom du processus, exécutez Get-AppVVirtualProcess. Terminez ensuite ce processus avec le Gestionnaire des tâches ou Stop-AppVClientPackage. [DNA-23624]

- Lorsque vous supprimez un package App-V de la bibliothèque d'applications, il est supprimé de l'affichage dans Studio, mais pas dans le VDA. Pour contourner le problème, exécutez les applets de commande suivantes à partir du VDA, avec des privilèges d'administrateur élevés :

  Import-Module AppvClient
  Get-AppVClientPackage -all
  #Identifie les PackageId et VersionId du package à supprimer
  Remove-AppVClientPackage -PackageId <*packageid*> -VersionId <*versionid*> [DNA-47379]

- En raison du comportement de Microsoft App-V, lorsque vous publiez plusieurs versions séquencées de la même application à l'aide de l'administrateur unique ou de la gestion double admin, une seule version de l'application peut être lancée à la fois par utilisateur sur le VDA. Quelle que soit la version qu'un utilisateur lance en premier, celle-ci détermine la version qui sera exécutée par la suite pour lui. Le même comportement se produit même lorsque les composants Citrix ne sont pas impliqués et l'utilisateur démarre les applications séquencées à partir de raccourcis de bureau qui pointent vers des chemins différents. À ce jour, nous (Citrix) avons observé ce comportement pour différentes versions des navigateurs Mozilla Firefox et Google Chrome. [APPV-60]

Citrix Director

- Dans un environnement comportant plusieurs sessions, lorsque vous accédez à **Filtres** > **Sessions** > **Tous** et que vous fermez une session, la session se ferme. Lorsque vous sélectionnez une autre session avec le même nom d'utilisateur pour la deuxième fois et que vous essayez de fermer la session, ce message d'erreur s'affiche :

  La source de données ne répond pas ou a signalé une erreur. Consultez les journaux d'événements du serveur Director pour plus d'informations. [LC8826]

Installation et mise à niveau

- Lorsque vous mettez à niveau VDA 7.14 vers VDA 7.15, les clés créées sous la clé de registre HKEY_LOCAL_MACHINE\Software\Policies\Citrix pour les paramètres de stratégie Citrix qui sont appliqués à l'aide du **modèle d'administration** peuvent être supprimées du VDA. [LCM-3876]
- Lors de l'installation des composants à l'aide de l'application Sélection automatique sur le support d'installation, le fichier autorun.log peut contenir des erreurs et des exceptions concernant les droits nécessaires. Si l'installation s'effectue avec succès, vous pouvez ignorer

ces erreurs. Toutefois, pour les éviter, lancez la sélection automatique avec **Exécuter en tant qu'administrateur**. [DNA-45937]

- Lors de la mise à niveau d'un déploiement XenDesktop 5.6 vers XenDesktop 7.15 LTSR, la stratégie de groupe est manquante. Pour contourner le problème, commencez par mettre à niveau XenDesktop 5.6 vers XenDesktop 7.13. Effectuez ensuite une mise à niveau de 7.13 vers 7.15 LTSR [DNA-44818]
- Lorsque vous installez un Controller et que vous sélectionnez **Je veux me connecter à Smart Tools et Call Home (recommandé)** sur la page **Smart Tools** de l'Assistant d'installation, Call Home peut ne pas être activé. Pour contourner le problème, utilisez la fonctionnalité de planification dans Citrix Scout ou activez [Call Home à l'aide de PowerShell].(/fr-fr/xenapp-and-xendesktop/7-15-ltsr/manage-deployment/cis.html) [CAM-9907]
- Lorsque vous installez un Delivery Controller sur Windows Server 2012 R2 ou Windows Server 2016, si vous choisissez de vous connecter à Smart Tools et que plusieurs organisations sont liées à votre compte Citrix Cloud, le processus d'ouverture de session peut ne pas se terminer une fois que vous avez saisi vos informations d'identification Citrix Cloud. Pour contourner le problème, effectuez l'une des opérations suivantes :
  - Assurez-vous que le serveur Windows et Internet Explorer ont été mis à jour.
  - Désactivez l'option de navigateur Internet Explorer : Options Internet > Sécurité > Intranet local > Sites > Inclure tous les sites qui n'utilisent pas de serveur proxy. [CAM-9816]
- Si StoreFront a été installé initialement à l'aide de l'exécutable du support d'installation, StoreFront ne s'affiche pas comme éligible pour la mise à niveau lorsque vous utilisez le programme d'installation du produit complet pour une version plus récente. Pour contourner le problème, mettez à niveau StoreFront à l'aide de l'exécutable du support d'installation. [DNA-47816]
- Lors de la mise à niveau du Delivery Controller d'une version antérieure à 7.13 vers la version 7.13 et versions ultérieures, une erreur (exception) peut se produire si le paramètre « Délai de reconnexion automatique des clients » est configuré dans une des stratégies. Cette erreur se produit si la valeur du paramètre « Délai de reconnexion automatique des clients » est en dehors de la plage autorisée de 0 à 300, qui a été introduite dans la version 7.13. Pour éviter cette erreur, utilisez le fournisseur PowerShell de stratégie de groupe Citrix pour annuler la configuration du paramètre, ou pour définir une valeur comprise dans la plage spécifiée. Pour un exemple, consultez l'article CTX22947. [DNA-52476]
- Lorsque vous sélectionnez des machines pour les ajouter à des groupes de mise à disposition existants, Studio vous permet d'ajouter des machines à partir de catalogues de machines incompatibles au même groupe de mise à disposition. (Si vous sélectionnez d'abord un groupe de mise à disposition avant de lui ajouter des machines, Studio empêche l'ajout de machines à partir de catalogues de machines incompatibles.) [DNA-39589]

Général

- Lorsque vous utilisez un certificat dans la session du Service d'authentification fédérée pour authentifier une connexion TLS 1.1 (ou version antérieure), la connexion peut échouer. L'ID d'événement 305 est consigné, indiquant un ID de hachage non pris en charge. Le Service d'authentification fédérée ne prend pas en charge le hachage SHAMD5. Pour contourner ce problème, utilisez les connexions TLS 1.2. Ce problème affecte XenApp et XenDesktop 7.9 jusqu'à cette version. [DNA-47628]
- Les paramètres de stratégie ne sont pas enregistrés dans la stratégie Mappage et compatibilité du pilote d'imprimante. Pour contourner ce problème, utilisez le fournisseur PowerShell de stratégie de groupe Citrix pour modifier ce paramètre. Pour plus d'informations sur cette solution, consultez CTX226589. [DNA-47423]
- Erreur de journal d'événements Windows : « Windows ne peut pas vérifier l'intégrité d'image du fichier MfApHook64.dll ». Pour plus d'informations, consultez CTX226397. [HDX-9063]
- Lorsque vous démarrez une application à partir de StoreFront, l'application risque de ne pas démarrer au premier plan ou l'application est au premier plan, mais n'a pas le focus. Pour contourner ce problème, cliquez sur l'icône dans la barre des tâches pour mettre l'application en premier plan ou dans l'écran de l'application pour lui donner le focus. [HDX-10126]
- Le contenu publié ne démarrera pas correctement lorsqu'il est lancé depuis Citrix Receiver. Le contenu lancé via le client web StoreFront (ou l'Interface Web) se lance comme prévu. [LC6316, RFWIN-4957]
- Lorsque vous supprimez un catalogue de machines Azure Resource Manager, les machines et les groupes de ressources associés sont supprimés d'Azure, même si vous indiquez qu'ils doivent être conservés. [DNA-37964]
- La multidiffusion peut ne pas afficher les vidéos lors de l'utilisation d'une version de Citrix Receiver pour Windows plus récente que la version 4.6. L'audio est toujours disponible. Pour contourner ce problème, ajoutez cette clé de Registre sur le point de terminaison :

HKEY_CURRENT_USER\Software\Citrix\HdxMediaStream\
Nom : DisableVMRSupport
Type : DWORD
Valeur : 4 [HDX-10055]

Impression

- L'arrêt ou le redémarrage de Citrix Print Manager Service peut entraîner le blocage du processus CpSvc.exe. Pour contourner ce problème, arrêtez le processus CpsSvc.exe avant d'arrêter ou de

redémarrer le service dans le composant logiciel enfichable Services, ou redémarrez le VDA pour éviter ce problème. [HDX-10071]

- Les imprimantes du serveur d'impression universelle sélectionnées dans le bureau virtuel n'apparaissent pas dans la fenêtre **Périphériques et imprimantes** du Panneau de configuration Windows. Toutefois, lorsque les utilisateurs travaillent dans les applications, ils peuvent imprimer à l'aide de ces imprimantes. Ce problème se produit uniquement sur les plates-formes Windows Server 2012, Windows 10 et Windows 8. Pour obtenir davantage d'informations, veuillez consulter l'article CTX213540 du centre de connaissances. [335153]

Enregistrement de session

- Lorsque Machine Creation Services (MCS) ou Provisioning Services (PVS) crée plusieurs VDA avec une image principale configurée et Microsoft Message Queuing (MSMQ) installé, ces VDA peuvent disposer de la même QMId dans certaines conditions. Cela peut entraîner différents problèmes, tels que :
  - Les sessions peuvent ne pas être enregistrées, même si l'accord d'enregistrement est accepté.
  - Le serveur d'enregistrement de session peut ne pas pouvoir recevoir les signaux de fermeture de session, par conséquent l'état des sessions peut être toujours Actif.

Consultez les articles d'installation de l'enregistrement de session pour trouver une solution. [528678]

Problèmes tiers

- Citrix et Microsoft ont identifié un problème lors du démarrage d'applications transparentes à partir d'un VDA de serveur exécutant Windows Server 2016. Lorsqu'un utilisateur démarre une application publiée à partir de ce VDA, Citrix Receiver affiche un écran noir couvrant l'espace de travail du moniteur pendant quelques secondes avant de démarrer l'application. Pour plus d'informations, voir CTX225819.

  Avertissement : si vous utilisez Azure Active Directory (AAD), ne modifiez pas le Registre comme décrit dans l'article CTX225819. Cette modification peut entraîner l'échec du lancement de sessions pour les utilisateurs AAD. [HDX-5000]

- Dans un environnement de test intensif, sur 20 000 connexions, Microsoft Windows WinLogon.exe peut se bloquer par intermittence avec une fréquence de <0,001 %. [HDX-9938]

Avis de tiers

February 28, 2019

Cette version de XenApp et XenDesktop peut inclure un logiciel tiers distribué sous une licence selon les conditions définies dans les documents suivants :

Citrix Virtual Apps and Desktops - Avis de tiers (Télécharger PDF)

Divulgation de logiciels non commerciaux pour FlexNet Publisher 2016 R1 (11.14.0.0)

Supplément à la documentation FLEXnet Publisher : Licences logicielles Open Source applicables à FlexNet Publisher 11.14.0 (téléchargement PDF)

Notices tierces Enregistrement de session (téléchargement PDF)

Fin de prise en charge

November 5, 2018

Les annonces de cet article visent à vous avertir à l'avance des plates-formes, des produits Citrix et des fonctionnalités qui vont disparaître pour que vous puissiez prendre les décisions appropriées. Citrix surveille l'utilisation des clients et leurs commentaires pour déterminer quand les retirer. Cette liste est susceptible d'être modifiée dans les versions ultérieures et peut ne pas contenir chaque fonctionnalité amenée à disparaître.

Les plates-formes, les produits Citrix et les fonctionnalités ci-dessous sont *obsolètes*. Cela ne signifie pas qu'elles seront supprimées immédiatement. Citrix continue à les prendre en charge dans XenApp et XenDesktop 7.15 Long Term Service Release (LTSR). Les éléments obsolètes seront supprimés dans une version suivante, après cette version LTSR. Nous suggérons des solutions alternatives pour les éléments obsolètes dans la mesure du possible.

Pour obtenir des informations sur la prise en charge du cycle de vie d'un produit, consultez l'article Politique relative au cycle de vie du support produit Citrix.

Élément	Abandon annoncé dans	Solution alternative
Expérience classique Citrix Receiver pour Web (interface utilisateur avec « bulles vertes »).	7.15 LTSR (et StoreFront 3.12)	Expérience unifiée Citrix Receiver pour Web.

Élément	Abandon annoncé dans	Solution alternative
VDA sur Windows 10 version 1511 (seuil 2) et versions antérieures des systèmes d'exploitation de bureau Windows, y compris Windows 8.x et Windows 7	7.15 LTSR (et 7.12)	Installez les VDA avec OS de bureau sur Windows 10 version 1607 (Redstone 1) ou des canaux semi-annuels (ciblés) plus récents. Si vous utilisez 1607 LTSB, nous vous recommandons un VDA 7.15.
VDA sur Windows Server 2008 R2 et Windows Server 2012 (y compris Service Packs).	7.15 LTSR (et 7.12)	Installez les VDA avec OS serveur sur les versions prises en charge, telles que Windows Server 2012 R2 ou Windows Server 2016.
Delivery Controller sur Windows Server 2012 et 2008 R2 (y compris Service Packs).	7.15 LTSR	Installez les Delivery Controller sur un autre système d'exploitation pris en charge
Studio sur Windows 7 (y compris Service Packs).	7.15 LTSR	Installez Studio sur un autre système d'exploitation pris en charge
Redirection Flash.	7.15 LTSR	Utilisez la vidéo HTML5. Pour de plus amples informations, consultez la rubrique Fin de la vie de la redirection Flash Redirection.
DirectX Command Remoting (DCR).	7.15 LTSR	Utilisez Thinwire.

Élément	Abandon annoncé dans	Solution alternative
Intégration de Citrix Online (produit Goto) avec StoreFront.	7.14 (et StoreFront 3.11)	À partir de StoreFront 3.12, cette fonctionnalité ne peut pas être configurée dans la console de gestion StoreFront. Si vous mettez à niveau vers StoreFront 3.12, vous pouvez continuer à utiliser cette fonctionnalité. Pour modifier votre configuration, utilisez l'applet de commande PowerShell, Update-DSGenericApplications. Pour de plus amples informations, consultez Intégrer des applications Citrix Online à des magasins.
Mises à niveau sur place depuis StoreFront 2.0, 2.1, 2.5 et 2.5.2.	7.13	Mettez à niveau à partir d'une de ces versions vers une version ultérieure prise en charge puis vers XenApp et XenDesktop 7.13.
Mises à niveau sur place depuis XenDesktop 5.6 ou 5.6 FP1.	7.12	Migrez votre déploiement XenDesktop 5.6 ou 5.6 FP1 vers la version actuelle de XenDesktop.
VDA sur Windows 8.1 et versions antérieures de bureau Windows.	7.12	Installez les VDA avec OS serveur sur les versions prises en charge, telles que Windows Server 2012 R2 ou Windows Server 2016.
XenDesktop 5.6 utilisé sur Windows XP. Aucune installation de VDA sur Windows XP n'est prise en charge.	7.12	Installez les VDA sur une version de Windows prise en charge.

Élément	Abandon annoncé dans	Solution alternative
Connexions CloudPlatform.	7.12	Utilisez un autre hyperviseur ou service de cloud pris en charge.
Connexions Azure Classic (également appelé Azure Service Management).	7.12	Utilisez le Gestionnaire de ressources Azure.
Installation de composants principaux (autres que Studio) sur des machines 32 bits : Delivery Controller, Director, StoreFront et serveur de licences.	7.12	Utilisez des machines 64 bits.
Location de connexions.	7.12	Utilisez le cache d'hôte local.
Mode Thinwire d'ancienne génération	7.12	Utilisez Thinwire.
Redirection Desktop Composition HDX (DCR)	7.12	

AppDisk et Personal vDisk

La fonctionnalité AppDisks et Personal vDisk disponible dans XenApp et XenDesktop est obsolète dans les versions actuelles*. Citrix remplace cette fonctionnalité par la technologie Unidesk acquise récemment (Citrix App Layering). Durant cette période de transition, Citrix continue à proposer les niveaux de prise en charge actuels décrits dans Options de maintenance de XenApp et XenDesktop.

La fonctionnalité AppDisks et Personal vDisk n'est pas couverte par l'option de maintenance Long Term Service versions (LTSR).

Section 508 Voluntary Product Accessibility Template (VPAT)

November 5, 2018

Modèle VPAT de Director pour Citrix XenApp et XenDesktop 7.15 (téléchargement PDF)

Modèle VPAT d'installation pour Citrix XenApp et XenDesktop 7.15 (téléchargement PDF)

Modèle VPAT de la console Licensing Administration Console pour Citrix XenApp et XenDesktop 7.15 (téléchargement PDF)

Modèle VPAT de Licensing Manager pour Citrix XenApp et XenDesktop 7.15 LTSR (téléchargement PDF)

Modèle VPAT de l'expérience classique de Receiver pour Web pour Citrix XenApp et XenDesktop 7.15 (téléchargement PDF)

Modèle VPAT de l'expérience unifiée de Receiver pour Web pour Citrix XenApp et XenDesktop 7.15 (téléchargement PDF)

Modèle VPAT de StoreFront pour Citrix XenApp et XenDesktop 7.15 (téléchargement PDF)

Modèle VPAT de Studio pour Citrix XenApp et XenDesktop 7.15 (téléchargement PDF)

Modèle VPAT de Boot Device Manager pour Citrix Provisioning Services (téléchargement PDF)

Modèle VPAT de BOOTPTAB Editor pour Citrix Provisioning Services (téléchargement PDF)

Modèle VPA du Client Side Imaging Wizard pour Citrix Provisioning Services (téléchargement PDF)

Modèle VPA du Configuration Wizard pour Citrix Provisioning Services (téléchargement PDF)

Modèle VPA de la console Citrix Provisioning Services (téléchargement PDF)

Modèle VPAT pour VDA Linux (téléchargement PDF)

Modèle VPAT pour Citrix Scout (téléchargement PDF)

Modèle VPAT du Lecteur d'enregistrement de session Citrix (téléchargement PDF)

Modèle VPAT de la console d'autorisation d'enregistrement de session Citrix (téléchargement PDF)

Modèle VPAT de Citrix Workspace Environment Management Administration Console (téléchargement PDF)

Modèle VPAT de Citrix Workspace Environment Management Infrastructure Service

Introduction

La configuration système requise détaillée dans ce document est valide lors de la publication de cette version du produit ; des mises à jour sont apportées régulièrement. La configuration système requise des composants non couverts dans ce document (telles que StoreFront, systèmes hôte, Citrix Receiver et plug-ins, et Provisioning Services) est décrite dans leur documentation respective.

Important : consultez l'article Préparer l'installation avant de procéder à l'installation.

Sauf spécification contraire, le programme d'installation du composant déploie automatiquement les composants logiciels requis (tels que les packs .NET et C++) si les versions requises ne sont pas détectées sur la machine. Le support d'installation Citrix contient également certains de ces logiciels requis.

Le support d'installation contient plusieurs composants tiers. Avant d'utiliser le logiciel Citrix, recherchez des mises à jour de sécurité à partir des composants tiers et installez-les.

Pour obtenir davantage d'informations sur la globalisation, veuillez consulter l'article CTX119253.

Les composants et les fonctionnalités qui peuvent être installés sur des serveurs Windows, ne peuvent pas être installés sur des serveurs Server Core et Nano Server, sauf indication contraire.

Pour les composants et fonctionnalités qui peuvent être utilisés sur les machines Windows 10, les options de maintenance et les éditions de Windows 10 suivantes sont prises en charge :

- Canal semi-annuel (ciblé) : Pro, Entreprise, Éducation, Mobile Entreprise (l'édition IoT Core Pro est uniquement prise en charge pour Citrix Receiver).
- Canal de maintenance à long terme (LTSC) : édition Enterprise LTSB

Pour plus de détails, voir CTX224843.

Configuration matérielle requise

Les valeurs RAM et d'espace disque s'ajoutent à la configuration requise pour l'image du produit, le système d'exploitation et d'autres logiciels sur la machine. Vos performances peuvent varier en fonction de votre configuration, y compris les fonctionnalités que vous utilisez, ainsi que le nombre d'utilisateurs et d'autres facteurs. Une configuration minimale peut ralentir les performances.

Par exemple, la quantité d'espace disque requise sur le Controller pour la location de connexion (activée par défaut) dépend du nombre d'utilisateurs, d'applications et du mode : 100 000 utilisateurs RDS avec 100 applications récemment utilisées requièrent approximativement 3 Go pour la connexion des baux ; les déploiements comportant un plus grand nombre d'applications peuvent nécessiter plus d'espace. Pour les bureaux VDI dédiés, 40 000 bureaux requièrent au moins 400 à 500 Mo d'espace. Dans tous les cas, Citrix suggère de prévoir plusieurs Go d'espace supplémentaire.

Le tableau suivant présente la configuration minimale requise pour les composants principaux.

Composant	Minimum
Tous les composants principaux sur un serveur, pour évaluation uniquement (ne pas installer sur un déploiement de production)	5 Go de RAM
Tous les composants principaux sur un serveur, pour un déploiement test ou un environnement de production de petite taille	12 Go de RAM
Delivery Controller (espace disque supplémentaire requis pour le cache d'hôte local)	5 Go de RAM, 800 Mo de disque dur, base de données : voir Recommandations sur le dimensionnement
Studio	1 Go de RAM, 100 Mo de disque dur
Director	2 Go de RAM, 200 Mo de disque dur
StoreFront	2 Go de RAM, consultez la documentation StoreFront pour les recommandations de disque
Serveur de licences	2 Go de RAM, consultez la documentation relative au système de licences pour les recommandations de disque

Dimensionnement des VM qui mettent à disposition les bureaux et les applications

Nous ne pouvons pas fournir de recommandations en raison de la nature complexe et dynamique du matériel et chaque déploiement XenApp et XenDesktop a des exigences différentes. En général, le dimensionnement d'une VM de XenApp est basé sur le matériel et non pas sur les charges de travail de l'utilisateur (à l'exception de la RAM, vous aurez besoin de RAM supplémentaire pour les applications qui consomment davantage). Le Guide et meilleures pratiques Citrix VDI contient les dernières recommandations sur le dimensionnement des VDA.

Versions Microsoft Visual C++ Runtime

L'installation de Microsoft Visual C++ 2017 Runtime sur une machine sur laquelle Microsoft Visual C++ 2015 Runtime est installé peut entraîner la suppression automatique de Visual C++ 2015 Runtime. Il s'agit là d'un comportement normal.

Si vous avez déjà installé des composants Citrix qui installent automatiquement Visual C++ 2015 Runtime, ces composants continueront à fonctionner correctement avec la version Visual C++ 2017.

Pour plus d'informations, veuillez consulter l'article Microsoft https://developercommunity.visualstudio.com/content/problem/332815/visual-c-redistributable-2017-install-removes-visu.html.

Delivery Controller

Systèmes d'exploitation pris en charge :

- Windows Server 2016, édition Standard et Datacenter
- Windows Server 2012 R2, édition Standard et Datacenter.
- Windows Server 2012, édition Standard et Datacenter.
- Windows Server 2008 R2 SP1, éditions Standard, Entreprise et Datacenter.

Exigences :

- Microsoft .NET Framework 3.5.1 (Windows Server 2008 R2 uniquement).
- Microsoft .NET Framework 4.5.2 (4.6 à 4.7 sont également pris en charge).
- Windows PowerShell 3.0 ou version ultérieure.
- Microsoft Visual C++ 2015 Runtime, 32 et 64 bits.

Bases de données

Les versions de Microsoft SQL Server prises en charge pour les bases de données de configuration de site, de journalisation de la configuration et de surveillance :

- SQL Server 2017, éditions Express, Standard et Entreprise.
- SQL Server 2016 SP1 et SP2 : éditions Express, Standard et Entreprise.
- SQL Server 2014 SP1 à SP3, éditions Express, Standard et Entreprise. Par défaut, SQL Server 2014 SP2 Express est installé lors de l'installation du Controller, si une installation de SQL Server prise en charge existante n'est pas détectée.
- SQL Server 2012 à SP4, éditions Express, Standard et Entreprise.
- SQL Server 2008 R2 SP2 et SP3 : éditions Express, Standard, Entreprise et Datacenter.

Les solutions haute disponibilité de base de données suivantes sont prises en charge (à l'exception de SQL Server Express qui prend uniquement en charge le mode autonome) :

- Instances de cluster de basculement AlwaysOn SQL Server
- Groupes de disponibilité SQL Server AlwaysOn (y compris les groupes de disponibilité de base)
- Mise en miroir de base de données SQL Server

L'authentification Windows est requise pour les connexions entre le Controller et la base de données de site SQL Server.

Lors de l'installation d'un Controller, une base de données SQL Server Express est installée par défaut pour être utilisée avec le cache d'hôte local. Cette installation est différente de l'installation de SQL Server Express par défaut pour la base de données du site.

Pour plus d'informations, consultez les articles suivants :

- Bases de données
- CTX114501
- Recommandations sur le dimensionnement des bases de données
- Cache d'hôte local

Citrix Studio

Systèmes d'exploitation pris en charge :

- Windows 10, voir éditions prises en charge dans la section *Introduction*.
- Windows 8.1, éditions Professionnelle et Entreprise.
- Windows 7 éditions Professionnelle, Entreprise et Intégrale.
- Windows Server 2016, édition Standard et Datacenter
- Windows Server 2012 R2, édition Standard et Datacenter.
- Windows Server 2012, édition Standard et Datacenter.
- Windows Server 2008 R2 SP1, éditions Standard, Entreprise et Datacenter.

Exigences :

- Microsoft .NET Framework 4.5.2 (4.6 à 4.7 sont également pris en charge).
- Microsoft Management Console 3.0 (incluse avec tous les systèmes d'exploitation pris en charge).
- Windows PowerShell 2.0

Citrix Director

Systèmes d'exploitation pris en charge :

- Windows Server 2016, édition Standard et Datacenter
- Windows Server 2012 R2, édition Standard et Datacenter.
- Windows Server 2012, édition Standard et Datacenter.
- Windows Server 2008 R2 SP1, éditions Standard, Entreprise et Datacenter.

Exigences :

- Microsoft .NET Framework 4.5.2 (4.6 à 4.7 sont également pris en charge).
- Microsoft .NET Framework 3.5 SP1 (Windows Server 2008 R2 uniquement).

- Microsoft Internet Information Services (IIS) 7.0 et ASP.NET 2.0. Assurez-vous que le service de rôle Contenu statique est installé sur le serveur IIS. S'ils ne sont pas déjà installés, vous êtes invité à insérer le support d'installation Windows Server et ils sont installés pour vous.

L'intégration de System Center Operations Manager (SCOM) requiert :

- Windows Server 2012 R2
- System Center 2012 R2 Operations Manager

Navigateurs pris en charge pour l'affichage de Director :

- Internet Explorer 11. (Vous pouvez utiliser Internet Explorer 10 uniquement sur des machines Windows Server 2012 R2). Le mode de compatibilité n'est pas pris en charge pour Internet Explorer. Vous devez utiliser les paramètres de navigateur recommandés pour accéder à Director. Lorsque vous installez Internet Explorer, acceptez la valeur par défaut pour utiliser les paramètres de sécurité et de compatibilité recommandés. Si vous avez déjà installé le navigateur et que vous avez choisi de ne pas utiliser les paramètres recommandés, rendez-vous dans Outils > Options Internet > Avancé > Réinitialiser et suivez les instructions.
- Microsoft Edge.
- Firefox ESR (version de prise en charge étendue).
- Chrome.

La résolution d'écran optimale recommandée pour afficher Director est 1366 x 1024.

Virtual Delivery Agent (VDA) pour système d'exploitation de bureau

Systèmes d'exploitation pris en charge :

- Windows 10, voir éditions prises en charge dans la section *Introduction*. Les fonctionnalités suivantes ne sont pas prises en charge sur Windows 10 : la redirection de la composition du bureau et le mode graphique d'ancienne génération.
- Windows 8.1, éditions Professionnelle et Entreprise.
- Windows 7 SP1, éditions Professionnelle, Entreprise et Intégrale.

Exigences :

- Microsoft .NET Framework 4.5.2 (4.6 à 4.7 sont également pris en charge).
- Microsoft .NET Framework 3.5.1 (Windows 7 uniquement).
- Microsoft Visual C++ 2013 et 2015 Runtime, 32 et 64 bits

Remote PC Access utilise ce VDA, que vous installez sur les PC de bureau physiques. Ce VDA prend en charge le démarrage sécurisé pour XenDesktop Remote PC Access sur Windows 10.

Plusieurs fonctionnalités d'accélération multimédia (telles que la redirection Windows Media HDX Mediastream) requièrent que Microsoft Media Foundation soit installé sur la machine sur laquelle vous installez le VDA. Si la machine ne possède pas Media Foundation installé, les fonctionnalités

d'accélération multimédia ne seront pas installées et ne fonctionneront pas. Ne supprimez pas Media Foundation de la machine après l'installation du logiciel Citrix ; sinon, les utilisateurs ne pourront pas ouvrir une session sur la machine. Sur la plupart des éditions d'OS de bureau Windows prises en charge, la prise en charge Media Foundation est déjà installée et ne peut pas être supprimée. Toutefois, N éditions n'incluent pas certaines technologies multimédia ; vous pouvez obtenir ce logiciel depuis Microsoft ou un composant tiers. Pour plus d'informations, veuillez consulter la section Préparer l'installation.

Lors de l'installation de VDA, vous pouvez choisir le mode HDX 3D Pro du VDA pour OS de bureau Windows. Ce mode convient tout particulièrement aux applications exploitant DirectX et OpenGL, ainsi qu'aux données multimédia riches telles que la vidéo. Voir la section HDX 3D Pro pour des informations supplémentaires sur la prise en charge.

Pour plus d'informations sur les VDA Linux, consultez les articles Virtual Delivery Agent Linux.

Pour utiliser la fonctionnalité Server VDI, vous pouvez utiliser l'interface de ligne de commande pour l'installation d'un VDA pour OS Windows Desktop sur un système d'exploitation serveur pris en charge. Consultez Server VDI pour plus d'informations.

Virtual Delivery Agent (VDA) pour système d'exploitation de serveur

Systèmes d'exploitation pris en charge :

- Windows Server 2016, édition Standard et Datacenter
- Windows Server 2012 R2, édition Standard et Datacenter.
- Windows Server 2012, édition Standard et Datacenter.
- Windows Server 2008 R2 SP1, éditions Standard, Entreprise et Datacenter.

Le programme d'installation déploie automatiquement la configuration requise, qui est également disponible sur le support d'installation Citrix dans les dossiers Support :

- Microsoft .NET Framework 4.5.2 (4.6 à 4.7 sont également pris en charge).
- Microsoft .NET Framework 3.5.1 (Windows Server 2008 R2 uniquement).
- Microsoft Visual C++ 2013 et 2015 Runtime, 32 et 64 bits

Le programme d'installation installe et active automatiquement les services de rôle des services Bureau à distance, s'ils ne sont pas déjà installés et activés.

Plusieurs fonctionnalités d'accélération multimédia (telles que la redirection Windows Media HDX Mediastream) requièrent que Microsoft Media Foundation soit installé sur la machine sur laquelle vous installez le VDA. Si la machine ne possède pas Media Foundation installé, les fonctionnalités d'accélération multimédia ne seront pas installées et ne fonctionneront pas. Ne supprimez pas Media Foundation de la machine après l'installation du logiciel Citrix ; sinon, les utilisateurs ne pourront pas ouvrir une session sur la machine. Sur la plupart des éditions Windows Server, la fonctionnalité Media

Foundation est installée au travers du Gestionnaire de serveur (pour Windows Server 2012 et ultérieur : ServerMediaFoundation, pour Windows Server 2008 R2 : DesktopExperience). Toutefois, N éditions n'incluent pas certaines technologies multimédia ; vous pouvez obtenir ce logiciel depuis Microsoft ou un composant tiers. Pour plus d'informations, veuillez consulter la section Préparer l'installation.

Si Media Foundation n'est pas présente sur le VDA, ces fonctionnalités multimédias ne fonctionnent pas :

- Redirection Flash
- Redirection Windows Media
- Redirection vidéo HTML5
- Redirection de webcam HDX en temps réel

Pour plus d'informations sur les VDA Linux, consultez les articles Virtual Delivery Agent Linux .

Hôtes et ressources de virtualisation

Certaines des fonctionnalités de XenApp et XenDesktop peuvent ne pas être prises en charge sur toutes les plates-formes hôte ou toutes les versions de plate-forme. Par exemple, les AppDisks sont pris en charge avec les hôtes XenServer, VMware et System Center Virtual Machine Manager. Pour de plus amples informations, consultez la documentation relative aux fonctionnalités.

La fonctionnalité Remote PC Access Wake on LAN requiert Microsoft System Center Configuration Manager minimum 2012.

IMPORTANT : les versions *major.minor* suivantes sont prises en charge, y compris les mises à jour de ces versions. L'article CTX131239 contient des informations sur la version la plus récente de l'hyperviseur, ainsi que des liens vers les problèmes connus.

XenServer

- XenServer 7.6
- XenServer 7.5
- XenServer 7.1 LTSR (jusqu'à CU2)

VMware vSphere (vCenter + ESXi)

aucune prise en charge n'est fournie pour l'opération vSphere vCenter Linked Mode.

- VMware vSphere 6.7 (XenApp et XenDesktop 7.15 LTSR CU3 uniquement)
- VMware vSphere 6.5
- VMware vSphere 6.0
- VMware vSphere 5.5

- VMware vSphere 5.1
- VMware vSphere 5.0
- Boîtier VMware vCenter 5.5, 6 et 6.5

System Center Virtual Machine Manager

Comprend toute version d'Hyper-V qui peut s'inscrire auprès des versions prises en charge de System Center Virtual Machine Manager.

- System Center Virtual Machine Manager 2016
- System Center Virtual Machine Manager 2012 R2
- System Center Virtual Machine Manager 2012 SP1
- System Center Virtual Machine Manager 2012

Nutanix Acropolis

- Lors de l'utilisation de PVS : 4.5 (ou versions ultérieures prises en charge)
- Lors de l'utilisation de MCS : 4.6.1 (ou versions ultérieures prises en charge ; voir CTX202032)

services Web Amazon (AWS)

- Vous pouvez configurer des applications et des bureaux sur les systèmes d'exploitation Windows pris en charge.
- Consultez la section Citrix XenDesktop sur AWS pour des informations supplémentaires.

CloudPlatform

- La version minimale prise en charge est 4.2.1 avec des corrections à chaud 4.2.1-4
- Les déploiements ont été testés à l'aide de XenServer 6.2 (avec Service Pack 1 et correction à chaud XS62ESP1003) et hyperviseurs vSphere 5.1
- CloudPlatform ne prend pas en charge les hyperviseurs Hyper-V.
- CloudPlatform 4.3.0.1 prend en charge VMware vSphere 5.5.
- Consultez la documentation de CloudPlatform (y compris les notes de publication pour votre version CloudPlatform) pour des informations supplémentaires.

Microsoft Azure

Microsoft Azure Resource Manager

Niveaux fonctionnels Active Directory

Les niveaux fonctionnels de la forêt et du domaine Active Directory sont pris en charge :

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003
- Windows 2000 natif (non pris en charge pour les contrôleurs de domaine)

HDX

L'audio UDP pour Multi-Stream ICA est pris en charge sur Receiver pour Windows et Citrix Receiver pour Linux 13.

L'annulation de l'écho est prise en charge sur Citrix Receiver pour Windows.

Consultez la prise en charge et la configuration requise pour chaque fonctionnalité HDX spécifique ci-dessous.

Redirection Desktop Composition HDX

La machine utilisateur ou le client léger Windows doit prendre en charge ou contenir :

- DirectX 9
- Pixel Shader 2.0 (pris en charge dans le matériel)
- 32 bits par pixel
- Processeur 1,5 GHz 32 bits ou 64 bits
- 1 Go de RAM
- 128 Mo de mémoire vidéo sur la carte graphique ou sur le processeur graphique intégré

HDX interroge la machine Windows pour vérifier qu'elle possède des capacités GPU et retourne automatiquement à la composition de bureau côté serveur si ce n'est pas le cas. Répertoriez les machines Windows avec les capacités de processeur graphique requise, qui ne répondent pas aux spécifications de vitesse de processeur ou de mémoire vive (RAM) doivent être répertoriées dans le groupe de l'objet de stratégie de groupe pour les appareils exclus de la Redirection Desktop Composition.

La valeur minimale de bande passante disponible est de 1,5 Mbps, la bande passante recommandée est de 5 Mbps. Ces valeurs intègrent la latence de bout en bout.

Mise à disposition Windows Media HDX

Les clients suivants sont pris en charge pour la récupération de contenu côté client Windows Media, la redirection Windows Media, le transcodage multimédia en temps réel de Windows Media : Citrix Receiver pour Windows, Citrix Receiver pour iOS et Citrix Receiver pour Linux.

Pour utiliser la récupération de contenu côté client Windows Media sur des machines Windows 8, définissez Citrix Multimedia Redirector comme programme par défaut : dans **Panneau de configuration > Programmes > Programmes par défaut > Choisir les programmes par défaut**, sélectionnez **Citrix Multimedia Redirector** et cliquez sur **Définir ce programme comme programme par défaut** ou **Choisir les paramètres par défaut pour ce programme**. Un transcodage GPU requiert un processeur graphique compatible NVIDIA CUDA avec Compute Capability 1.1 ou version ultérieure ; voir https://developer.nvidia.com/cuda/cuda-gpus.

Redirection HDX Flash

Les clients et les lecteurs Adobe Flash suivants sont pris en charge :

- Citrix Receiver pour Windows (pour les fonctionnalités de redirection Flash de deuxième génération) : les fonctionnalités de redirection Flash de deuxième génération nécessitent Adobe Flash Player pour d'autres navigateurs, parfois appelé NPAPI (Netscape Plugin Application Programming Interface) de Flash Player.
- Citrix Receiver pour Linux (pour les fonctionnalités de redirection Flash de deuxième génération) : les fonctionnalités de redirection Flash de deuxième génération nécessitent Adobe Flash Player pour Linux ou Adobe Flash Player pour Ubuntu.
- Citrix Online Plug-in 12.1 (pour les fonctionnalités de redirection Flash d'ancienne génération) : les fonctionnalités de redirection Flash d'ancienne génération nécessitent Adobe Flash Player pour Windows Internet Explorer (parfois appelé lecteur ActiveX).

le numéro de version majeur du lecteur Flash Player sur la machine utilisateur doit être supérieur ou égal au numéro de version majeur du lecteur Flash Player sur le serveur. Si une version antérieure de Flash Player est installée sur la machine utilisateur, ou si le lecteur Flash Player ne peut pas être installé sur la machine utilisateur, le contenu Flash est restitué sur le serveur.

Les machines exécutant VDA requièrent :

- Adobe Flash Player pour Windows Internet Explorer (le lecteur ActiveX) ;
- Internet Explorer 11 (en mode UI non-moderne). Vous pouvez utiliser Internet Explorer versions 7-10, mais Microsoft prend en charge la version 11 (et Citrix vous recommande d'utiliser cette

version). la redirection Flash requiert Internet Explorer sur le serveur ; avec d'autres navigateurs, le contenu Flash est restitué sur le serveur.
- Le mode protégé désactivé dans Internet Explorer (Outils > Options Internet > onglet Sécurité > case à cocher Activer le mode protégé désactivée). Redémarrez Internet Explorer pour appliquer la modification.

HDX 3D Pro

Si vous installez un VDA pour OS de bureau Windows, vous pouvez choisir d'installer la version HDX 3D Pro.

La machine physique ou virtuelle qui héberge l'application peut utiliser la fonctionnalité GPU Passthrough de traitement graphique (GPU) ou virtuel (vGPU) :

- La fonctionnalité GPU Passthrough est disponible avec Citrix XenServer, Nutanix AHV, VMware vSphere et VMware ESX, où elle est appelée accélération graphique virtuelle (vDGA), et avec Microsoft Hyper-V dans Windows Server 2016 où elle est appelée Discrete Device Assignment (DDA).
- vGPU est disponible avec Citrix XenServer, Nutanix AHV et VMware vSphere ; voir https://www.citrix.com/products/xenapp-xendesktop/hdx-3d-pro.html.

Citrix recommande que l'ordinateur hôte dispose au minimum de 4 Go de mémoire vive et d'une UC à quadruple cœur offrant une vitesse d'horloge de 2,3 GHz ou plus.

Unité de traitement graphique (GPU) :

- Pour la compression basée sur l'UC, y compris la compression sans perte, HDX 3D Pro prend en charge toute carte vidéo sur l'ordinateur hôte compatible avec l'application que vous mettez à disposition.
- Pour l'accélération graphique virtuelle à l'aide de NVIDIA GRID API, HDX 3D Pro peut être utilisé avec des cartes NVIDIA prises en charge (voir NVIDIA GRID). Le NVIDIA GRID offre une haute fréquence d'images, ce qui entraîne une expérience utilisateur hautement interactive.
- L'accélération graphique virtuelle est prise en charge sur les processeurs Intel Xeon de la famille E3 pour les graphiques de centre de données. Pour plus d'informations, veuillez consulter https://www.citrix.com/intel et https://www.intel.com/content/www/us/en/servers/data-center-graphics.html.
- L'accélération graphique virtuelle est prise en charge avec AMD RapidFire sur les cartes pour serveur AMD FirePro S-series (voir la section Solution de virtualisation AMD).

Machine utilisateur :

- HDX 3D Pro prend en charge toutes les résolutions de moniteur prises en charge par le processeur graphique de l'ordinateur hôte. Toutefois, pour des performances optimales avec les spécifications minimales recommandées pour la machine utilisateur et le processeur

graphique, Citrix recommande de ne pas dépasser, sur la machine utilisateur, la résolution de 1920 x 1200 pixels pour les connexions en réseau local et de 1280 x 1024 pixels pour les connexions en réseau étendu.

- Citrix recommande qu'au minimum, les machines utilisateur disposent de 1 Go de mémoire vive et d'une UC avec une vitesse d'horloge de 1,6 GHz ou plus. L'utilisation du codec de compression profonde par défaut, qui est requis sur les connexions à faible bande passante, requiert un processeur plus puissant à moins que le décodage ne soit effectué dans le matériel. Pour des performances optimales, Citrix recommande que les machines utilisateur soient équipées de 2 Go de mémoire vive et d'un processeur double cœur offrant une vitesse d'horloge de 3 GHz ou plus.
- Pour accéder à plusieurs moniteurs, Citrix recommande que les machines utilisateur soient équipées d'UC quadruple cœur.
- Les machines utilisateur n'ont pas besoin d'un processeur graphique pour accéder aux bureaux ou aux applications mises à disposition avec HDX 3D Pro.
- Citrix Receiver doit être installé.

Pour de plus amples informations, consultez les articles HDX 3D Pro et www.citrix.com/xenapp/3d.

Configuration requise pour les conférences vidéo pour la compression vidéo de webcam HDX

Clients pris en charge : Citrix Receiver pour Windows, Citrix Receiver pour Mac et Citrix Receiver pour Linux.

Applications de visioconférence prises en charge :

- Adobe Connect
- Cisco WebEx
- Citrix GoToMeeting HD Faces
- Google+ Hangouts
- IBM Sametime
- Applications vidéo Media Foundation sur Windows 8.x, Windows Server 2012 et Windows Server 2012 R2
- Microsoft Lync 2010 et 2013
- Microsoft Office Communicator
- Microsoft Skype 6.7

Pour utiliser Skype sur un client Windows, modifiez le registre sur le client et le serveur :

Clé de Registre cliente HKEY_CURRENT_USER\Software\Citrix\HdxRealTime

Nom : DefaultHeight , Type : REG_DWORD, Données : 240

Nom : DefaultWidth, Type : REG_DWORD, Données : 320

Clé de Registre serveur HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Vd3d\Compatibility

Nom : skype.exe, Type : REG_DWORD, Données : défini sur 0

Autres configurations requises pour la machine utilisateur :

- Un matériel approprié pour produire des sons.
- Une webcam compatible DirectShow (utilisez les paramètres par défaut de la webcam). Des webcams avec encodeur matériel réduisent l'utilisation de l'UC du côté client.
- Les pilotes de webcam, obtenus à partir du fournisseur de caméra si possible.

Enregistrement de session

Composants de l'administration d'enregistrement de session

Vous pouvez installer les composants de l'administration d'enregistrement de session (base de données d'enregistrement de session, serveur d'enregistrement de session et console de stratégie d'enregistrement de session) sur un serveur unique où sur des serveurs différents.

Base de données d'enregistrement de session

Systèmes d'exploitation pris en charge :

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 SP1

Versions Microsoft SQL Server prises en charge :

- Microsoft SQL Server 2016 SP1 éditions Enterprise, Express et Standard
- Microsoft SQL Server 2014 SP2 éditions Enterprise, Express et Standard
- Microsoft SQL Server 2012 SP3 éditions Enterprise, Express et Standard
- Microsoft SQL Server 2008 R2 SP3 éditions Enterprise, Express et Standard

Configuration requise : .NET Framework 4.7, 4.6.2 ou 4.5.2

Serveur d'enregistrement de session

Systèmes d'exploitation pris en charge :

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 SP1

Autres éléments requis :

- Internet Information Services (IIS) 10, 8.5, 8.0 ou 7.5
- .NET Framework version 4.7, 4.6.2 ou 4.5.2
- Si le serveur d'enregistrement de session utilise HTTPS comme protocole de communication, ajoutez un certificat valide. L'enregistrement de session utilise HTTPS par défaut, selon les recommandations de Citrix.
- Microsoft Message Queuing (MSMQ), avec intégration Active Directory désactivée et la prise en charge de MSMQ HTTP activée.
- Journalisation de l'administrateur : dernière version de Chrome, Firefox ou Internet Explorer 11.

Console de stratégie d'enregistrement de session

Systèmes d'exploitation pris en charge :

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 SP1

Configuration requise : .NET Framework 4.7, 4.6.2 ou 4.5.2

Agent d'enregistrement de session

L'installation de l'agent d'enregistrement de session s'effectue sur chaque serveur XenApp et XenDesktop pour lequel vous souhaitez enregistrer des sessions.

Systèmes d'exploitation pris en charge :

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 SP1
- Windows 10
- Windows 8.1
- Windows 7 SP1

Exigences :

- XenApp/XenDesktop 7.15 avec licence Platinum
- XenApp/XenDesktop 7.6.4000 avec licence Platinum (VDA pour OS de serveur Windows uniquement ; VDA pour OS de bureau Windows non pris en charge)
- .NET Framework 4.7, 4.6.2 ou 4.5.2

- Microsoft Message Queuing (MSMQ), avec intégration Active Directory désactivée et la prise en charge de MSMQ HTTP activée

Lecteur d'enregistrement de session

Systèmes d'exploitation pris en charge :

- Windows 10
- Windows 8.1
- Windows 7 SP1

Configuration requise : .NET Framework 4.7, 4.6.2 ou 4.5.2

Pour obtenir des résultats optimaux, installez le lecteur d'enregistrement de session sur une station de travail disposant des caractéristiques suivantes :

- Résolution d'écran de 1024 x 768.
- Profondeur de couleur d'au moins 32 bits.
- 2 Go de RAM minimum ; des ressources supplémentaires en RAM et UC/GPU peuvent améliorer les performances lors de la lecture d'enregistrements riches en graphiques ; plus particulièrement si les enregistrements contiennent beaucoup d'animations.

Le délai de réponse de la recherche dépend de la taille de l'enregistrement et des spécifications matérielles de votre ordinateur.

Serveur d'impression universelle

Le serveur d'impression universelle comprend les composants client et serveur. Le composant UpsClient est inclus dans l'installation du VDA. Vous installez le composant UpsServer sur chaque serveur d'impression où les imprimantes partagées résident que vous souhaitez provisionner avec le pilote d'impression universelle Citrix dans les sessions utilisateur.

Le composant UpsServer est pris en charge sur :

- Windows Server 2016
- Windows Server 2012 R2 et 2012.
- Windows Server 2008 R2 SP1

Configuration requise : Microsoft Visual C++ 2013 Runtime, 32 et 64 bits

Pour les VDA pour OS Windows Server, l'authentification de l'utilisateur lors des opérations d'impression nécessite que le Serveur d'impression universelle appartienne au même domaine que le VDA.

Des packs de composants client et serveur autonomes peuvent également être téléchargés.

Pour de plus amples informations, consultez la section Provisionner des imprimantes.

Autre

StoreFront 3.12.2000 est la version minimale prise en charge avec cette version. Pour utiliser la fonctionnalité de préférence de zone, vous devez utiliser StoreFront 3.12.2000 ou version ultérieure et NetScaler Gateway 11.0-65.x au minimum.

Lors de l'utilisation de Provisioning Services avec cette version, la version minimale de Provisioning Services prise en charge est la version 7.15.3.

Le serveur de licences Citrix 11.15 est pris en charge.

La console de gestion des stratégies de groupe de Microsoft (GPMC) est nécessaire si vous stockez les informations de stratégie Citrix dans Active Directory au lieu de la base de données de configuration de site. Si vous installez CitrixGroupPolicyManagement_x64.msi séparément (par exemple, sur une machine sur laquelle n'est pas installé de composant principal XenApp ou XenDesktop), Visual Studio 2015 Runtime doit être installé sur cette machine. Pour plus d'informations, veuillez consulter la documentation Microsoft.

Plusieurs cartes d'interface réseau sont prises en charge.

Par défaut, Citrix Receiver pour Windows est installé lorsque vous installez un VDA. Pour plus d'informations, consultez la documentation Citrix Receiver pour Windows.

Consultez la section App-V pour les versions prises en charge de Microsoft App-V.

Consultez la section Local App Access pour des informations sur les navigateurs pris en charge pour cette fonctionnalité.

Consultez la documentation Réinitialisation en libre-service des mots de passe pour plus d'informations sur la prise en charge et la configuration requise.

Redirection de dossiers clients : systèmes d'exploitation pris en charge :

- Serveur : Windows Server 2008 R2 SP1, Windows Server 2012 et Windows Server 2012 R2
- Client (avec la dernière version de Citrix Receiver pour Windows) : Windows 7, Windows 8 et Windows 8.1

Résolutions mixtes avec plusieurs moniteurs. L'utilisation de différentes résolutions entre les moniteurs n'est pas prise en charge dans les environnements Citrix XenDesktop et XenApp. Vous pouvez vérifier la résolution (% de mise à l'échelle) sous Panneau de configuration de Windows > Affichage. Si vous utilisez une machine cliente Windows 8.1 ou Windows 10, l'activation de l'option **Me laisser choisir un niveau de mise à l'échelle pour tous mes affichages** dans le Panneau de configuration de Windows > Affichage configure les moniteurs de manière appropriée. Pour plus d'informations, veuillez consulter l'article CTX201696.

Cette version de XenApp et XenDesktop n'est pas compatible avec AppDNA 7.8 et AppDNA 7.9. Citrix recommande d'utiliser la version actuelle de AppDNA.

Vue d'ensemble technique

January 23, 2019

XenApp et XenDesktop sont des solutions de virtualisation qui fournissent au personnel informatique un contrôle des machines virtuelles, des applications, des licences et de la sécurité tout en offrant un accès à n'importe quel appareil.

XenApp et XenDesktop permettent :

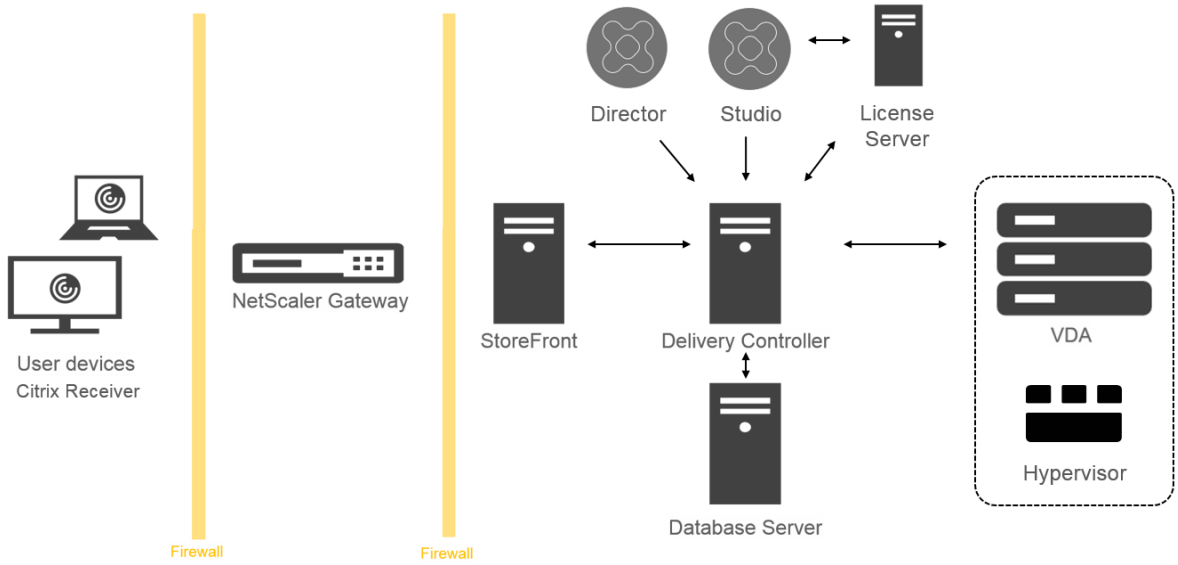
- Aux utilisateurs d'exécuter des applications et des bureaux indépendamment du système d'exploitation et de l'interface de l'appareil.
- Aux administrateurs de gérer le réseau et contrôler l'accès à partir d'appareils sélectionnés ou depuis tous les appareils.
- Aux administrateurs de gérer l'ensemble d'un réseau à partir d'un centre de données unique.

XenApp et XenDesktop partagent une architecture unifiée appelée FlexCast Management Architecture (FMA). Les fonctionnalités clé de FMA comprennent la possibilité d'exécuter plusieurs versions de XenApp ou XenDesktop à partir d'un site unique et un provisioning intégré.

Composants principaux de XenApp et XenDesktop

Cet article est particulièrement utile si vous ne connaissez pas XenApp ou XenDesktop. Si vous disposez actuellement d'une batterie XenApp 6.x ou version antérieure, ou d'un site XenDesktop 5.6 ou version antérieure, consultez également l'article Modifications apportées dans la version 7.x.

Cette illustration affiche les composants principaux d'un déploiement typique, qui est appelé un site.



Delivery Controller :

Delivery Controller est le composant de gestion centralisée d'un site XenApp ou XenDesktop. Chaque site possède un ou plusieurs Delivery Controller. Il est installé sur au moins un serveur dans le centre de données. Pour la fiabilité et la disponibilité du site, installez des Controller sur plusieurs serveurs. Si votre déploiement comprend des machines virtuelles hébergées sur un hyperviseur ou un service de cloud, les services Controller communiquent avec l'hyperviseur pour distribuer des applications et des bureaux, s'authentifier et gérer l'accès des utilisateurs, négocier des connexions entre les utilisateurs et leurs applications et bureaux virtuels, optimiser l'utilisation des connexions et équilibrer la charge de ces connexions.

Le service broker du Controller contrôle quels utilisateurs sont connectés et depuis quel endroit, quelles ressources de session les utilisateurs possèdent-ils et si les utilisateurs doivent se reconnecter aux applications existantes. Le service broker exécute des applets de commande PowerShell et communique avec l'agent broker situé sur les VDA via le port TCP 80. Il n'est pas possible d'utiliser le port TCP 443.

Monitor Service collecte les données historiques et les place dans la base de données de contrôle. Ce service utilise le port TCP 80 ou 443.

Les données provenant des services Controller sont stockées dans la base de données du site.

Le Controller gère l'état des bureaux, les démarre ou les arrête à la demande et en fonction de la configuration de l'administration. Dans certaines éditions, le Controller permet d'installer Profile Management pour gérer les paramètres de personnalisation des utilisateurs dans des environnements Windows physiques ou virtualisés.

Base de données :

Au moins une base de données Microsoft SQL Server est requise pour chaque site XenApp ou XenDesktop pour stocker toutes les informations de configuration et de session. Cette base de données stocke les données collectées et gérés par les services qui constituent le Controller. Installez la base de données dans votre centre de données et assurez-vous qu'elle possède une connexion permanente au Controller. Le site utilise également une base de données de journalisation de la configuration et une base de données de contrôle. Par défaut, ces bases de données sont installées dans le même emplacement que la base de données du site, mais vous pouvez modifier ce paramètre.

Virtual Delivery Agent (VDA) :

Le VDA est installé sur chaque machine physique ou virtuelle de votre site que vous mettez à disposition des utilisateurs. Ces machines fournissent des applications ou des postes de travail. Le VDA permet aux machines de s'enregistrer auprès du Controller, qui permet à la machine et aux ressources qu'elle héberge d'être mise à la disposition des utilisateurs. Les VDA établissent et gèrent la connexion entre la machine et l'appareil de l'utilisateur, vérifient qu'une licence Citrix est disponible pour l'utilisateur ou la session, et appliquent toute stratégie qui a été configurée pour la session.

Le VDA communique des informations de session au service Broker dans le Controller via l'agent Broker dans le VDA. L'agent broker héberge de multiples plug-ins et collecte des données en temps réel.

Il communique avec le Controller sur le port TCP 80.

Le mot « VDA » est souvent utilisé pour faire référence à l'agent ainsi qu'à la machine sur laquelle il est installé.

Les VDA sont disponibles pour les systèmes d'exploitation de serveur et de bureau Windows. Les VDA pour les systèmes d'exploitation de serveur Windows Server autorisent plusieurs utilisateurs à se connecter au serveur à un moment donné. Les VDA pour les systèmes d'exploitation de bureau Windows ne permettent qu'à un seul utilisateur de se connecter au bureau à la fois. Les VDA Linux sont également disponibles.

Citrix StoreFront :

StoreFront authentifie les utilisateurs sur les sites hébergeant les ressources et gère les magasins de bureaux et d'applications auxquels les utilisateurs accèdent. Il peut héberger votre magasin d'applications d'entreprise qui fournit aux utilisateurs un accès en libre-service aux bureaux et aux applications que vous mettez à leur disposition. Il assure également le suivi des abonnements aux applications des utilisateurs, des noms de raccourcis et d'autres données. Cela permet de garantir que les utilisateurs ont une expérience cohérente sur plusieurs appareils.

Citrix Receiver :

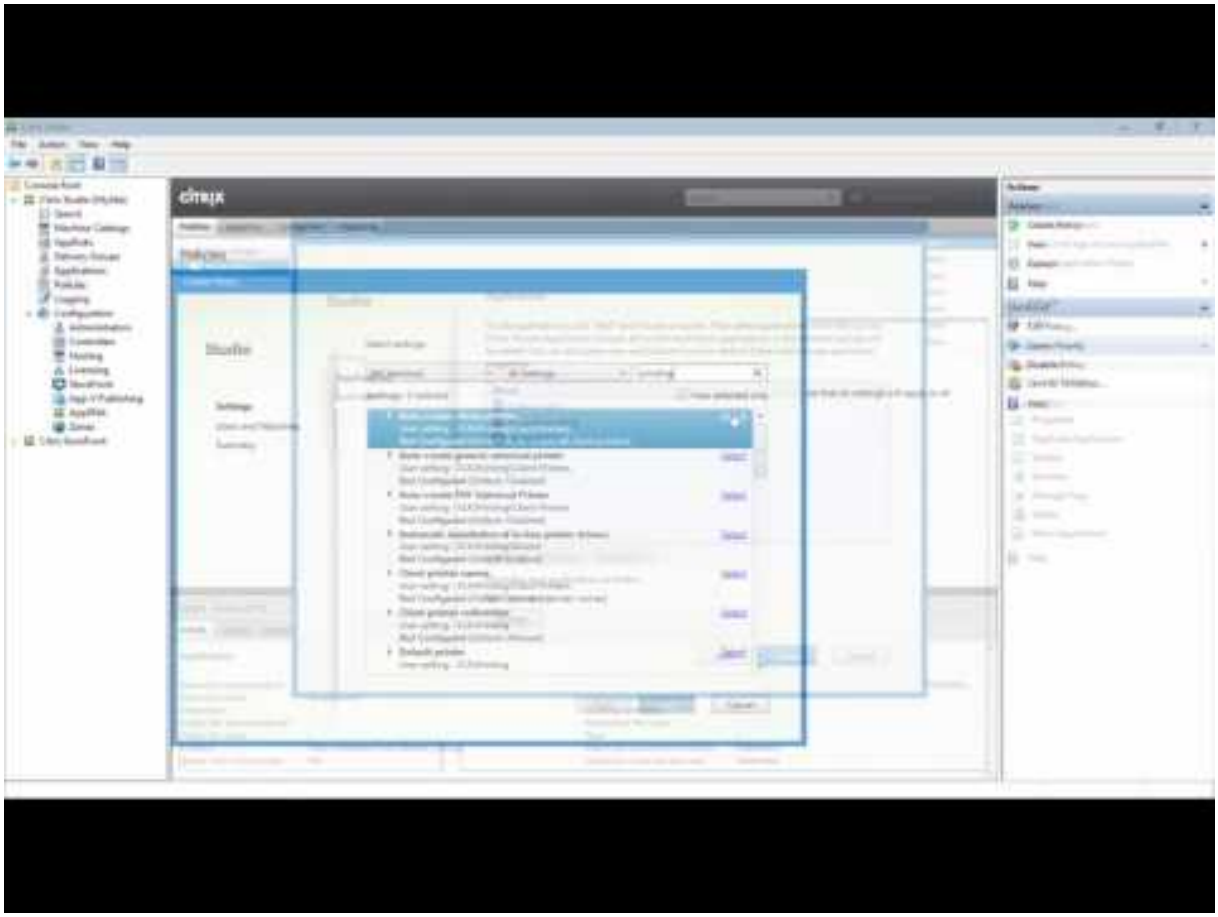
Installé sur les machines utilisateur et autres points de terminaison, tels que les bureaux virtuels, Citrix Receiver offre aux utilisateurs un accès en libre-service, rapide et sécurisé aux documents, applications et bureaux à partir de tout appareil utilisateur, y compris les smartphones, tablettes et PC. Citrix Receiver offre également un accès à la demande aux applications Windows, Web et SaaS (Software as a Service). Pour les périphériques qui ne peuvent pas installer le logiciel Citrix Receiver, Citrix Receiver pour HTML5 offre une connexion via un navigateur Web compatible HTML5.

Citrix Studio :

Studio est la console de gestion qui vous permet de configurer et de gérer votre déploiement XenApp et XenDesktop. Cette console élimine le besoin de consoles de gestion distinctes pour gérer la mise à disposition des applications et des postes de travail. Studio offre des assistants pour vous guider dans le processus de configuration de votre environnement, créer vos charges de travail pour héberger les applications et bureaux, et attribuer des applications et des bureaux aux utilisateurs. Vous pouvez également utiliser Studio pour allouer et suivre les licences Citrix pour votre site.

Studio obtient les informations qu'il affiche à partir du Broker Service dans le Controller, communiquant via le port TCP 80.

Pour plus d'informations, cliquez sur ce graphique :



Citrix Director :

Director est un outil Web qui permet aux équipes d'assistance informatique de surveiller un environnement, de résoudre les problèmes avant qu'ils ne deviennent critiques et de réaliser des tâches d'assistance pour les utilisateurs finaux. Vous pouvez utiliser un déploiement de Director pour vous connecter à et contrôler plusieurs sites XenApp ou XenDesktop.

Director affiche les éléments suivants :

Données de session en temps réel du Broker Service dans le Controller. Cela inclut les données que le service Broker obtient du Broker Agent dans le VDA.

Données de site historiques provenant du service Monitoring dans le Controller.

Données de trafic HDX (également appelé trafic ICA) capturé par HDX Insight depuis NetScaler, si votre déploiement comprend un boîtier NetScaler et votre édition XenApp ou XenDesktop comprend HDX Insight.

Vous pouvez également afficher et interagir avec les sessions d'un utilisateur via Director, à l'aide de l'Assistance à distance Windows.

Serveur de licences Citrix :

Le serveur de licences gère les licences de vos produits Citrix. Il communique avec le Controller pour gérer les licences pour chaque session utilisateur et avec Studio pour allouer les fichiers de licences. Vous devez créer au moins un serveur de licences pour stocker et gérer vos fichiers de licences.

Hyperviseur ou service de cloud :

L'hyperviseur ou le service de cloud héberge les machines virtuelles de votre site. Il peut s'agir des machines virtuelles que vous utilisez pour héberger les applications et les bureaux, ainsi que les machines virtuelles que vous utilisez pour héberger les composants de XenApp et XenDesktop. Un hyperviseur est installé sur un ordinateur hôte entièrement dédié à l'exécution de l'hyperviseur et l'hébergement des machines virtuelles.

XenApp et XenDesktop prennent en charge un grand nombre d'hyperviseurs et de services de cloud.

Bien que de nombreux déploiements XenApp et XenDesktop requièrent un hyperviseur, vous n'en avez pas besoin pour fournir un accès PC distant. De même, un hyperviseur n'est pas requis lorsque vous utilisez Provisioning Services (PVS) pour provisionner des machines virtuelles.

Pour plus d'informations sur :

- les ports, consultez Ports réseau ;
- les bases de données, consultez Bases de données ;
- les services Windows des composants de XenApp et XenDesktop, consultez Configurer les droits des utilisateurs.
- les hyperviseurs et les services de cloud pris en charge, consultez Configuration système requise.

Composants supplémentaires

Les composants supplémentaires suivants, non affichés dans le diagramme ci-dessus, peuvent également être inclus dans les déploiements XenApp ou XenDesktop. Pour de plus amples informations, consultez leur documentation respective.

Provisioning Services (PVS) :

PVS est un composant facultatif, disponible dans certaines éditions. Il offre une alternative à MCS pour le provisioning des machines virtuelles. Alors que MCS permet de créer des copies d'une image principale, PVS livre l'image principale en streaming vers la machine utilisateur. PVS ne nécessite pas d'hyperviseur pour effectuer cette opération, vous pouvez donc l'utiliser pour héberger des machines physiques. PVS communique avec le Controller afin de fournir aux utilisateurs des ressources.

NetScaler Gateway :

Lorsque les utilisateurs se connectent en dehors du pare-feu d'entreprise, XenApp et XenDesktop peuvent utiliser la technologie Citrix NetScaler Gateway (anciennement Access Gateway) pour sécuriser les connexions avec le protocole TLS. Le boîtier virtuel NetScaler Gateway ou NetScaler

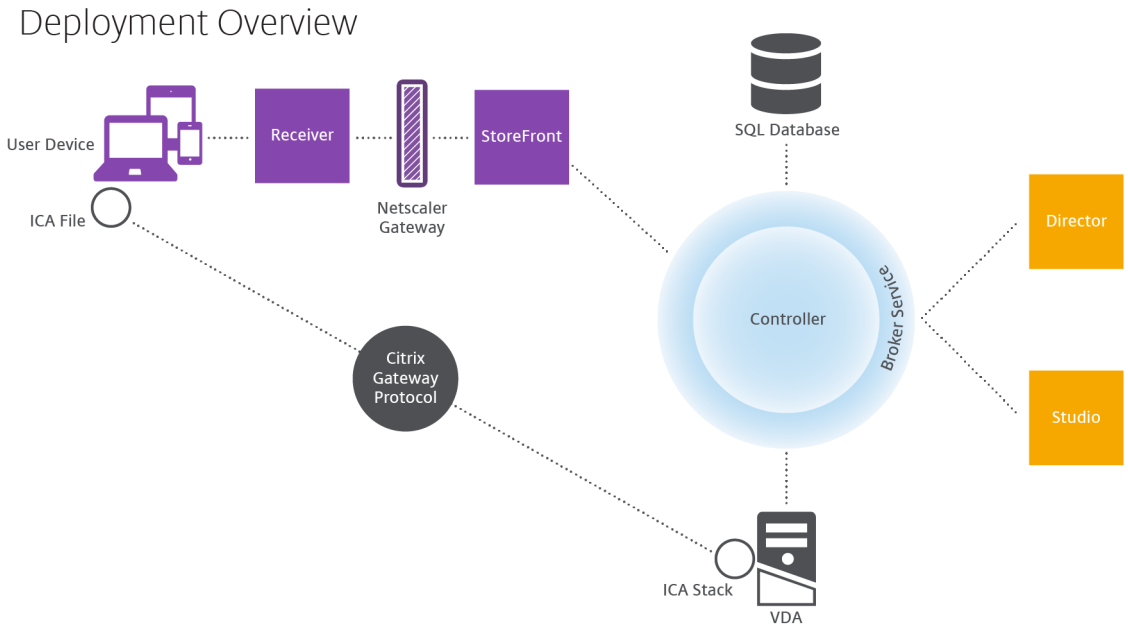
VPX est un boîtier SSL VPN déployé dans la zone démilitarisée (DMZ) pour fournir un point d'accès sécurisé unique via le pare-feu de l'entreprise.

NetScaler SD-WAN :

Dans les déploiements dans lesquels des bureaux virtuels sont mis à disposition auprès des utilisateurs dans des emplacements distants, des succursales par exemple, la technologie Citrix NetScaler SD-WAN peut être utilisée pour optimiser les performances. (Cette technologie était auparavant Citrix CloudBridge, Branch Repeater ou WANScaler.) Les répéteurs accélèrent les performances sur les réseaux étendus. Avec les répéteurs, les utilisateurs des succursales bénéficient des performances d'un réseau local sur le réseau étendu. NetScaler SD-WAN permet de définir des priorités dans l'expérience des utilisateurs. Par exemple pour éviter une dégradation des performances au niveau de la succursale en cas d'envoi de fichiers volumineux ou de tâches d'impression importantes sur le réseau. L'optimisation WAN HDX assure une compression avec système de jetons et déduplication des données, réduisant les besoins en bande passante tout en améliorant les performances.

Comment fonctionnent les déploiements typiques

Un site est composé de machines avec des rôles dédiés qui permettent de garantir une certaine évolutivité, une haute disponibilité, la capacité de basculement, et fournir une solution qui est sécurisé par nature. Un site comprend des serveurs et des machines de bureau installés sur un VDA, ainsi que le Delivery Controller, qui gère l'accès.



Le VDA permet aux utilisateurs de se connecter à des bureaux et des applications. Il est installé sur des machines de serveur ou de bureaux dans le centre de données pour la plupart des méthodes de

mise à disposition, mais il peut également être installé sur des ordinateurs physiques pour Remote PC Access.

Le Controller est constitué de services Windows indépendants qui permettent de gérer les ressources, les applications et les bureaux, et optimiser et équilibrer les connexions utilisateur. Chaque site possède un ou plusieurs Delivery Controller. Étant donné que les sessions sont affectées par la latence, de la bande passante et de fiabilité du réseau, tous les Controller devraient idéalement se trouver sur le même réseau local.

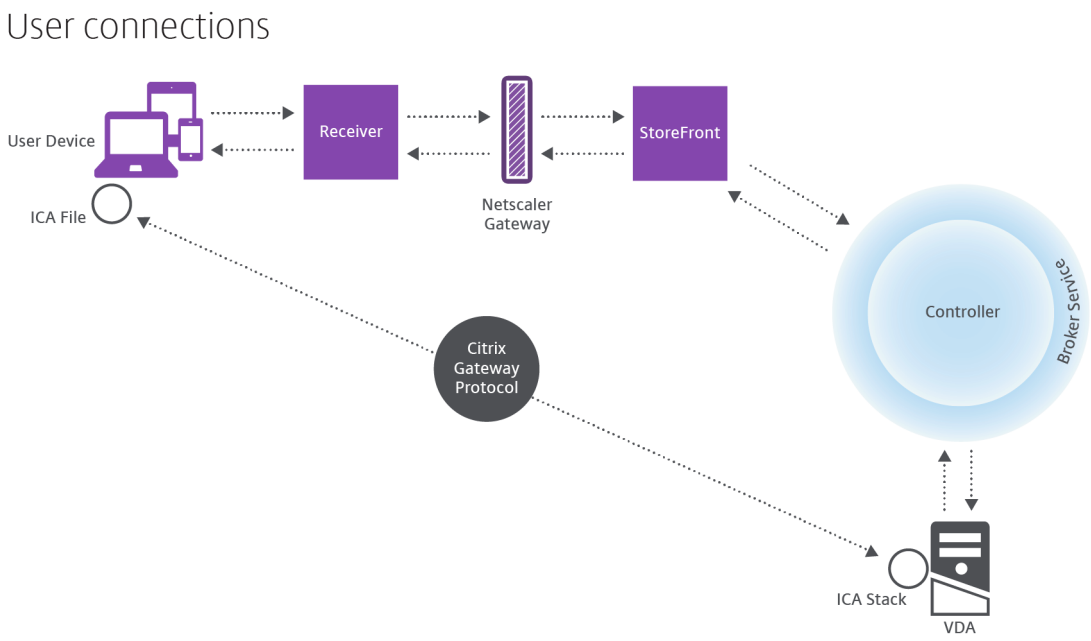
Les utilisateurs n'accèdent jamais directement au Controller. Le VDA est utilisé en tant que intermédiaire entre les utilisateurs et le Controller. Lorsque les utilisateurs se connectent au site à l'aide de StoreFront, leurs informations d'identification sont transmises au service Broker sur le Controller. Le service Broker obtient ensuite leurs profils et les ressources disponibles en fonction des stratégies définies.

Comment sont traitées les connexions utilisateur

Pour démarrer une session, l'utilisateur se connecte, soit via Citrix Receiver installé sur la machine utilisateur, soit par le biais d'un site StoreFront Citrix Receiver pour Web.

L'utilisateur sélectionne les bureaux virtuels ou physiques ou l'application virtuelle nécessaire(s).

Les informations d'identification de l'utilisateur passent par le biais de cette piste pour accéder au Controller, qui détermine quelles ressources sont nécessaires à la communication avec un service Broker. Citrix recommande aux administrateurs de placer un certificat SSL sur StoreFront pour chiffrer les informations d'identification provenant de Citrix Receiver.



Le Service Broker détermine la nature des bureaux et des applications que l'utilisateur est autorisé à accéder.

Une fois les informations d'identification vérifiées, les informations sur les applications ou les bureaux disponibles sont envoyées à l'utilisateur au travers de la piste StoreFront-Citrix Receiver. Lorsque l'utilisateur sélectionne des applications ou des bureaux depuis cette liste, ces informations retournent à la piste vers le Delivery Controller. Le Controller détermine ensuite le VDA approprié pour héberger les applications ou le bureau spécifiques.

Le Controller envoie un message au VDA avec les informations d'identification de l'utilisateur et envoie toutes les données à propos de l'utilisateur et de la connexion au VDA. Le VDA accepte la connexion et renvoie les informations vers les mêmes pistes jusqu'au Citrix Receiver. Un ensemble de paramètres requis est collecté sur StoreFront. Ces paramètres sont ensuite envoyés à Citrix Receiver, soit dans le cadre de la conversation de protocole entre Receiver et StoreFront, ou convertis en fichier ICA (Independent Computing Architecture) et téléchargés. Tant que le site a été correctement configuré, les informations d'identification sont chiffrées dans ce processus.

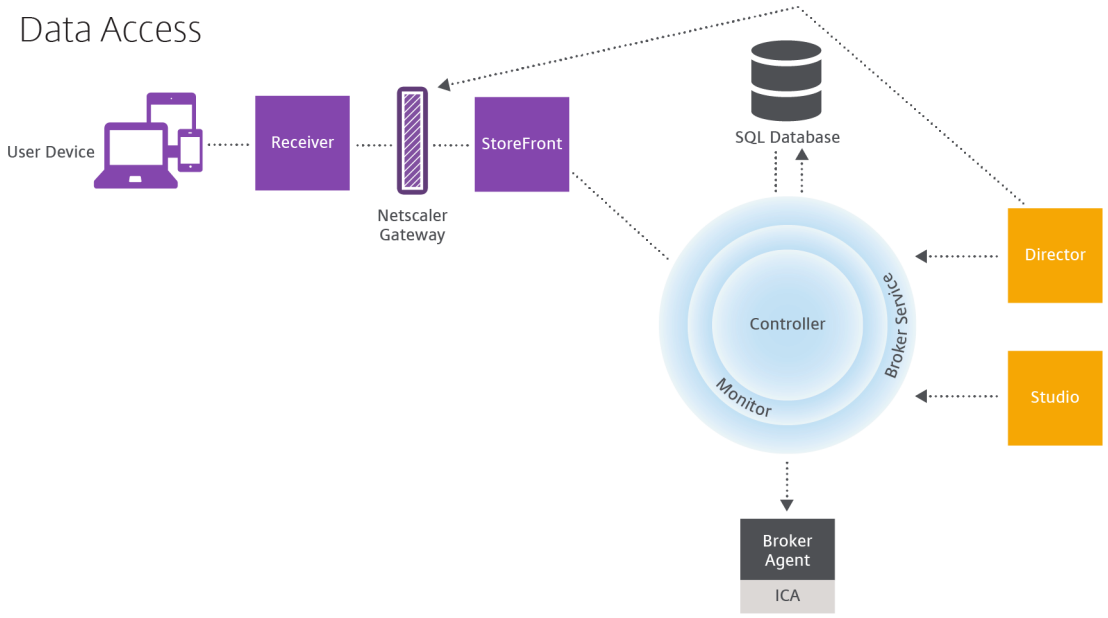
Le fichier ICA est copié vers la machine de l'utilisateur et établit une connexion directe entre le périphérique et la pile ICA en cours d'exécution sur le VDA. Cette connexion ignore l'infrastructure de gestion (Citrix Receiver, StoreFront et Controller).

La connexion entre Citrix Receiver et le VDA utilise Citrix Gateway Protocol (CGP). Si une connexion est interrompue, la fonction de fiabilité de session permet à l'utilisateur de se reconnecter au VDA plutôt que d'avoir à redémarrer via l'infrastructure de gestion. La fiabilité de session peut être activée ou désactivée à l'aide de stratégies Citrix.

Une fois que le client est connecté au VDA, le VDA notifie le Controller que l'utilisateur est connecté. Le Controller envoie ces informations à la base de données du site et commence à enregistrer les données dans la base de données de surveillance.

Comment fonctionne l'accès aux données

Chaque session génère des données auxquelles le service informatique peut accéder au travers de Studio ou Director. Studio permet aux administrateurs d'accéder à des données en temps réel à partir de l'agent Broker afin de gérer les sites. Director accède aux mêmes données en temps réel et aux données historiques stockées dans la base de données de surveillance. Director accède également aux données HDX de NetScaler Gateway pour le support et le dépannage du service d'assistance.



Dans le Controller, le service Broker signale des données de session pour chaque session sur la machine fournissant des données en temps réel. Le service Moniteur suit également les données en temps réel et les stocke en tant que données d'historique dans la base de données de surveillance.

Studio communique uniquement avec le service Broker ; il accède uniquement aux données en temps réel. Director communique avec le service Broker (via un plug-in dans l'agent Broker) pour accéder à la base de données du site.

Director peut également accéder à NetScaler Gateway pour obtenir des informations sur les données HDX.

Mise à disposition de bureaux et d'applications : catalogues de machines, groupes de mise à disposition et groupes d'applications

Vous configurez les machines qui mettront à disposition les applications et les bureaux avec des catalogues de machines. Ensuite, vous créez des groupes de mise à disposition qui spécifient les applications et bureaux qui seront disponibles (à l'aide de certaines ou de toutes les machines des catalogues), et les utilisateurs qui peuvent y accéder.

Catalogues de machines :

Les catalogues de machines sont des collections de machines physiques ou virtuelles que vous gérez comme une seule entité. Ces machines, et les applications ou les bureaux virtuels sur celles-ci, sont les ressources que vous mettez à la disposition des utilisateurs. Toutes les machines d'un catalogue ont le même système d'exploitation et VDA installé. Elles possèdent également les mêmes applications ou bureaux virtuels.

En général, vous pouvez créer une image principale et l'utiliser pour créer les mêmes machines virtuelles dans le catalogue. Pour les VM, vous pouvez spécifier la méthode de provisioning pour les machines de ce catalogue : outils Citrix (PVS ou MCS) ou autres outils. Vous pouvez également utiliser vos propres images existantes. Dans ce cas, vous devez gérer les machines cibles individuellement ou collectivement à l'aide d'outils de distribution logiciel électronique tiers (ESD).

Les types de machines valides sont les suivants :

- **Machines avec OS de serveur :** machines virtuelles ou physiques basées sur un système d'exploitation serveur. Utilisé pour mettre à disposition des applications publiées XenApp (appelées applications hébergées sur un serveur) et les bureaux publiés XenApp (appelés bureaux hébergés sur un serveur). Ces machines autorisent plusieurs utilisateurs à se connecter à un moment donné.
- **Machines avec OS de bureau :** machines virtuelles ou physiques basées sur un système d'exploitation bureau. Utilisé pour fournir des postes de travail VDI (pouvant être personnalisés), des applications hébergées sur machine virtuelle (applications sur des systèmes d'exploitation de bureau) et des postes de travail physiques hébergés. Un seul utilisateur à la fois peut se connecter à chacun de ces bureaux.
- **Remote PC Access :** permet aux utilisateurs distants d'accéder à leurs ordinateurs de bureau physiques à partir de n'importe quel périphérique exécutant Citrix Receiver. Les ordinateurs de bureau sont gérés par le déploiement XenDesktop et requièrent que les périphériques utilisateur soient spécifiés dans une liste blanche.

Pour de plus amples informations, consultez l'article Créer des catalogues de machines.

Groupes de mise à disposition :

Les groupes de mise à disposition spécifient quels utilisateurs ont accès à quelles applications et/ou quels bureaux sur quelles machines. Les groupes de mise à disposition contiennent les machines de vos catalogues de machines et les utilisateurs Active Directory qui ont accès à votre site. Vous pouvez attribuer des utilisateurs à vos groupes de mise à disposition en fonction de leur groupe Active Directory, car les groupes Active Directory et les groupes de mise à disposition représentent des modes de regroupement des utilisateurs ayant les mêmes spécifications.

Chaque groupe de mise à disposition peut contenir des machines provenant de plusieurs catalogues de machines et chaque catalogue peut contribuer des machines à plus d'un groupe de mise à disposition. Toutefois, une machine individuelle peut appartenir à un seul groupe de mise à disposition à la fois.

Vous définissez les ressources auxquelles les utilisateurs dans le groupe de mise à disposition peuvent accéder. Par exemple, pour mettre à disposition des applications différentes pour différents utilisateurs, vous pouvez installer toutes les applications sur l'image principale pour un catalogue et créer suffisamment de machines dans ce catalogue à répartir sur plusieurs groupes de mise à disposition. Vous pouvez ensuite configurer chaque groupe de mise à disposition pour fournir un sous-ensemble

différent d'applications installées sur les machines.

Pour plus d'informations, consultez la section Créer des groupes de mise à disposition.

Groupes d'applications :

Comparativement à l'utilisation d'un plus grand nombre de groupes de mise à disposition, les groupes d'applications permettent de gérer les applications et de contrôler les ressources : Avec les restrictions de balise, vous pouvez utiliser des machines existantes pour plusieurs tâches de publication, éliminant ainsi les coûts associés avec le déploiement et la gestion de machines supplémentaires. L'utilisation d'une restriction de balise équivaut à diviser (ou partitionner) des machines dans un groupe de mise à disposition. Les groupes d'applications peuvent également être utiles pour isoler et dépanner un sous-ensemble de machines dans un groupe de mise à disposition.

Pour de plus amples informations, consultez l'article Créer des groupes d'applications.

Active Directory

November 6, 2018

Active Directory est requis pour l'authentification et l'autorisation. L'infrastructure Kerberos dans Active Directory est utilisée pour garantir l'authenticité et la confidentialité des communications avec les Delivery Controller. Pour de plus amples informations sur Kerberos, veuillez consulter la documentation Microsoft.

L'article Configuration système requise répertorie les niveaux fonctionnels pris en charge de la forêt et du domaine. Pour utiliser la modélisation de stratégie, le contrôleur de domaine doit s'exécuter sur Windows Server 2003 à Windows Server 2012 R2 ; cela n'affecte pas le niveau fonctionnel du domaine.

Ce produit prend en charge ce qui suit :

- Déploiements dans lesquels les comptes d'utilisateurs et les comptes d'ordinateurs existent dans les domaines d'une forêt Active Directory unique. Les comptes d'utilisateurs et d'ordinateurs peuvent exister dans des domaines arbitraires d'une forêt unique. Tous les niveaux fonctionnels de domaine et de forêt sont pris en charge dans ce type de déploiement.
- Déploiements dans lesquels les comptes d'utilisateurs existent dans une forêt Active Directory qui est différente de celle contenant les comptes d'ordinateurs des contrôleurs et des bureaux virtuels. Dans ce type de déploiement, les domaines contenant les comptes d'ordinateurs des contrôleurs et des bureaux virtuels doivent établir l'approbation des domaines dans lesquels figurent les comptes d'utilisateurs. Des approbations de forêt ou des approbations externes peuvent être utilisées. Tous les niveaux fonctionnels de domaine et de forêt sont pris en charge dans ce type de déploiement.
- Déploiements dans lesquels les comptes d'ordinateurs des contrôleurs figurent dans une forêt Active Directory différente d'une ou de plusieurs forêts Active Directory supplémentaires con-

tenant les comptes d'ordinateurs des bureaux virtuels. Dans ce type de déploiement, une approbation bilatérale doit exister entre les domaines contenant les comptes d'ordinateurs des contrôleurs et l'ensemble des domaines contenant les comptes d'ordinateurs des bureaux virtuels. Dans ce type de déploiement, tous les domaines contenant les comptes d'ordinateurs des contrôleurs ou des bureaux virtuels doivent figurer au niveau fonctionnel « natif de Windows 2000 » ou supérieur. Tous les niveaux fonctionnels de forêt sont pris en charge.

- Contrôleurs de domaine accessibles en écriture. Les contrôleurs de domaine en lecture seule ne sont pas pris en charge.

Facultativement, les VDA (Virtual Delivery Agents) peuvent utiliser des informations publiées dans Active Directory pour déterminer les Controller avec lesquels ils peuvent s'enregistrer (découverte). Cette méthode est principalement prise en charge pour la rétrocompatibilité, et est uniquement disponible si les VDA se trouvent dans la même forêt Active Directory que les Controller. Pour de plus amples informations sur cette méthode de découverte, consultez Découverte basée sur unité d'organisation Active Directory et l'article CTX118976.

> **Conseil**
>
> Ne modifiez pas le nom de l'ordinateur ou l'appartenance à un domaine d'un Delivery Controller une fois que le site est configuré.

Déployer dans un environnement Active Directory avec des forêts multiples

Ces informations s'appliquent à XenDesktop 7.1 et XenDesktop 7.5 (versions minimum). Elles ne s'appliquent pas aux versions antérieures de XenDesktop ou XenApp.

Dans un environnement Active Directory avec plusieurs forêts, si des approbations à sens unique ou bidirectionnelles sont en place, vous pouvez utiliser les redirecteurs DNS pour la recherche de nom et l'enregistrement. Pour autoriser les utilisateurs Active Directory appropriés à créer des comptes d'ordinateurs, utilisez l'Assistant Délégation de contrôle. Reportez-vous à la documentation Microsoft pour plus d'informations sur cet assistant.

Aucune zone DNS inversée n'est nécessaire dans l'infrastructure DNS si des redirecteurs DNS appropriés sont en place entre les forêts.

La clé SupportMultipleForest n'est nécessaire que si le VDA et le Controller se trouvent dans des forêts différentes que les noms Active Directory et NetBIOS soient différents ou non. La clé SupportMultipleForest est uniquement nécessaire sur le VDA. Utilisez les informations suivantes pour ajouter la clé de registre :

> **Avertissement :**
> toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de

> résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Effectuez une copie de sauvegarde de votre registre avant de le modifier.

- HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\SupportMultipleForest
  - Nom : SupportMultipleForest
  - Type : REG_DWORD
  - Données : 0x00000001 (1)

Vous aurez peut-être besoin d'utiliser une configuration DNS inversée si l'espace de noms DNS est différent de celui d'Active Directory.

Si des approbations externes sont en place au cours de l'installation, la clé de registre ListOfSIDs est requise. La clé de registre ListOfSIDs est également nécessaire si le nom de domaine complet (FQDN) Active Directory est différent du FQDN DNS ou si le domaine contenant le contrôleur de domaine porte un nom NetBIOS autre que le FQDN Active Directory. Pour ajouter la clé de registre, utilisez les informations suivantes :

- Pour un VDA 32 bits ou 64 bits, accédez à la clé de registre : HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDe
  - Nom : ListOfSIDs
  - Type : REG_SZ
  - Données : identificateur de sécurité (SID) des Controller

Lorsque des approbations externes sont en place, apportez les modifications suivantes sur le VDA :

1. Recherchez le fichier <ProgramFiles>\Citrix\Virtual Desktop Agent\brokeragentconfig.exe.config
2. Créez une copie de sauvegarde du fichier.
3. Ouvrez le fichier dans un éditeur de texte tel que le Bloc-notes.
4. Recherchez le texte allowNtlm="false" et modifiez le texte en allowNtlm="true".
5. Enregistrez le fichier.

Après l'ajout de la clé de registre ListOfSIDs et la modification du fichier brokeragent.exe.config, redémarrez le service Citrix Desktop pour appliquer les modifications.

Le tableau suivant dresse la liste des types de prise en charge de l'approbation :

Type d'approbation	Transitivité	Sens	Pris en charge dans cette version
Parent et enfant	Transitive	Bidirectionnelle	Oui
Racine d'arborescence	Transitive	Bidirectionnelle	Oui
Externe	Non transitive	Unidirectionnelle ou bidirectionnelle	Oui

Type d'approbation	Transitivité	Sens	Pris en charge dans cette version
Forêt	Transitive	Unidirectionnelle ou bidirectionnelle	Oui
Raccourci	Transitive	Unidirectionnelle ou bidirectionnelle	Oui
Domaine	Transitive ou non transitive	Unidirectionnelle ou bidirectionnelle	Non

Pour de plus amples informations sur les environnements Active Directory complexes, consultez l'article CTX134971.

Bases de données

February 28, 2019

Un site XenApp ou XenDesktop utilise trois bases de données SQL Server :

- **Site :** (également appelé Configuration de site) stocke les données de configuration du site, ainsi que les informations sur l'état de la session et la connexion.
- **Journalisation de la configuration :** (également appelée Journalisation) stocke des informations sur les modifications apportées à la configuration du site et les activités administratives. Cette base de données est utilisée lorsque la fonction Journalisation de la configuration est activée (valeur par défaut=activée).
- **Contrôle :** stocke les données utilisées par Director, telles que les informations de session et de connexion.

Chaque Delivery Controller communique directement avec la base de données du site. L'authentification Windows est requise entre le Controller et les bases de données. Il est possible de déconnecter un Controller ou de le mettre hors tension sans affecter les autres Controller du site. L'unique point de défaillance reste par conséquent la base de données. Si le serveur de base de données échoue, les connexions existantes continuent de fonctionner jusqu'à ce que l'utilisateur ferme sa session ou se déconnecte. Pour plus d'informations sur le comportement de la connexion lorsque la base de données de site devient indisponible, consultez la section Cache d'hôte Local.

Citrix vous recommande de sauvegarder régulièrement les bases de données afin de pouvoir la restaurer en cas de défaillance du serveur de base de données. La stratégie de sauvegarde pour chaque base de données peut différer. Pour obtenir des instructions, consultez l'article CTX135207.

Si votre site contient plus d'une zone, la base de données du site doit toujours se trouver dans la zone principale. Les Controller de chaque zone communiquent avec cette base de données.

Haute disponibilité

Il existe trois solutions de haute disponibilité à considérer pour garantir le basculement automatique :

- **Groupes de disponibilité AlwaysOn (y compris les groupes de disponibilité de base) :** cette solution à haute disponibilité et reprise après sinistre introduite dans SQL Server 2012 vous permet d'optimiser la disponibilité pour une ou plusieurs bases de données. Les Groupes de disponibilité AlwaysOn nécessitent que les instances SQL Server résident les nœuds WSFC (Windows Server Failover Clustering). Pour plus d'informations, veuillez consulter l'article https://msdn.microsoft.com/en-us/library/hh510230.
- **Mise en miroir de la base de données SQL Server :** la mise en miroir de la base de données garantit qu'en cas d'indisponibilité soudaine du serveur de base de données actif, le basculement automatique se produit au bout de quelques secondes seulement, évitant généralement toute gêne pour les utilisateurs. Cette méthode est plus coûteuse que d'autres solutions car les licences complètes de SQL Server sont requises sur chaque serveur de base de données ; vous ne pouvez pas utiliser SQL Server édition Express pour un environnement de mise en miroir.
- **Mise en cluster SQL :** la technologie de mise en cluster SQL de Microsoft peut être utilisée pour permettre à un serveur d'assurer automatiquement la reprise des tâches et des responsabilités d'un autre serveur défaillant. Toutefois, cette solution est plus complexe à mettre en place et le basculement automatique est généralement plus lent qu'avec les autres méthodes, comme la mise en miroir SQL.
- **À l'aide des fonctionnalités de haute disponibilité de l'hyperviseur :** avec cette méthode, vous déployez la base de données en tant que machine virtuelle et utilisez les fonctionnalités de haute disponibilité de votre hyperviseur. Cette solution est moins coûteuse que la mise en miroir du fait qu'elle utilise votre logiciel d'hyperviseur et que vous pouvez également utiliser l'édition SQL Server Express. Cependant, le processus de basculement automatique est plus lent car il faut un certain temps pour qu'une nouvelle machine démarre pour la base de données, avec le risque d'interrompre le service fourni aux utilisateurs.

La fonctionnalité de cache d'hôte local complète les meilleures pratiques de la haute disponibilité du serveur SQL Server en permettant aux utilisateurs de se connecter et de se reconnecter à leurs applications et bureaux même lorsque la base de données du site n'est pas disponible. Pour plus d'informations, veuillez consulter la section Cache d'hôte local.

Si tous les Controller d'un site échouent, vous pouvez configurer les VDA pour fonctionner en mode haute disponibilité de sorte à ce que les utilisateurs puissent continuer à accéder à leurs bureaux et applications et les utiliser. En mode haute disponibilité, le VDA accepte des connexions ICA directes provenant des utilisateurs, plutôt que des connexions négociées par le Controller. Utilisez cette fonctionnalité uniquement dans les rares cas où la communication avec tous les Controllers échoue. Il ne s'agit pas d'une solution alternative aux autres solutions de haute disponibilité. Pour plus d'informations, veuillez consulter l'article CTX 127564.

> **Remarque**
>
> L'installation d'un Controller sur un nœud dans une installation de mise en cluster SQL ou mise en miroir SQL n'est pas prise en charge.

Installer le logiciel de base de données

Par défaut, l'édition SQL Server Express est installée lorsque vous installez le premier Delivery Controller, si une autre instance SQL Server n'est pas détectée sur ce serveur. Cette mesure par défaut est généralement suffisante pour la preuve de concept ou pour les déploiements pilotes. Toutefois, SQL Server Express ne prend pas en charge les fonctionnalités de haute disponibilité de Microsoft.

L'installation par défaut utilise les comptes de service et autorisations Windows par défaut. Reportez-vous à la documentation Microsoft pour de plus amples informations sur ces défauts, y compris l'ajout de comptes de service Windows au rôle sysadmin. Le Controller utilise le compte de service réseau de cette configuration. Le Controller ne requiert aucun rôle ni autorisation SQL Server supplémentaire.

Le cas échéant, vous pouvez sélectionner **Masquer l'instance** pour l'instance de base de données. Lors de la configuration de l'adresse de la base de données dans Studio, entrez le numéro de port statique de l'instance plutôt que son nom. Reportez-vous à la documentation Microsoft pour de plus amples informations sur le masquage d'une instance du moteur de base de données SQL Server.

La plupart des déploiements de production, et tout déploiement qui utilise les fonctionnalités de haute disponibilité de Microsoft, utilisent des éditions non-Express prises en charge de SQL Server installées sur des machines autres que le serveur sur lequel le premier Delivery Controller est installé. L'article Configuration système requise répertorie les versions prises en charge de SQL Server. Les bases de données peuvent résider sur une ou plusieurs machines.

Assurez-vous que le logiciel SQL Server est installé avant de créer un site. Vous n'avez pas besoin de créer la base de données, mais si vous le faites, elle doit être vide. La configuration de technologies haute disponibilité de Microsoft est également recommandée.

Utilisez Windows Update pour conserver SQL Server à jour.

Configurer les bases de données à partir de l'assistant de création de site

Indiquez le nom et l'adresse des bases de données (emplacement) sur la page **Bases de données** dans l'assistant de création de site. Voir Formats d'adresse de base de données. Pour éviter des erreurs lorsque Director interroge le service Monitor, n'utilisez pas d'espaces dans le nom de la base de données de contrôle.

La page **Bases de données** offre deux options pour configurer les bases de données : automatiquement et à l'aide de scripts. En général, vous pouvez utiliser l'option automatique si vous (utilisateur

de Studio et administrateur de Citrix) disposez des privilèges de base de données requis ; veuillez consulter la section Autorisations requises pour configurer les bases de données ci-dessous.

Vous pouvez modifier l'emplacement des bases de données de journalisation de la configuration et de contrôle après la création du site. Voir Modifier l'emplacement des bases de données.

Pour configurer un site pour utiliser une base de données mise en miroir, effectuez les étapes suivantes, puis passez à la procédure de configuration automatique ou à l'aide d'un script.

1. Installez le logiciel SQL Server sur deux serveurs, A et B
2. Sur le serveur A, créez la base de données destinée à être utilisée comme base de données principale. Sauvegardez la base de données sur le serveur A, puis copiez-la sur le serveur B.
3. Sur le serveur B, restaurez le fichier de sauvegarde.
4. Démarrez la mise en miroir sur le serveur A.

Pour vérifier la mise en miroir après la création du site, exécutez le cmdlet PowerShell `get-configdbconnection` pour vous assurer que le partenaire de basculement a été défini dans la chaîne de connexion pour le miroir.

Si vous ajoutez, déplacez ou supprimez un Delivery Controller dans un environnement de base de données mise en miroir ultérieurement, consultez l'article Delivery Controller.

Configuration automatique

Si vous possédez les privilèges de base de données requis, sélectionnez l'option Créer et configurer les bases de données à partir de Studio sur la page **Bases de données** de l'assistant de création de site, puis fournissez les noms et adresses des bases de données principales.

Si une base de données existe sur une adresse spécifiée, elle doit être vide. Si les bases de données n'existent pas sur une adresse spécifiée, vous êtes informé qu'aucune base de données n'a été détectée, puis vous êtes invité à indiquer si vous souhaitez que la base de données soit créée pour vous. Lorsque vous confirmez, Studio crée automatiquement les bases de données, puis applique les scripts d'initialisation pour les bases de données principales et les copies.

Installation à l'aide de scripts

Si vous ne disposez pas des privilèges de base de données requis, un utilisateur avec ces autorisations, tel qu'un administrateur de base de données, doit vous aider. Voici la séquence :

1. Dans l'assistant de création de site, sélectionnez l'option **Générer des scripts**. Six scripts sont générés : deux pour chacune des trois de bases de données, un pour chaque base de données principale et un autre pour chaque copie. Vous pouvez indiquer l'emplacement de stockage des scripts.

2. Donnez ces scripts à votre administrateur de base de données. L'assistant de création de site s'arrête automatiquement à ce stade ; vous serez invité lorsque vous y reviendrez plus tard à continuer la création de site.

L'administrateur de base de données crée alors les bases de données. Chaque base de données doit présenter les caractéristiques suivantes :

- Utilisez un classement qui se termine par « _CI_AS_KS ». Citrix vous recommande d'utiliser un classement qui se termine par « _100_CI_AS_KS ».
- Pour des performances optimales, activez l'option Capture instantanée Read Committed de SQL Server. Pour plus d'informations, veuillez consulter l'article CTX 137161.
- Les fonctionnalités haute disponibilité doivent être configurées, le cas échéant.
- Pour configurer la mise en miroir, vous devez tout d'abord définir la base de données pour utiliser le modèle de récupération complet (le modèle simple est la valeur par défaut). Sauvegardez la base de données principale dans un fichier et copiez-la sur le serveur miroir. Sur la base de données miroir, restaurez le fichier de sauvegarde sur le serveur miroir. Ensuite, démarrez la mise en miroir sur le serveur principal.

L'administrateur de base de données utilise l'utilitaire de ligne de commande SQLCMD ou SQL Server Management Studio dans le mode SQLCMD pour exécuter chacun des scripts xxx_Replica.sql sur les instances de base de données SQL Server haute disponibilité (si la haute disponibilité est configurée), puis exécute chacun des scripts xxx_Principal.sql sur les instances de base de données SQL Server principales. Consultez la documentation Microsoft sur SQLCMD pour plus de détails.

Lorsque tous les scripts sont terminés, l'administrateur de la base de données donne à l'administrateur Citrix les trois adresses de base de données principale.

Dans Studio, vous êtes invité à continuer la création de site et renvoyé à la page **Bases de données**. Entrez les adresses. Si l'un des serveurs hébergeant une base de données ne peut pas être contacté, un message d'erreur s'affiche.

Autorisations requises pour configurer les bases de données

Vous devez être un administrateur local et un utilisateur du domaine pour créer et initialiser les bases de données (ou modifier l'emplacement de la base de données). Vous devez également disposer de certaines autorisations SQL Server. Les autorisations suivantes peuvent être explicitement configurées ou acquises par l'appartenance à un groupe Active Directory. Si vos informations d'identification d'utilisateur Studio ne comprennent pas ces autorisations, vous êtes invité à entrer les informations d'identification d'utilisateur SQL Server.

Opération	Objectif	Rôle de serveur	Rôle de base de données
Créer une base de données	Créer une base de données vide appropriée	dbcreator	
Créer un schéma	Créer tous les schémas spécifiques au service et ajouter le premier Controller au site	securityadmin*	db_owner
Ajouter un Controller	Ajouter un Controller (autre que le premier) au site	securityadmin*	db_owner
Ajouter un Controller (serveur miroir)	Ajouter une ouverture de session Controller au serveur de base de données assumant actuellement le rôle de miroir d'une base de données en miroir	securityadmin*	
Mettre à jour un schéma	Appliquer les mises à jour ou correctifs au schéma		db_owner

* Bien qu'il soit plus restrictif techniquement, en pratique, le rôle de serveur securityadmin doit être considéré comme équivalent au rôle de serveur sysadmin.

Lorsque vous utilisez Studio pour effectuer ces opérations, le compte d'utilisateur doit être un membre du rôle de serveur sysadmin.

Formats d'adresse de base de données

Vous pouvez spécifier une adresse de base de données dans l'un des formats suivants :

- `ServerName`
- `ServerName\\InstanceName`
- `ServerName,PortNumber`

Pour un groupe de disponibilité AlwaysOn, spécifiez l'écouteur du groupe dans le champ d'emplacement.

Modifier l'emplacement des bases de données

Après avoir créé un site, vous pouvez modifier l'emplacement des bases de données de journalisation de la configuration et de contrôle. (Vous ne pouvez pas modifier l'emplacement de la base de données du site.) Lorsque vous modifiez l'emplacement d'une base de données :

- Les données provenant de la base de données précédente ne sont pas importées vers la nouvelle base de données.
- Les journaux ne peuvent pas être regroupés pour les deux bases de données lors de la récupération des journaux.
- La première entrée du journal dans la nouvelle base de données indique qu'une modification a été apportée dans une base de données, mais elle n'identifie pas la base de données précédente.

Vous ne pouvez pas modifier l'emplacement de la base de données de journalisation de la configuration lorsque la journalisation obligatoire est activée.

Pour modifier l'emplacement d'une base de données :

1. Assurez-vous qu'une version prise en charge de Microsoft SQL Server est installée sur le serveur sur lequel vous souhaitez que la base de données réside. Configurez les fonctionnalités de haute disponibilité en fonction de vos besoins.
2. Sélectionnez une **configuration** dans le volet de navigation Studio.
3. Sélectionnez la base de données pour laquelle vous souhaitez spécifier un autre emplacement, puis sélectionnez **Modifier la base de données** dans le volet **Actions**.
4. Spécifiez le nouvel emplacement et le nom de la base de données.
5. Si vous souhaitez que Studio crée la base de données et que vous possédez les autorisations appropriées, cliquez sur **OK**. Lorsque vous y êtes invité, cliquez sur **OK** et Studio crée la base de données automatiquement. Studio tente d'accéder à la base de données à l'aide de vos informations d'identification. Si la tentative échoue, vous êtes invité à entrer les informations d'identification de l'utilisateur de la base de données. Studio télécharge ensuite le schéma de base de données vers la base de données. Les informations d'identification ne sont conservées que durant la création de la base de données.
6. Si vous ne souhaitez pas que Studio crée la base de données, ou si vous ne disposez pas des autorisations suffisantes, cliquez sur **Générer script**. Les scripts générés contiennent des instructions permettant de créer manuellement la base de données et une base de données miroir, si nécessaire. Avant le chargement du schéma, assurez-vous que la base de données est vide et qu'au moins un utilisateur est autorisé à accéder et modifier la base de données.

Informations supplémentaires

- Outil de dimensionnement de base de données.
- Le dimensionnement de la base de données du site et la configuration des chaînes de connexion lors de l'utilisation de solutions de haute disponibilité de SQL Server.

Méthodes de mise à disposition

January 23, 2019

Il est difficile de répondre aux besoins de chaque utilisateur avec un déploiement de virtualisation. XenApp et XenDesktop permettent aux administrateurs de personnaliser l'expérience de l'utilisateur avec une variété de méthodes parfois appelées modèles FlexCast.

Cette collection de méthodes de mise à disposition, chacune avec ses propres avantages et inconvénients respectifs : fournit la meilleure expérience utilisateur dans un scénario au cas par cas.

Mobiliser des applications Windows sur les périphériques mobiles :

Les périphériques à écran tactile, tels que les tablettes et les smartphones, sont maintenant standard en mobilité. Ces périphériques peuvent entraîner des problèmes lors de l'exécution d'applications Windows qui utilisent les écrans en plein écran et s'appuient sur les entrées utilisant le bouton droit de la souris pour une fonctionnalité totale.

XenApp avec Citrix Receiver offre une solution sécurisée qui permet aux utilisateurs de périphériques mobiles un accès à toutes les fonctionnalités dans leurs applications Windows sans le coût de réécriture de ces applications pour les plateformes mobiles natives.

La méthode de mise à disposition des applications publiées XenApp utilise la technologie HDX Mobile qui résout les problèmes associés à la mobilisation des applications Windows. Cette méthode permet aux applications Windows d'être restructurées pour une expérience tactile tout en gérant des fonctionnalités telles que les gestes multitouch, les commandes de menu natif et GPS, la caméra et les fonctions GPS. De nombreuses fonctions tactiles sont disponibles en mode natif dans XenApp et XenDesktop et ne requièrent aucune activation des modifications du code source de l'application.

Ces fonctionnalités comprennent :

- Affichage automatique du clavier de l'appareil lorsqu'un champ modifiable est actif
- Plus grand contrôle de sélecteur pour remplacer le contrôle de la zone combinée Windows
- Gestes multitouch, comme l'action de pincer et de zoom
- Défilement lié à l'inertie
- Navigation via touchpad ou directement via le curseur

Réduit les coûts d'actualisation de votre PC :

La mise à niveau des machines physiques est une tâche difficile à laquelle de nombreuses entreprises doivent faire face tous les trois à cinq ans, spécialement si votre entreprise doit gérer les versions les plus récentes des systèmes d'exploitation et des applications. Les entreprises en croissance font également face à des frais généraux impressionnants d'ajout de nouvelles machines à leur réseau.

La méthode de mise à disposition VDI Personal vDisk offre des systèmes d'exploitation de bureaux complètement personnalisés à des utilisateurs uniques sur n'importe quelle machine ou client fin utilisant des ressources serveur. Les administrateurs peuvent créer des machines virtuelles dont les ressources, tels que le traitement, la mémoire et le stockage, sont stockés dans le centre de données du réseau.

Cela peut prolonger la durée de vie des machines plus anciennes, permettre de garder le logiciel à jour, et réduire les temps d'arrêt lors des mises à niveau.

Accès sécurisé aux applications et bureaux virtuels pour les fournisseurs et les partenaires :

La sécurité du réseau est un problème grandissant, plus particulièrement lorsque vous travaillez avec les fournisseurs, partenaires et autres travailleurs de contingent tiers qui nécessitent un accès aux applications et données d'une entreprise. Il se peut que les utilisateurs nécessitent également des ordinateurs portables ou autres périphériques en prêt, ce qui entraîne des problèmes de coût supplémentaires.

Les données, applications et bureaux sont stockés derrière le pare-feu du réseau sécurisé avec XenDesktop et XenApp, et la seule chose transmise par l'utilisateur final correspond à des entrées et sorties effectuées sur le périphérique utilisateur, telles que les frappes clavier, des clics souris, et des mises à jour audio et de l'écran. En effectuant la gestion de ces ressources dans un centre de données, XenDesktop et XenApp offre une solution d'accès à distance plus sécurisée que d'utiliser VPN SSL typique.

Avec un déploiement VDI avec Personal vDisk, les administrateurs peuvent utiliser des clients légers ou des périphériques personnels utilisateurs en créant une machine virtuelle sur un serveur réseau et en fournissant un système d'exploitation de bureau mono-utilisateur. Ceci permet au département informatique de maintenir la sécurité des travailleurs tiers sans devoir acquérir d'équipement coûteux.

Accélérer la migration :

Lors du basculement vers un nouveau système d'exploitation, le service informatique peut faire face à un test de mise à disposition d'applications d'ancienne génération et non compatibles.

Avec les applications hébergées sur des machines virtuelles, les utilisateurs peuvent exécuter des applications plus anciennes par le biais de Citrix Receiver sur la machine virtuelle mise à niveau sans aucun problème de compatibilité. Ceci laisse au service informatique du temps supplémentaire pour résoudre et tester les problèmes de compatibilité, faciliter la transition des utilisateurs et rendre plus efficace les appels au service d'assistance.

Les autres avantages de l'utilisation de XenDesktop pendant la migration comprennent :

- La réduction de la complexité des bureaux
- L'amélioration du contrôle informatique
- L'amélioration de la flexibilité de l'utilisateur en termes de l'utilisation des périphériques et l'emplacement de l'espace de travail

Aider les concepteurs et les ingénieurs en virtualisant les applications graphiques 3D professionnelles :

De nombreuses entreprises de conception et de fabrication reposent fortement sur des applications graphiques 3D professionnelles. Ces entreprises font face à des contraintes financières découlant de coûts matériel élevés pour prendre en charge ce type de logiciel ainsi que les problèmes logistiques qui se produisent éventuellement avec le partage de fichiers de conception importants via FTP, e-mail et des méthodes similaires.

La méthode de mise à disposition du bureau physique hébergé offre une seule image de bureau aux stations de travail et aux serveurs lames, sans que des hyperviseurs aient à exécuter d'applications 3D gourmandes en graphiques sur un système d'exploitation natif.

Tous les fichiers sont enregistrés dans un centre de données central au sein du réseau, ainsi le partage de fichiers volumineux avec d'autres utilisateurs du réseau est plus rapide et plus sécurisé car les fichiers ne sont pas transférés d'une station de travail à une autre.

Transformer les centres d'appels :

Les entreprises nécessitant des centres d'appel à grande échelle font face à des difficultés à grande échelle de gestion de personnel adéquate lors des périodes de pointe tout en n'effectuant de provisioning supplémentaire des machines lors des heures creuses.

La méthode de mise à disposition VDI regroupés fournit l'accès à un bureau standard à plusieurs utilisateurs de manière dynamique à un coût minimum lors du provisioning d'un grand nombre d'utilisateurs. Les machines regroupées sont attribuées session par session, premier arrivé, premier servi.

La gestion quotidienne de ces machines virtuelles est allégée, car toute modification effectuée au cours de la session est supprimée lorsque l'utilisateur ferme sa session. Cela augmente également la sécurité.

La méthode de mise à disposition des bureaux hébergés est une autre option viable de transformation des centres d'appels. Cette méthode héberge de multiples bureaux utilisateur sur un seul système d'exploitation de serveur.

Cette méthode est plus rentable que VDI regroupés, mais avec les bureaux hébergés, les utilisateurs sont restreints à l'installation d'applications, à la modification des paramètres système et au démarrage du serveur.

Applications et bureaux publiés XenApp

November 6, 2018

Utilisez les machines avec OS de serveur pour mettre à disposition des applications publiées XenApp et des bureaux publiés.

Cas d'utilisation :

- Une mise à disposition peu onéreuse sur le serveur pour réduire le coût de mise à disposition des applications pour un grand nombre d'utilisateurs, tout en offrant une expérience utilisateur haute définition en toute sécurité.
- Vos utilisateurs effectuent des tâches clairement définies, et qui ne requièrent aucune personnalisation ou accès en mode déconnecté aux applications. Les utilisateurs peuvent inclure les travailleurs productifs, tels que des opérateurs de centre d'appel et des travailleurs au détail, ou des utilisateurs qui partagent des stations de travail.
- Types d'application : toute application.

Avantages et considérations :

- Solution gérable et évolutive dans votre centre de données.
- Solution de mise à disposition des applications la moins onéreuse.
- Les applications hébergées sont gérées de manière centralisée et les utilisateurs ne peuvent pas modifier l'application, offrant une expérience utilisateur cohérente, sécurisée et fiable.
- Les utilisateurs doivent être en ligne pour accéder à leurs applications.

Expérience utilisateur :

- L'utilisateur demande une ou plusieurs applications depuis StoreFront, leur menu Démarrer ou une adresse URL que vous leur fournissez.
- Les applications sont mises à disposition virtuellement et s'affichent en toute transparence en haute définition sur les machines utilisateur.
- En fonction des paramètres de profil, les modifications apportées par l'utilisateur sont enregistrées lorsque la session applicative de l'utilisateur prend fin. Sinon, les modifications sont supprimées.

Traiter, héberger et mettre à disposition des applications :

- Le traitement de l'application a lieu sur les machines hôtes, plutôt que sur les machines utilisateur. La machine hôte peut être une machine physique ou virtuelle.
- Les applications et les bureaux résident sur une machine équipée d'un système d'exploitation serveur.
- Les machines deviennent disponibles au travers des catalogues de machines.
- Les machines présentes dans des catalogues sont organisées en groupes de mise à disposition qui mettent à disposition le même ensemble d'applications vers des groupes d'utilisateurs.

- Les machines avec système d'exploitation serveur prennent en charge les groupes de mise à disposition qui hébergent des applications ou bureaux, ou les deux.

Gestion et attribution de sessions :

- Les machines équipées d'un système d'exploitation serveur exécutent plusieurs sessions à partir d'une seule machine pour mettre à disposition plusieurs applications et bureaux vers de multiples utilisateurs connectés simultanément. Chaque utilisateur requiert une seule session depuis laquelle il peut exécuter toutes ses applications hébergées.

Par exemple, un utilisateur ouvre une session et requiert une application. Une session sur cette machine devient indisponible pour d'autres utilisateurs. Un second utilisateur ouvre une session et requiert une application que cette machine héberge. Une seconde session sur la même machine est maintenant disponible. Si les deux utilisateurs demandent des applications supplémentaires, aucune des sessions supplémentaires n'est requise, car un utilisateur peut exécuter de multiples applications à l'aide de la même session. Si deux utilisateurs ou plus ouvrent une session et demandent des bureaux, et deux sessions sont disponibles sur la même machine, cette machine unique utilise maintenant quatre sessions pour héberger quatre utilisateurs différents.

- Dans le groupe de mise à disposition auquel un utilisateur est attribué, une machine sur le serveur le moins chargé est sélectionnée. Une machine avec une session de disponibilité est attribuée de manière aléatoire pour mettre à disposition les applications à un utilisateur lorsque ce dernier ouvre une session.

Pour mettre à disposition des applications et bureaux publiés XenApp :

1. Installez les applications que vous souhaitez mettre à disposition sur une image principale exécutant un système d'exploitation de serveur Windows pris en charge.
2. Créez un catalogue de machines pour cette image principale ou mettre à jour un catalogue existant avec l'image principale.
3. Créez un groupe de mise à disposition pour mettre à disposition les applications et bureaux auprès des utilisateurs. Si vous effectuez la mise à disposition d'applications, sélectionnez les applications que vous souhaitez mettre à disposition.

Voir les articles sur l'installation et la configuration pour plus de détails.

VM hosted Apps

November 6, 2018

Utilisez les machines avec OS de bureau pour mettre à disposition des applications hébergées sur une machine virtuelle.

Cas d'utilisation :

- Vous recherchez une solution de mise à disposition d'applications basée sur client qui soit sécurisée, offre une gestion centralisée et prenne en charge un grand nombre d'utilisateurs par serveur hôte (ou hyperviseur), tout en offrant aux utilisateurs des applications qui s'affichent en haute définition.
- Vos utilisateurs sont des sous-traitants internes ou externes, des collaborateurs tiers et autres membres d'équipe provisoire. Vos utilisateurs ne requièrent aucun accès à des applications hébergées en mode déconnecté.
- Types d'application : applications qui risquent de ne pas fonctionner correctement avec d'autres applications ou qui peuvent interagir avec le système d'exploitation, telles que .NET Framework. Ces types d'applications sont idéaux pour l'hébergement sur des machines virtuelles.

Avantages et considérations :

- Les applications et les bureaux sur l'image principale sont hébergés, gérés et exécutés en toute sécurité sur les machines de votre centre de données, qui fournissent une solution de mise à disposition d'applications la moins onéreuse.
- Dès l'ouverture de session, les utilisateurs peuvent être attribués à une machine de manière aléatoire au sein d'un groupe de mise à disposition qui est configuré pour héberger la même application. Vous pouvez également attribuer une machine unique pour mettre une application une application vers un seul utilisateur chaque fois que l'utilisateur ouvre une session. Les machines attribuées de manière statique permettent aux utilisateurs d'installer et de gérer leurs propres applications sur la machine virtuelle.
- L'exécution de plusieurs sessions n'est pas prise en charge sur des machines équipées d'un système d'exploitation de bureau. Par conséquent, chaque utilisateur utilise une seule machine au sein d'un groupe de mise à disposition lorsqu'il ouvre une session, et les utilisateurs doivent être en ligne pour accéder à leurs applications.
- Cette méthode peut augmenter la quantité de ressources serveur pour le traitement des applications et augmenter la quantité de stockage pour les Personal vDisks des utilisateurs.

Expérience utilisateur :

La même expérience d'application transparente que l'hébergement des applications partagées sur les machines équipées d'un système d'exploitation serveur.

Traiter, héberger et mettre à disposition des applications :

Le même que les machines équipées d'un système d'exploitation serveur, mis à part qu'elles sont des machines de systèmes d'exploitation de bureau virtuel.

Gestion et attribution de sessions :

- Les machines équipées d'un système d'exploitation de bureau exécutent une seule session de bureau à partir d'une seule machine. Lors de l'accès à des applications uniquement, un seul

utilisateur peut utiliser plusieurs applications (et n'est pas limité à une seule application), car le système d'exploitation accède à chaque application comme une nouvelle session.

- Dans un groupe de mise à disposition, lorsque les utilisateurs ouvrent une session, ils peuvent accéder à une machine affectée de manière statique (à chaque fois que l'utilisateur ouvre une session sur la même machine) ou une machine affectée de manière aléatoire qui est sélectionnée en fonction de la disponibilité de session.

Pour mettre à disposition des applications hébergées sur une machine virtuelle :

1. Installez les applications que vous souhaitez mettre à disposition sur une image principale exécutant un système d'exploitation de bureau Windows pris en charge.
2. Créez un catalogue de machines pour cette image principale ou mettre à jour un catalogue existant avec l'image principale.
3. Lors de la définition de l'expérience de bureau pour le catalogue, déterminez si vous souhaitez que les utilisateurs se connectent à une nouvelle VM ou se connectent à la même machine chaque fois qu'ils ouvrent une session.
4. Créez un groupe de mise à disposition pour mettre à disposition l'application auprès des utilisateurs.
5. À partir de la liste des applications installées, sélectionnez l'application que vous souhaitez mettre à disposition.

Voir les articles sur l'installation et la configuration pour plus de détails.

Bureaux VDI

November 6, 2018

Utilisez des machines avec OS de bureau pour mettre à disposition des bureaux VDI.

Les bureaux VDI sont hébergés sur des machines virtuelles et fournissent à chaque utilisateur un système d'exploitation de bureau.

Les bureaux VDI requièrent plus de ressources que les bureaux publiés XenApp, mais n'exigent pas que les applications installées sur ceux-ci prennent en charge des systèmes d'exploitation serveur. De plus, selon le type de bureau VDI que vous choisissez, ces bureaux peuvent être affectés à des utilisateurs individuels et permettre à ces utilisateurs un haut degré de personnalisation.

Lorsque vous créez un catalogue de machines pour les bureaux VDI, vous créez un des types de bureaux suivants :

- **Bureaux aléatoires non persistants**, également appelé bureaux VDI regroupés. Chaque fois qu'un utilisateur ouvre une session sur l'un de ces bureaux, ils se connectent à un bureau sélectionné de manière dynamique dans un groupe de bureaux basés sur une image principale. Toutes les modifications apportées au bureau sont perdues lorsque la machine redémarre.

- **Bureau statique non persistant**. La première fois qu'un utilisateur ouvre une session pour utiliser l'un de ces bureaux, l'utilisateur se voit attribuer un bureau depuis un groupe de bureaux basés sur une image principale. Après la première utilisation, chaque fois qu'un utilisateur ouvre une session pour utiliser l'un de ces bureaux, l'utilisateur se connecte au bureau affecté lors de la première utilisation. Toutes les modifications apportées au bureau sont perdues lorsque la machine redémarre.
- **Statique persistant**, également appelé VDI avec Personal vDisk. À l'inverse d'autres types de bureaux VDI, ces bureaux peuvent être entièrement personnalisés par les utilisateurs. La première fois qu'un utilisateur ouvre une session pour utiliser l'un de ces bureaux, l'utilisateur se voit attribuer un bureau depuis un groupe de bureaux basés sur une image principale. Les ouvertures de session suivantes de cet utilisateur se connectent au bureau qui a été affecté lors de la première utilisation. Les modifications apportées aux bureaux sont conservées lorsque la machine redémarre, car ils sont stockés dans un Personal vDisk.

Pour mettre à disposition des bureaux VDI :

1. Créer une image principale exécutant un système d'exploitation de bureau Windows pris en charge.
2. Créez un catalogue de machines pour cette image principale ou mettre à jour un catalogue existant avec l'image principale. Lors de la définition de l'expérience de bureau pour le catalogue de machines, déterminez si vous souhaitez que les utilisateurs se connectent à une nouvelle VM ou se connectent à la même machine chaque fois qu'ils ouvrent une session. Si les utilisateurs se connectent à la même machine, vous pouvez spécifier comment les modifications apportées au bureau sont conservées.
3. Créez un groupe de mise à disposition pour mettre à disposition les bureaux auprès des utilisateurs.

Voir les articles sur l'installation et la configuration pour plus de détails.

Ports réseau

February 28, 2019

Le tableau suivant répertorie les ports réseau par défaut utilisés par les Delivery Controller de XenApp et XenDesktop, les VDA Windows, Director et le serveur de licences Citrix. Lorsque les composants Citrix sont installés, le pare-feu hôte du système d'exploitation est également mis à jour pour correspondre à ces ports réseau par défaut.

Pour un aperçu des ports de communication utilisés dans d'autres technologies et composants Citrix, voir l'article CTX101810.

Ces informations de port peuvent vous être utiles :

- À des fins de conformité réglementaire.
- S'il existe un pare-feu réseau entre ces composants et d'autres produits ou composants Citrix, de façon à ce que vous puissiez configurer ce pare-feu correctement.
- Si vous utilisez un pare-feu hôte tiers, tel que celui fourni avec un logiciel anti-malware, plutôt que l'hôte pare-feu du système d'exploitation.
- Si vous modifiez la configuration du pare-feu hôte sur ces composants (généralement le service Pare-feu Windows).
- Si vous reconfigurez des fonctionnalités de ces composants afin d'utiliser une plage de ports ou un port différent, et que vous voulez désactiver ou bloquer les ports non utilisés dans votre configuration. Pour obtenir plus d'informations, veuillez consulter la documentation accompagnant le composant.

Pour obtenir des informations sur les ports d'autres composants tels que StoreFront et Provisioning Services, consultez l'article « Configuration système requise » relatif au composant en question.

Le tableau répertorie uniquement les ports entrants ; les ports sortants sont généralement déterminés par le système d'exploitation et utilisent des numéros sans relation. L'information sur les ports sortants n'est généralement pas nécessaire aux fins énumérées ci-dessus.

Certains de ces ports sont enregistrés auprès de l'IANA (Internet Assigned Numbers Authority). De plus amples informations sur ces attributions sont disponibles sur https://www.iana.org/assignments/port-numbers ; toutefois, les informations détenues par l'IANA ne reflètent pas toujours l'usage actuel des ports.

Par ailleurs, le système d'exploitation sur le VDA et Delivery Controller nécessitera des ports entrants pour son propre usage. Consultez la documentation Microsoft Windows pour plus de détails.

VDA, Delivery Controller et Director

Composant	Utilisation	Protocole	Port entrant par défaut	Remarques
VDA	ICA/HDX	TCP, UDP	1494	Avec le protocole EDT, 1494 doit être ouvert pour UDP. Consultez la section Paramètres de stratégie ICA.

Composant	Utilisation	Protocole	Port entrant par défaut	Remarques
VDA	ICA/HDX avec fiabilité de session	TCP, UDP	2598	Avec le protocole EDT, 2598 doit être ouvert pour UDP. Consultez la section Paramètres de stratégie ICA.
VDA	ICA/HDX sur TLS	TCP	443	Tous les Citrix Receiver
VDA	ICA/HDX sur WebSocket	TCP	8008	Citrix Receiver pour HTML5 et Citrix Receiver pour Chrome 1.6 et versions antérieures uniquement
VDA	Transport en temps réel audio ICA/HDX sur UDP	UDP	16500..16509	
VDA	ICA/HDX Framehawk	UDP	3224-3324	
VDA	ICA/Serveur d'impression universelle	TCP	7229	Utilisé par l'écouteur CGP (Common Gateway Protocol) du flux de données d'impression Serveur d'impression universelle.

Composant	Utilisation	Protocole	Port entrant par défaut	Remarques
VDA	ICA/Universal Print Server	TCP	8080	Utilisé par l'écouteur Serveur d'impression universelle pour les requêtes HTTP/SOAP entrantes.
VDA	Wake On LAN	UDP	9	Gestion de l'alimentation Remote PC Access
VDA	Proxy de mise en éveil	TCP	135	Gestion de l'alimentation Remote PC Access
VDA	Delivery Controller	TCP	80	
Delivery Controller	VDA, StoreFront, Director, Studio	TCP	80	
Delivery Controller	StoreFront, Director, Studio sur TLS	TCP	443	
Delivery Controller	Delivery Controller, VDA	TCP	89	Cache d'hôte local (cette utilisation du port 89 pourrait changer dans les prochaines versions.)
Delivery Controller	Orchestration	TCP	9095	Orchestration
Director	Delivery Controller	TCP	80, 443	

Système de licences Citrix

Les ports suivants sont utilisés pour les licences Citrix.

Composant	Utilisation	Protocole	Port entrant par défaut
Serveur de licences	Serveur de licences	TCP	27000
Serveur de licences	Serveur de licences pour Citrix (démon vendeur)	TCP	7279
Serveur de licences	License Administration Console	TCP	8082
Serveur de licences	Web Services for Licensing	TCP	8083

HDX

February 28, 2019

> **Avertissement**
>
> Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Citrix HDX intègre une large gamme de technologies conçues pour apporter une expérience utilisateur haute définition.

Sur la machine :

HDX utilise les capacités informatiques des machines utilisateur pour améliorer et optimiser l'expérience utilisateur. La technologie HDX offre aux utilisateurs un rendu fluide et transparent du contenu multimédia disponible sur leur bureau ou application virtuels. Le contrôle de l'espace de travail permet aux utilisateurs de suspendre les applications et les bureaux virtuels et de continuer à travailler à partir d'une autre machine, à l'endroit où ils l'ont laissé.

Sur le réseau :

HDX offre des fonctionnalités d'accélération et d'optimisation pour mettre à disposition les meilleures performances réseau, y compris sur les connexions à faible bande passante ou en réseau étendu présentant une forte latence.

Les fonctionnalités HDX s'adaptent aux modifications de l'environnement. Elles équilibrent les performances et la bande passante. Elles appliquent les meilleures technologies possibles à chaque scénario, que le bureau ou l'application soit accessible localement sur le réseau d'entreprise ou à distance, en dehors du pare-feu de l'entreprise.

Dans le data center :

HDX utilise la puissance de calcul et de l'évolutivité des serveurs de façon à offrir des performances graphiques avancées, quelles que soient les capacités de la machine utilisateur.

La surveillance du canal HDX, fournie par Citrix Director, affiche le statut des canaux HDX connectés sur les machines utilisateur.

HDX Insight

HDX Insight est l'intégration de NetScaler Network Inspector et de Performance Manager avec Director. Il capture des données sur le trafic ICA et offre un tableau de bord des données en temps réel et historiques. Ces données comprennent la latence de session ICA côté client et côté serveur, l'utilisation de bande passante des canaux ICA et la durée des boucles ICA de chaque session.

Bénéficiez des capacités HDX de votre bureau virtuel

- Découvrez comment la redirection Flash, une des trois technologies de redirection multimédia HDX, accélère la mise à disposition de contenu multimédia Adobe Flash :
  1. Téléchargez le lecteur Adobe Flash (https://get.adobe.com/flashplayer/) et installez-le sur le bureau virtuel et la machine utilisateur.
  2. Sur la barre d'outils de Desktop Viewer, sélectionnez **Préférences**. Dans la boîte de dialogue Préférences de Desktop Viewer, sélectionnez l'onglet **Flash** puis sélectionnez **Optimiser le contenu**.
  3. Pour bénéficier de la manière dont la redirection Flash accélère la mise à disposition du contenu Flash multimédia vers des bureaux virtuels, affichez une vidéo sur votre bureau à partir d'un site Web contenant des vidéos Flash, comme YouTube. La Redirection Flash est transparente, si bien que les utilisateurs ne savent pas quand elle s'exécute. Vous pouvez toutefois vérifier si la Redirection Flash est utilisée. Recherchez un bloc de couleur qui apparaît momentanément avant le démarrage du lecteur Flash ou en cliquant avec le bouton droit sur la vidéo et en recherchant la Redirection Flash dans le menu.
- Voir comment HDX diffuse l'audio à définition élevée :

1. Configurez le client Citrix pour une qualité audio maximale ; consultez la documentation relative à Citrix Receiver pour plus de détails.
2. Lire les fichiers musicaux à l'aide d'un lecteur audio numérique (tels que iTunes) sur votre bureau.

HDX offre des graphiques et une expérience vidéo supérieurs pour la plupart des utilisateurs par défaut, sans configuration requise. Les paramètres de stratégie Citrix qui offrent la meilleure expérience possible à la plupart des cas d'utilisation sont activés par défaut.

- HDX sélectionne automatiquement la meilleure méthode de mise à disposition basée sur le client, la plate-forme, l'application et la bande passante réseau, puis ajuste le tout basé sur la modification des conditions.
- HDX optimise les performances de graphiques 2D et 3D et de la vidéo.
- HDX permet aux machines utilisateur de livrer en streaming des fichiers multimédia directement à partir du fournisseur source sur Internet ou l'intranet, plutôt qu'au travers du serveur hôte. Si la configuration requise pour la récupération de contenu côté client n'est pas présente, la diffusion de contenu multimédia revient à la redirection multimédia et à la récupération de contenu côté serveur. En général, aucune modification des stratégies de fonctionnalité de la redirection multimédia n'est nécessaire.
- HDX diffuse des vidéos riches en contenu, générées par le serveur, sur les bureaux virtuels lorsque la redirection multimédia n'est pas disponible : afficher une vidéo sur un site Web contenant des vidéos haute définition, par exemple, https://www.microsoft.com/silverlight/iis-smooth-streaming/demo/.

À savoir

- Pour plus d'informations sur la prise en charge et la configuration requise pour les fonctionnalités HDX, consultez l'article Configuration système requise. Sauf mention contraire, les fonctionnalités HDX sont disponibles pour la prise en charge des machines avec OS de serveur Windows et avec OS de bureau Windows et les bureaux Remote PC Access.
- Ce contenu décrit comment optimiser davantage l'expérience utilisateur, améliorer l'extensibilité du serveur ou réduire les besoins en bande passante. Pour de plus amples informations sur l'utilisation des stratégies Citrix et des paramètres de stratégie, consultez la documentation relative aux stratégies Citrix pour cette version.
- Pour obtenir des instructions qui incluent la modification du Registre, faites attention : la modification du Registre peut entraîner de sérieux problèmes qui pourraient nécessiter la réinstallation de votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Limitation

Lorsque vous utilisez le lecteur Windows Media avec RAVE activé dans une session, un écran noir peut s'afficher si vous effectuez un clic droit sur le contenu de la vidéo et sélectionnez **Lecture en cours toujours visible**.

Reconnexion automatique des clients et fiabilité de session

Lors de l'accès à des applications ou bureaux hébergés, une interruption du réseau peut se produire. Pour bénéficier d'une reconnexion plus fluide, nous offrons la reconnexion automatique des clients et la fiabilité de session. Dans une configuration par défaut, la fiabilité de session commence, puis la reconnexion automatique des clients suit.

Reconnexion automatique des clients :

La reconnexion automatique des clients relance le moteur client pour reconnecter une session déconnectée. La fonction de reconnexion automatique des clients ferme (ou déconnecte) la session utilisateur après la durée spécifiée dans le paramètre. Si la reconnexion automatique des clients est en cours, le système envoie à l'utilisateur une notification d'interruption du réseau pour les applications et les bureaux comme suit :

- **Bureaux.** La fenêtre de session est grisée et un minuteur affiche le temps restant avant la reconnexion.
- **Les applications.** La fenêtre de session se ferme et une boîte de dialogue s'affiche avec un minuteur qui indique le temps restant avant les tentatives de reconnexion.

Lors d'une reconnexion automatique de client, les sessions redémarrent en supposant une connectivité réseau. L'utilisateur ne peut pas interagir avec les sessions pendant que la reconnexion automatique des clients est en cours.

À la reconnexion, les sessions déconnectées se reconnectent à l'aide des informations de connexion enregistrées. L'utilisateur peut interagir normalement avec les applications et bureaux.

Paramètres de reconnexion automatique des clients par défaut :

- Délai de reconnexion automatique des clients : 120 secondes
- Reconnexion automatique des clients : activée
- Authentification de la reconnexion automatique des clients : désactivée
- Journalisation de la reconnexion automatique des clients : désactivée

Pour plus d'informations, consultez la section Paramètres de stratégie Reconnexion automatique des clients.

Fiabilité de session :

La fiabilité de session reconnecte les sessions ICA en toute transparence pour toutes les interruptions réseau. La fonction de fiabilité de session ferme (ou déconnecte) la session utilisateur après la durée spécifiée dans le paramètre. Après l'expiration du délai de fiabilité de session, les paramètres de reconnexion automatique des clients s'appliquent et la fonction tente d'opérer la reconnexion de l'utilisateur à la session déconnectée. Lorsque la fiabilité de session est en cours, une notification d'interruption du réseau pour les applications et les bureaux est envoyée comme suit à l'utilisateur :

- **Bureaux.** La fenêtre de session devient translucide et un minuteur affiche le temps restant avant la reconnexion.
- **Les applications.** La fenêtre devient translucide et des messages de connexion interrompue s'affichent depuis la zone de notification.

Lorsque la fiabilité de session est active, l'utilisateur ne peut pas interagir avec les sessions ICA. Toutefois, les actions utilisateur telles que les frappes au clavier sont mises en mémoire tampon pendant quelques secondes immédiatement après l'interruption du réseau et retransmises une fois que le réseau est disponible.

À la reconnexion, le client et le serveur reprennent au point où ils se trouvaient dans leur échange de protocole. Les fenêtres de session ne sont plus translucides et des messages de zone de notification appropriés s'affichent pour les applications.

Paramètres de fiabilité de session par défaut

- Expiration de délai de la fiabilité de session : 180 secondes
- Niveau de transparence de l'interface durant la reconnexion : 80 %
- Connexion de fiabilité de session : activée
- Numéro de port de la fiabilité de session

Pour plus d'informations, consultez la section Paramètres de stratégie Fiabilité de session.

NetScaler avec reconnexion automatique des clients et fiabilité de session :

Si les stratégies Multi-Stream et Multi-Port sont activées sur le serveur et que tout ou partie de ces informations sont vraies, la reconnexion automatique des clients ne fonctionne pas :

- La fonction de fiabilité de session est désactivée sur NetScaler Gateway.
- Un basculement est effectué sur le boîtier NetScaler.
- NetScaler SD-WAN est utilisé avec NetScaler Gateway.

Mode tablette pour appareils à écran tactile

Par défaut, tout appareil tactile qui se connecte à/suit un VDA Windows 10 démarre en mode tablette.

Le mode tablette nécessite au minimum la version XenServer 7.2. XenServer 7.2 s'intègre au VDA XenDesktop, modifiant l'hyperviseur pour activer les paramètres de microprogramme virtuel pour les appareils 2-en-1. Windows 10 charge le pilote GPIO sur la machine virtuelle

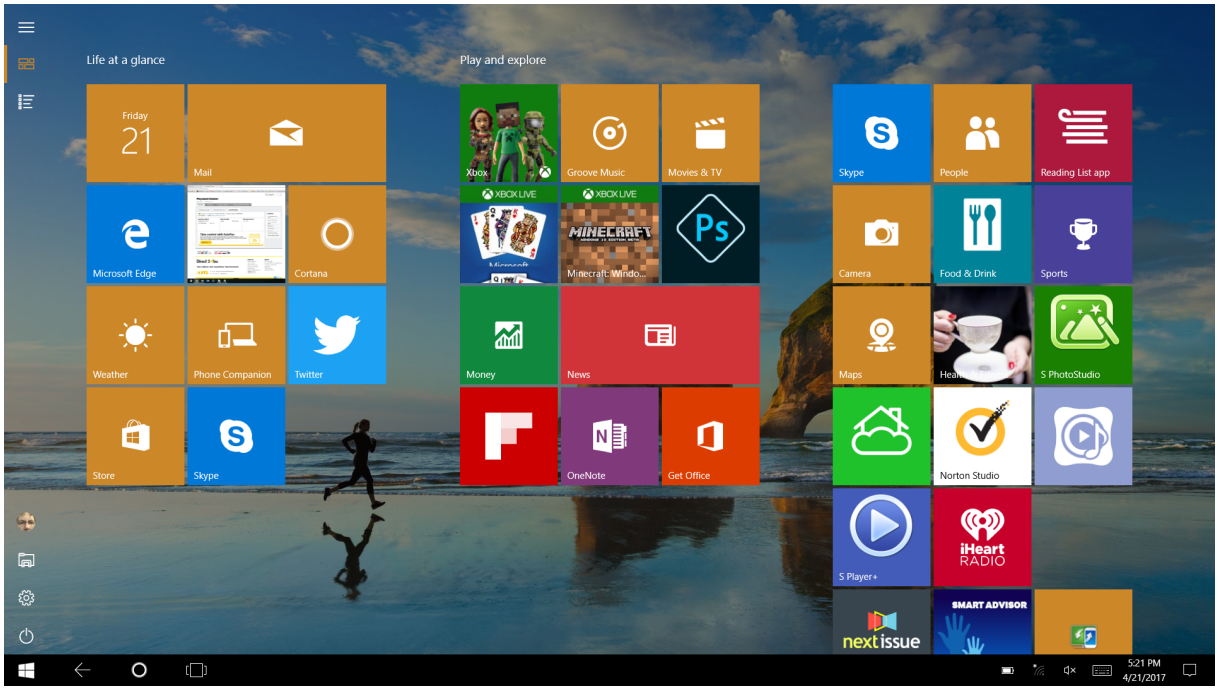
cible en fonction de ce BIOS mis à jour. Il est utilisé pour basculer entre les modes de tablette et de bureau dans la machine virtuelle. Pour plus d'informations, veuillez consulter l'article https:/docs.citrix.com/en-us/xenserver/current-release/downloads/release-notes.pdf.

Le mode tablette offre une interface utilisateur qui est mieux adaptée aux écrans tactiles :

- Boutons légèrement plus grands.
- L'écran de démarrage et les applications que vous démarrez s'ouvrent en mode plein écran.
- La barre des tâches contient un bouton Précédent.
- Les icônes sont retirées de la barre des tâches.

Vous avez accès à l'Explorateur de fichiers.

Les Web Receiver ne prennent pas en charge le mode tablette.



Exécutez la commande CLI XenServer pour permettre le basculement ordinateur portable/tablette :

```
xe vm-param-set uuid=\<VM\\_UUID\> platform:acpi\\_laptop\\_slate=1
```

Pour désactiver activer le mode tablette, configurez ce paramètre de Registre sur XenApp et XenDesktop :

HKEY_LOCAL_MACHINE\Software\Citrix\Sessions

Nom : CitrixEnhancedUserExperience
Type : REG_DWORD

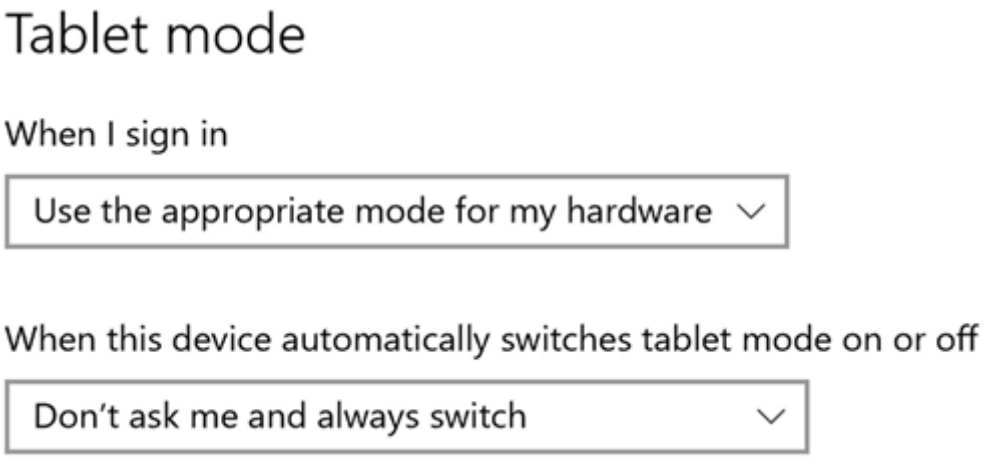
Valeur :
0 (Désactiver)
1 (Activer)

Avant de démarrer une session :

Nous vous recommandons d'accéder à **Paramètres > Système > Mode tablette** sur le VDA avant le démarrage d'une session et de définir les options suivantes dans les menus déroulants :

- Utiliser le mode approprié à mon matériel
- Ne pas me demander et toujours changer de mode

Si vous ne définissez pas ces options avant de démarrer la session, définissez les options une fois que vous avez démarré la session et redémarré le VDA.



Améliorer la qualité d'image envoyée aux machines utilisateur

Les paramètres de stratégie d'affichage visuel suivants contrôlent la qualité des images envoyées depuis des bureaux virtuels vers les machines utilisateur.

- Qualité visuelle. Contrôle la qualité visuelle des images affichées sur la machine utilisateur : moyenne, élevée, toujours sans perte, sans perte si possible (valeur par défaut = moyenne). La qualité de la vidéo avec le paramètre par défaut « moyenne » dépend de la bande passante disponible.
- Taux de trames cible. Spécifie le nombre maximal de trames par seconde envoyées depuis le bureau virtuel vers la machine utilisateur (valeur par défaut = 30). Pour les périphériques avec des UC plus lents, la spécification d'une valeur inférieure permet d'améliorer l'expérience de l'utilisateur. Le taux maximal pris en charge est 60 trames par seconde.
- Limite de mémoire d'affichage. Spécifie la taille maximale de la mémoire tampon vidéo (en kilo-octets) pour la session (valeur par défaut = 65536 Ko). Pour les connexions nécessitant un nombre de couleurs et une résolution élevés, augmentez la limite. Vous pouvez calculer la mémoire maximale nécessaire.

Améliorer les performances de conférence vidéo

Plusieurs applications de visioconférence populaires sont optimisées pour la mise à disposition à partir de XenApp et XenDesktop via la redirection multimédia (voir, par exemple, le pack d'optimisation HDX RealTime). Pour les applications qui ne sont pas optimisées, la compression vidéo de webcam HDX permet d'améliorer l'efficacité de la bande passante et la tolérance à la latence pour les webcams durant la visioconférence dans une session. Cette technologie livre en streaming le trafic de webcam sur un canal virtuel multimédia dédié. Cette technologie utilise moins de bande passante par rapport à la prise en charge de la redirection USB Plug-n-Play HDX isochrone et fonctionne bien sur des connexions en réseau étendu.

Toutefois, les utilisateurs de Citrix Receiver peuvent remplacer le comportement par défaut en choisissant le paramètre Mic & Webcam de Desktop Viewer : **Ne pas utiliser mon micro ou ma webcam**. Pour empêcher les utilisateurs de basculer depuis la compression vidéo de webcam HDX, désactivez la redirection du périphérique USB en utilisant les paramètres de stratégie sous ICA > Périphériques USB.

La compression vidéo de webcam HDX nécessite que les paramètres de stratégie suivants soient activés (tous sont activés par défaut).

- Redirection audio cliente
- Redirection du microphone client
- Conférences multimédia
- Redirection Windows Media

Si une webcam prend en charge le codage matériel H.264, la compression vidéo HDX utilise le codage matériel par défaut. Le codage matériel peut consommer plus de bande passante que le logiciel de codage. Pour forcer la compression logicielle, ajoutez la valeur de clé DWORD suivante pour la clé de Registre HKCU\Software\Citrix\HdxRealTime: DeepCompress_ForceSWEncode=1.

Priorités du trafic réseau

Les priorités sont attribuées au trafic réseau sur plusieurs connexions pour une session à l'aide de routeurs prenant en charge la qualité de service (QoS). Quatre flux TCP (en temps réel, interactifs, arrière-plan et en bloc) et deux flux UDP (pour la voix et pour la communication à distance d'écran Framehawk) sont disponibles pour transporter le trafic ICA entre la machine utilisateur et le serveur. Chaque canal virtuel est associé à une priorité spécifique et transporté dans la connexion correspondante. Vous pouvez définir les canaux indépendamment, en fonction du numéro de port TCP utilisé pour la connexion.

Les connexions en streaming de canal multiples sont prises en charge pour les Virtual Delivery Agents (VDA) installés sur les machines Windows 10, Windows 8 et Windows 7. Travaillez avec votre adminis-

trateur réseau pour vous assurer que les ports CGP configurés dans le paramètre Stratégie Multi-Port sont correctement attribués sur les routeurs réseau.

La qualité de service n'est prise en charge que lorsque des ports de fiabilité de session multiples, ou des ports CGP, sont configurés.

> **Avertissement :**
>
> lors de l'utilisation de cette fonctionnalité, assurez-vous que le transport est sécurisé. Citrix vous recommande d'utiliser Internet Protocol Security (IPsec) ou Transport Layer Security (TLS). Les connexions TLS sont prises en charge uniquement lorsque les connexions traversent une passerelle NetScaler Gateway qui prend en charge Multi-Stream ICA. Sur un réseau d'entreprise interne, les connexions multi-stream avec TLS ne sont pas prises en charge.

Pour définir la qualité de service pour plusieurs connexions en streaming, ajoutez les paramètres de stratégie Citrix suivants pour une stratégie (voir Paramètres de stratégie Connexions Multi-Stream pour plus de détails) :

- Stratégie Multi-Port : ce paramètre spécifie les ports pour le trafic ICA au travers de plusieurs connexions et établit des priorités de réseau.
  - Sélectionnez une priorité dans la liste Priorité de port CGP par défaut. Par défaut, le port principal (2598) a une priorité élevée.
  - Entrez des ports CGP supplémentaires dans Port1 CGP, port2 CGP et port3 CGP le cas échéant et attribuez-leur des priorités. Chaque port doit disposer d'une priorité unique.

  Configurez explicitement les pare-feu sur les VDA pour autoriser le trafic TCP supplémentaire.
- Paramètre d'ordinateur Multi-Stream : ce paramètre est désactivé par défaut. Si vous utilisez Citrix NetScaler SD-WAN et que le Multi-Stream est pris en charge dans votre environnement, il n'est pas nécessaire de configurer ce paramètre. Configurez ce paramètre de stratégie lorsque vous utilisez des routeurs tiers ou des Branch Repeater d'ancienne génération pour réaliser la qualité de service désirée.
- Paramètre utilisateur Multi-Stream : ce paramètre est désactivé par défaut.

Pour que les stratégies contenant ces paramètres soient appliquées, les utilisateurs doivent fermer leur session, puis ouvrir une session sur le réseau.

Mappage de clavier Unicode

Citrix Receiver non Windows utilise la disposition du clavier local (Unicode). Si un utilisateur modifie la disposition du clavier local et la disposition du clavier du serveur (code d'analyse), il se peut qu'ils ne soient pas synchronisés et que la sortie soit incorrecte. Par exemple, Utilisateur1 modifie la disposition du clavier local de l'anglais vers l'allemand. Utilisateur1 change ensuite le clavier côté serveur vers

l'allemand. Même si les deux dispositions de clavier sont en allemand, il se peut qu'elles ne soient pas synchronisées, ce qui entraîne une sortie de caractère incorrecte.

Activer ou désactiver le mappage de disposition du clavier Unicode :

Par défaut, la fonctionnalité est désactivée sur le VDA. Pour activer la fonctionnalité, utilisez l'éditeur de registre regedit sur le VDA.
Sous HKEY_LOCAL_MACHINE/SOFTWARE/Citrix, créez la clé CtxKlMap.
Définissez la valeur DWORD de EnableKlMap = 1

Pour désactiver cette fonctionnalité, définissez la valeur DWORD EnableKlMap = 0 ou supprimez la clé CtxKlMap.

Activer le mode compatible de mappage de disposition du clavier Unicode :

Par défaut, le mappage de disposition du clavier Unicode effectue automatiquement un hooking sur certaines API de Windows pour recharger le nouveau mappage de disposition de clavier Unicode lorsque vous modifiez la disposition du clavier côté serveur. Certaines applications ne peuvent pas être accrochées dans le cadre d'un hooking. Pour conserver la compatibilité, vous pouvez modifier la fonctionnalité vers le mode compatible pour prendre en charge ces applications non accrochées.

1. Sous la clé HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap, définissez la valeur DWORD DisableWindowHook = 1.
2. Pour utiliser le mappage de disposition du clavier Unicode normal, définissez la valeur DWORD DisableWindowHook = 0.

Informations connexes

- Graphiques
- Multimédia
- Redirection de contenu générale
- Transport adaptatif

Transport adaptatif

February 28, 2019

Introduction

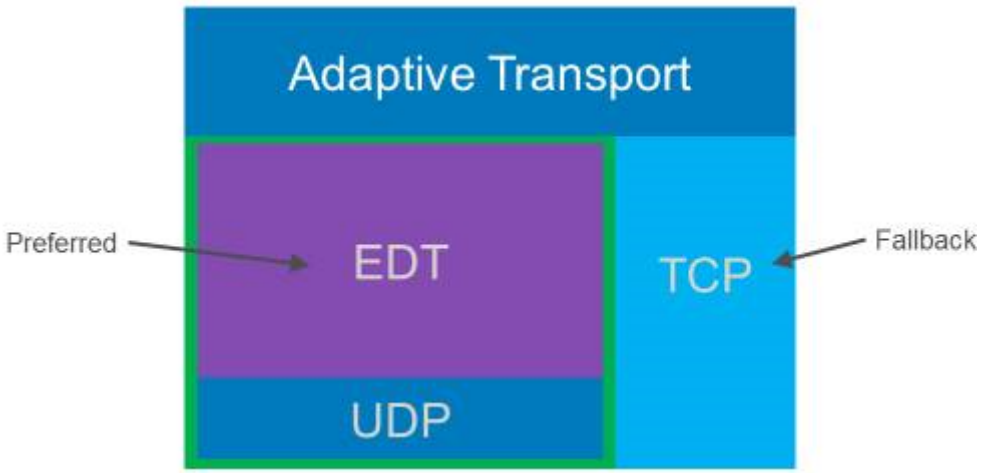
Le transport adaptatif est un nouveau mécanisme de transport de données pour XenApp et XenDesktop. Plus rapide et plus évolutif, il améliore l'interactivité avec les applications et il est plus adapté aux connexions WAN et Internet longue distance difficiles. Le transport adaptatif assure une capacité

à monter en charge élevée du serveur et une utilisation efficace de la bande passante. Le transport adaptatif permet aux canaux virtuels ICA de répondre automatiquement aux conditions changeantes du réseau. Les canaux basculent intelligemment entre le nouveau protocole Citrix appelé Enlightened Data Transport (EDT) et TCP afin d'offrir des performances optimales. Cela améliore le transfert de données pour tous les canaux virtuels ICA, y compris la communication à distance d'écran Thinwire, le transfert de fichiers (mappage des lecteurs clients), l'impression et la redirection multimédia. Le même paramètre s'applique aux conditions LAN et WAN.

Lorsque l'option est définie sur **Préféré**, le transfert de données via EDT est utilisé et revient sur TCP.

Par défaut, le transport adaptatif est défini sur **Désactivé** et TCP est toujours utilisé.

À des fins de test, vous pouvez définir le **Mode de diagnostic** ; dans ce cas, seul EDT est utilisé, et le retour vers TCP est désactivé.



Interopérabilité avec l'optimisation WAN de Citrix SD-WAN

L'optimisation WAN de Citrix SD-WAN (WANOP) offre une compression à jetons intersession (déduplication des données), y compris la mise en cache vidéo basée sur l'URL. WANOP permet une réduction significative de la bande passante si, dans un bureau, plusieurs personnes regardent la même vidéo récupérée par le client ou transfèrent ou impriment des parties significatives du même fichier ou document. En outre, en exécutant les processus de réduction des données ICA et de compression des travaux d'impression au niveau de l'appliance de la succursale, WANOP décharge l'UC du serveur VDA et permet une plus grande capacité à monter en charge des serveurs XenApp et XenDesktop.

> **Important :**
>
> lorsque TCP est utilisé comme protocole de transport de données, Citrix WANOP prend en charge les optimisations décrites dans le paragraphe précédent. Lorsque vous utilisez Citrix WANOP sur des connexions réseau, choisissez TCP. En utilisant le contrôle de flux et le contrôle d'encombrement TCP, WANOP assure une interactivité équivalente à EDT avec une latence

> élevée et une perte de paquets modérée.

Configuration requise et considérations

- XenApp et XenDesktop : version minimale 7.13
- VDA pour OS de bureau : version minimale 7.13
- VDA pour OS de serveur : version minimale 7.13
- StoreFront : version minimale 3.9
- Citrix Receiver pour Windows : version minimale 4.7
- Citrix Receiver pour Mac : version minimale 12.5
- Citrix Receiver pour iOS : version minimale 7.2
- Citrix Receiver pour Linux : version 13.6 pour les connexions VDA directes uniquement et 13.7 pour la prise en charge DTLS à l'aide de NetScaler Gateway (ou DTLS for les connexions VDA directes)
- Citrix Receiver pour Android : version 3.12.3 pour les connexions VDA directes uniquement et 3.13 pour la prise en charge DTLS à l'aide de NetScaler Gateway (ou DTLS for les connexions VDA directes)
- VDA IPv4 uniquement. Les configurations IPv6 et IPv4/IPv6 ne sont pas prises en charge.
- NetScaler : version minimale 11.1-51.21 Pour de plus amples informations sur la configuration de NetScaler, consultez la section Configuration de NetScaler Gateway pour prendre en charge le transport adaptatif.

Configuration

1. Installez XenApp et XenDesktop.
2. Installez StoreFront.
3. Installez le VDA (pour OS de bureau ou OS de serveur).
4. Installez Citrix Receiver pour Windows (Citrix Receiver pour Mac ou Citrix Receiver pour iOS).
5. Dans Studio, activez le paramètre de stratégie HDX Adaptive Transport (il est désactivé par défaut). Nous recommandons de ne pas activer cette fonctionnalité en tant que stratégie universelle pour tous les objets du site.
    - Pour activer le paramètre de stratégie, définissez la valeur sur Préféré et cliquez sur OK.
        - **Préféré.** Le transport adaptatif via EDT est utilisé autant que possible, avec retour vers TCP.
        - **Mode de diagnostic.** EDT est activé par défaut avec retour sur TCP s'il est désactivé. Nous vous recommandons de n'utiliser ce paramètre qu'à des fins de dépannage.
        - **Désactivé.** TCP est activé par défaut avec retour sur EDT s'il est désactivé.
6. Cliquez sur Suivant, et suivez les étapes de l'assistant.

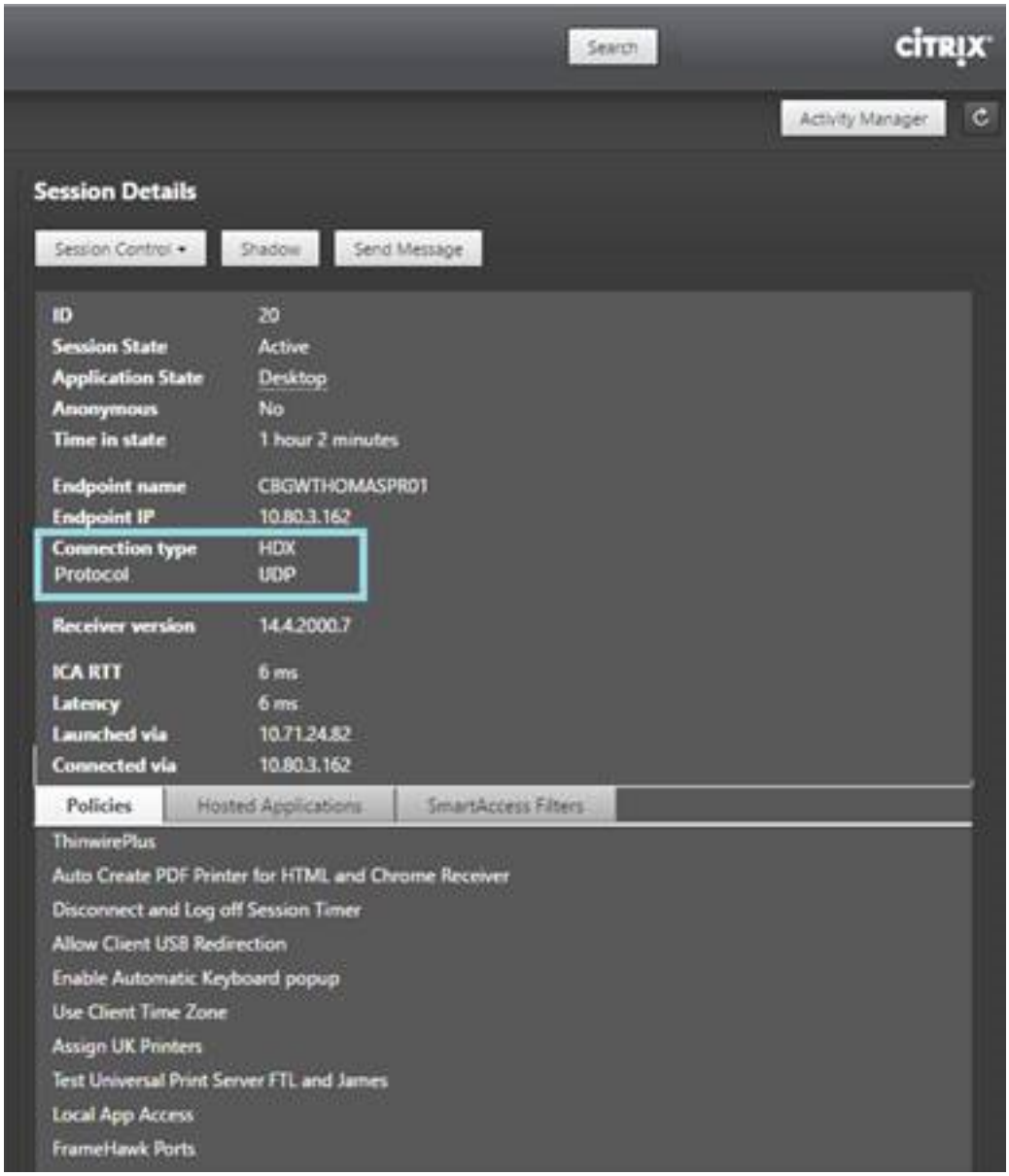
7. La stratégie prend effet lorsque l'utilisateur se reconnecte à la session ICA. Bien que cela ne soit pas obligatoire, vous pouvez exécuter **gpupdate /force** pour extraire le paramètre de stratégie du serveur, mais l'utilisateur doit toujours se reconnecter à la session ICA.
8. Démarrez une session à partir d'un Citrix Receiver pris en charge pour établir une connexion à l'aide du transport adaptatif.
9. Pour un accès en externe sécurisé, configurez le cryptage DTLS sur NetScaler Unified Gateway. Pour de plus amples informations, consultez la section Configuration de NetScaler Gateway pour prendre en charge Englightened Data Transport.

Pour confirmer que le paramètre de stratégie est appliqué :

- Vérifiez que les services UDP ICA sont activés sur un VDA à l'aide de netstat -a**.
- Vérifiez que les canaux virtuels sont en cours d'exécution sur EDT à l'aide de **Director** ou utilisez l'utilitaire de ligne de commande **CtxSession.exe** disponible sur le VDA.

Exemple Director :

Dans Director, **Détails de la session > Type de connexion** affiche les paramètres de stratégie. Recherchez le type de connexion **HDX**. Si le protocole est **UDP**, EDT est actif pour la session. Si le protocole est **TCP**, la session est en mode de retour ou mode par défaut. Si le type de connexion est **RDP**, ICA n'est pas utilisé et le protocole est **S/O**. Pour de plus amples informations, consultez la section Contrôler les sessions.



Exemple CtxSession.exe :

Cet exemple montre que EDT sur UDP est actif pour la session. Dans la ligne de commande, tapez CtxSession.exe.

C:\Program Files (x86)\Citrix\System32>CtxSession

Protocoles de transport Session 2 : UDP > CGP > ICA

Pour afficher des statistiques détaillées, utilisez l'option -v :

```
CtxSession -v
```


Installer et configurer

November 30, 2018

Consultez les articles référencés avant de démarrer chaque étape de déploiement, de façon à être informé sur ce que vous voyez et sélectionnez lors du déploiement.

Utilisez la séquence suivante pour déployer XenApp ou XenDesktop.

Préparer

Consultez Préparer l'installation et effectuez toutes les tâches nécessaires.

- Où trouver des informations sur les concepts, les fonctionnalités, les différences avec les versions antérieures, la configuration système requise et les bases de données.
- Considérations à prendre en compte lorsque vous choisissez où vous allez installer les composants principaux.
- Autorisations et configuration Active Directory requise.
- Informations sur les programmes d'installation, outils et interfaces disponibles.

Installer les composants principaux

Installez Delivery Controller, Citrix Studio, Citrix Director, le serveur de licences et Citrix StoreFront. Pour de plus amples informations, consultez Installer les composants principaux ou Installer à l'aide de la ligne de commande.

Créer un site

Après avoir installé les composants principaux et démarré Studio, vous êtes automatiquement invité à créer un site.

Installer un ou plusieurs Virtual Delivery Agents (VDA)

Installez un VDA sur une machine exécutant un système d'exploitation Windows, soit sur une image principale soit directement sur chaque machine. Consultez Installer des VDA ou Installer à l'aide de la ligne de commande. Des exemples de scripts sont fournis si vous souhaitez installer des VDA à l'aide d'Active Directory.

Pour les machines avec un système d'exploitation Linux, suivez les instructions dans Virtual Delivery Agent Linux.

Pour un déploiement Remote PC Access, installez un VDA pour OS de bureau sur chaque PC de bureau. Si vous n'avez besoin que des services VDA principaux, utilisez le programme d'installation VDAWorkstationCoreSetup.exe autonome et vos méthodes ESD (distribution électronique de logiciels) existantes. (Préparer l'installation contient des informations complètes sur les programmes d'installation de VDA disponibles.)

Installer les autres composants facultatifs

Si vous prévoyez d'utiliser le serveur d'impression universelle Citrix, installez son composant serveur sur vos serveurs d'impression. Consultez Installer les composants principaux ou Installer à l'aide de la ligne de commande.

Pour permettre à StoreFront d'utiliser des options d'authentification telles que les assertions SAML, installez le Service d'authentification fédérée de Citrix.

Pour donner aux utilisateurs un plus grand contrôle sur leurs comptes d'utilisateur, installez la réinitialisation en libre-service des mots de passe. Consultez la documentation Réinitialisation en libre-service des mots de passe pour plus d'informations.

Si vous le souhaitez, vous pouvez intégrer d'autres composants Citrix dans votre déploiement XenApp ou XenDesktop.

- Provisioning Services est un composant facultatif de XenApp et XenDesktop qui provisionne les machines en livrant en streaming une image principale vers les machines cibles.
- Citrix NetScaler Gateway est une solution garantissant un accès sécurisé aux applications. Grâce à des stratégies de contrôle d'accès et d'action avancées, elle permet aux administrateurs de renforcer l'accès aux applications et données.
- Citrix NetScaler SD-WAN est un ensemble d'appliances qui permet d'optimiser les performances du réseau étendu.

Pour obtenir des instructions d'installation, consultez la documentation accompagnant ces composants, fonctionnalités et technologies.

Créer un catalogue de machines

Lorsque vous créez un site dans Studio, vous êtes guidé dans la création d'un catalogue de machines.

Un catalogue peut contenir des machines physiques ou virtuelles (VM). Les machines virtuelles peuvent être créées à partir d'une image principale. Si vous utilisez un hyperviseur ou un service de cloud pour fournir des machines virtuelles, vous créez d'abord une image principale sur cet hôte. Ensuite, lorsque vous créez le catalogue, vous spécifiez cette image, qui est utilisée lors de la création de machines virtuelles.

Créer un groupe de mise à disposition

Lorsque vous créez votre premier catalogue de machines dans Studio, vous êtes guidé dans la création d'un groupe de mise à disposition.

Un groupe de mise à disposition spécifie quels utilisateurs peuvent accéder aux machines dans un catalogue spécifique et les applications disponibles pour ces utilisateurs.

Créer un groupe d'applications (facultatif)

Lorsque vous créez un groupe de mise à disposition, vous pouvez également créer un groupe d'applications. Vous pouvez créer des groupes d'applications pour les applications qui sont partagées entre différents groupes de mise à disposition ou utilisées par un sous-ensemble d'utilisateurs au sein de groupes de mise à disposition.

Préparer l'installation

March 6, 2019

Le déploiement de XenApp et XenDesktop commence par l'installation des composants suivants. Ce processus prépare la mise à disposition d'applications et de bureaux auprès des utilisateurs se trouvant *au sein de* votre pare-feu.

- Un ou plusieurs Delivery Controller
- Citrix Studio
- Citrix Director
- Citrix StoreFront
- Serveur de licences Citrix
- Un ou plusieurs Citrix Virtual Delivery Agents (VDA)
- Composants et technologies facultatifs tels que le serveur d'impression universelle, le service d'authentification fédérée et la réinitialisation en libre-service des mots de passe

Pour les utilisateurs *en dehors* de votre pare-feu, installez et configurez un composant supplémentaire, tel que NetScaler. Pour une introduction à l'utilisation de NetScaler avec StoreFront, consultez la sectionIntégrer XenApp et XenDesktop avec NetScaler Gateway.

Comment installer les composants

Vous pouvez utiliser le programme d'installation du produit entier sur l'image ISO de XenApp et XenDesktop pour déployer plusieurs composants et technologies. Vous pouvez utiliser un programme

d'installation de VDA autonome pour installer les VDA. Tous les programmes d'installation offrent des interfaces graphique et de ligne de commande. Voir Programmes d'installation.

L'ISO du produit contient des exemples de scripts qui permettent d'installer, mettre à niveau ou supprimer les VDA pour les machines dans Active Directory. Vous pouvez également utiliser les scripts pour gérer les images principales utilisées par Machine Creation Services (MCS) et Provisioning Services (PVS). Pour de plus amples informations, consultez Installer les VDA à l'aide de scripts.

En tant qu'alternative automatisée à l'utilisation des programmes d'installation, Citrix Smart Tools utilise des plans pour créer un déploiement XenApp et XenDesktop. Pour plus d'informations, consultez la documentation produit Smart Tools.

Informations à consulter avant l'installation

- Vue d'ensemble technique : si vous ne connaissez pas le produit et ses composants.
- Modifications apportées dans 7.x : si vous migrez depuis un déploiement XenApp 6.x ou XenDesktop 5.6 vers la version actuelle.
- Sécurité : lors de la planification de votre environnement de déploiement.
- Problèmes connus : problèmes que vous êtes susceptibles de rencontrer dans cette version.
- Bases de données : pour en apprendre davantage sur les bases de données du système et leur configuration. Lors de l'installation du Controller, vous pouvez installer SQL Server Express pour l'utiliser en tant que base de données du site. Vous configurez la plupart des informations de base de données lorsque vous créez un site, après avoir installé les composants principaux.
- Remote PC Access : si vous déployez un environnement qui permet à vos utilisateurs d'accéder à distance à leurs machines physiques de bureau.
- Connexions et ressources : si vous utilisez un hyperviseur ou un service de cloud pour héberger ou provisionner des machines virtuelles pour les applications et bureaux. Vous pouvez configurer la première connexion lorsque vous créez un site (après avoir installé les composants principaux). Configurez votre environnement de virtualisation à tout moment au préalable.
- Microsoft System Center Configuration Manager : si vous utilisez ConfigMgr pour gérer l'accès aux applications et bureaux, ou si vous utilisez la fonctionnalité Wake-on-LAN avec Remote PC Access.

Emplacement d'installation des composants

ConsultezConfiguration système requisepour connaître les plates-formes, systèmes d'exploitation et versions pris en charge. Les composants requis sont installés automatiquement, sauf indication contraire. Consultez la documentation relative à Citrix StoreFront et au serveur de licences Citrix pour connaître les plates-formes prises en charge et les composants requis.

Vous pouvez installer les composants principaux sur le même serveur ou sur des serveurs différents.

- L'installation de tous les composants principaux sur un seul serveur peut fonctionner pour les déploiements d'évaluation, de test ou de production de petite taille.
- Il est peut être avisé d'installer les composants sur des serveurs différents en prévision d'une expansion future. Par exemple, l'installation de Studio sur une autre machine que le serveur sur lequel vous avez installé le Controller vous permet de gérer le site à distance.
- Pour la plupart des déploiements de production, l'installation des composants principaux sur des serveurs distincts est recommandée.

Vous pouvez installer un Delivery Controller et un VDA pour OS de serveur sur le même serveur. Lancez le programme d'installation et sélectionnez le Delivery Controller (ainsi que tout autre composant principal que vous souhaitez sur cette machine). Ensuite, lancez de nouveau le programme d'installation et sélectionnez le Virtual Delivery Agent pour OS de serveur.

Assurez-vous que chaque système d'exploitation dispose des dernières mises à jour. Par exemple, l'installation d'un Controller sur Windows Server 2012 R2, ou d'un VDA sur Windows 8.1 ou Windows Server 2012 R2 échoue si la mise à jour Windows KB2919355 n'a pas été installée.

Assurez-vous que les horloges système de toutes les machines sont synchronisées. L'infrastructure Kerberos qui sécurise la communication entre les machines requiert une synchronisation.

Le guide d'optimisation pour les machines Windows 10 est disponible dans l'article CTX216252.

Emplacements d'installation des composants non pris en charge

- N'installez pas les composants sur un contrôleur de domaine Active Directory.
- L'installation d'un Controller sur un nœud dans une installation de mise en cluster SQL Server, de mise en miroir SQL Server où sur un serveur exécutant Hyper-V n'est pas prise en charge.
- N'installez pas Studio sur un serveur exécutant XenApp 6.5 Feature Pack 2 pour Windows Server 2008 R2 ou toute version antérieure de XenApp.

Autorisations et configuration Active Directory requise

Vous devez être un utilisateur du domaine et un administrateur local sur les machines sur lesquelles vous installez les composants.

Pour utiliser le programme d'installation de VDA autonome, vous devez disposer de privilèges d'administrateur ou utiliser **Exécuter en tant qu'administrateur**.

Configurez votre domaine Active Directory avant de procéder à l'installation.

- La section Configuration système requise répertorie les niveaux fonctionnels d'Active Directory pris en charge. La section Active Directory contient des informations supplémentaires.
- Vous devez disposer d'au moins un contrôleur de domaine exécutant les services de domaine Active Directory.
- N'installez pas les composants XenApp ou XenDesktop sur un contrôleur de domaine.

- N'utilisez pas de barre oblique (/) lorsque vous spécifiez les noms d'unité d'organisation dans Studio.

Le compte d'utilisateur Windows utilisé pour installer le serveur de licences Citrix est automatiquement configuré en tant qu'administrateur complet d'administration déléguée sur le serveur de licences.

Informations supplémentaires :

- Bonnes pratiques en matière de sécurité
- Administration déléguée
- Documentation Microsoft sur la configuration d'Active Directory

Instructions d'installation, considérations et meilleures pratiques

Lors de l'installation d'un composant

En général, si un composant requiert certains éléments, le programme d'installation déploie ces derniers s'ils ne sont pas présents. Certains éléments requis peuvent nécessiter un redémarrage de la machine.

Lorsque vous créez des objets avant, pendant et après l'installation, spécifiez des noms uniques pour chaque objet. Par exemple, fournissez des noms uniques pour les réseaux, groupes, catalogues et ressources.

Si un composant n'est pas installé correctement, l'installation s'arrête et un message d'erreur s'affiche. Les composants installés correctement sont conservés. Vous n'avez pas besoin de les réinstaller.

Des données d'analyse sont collectées lorsque vous installez (mettez à niveau) les composants. Par défaut, ces données sont téléchargées automatiquement vers Citrix lorsque l'installation est terminée. Par ailleurs, lorsque vous installez des composants, vous êtes automatiquement inscrit au Programme d'amélioration de l'expérience utilisateur Citrix (CEIP), qui télécharge des données anonymes. Lors de l'installation, vous pouvez également choisir de participer à d'autres technologies Citrix (telles que Smart Tools) qui collectent les diagnostics pour le dépannage et la maintenance. Pour de plus amples informations sur ces programmes, consultez Citrix Insight Services.

Lors de l'installation de VDA

Citrix Receiver pour Windows est inclus par défaut lorsque vous installez un VDA (sauf si vous utilisez le programme d'installation VDAWorkstationCoreSetup.exe). Vous pouvez exclure Citrix Receiver de l'installation. Vous ou vos utilisateurs pouvez télécharger et installer (et mettre à niveau) les versions ultérieures de ce Citrix Receiver et d'autres Citrix Receiver à partir du site Web de Citrix. Vous pouvez aussi mettre à disposition ces Citrix Receiver à partir de votre serveur StoreFront. Consultez la section

Mettre à disposition des fichiers d'installation Citrix Receiver sur le serveur, ou le contenu équivalent dans la version de StoreFront que vous utilisez.

Le service Spouleur d'impression est activé par défaut sur les serveurs Windows pris en charge. Si vous désactivez ce service, vous ne pouvez pas installer correctement un VDA pour OS de serveur Windows ; assurez-vous donc que ce service est activé avant d'installer un VDA.

La plupart des éditions Windows prises en charge sont fournies avec Microsoft Media Foundation. Si la machine sur laquelle vous installez un VDA n'est pas dotée de Media Foundation (éditions N par exemple), plusieurs fonctionnalités multimédia ne seront pas installées et ne fonctionneront pas. Vous pouvez accepter cette limitation, ou mettre fin à l'installation du VDA et la redémarrer plus tard, après l'installation de Media Foundation. Dans l'interface graphique, ce choix est présenté dans un message. Dans la ligne de commande, vous pouvez utiliser /no_mediafoundation_ack pour confirmer la limitation.

Lorsque vous installez le VDA, un nouveau groupe d'utilisateurs locaux appelé Direct Access Users est créé automatiquement. Sur un VDA pour OS de bureau, ce groupe s'applique uniquement aux connexions RDP. Sur un VDA pour OS de serveur, ce groupe s'applique aux connexions ICA et RDP.

Le VDA doit avoir des adresses Controller valides avec lesquelles communiquer. Sinon, les sessions ne peuvent pas être établies. Vous pouvez spécifier les adresses Controller lorsque vous installez le VDA ou ultérieurement. Mais surtout n'oubliez pas, car cette opération est indispensable !

Redémarrages après et lors de l'installation de VDA

Un redémarrage est requis à la fin de l'installation du VDA. Ce redémarrage se produit automatiquement par défaut.

Pour minimiser le nombre de redémarrages requis durant l'installation de VDA :

- Assurez-vous qu'une version de .NET Framework prise en charge est installée avant d'installer le VDA.
- Pour les machines équipées d'un OS de serveur Windows, installez et activez les services de rôle RDS avant d'installer le VDA.

Si vous n'installez pas les composants requis avant d'installer le VDA :

- Si vous utilisez l'interface graphique ou l'interface de ligne de commande sans l'option /noreboot, la machine redémarre automatiquement après l'installation des composants requis.
- Si vous utilisez l'interface de ligne de commande avec l'option /noreboot, vous devez lancer le redémarrage.

Après chaque redémarrage, réexécutez le programme d'installation ou la commande pour poursuivre l'installation du VDA.

Programmes d'installation

Programme d'installation du produit entier

À l'aide du programme d'installation du produit entier, fourni dans XenApp et XenDesktop, vous pouvez :

- installer, mettre à niveau ou supprimer des composants principaux de XenApp et XenDesktop : Delivery Controller, Studio, Director, StoreFront, le serveur de licences ;
- installer ou mettre à niveau des VDA Windows pour systèmes d'exploitation de serveur ou de bureau ;
- installer le composant Ups Server du Serveur d'impression universelle sur vos serveurs d'impression ;
- installer le Service d'authentification fédérée ;
- installer le service de réinitialisation en libre-service des mots de passe.

Pour mettre à disposition un bureau depuis un OS de serveur pour un utilisateur unique (par exemple, à des fins de développement Web), utilisez l'interface de ligne de commande du programme d'installation du produit entier. Pour de plus amples informations, consultez la section Server VDI.

Programmes d'installation de VDA autonomes

Les programmes d'installation de VDA autonomes sont disponibles sur les pages de téléchargement de Citrix. Les programmes d'installation de VDA autonomes sont beaucoup plus petits que l'image ISO du produit complet. Ils conviennent aux déploiements qui :

- utilisent des packages ESD (distribution électronique de logiciels) qui sont préparés ou copiés localement ;
- incluent des machines physiques ;
- incluent des bureaux à distance.

Par défaut, les fichiers contenus dans le pack VDA autonome auto-extractible sont extraits dans le dossier Temp. L'espace disque nécessaire sur la machine lors de l'extraction sur le dossier Temp est plus important que lors de l'utilisation du programme d'installation du produit entier. Toutefois, les fichiers extraits dans le dossier Temp sont automatiquement supprimés après la fin de l'installation. Vous pouvez aussi utiliser la commande /extract avec un chemin d'accès absolu.

Trois programmes d'installation de VDA autonomes sont disponibles en téléchargement.

VDAServerSetup.exe

Installe un VDA pour OS de serveur. Il prend en charge toutes les options de VDA pour OS de serveur qui sont disponibles avec le programme d'installation du produit entier.

VDAWorkstationSetup.exe

Installe un VDA pour OS de bureau. Il prend en charge toutes les options de VDA pour OS de bureau qui sont disponibles avec le programme d'installation du produit entier.

VDAWorkstationCoreSetup.exe

Installe un VDA pour OS de bureau qui est optimisé pour les déploiements Remote PC Access ou les installations VDI de base. Remote PC Access utilise des machines physiques. Les installations VDI de base sont des machines virtuelles qui ne sont pas utilisées en tant qu'image principale. Seuls les services fondamentaux nécessaires aux connexions VDA de tels déploiements sont installés. Par conséquent, il ne prend en charge qu'un sous-ensemble des options qui sont valides avec les programmes d'installation (VDAWorkstationSetup).

Ce programme d'installation n'installe pas et ne contient pas les composants utilisés pour :

- App-V.
- Profile Management. L'exclusion de Citrix Profile Management de l'installation affecte les écrans de Citrix Director. Pour plus amples informations, consultez la section Installer des VDA.
- Machine Identity Service.
- Personal vDisk ou AppDisks.

Le programme d'installation **VDAWorkstationCoreSetup.exe** n'installe pas et ne contient pas Citrix Receiver pour Windows.

L'utilisation de **VDAWorkstationCoreSetup.exe** équivaut à l'utilisation du programme d'installation du produit entier ou **VDAWorkstationSetup.exe** pour installer un VDA avec OS de bureau et :

- Dans l'interface graphique : en sélectionnant l'option Remote PC Access sur la page **Environnement** de Citrix Receiver et en désactivant la case à cocher sur la page **Composants**.
- Dans l'interface de ligne de commande : en spécifiant les options /remotepc et /components vda.
- Dans l'interface de ligne de commande : en spécifiant /components vda et /exclude "Citrix Personalization for App-V - VDA" "Personal vDisk" "Machine Identity Service" "Citrix User Profile Manager" "Citrix User Profile Manager WMIPlugin".

Vous pouvez installer les composants/fonctionnalités omis ultérieurement en réexécutant le programme d'installation du produit entier. Cette action installe tous les composants manquants.

Environnements de virtualisation Microsoft Azure Resource Manager

January 23, 2019

Suivez ce guide si vous utilisez Microsoft Azure Resource Manager pour provisionner des machines virtuelles dans votre déploiement XenApp ou XenDesktop.

Vous pouvez configurer XenApp ou XenDesktop pour provisionner des ressources dans Azure Resource Manager lorsque vous créez le site XenApp ou XenDesktop (qui comprend la création d'une connexion), ou lorsque vous créez une connexion hôte plus tard (après la création du site).

Vous devriez vous familiariser avec les informations suivantes :

- Azure Active Directory : https://azure.microsoft.com/en-us/documentation/articles/active-directory-howto-tenant/
- Infrastructure Consent : https://azure.microsoft.com/en-us/documentation/articles/active-directory-integrating-applications/
- Principal de service : https://azure.microsoft.com/en-us/documentation/articles/active-directory-application-objects/

Azure Disk Encryption n'est pas pris en charge lors de l'utilisation de Machine Creation Services.

Créer une connexion à Azure Resource Manager

Consultez les articles Créer un site et Connexions et ressources pour des informations complètes sur les pages dans les assistants de création d'un site ou d'une connexion. Les informations suivantes traitent uniquement d'informations spécifiques aux connexions de Azure Resource Manager.

Il existe deux méthodes permettant d'établir une connexion hôte avec Azure Resource Manager :

- S'authentifier auprès d'Azure Resource Manager pour créer un nouveau principal de service.
- Utiliser les détails d'un principal de service créé précédemment pour se connecter à Azure Resource Manager.

S'authentifier auprès d'Azure Resource Manager pour créer un nouveau principal de service

Avant de commencer, assurez-vous que :

- Vous disposez d'un compte utilisateur dans le locataire Azure Active Directory de votre abonnement.
- Le compte d'utilisateur Azure AD est également un co-administrateur pour l'abonnement Azure que vous utiliserez pour les ressources de provisioning.

Dans l'assistant Création d'un site ou Ajouter une connexion et des ressources :

1. Sur la page **Connexion**, sélectionnez le type de connexion **Microsoft Azure** et votre environnement Azure.

2. Sur la page **Détails de la connexion**, entrez votre ID d'abonnement Azure et un nom pour la connexion. Le nom de la connexion peut contenir entre 1 et 64 caractères, et ne peut pas contenir uniquement des espaces ou les caractères \/;:#.*?=<>|[]{}"'()'). Lorsque vous entrez l'ID d'abonnement et le nom de connexion, le bouton **Créer nouveau** est activé.
3. Entrez le nom d'utilisateur et le mot de passe du compte Azure Active Directory.
4. Cliquez sur **Connexion**.
5. Cliquez sur **Accepter** pour accorder les autorisations indiquées à XenApp ou XenDesktop. XenApp ou XenDesktop crée un principal de service qui lui permet de gérer les ressources Azure Resource Manager pour le compte d'utilisateur spécifié.
6. Lorsque vous cliquez sur **Accepter**, vous revenez à la page **Connexion** dans Studio. Notez que lorsque vous avez réussi à vous authentifier auprès d'Azure, les boutons **Créer nouveau** et **Utiliser existant** sont remplacés par **Connecté**, et une coche verte indique la réussite de la connexion à votre abonnement Azure.
7. Indiquez les outils à utiliser pour créer les machines virtuelles, puis cliquez sur **Suivant**. (vous ne pouvez pas progresser au-delà de cette page de l'assistant tant que vous n'avez pas réussi à vous authentifier auprès d'Azure et accepté d'accorder les autorisations nécessaires).

Les ressources comprennent la région et le réseau.

- Sur la page **Région**, sélectionnez une région.
- Sur la page **Réseau** :
  - tapez un nom de ressources comportant entre 1 et 64 caractères pour vous aider à identifier la combinaison région/réseau dans Studio. Un nom de ressource ne peut pas contenir uniquement des espaces, et ne peut pas contenir les caractères \/;:#.*?=<>|[]{}"'()'.
  - Sélectionnez une paire réseau virtuel et groupe de ressources (étant donné que vous pouvez posséder plusieurs réseaux virtuels avec le même nom, le couplage du nom du réseau avec le groupe de ressources fournit des combinaisons uniques). Si, sur la page précédente, vous avez sélectionné une région qui ne dispose pas de réseaux virtuels, vous devez retourner à cette page et sélectionner une région contenant des réseaux virtuels.

Suivez les instructions de l'assistant.

Utiliser les détails d'un principal de service créé précédemment pour se connecter à Azure Resource Manager

Pour créer un principal de service manuellement, connectez-vous à votre abonnement Azure Resource Manager et utilisez les applets de commande PowerShell fournies ci-dessous.

Conditions préalables :

- $SubscriptionId : ID d'abonnement Azure Resource Manager pour l'abonnement sur lequel vous souhaitez provisionner les VDA.
- $AADUser : compte utilisateur Azure AD pour le locataire AD de votre abonnement.

- Définissez $AADUser comme co-administrateur pour votre abonnement.
- $ApplicationName : nom pour l'application à créer dans Azure Active Directory.
- $ApplicationPassword : mot de passe pour l'application. Vous utiliserez ce mot de passe comme secret de l'application lors de la création de la connexion hôte.

Pour créer un principal de service :

Étape 1 : connectez-vous à votre abonnement Azure Resource Manager.

```
1 Login-AzureRmAccount.
```

Étape 2 : sélectionnez l'abonnement Azure Resource Manager sur lequel vous souhaitez créer le principal de service.

```
1 Select-AzureRmSubscription -SubscriptionID $SubscriptionId;
```

Étape 3 : créez l'application dans votre locataire AD.

```
1 $AzureADApplication = New-AzureRmADApplication -DisplayName
    $ApplicationName -HomePage "https://localhost/$ApplicationName" -
    IdentifierUris https://$ApplicationName -Password
    $ApplicationPassword
```

Étape 4 : créez un principal de service.

```
1 New-AzureRmADServicePrincipal -ApplicationId $AzureADApplication.
    ApplicationId
```

Étape 5 : attribuez un rôle au principal de service.

```
1 New-AzureRmRoleAssignment -RoleDefinitionName Contributor -
    ServicePrincipalName $AzureADApplication.ApplicationId - scope /
    subscriptions/$SubscriptionId
```

Étape 6 : dans la sortie de la fenêtre de la console PowerShell, notez la valeur ApplicationId. Vous devez fournir cet ID lors de la création de la connexion hôte.

Dans l'assistant Création d'un site ou Ajouter une connexion et des ressources :

1. Sur la page **Connexion**, sélectionnez le type de connexion **Microsoft Azure** et votre environnement Azure.
2. Sur la page **Détails de la connexion**, entrez votre ID d'abonnement Azure et un nom pour la connexion. (Le nom de la connexion peut contenir entre 1 et 64 caractères, et ne peut pas contenir uniquement des espaces ou les caractères \/;:#.*?=<>|[]{}"'()').)
3. Cliquez sur **Utiliser existant**. Entrez l'ID d'abonnement, le nom de l'abonnement, l'URL d'authentification, l'URL de gestion, le suffixe de stockage, l'ID Active Directory ou l'ID du

locataire, l'ID de l'application et le secret de l'application du principal de service existant. Une fois que vous avez saisi les détails, le bouton **OK** est activé. Cliquez sur **OK**.

4. Indiquez les outils à utiliser pour créer les machines virtuelles, puis cliquez sur **Suivant**. Les informations que vous avez fournies sur le principal de service seront utilisées pour la connexion à votre abonnement Azure. (vous ne pouvez pas progresser au-delà de cette page de l'assistant tant que vous n'avez pas fourni d'informations sur l'option Utiliser existant).

Les ressources comprennent la région et le réseau.

- Sur la page **Région**, sélectionnez une région.
- Sur la page **Réseau** :
  - tapez un nom de ressources comportant entre 1 et 64 caractères pour vous aider à identifier la combinaison région/réseau dans Studio. Un nom de ressource ne peut pas contenir uniquement des espaces, et ne peut pas contenir les caractères \/;:#.*?=<>|[]{}"'()'.
  - Sélectionnez une paire réseau virtuel et groupe de ressources (étant donné que vous pouvez posséder plusieurs réseaux virtuels avec le même nom, le couplage du nom du réseau avec le groupe de ressources fournit des combinaisons uniques). Si, sur la page précédente, vous avez sélectionné une région qui ne dispose pas de réseaux virtuels, vous devez retourner à cette page et sélectionner une région contenant des réseaux virtuels.

Suivez les instructions de l'assistant.

Créer un catalogue de machines à l'aide d'une image principale Azure Resource Manager

Ces informations étayent les instructions disponibles dans l'article Créer des catalogues de machines.

Une image principale est le modèle qui sera utilisé pour créer les machines virtuelles dans un catalogue de machines. Avant de créer le catalogue de machines, créez une image principale dans Azure Resource Manager. Pour de plus amples informations sur les images principales en général, consultez l'article Créer des catalogues de machines.

Lorsque vous créez un catalogue de machines dans Studio :

- Les pages **Système d'exploitation** et **Gestion des machines** ne contiennent aucune information spécifique à Azure. Suivez les instructions de l'article Créer des catalogues de machines.
- Sur la page **Image principale**, sélectionnez un groupe de ressources et naviguez dans les conteneurs pour accéder au disque dur virtuel Azure que vous voulez utiliser en tant qu'image principale. Un VDA Citrix doit être installé sur le disque. Si le disque dur virtuel est connecté à une VM, la VM doit être arrêtée.
- La page **Types de stockage et de licence** s'affiche uniquement lors de l'utilisation de l'image principale Azure Resource Manager.

Sélectionnez un type de stockage : premium ou standard. Le type de stockage affecte les tailles de machine qui sont disponibles sur la page Machines virtuelles de l'assistant. Les deux types de stockage créent de multiples copies synchrones de vos données dans un seul data center. Pour de plus amples informations sur les types de stockage et la réplication de stockage Azure, consultez les rubriques suivantes :

https://azure.microsoft.com/en-us/documentation/articles/storage-introduction/

https://azure.microsoft.com/en-us/documentation/articles/storage-premium-storage/

https://azure.microsoft.com/en-us/documentation/articles/storage-redundancy/

Indiquez si vous souhaitez utiliser des licences Windows Server locales existantes. Si c'est le cas et que vous utilisez les images Windows Server locales existantes, Azure Hybrid Use Benefits (HUB) est utilisé. Plus de détails sont disponibles sur https://azure.microsoft.com/pricing/hybrid-use-benefit/.

HUB réduit les coûts d'exécution de VM dans Azure au taux de calcul de base, car les licences Windows Server supplémentaires de la galerie Azure sont gratuites. Vous devez inclure vos images Windows Server locales à Azure pour utiliser HUB. Les images de la galerie Azure ne sont pas prises en charge. Les licences Windows Client locales ne sont pas prises en charge. Veuillez consulter la section https://blogs.msdn.microsoft.com/azureedu/2016/04/13/how-can-i-use-the-hybrid-use-benefit-in-azure/.

Pour vérifier si les machines virtuelles provisionnées utilisent effectivement HUB, exécutez la commande PowerShell suivante

```
1  Get-AzureRmVM -ResourceGroup MyResourceGroup -Name MyVM
```

et vérifiez que le type de licence est Windows_Server. Des instructions supplémentaires sont disponibles sur https://azure.microsoft.com/en-us/documentation/articles/virtual-machines-windows-hybrid-use-benefit-licensing/.

- Sur la page **Machines virtuelles**, indiquez le nombre de machines virtuelles à créer ; vous devez spécifier au moins une. Sélectionnez une taille de machine. Une fois que vous avez créé un catalogue de machines, vous ne pouvez pas modifier la taille de machine. Si vous souhaitez changer de taille, supprimez le catalogue, puis créez un nouveau catalogue qui utilise la même image principale et spécifie la taille de machine souhaitée.

Les noms de machine virtuelle ne peuvent pas contenir de caractères non ASCII ou spéciaux.

- Les pages **Cartes réseau**, **Comptes d'ordinateurs** et **Résumé** ne contiennent aucune information spécifique à Azure. Suivez les instructions de l'article Créer des catalogues de machines.

Suivez les instructions de l'assistant.

Environnements de virtualisation Microsoft System Center Virtual Machine Manager

February 28, 2019

Suivez ce guide si vous utilisez Hyper-V avec Microsoft System Center Virtual Machine Manager (VMM) pour fournir des machines virtuelles.

Cette version prend en charge les versions de VMM indiquées dans l'article Configuration système requise.

Vous pouvez utiliser Machine Creation Services et Provisioning Services pour provisionner :

- Machines virtuelles avec OS de serveur ou de bureau génération 1
- Machines virtuelles Windows Server 2012 R2, Windows Server 2016 et Windows 10 génération 2 (avec ou sans démarrage sécurisé)

Mettre à niveau VMM

- Mise à niveau de VMM 2012 vers VMM 2012 SP1 ou VMM 2012 R2

  Pour la configuration requise pour les hôtes VMM et Hyper-V, voir https://technet.microsoft.com/en-us/library/gg610649.aspx. Pour la configuration requise pour la console VMM, voir https://technet.microsoft.com/en-us/library/gg610640.aspx.

  Un cluster Hyper-V mixte n'est pas pris en charge. Un exemple de cluster mixte est un cluster dans lequel la moitié du cluster exécute Hyper-V 2008 et l'autre moitié exécute Hyper-V 2012.

- Mettre à niveau VMM 2008 R2 vers VMM 2012 SP1.

  Si vous effectuez une mise à niveau depuis XenDesktop 5.6 sur VMM 2008 R2, suivez cette séquence pour éviter l'interruption de XenDesktop.

  1. Mettre à niveau VMM 2012 (désormais exécutant XenDesktop 5,6 et VMM 2012) ;
  2. Mettre à niveau XenDesktop vers la version la plus récente (désormais exécutant la dernière version de XenDesktop et de VMM 2012)
  3. Mettre à niveau VMM de 2012 à 2012 SP1 (exécutant désormais XenDesktop et VMM 2012 SP1)

- Mise à niveau de VMM 2012 SP1 vers VMM 2012 R2

  Si vous démarrez depuis XenDesktop ou XenApp 7.x sur VMM 2012 SP1, suivez cette séquence pour éviter l'interruption de XenDesktop.

  1. Mettre à niveau XenDesktop ou XenApp vers la dernière version (désormais exécutant la dernière version de XenDesktop ou XenApp, et VMM 2012 SP1)

2. Mettre à niveau VMM 2012 SP1 vers 2012 R2 (désormais exécutant XenDesktop ou XenApp, et VMM 2012 R2)

Résumé de l'installation et de la configuration

1. Installez et configurez un hyperviseur.
   a) Installez Microsoft Hyper-V Server et VMM sur vos serveurs. Tous les Delivery Controller doivent se trouver dans la même forêt que les serveurs VMM.
   b) Installez la console System Center Virtual Machine Manager Console sur tous les Controller. La version de la console doit correspondre à la version du serveur de gestion. Bien qu'une console antérieure puisse se connecter au serveur de gestion, le provisioning des VDA échoue si les versions diffèrent.
   c) Vérifiez les informations de compte suivantes :
      - Le compte que vous utilisez pour spécifier des hôtes dans Studio est un administrateur VMM ou un administrateur VMM délégué pour les machines Hyper-V appropriées. Si ce compte possède uniquement le rôle d'administrateur délégué dans VMM, les données de stockage ne sont pas répertoriées dans Studio lors du processus de création de l'hôte.
      - Le compte d'utilisateur utilisé pour l'intégration de Studio doit également être un membre du groupe de sécurité Administrateurs local sur chaque serveur Hyper-V pour prendre en charge la gestion du cycle de vie des VM (telles que pour la création, la mise à jour et la suppression de VM).
        Remarque : l'installation du Controller sur un serveur exécutant Hyper-V n'est pas prise en charge.
2. Créez une VM principale.
   a) Installez Virtual Desktop Agent sur la VM principale, et sélectionnez l'option d'optimisation du bureau. Cela améliore les performances.
   b) Réalisez un instantané de la VM principale à utiliser comme sauvegarde.
3. Créez des bureaux virtuels. Si vous utilisez MCS pour créer des VM, lors de la création d'un site ou d'une connexion,
   a) sélectionnez le type d'hôte de virtualisation Microsoft.
   b) Entrez l'adresse en tant que nom de domaine complet du serveur hôte.
   c) Entrez les informations d'identification du compte d'administrateur créé préalablement disposant des permissions requises pour créer de nouvelles VM.
   d) Dans la boîte de dialogue Détails d'hôte, sélectionnez le cluster ou l'hôte autonome à utiliser pour créer vos nouvelles VM.
      Important :
      recherchez et sélectionnez un cluster ou un hôte autonome, même si vous utilisez un déploiement d'hôte Hyper-V unique.

MCS sur des partages de fichiers SMB 3

Pour les catalogues de machines créés avec MCS sur des partages de fichiers SMB 3 pour le stockage de VM, assurez-vous que les informations d'identification sont définies comme suit pour que des appels provenant de Hypervisor Communications Library (HCL) d'un Controller puissent se connecter avec succès au stockage SMB :

- Les informations d'identification de l'utilisateur VMM doivent inclure un accès en écriture complet au stockage SMB.
- Les opérations de disque virtuel de stockage pendant les événements du cycle de vie des VM sont effectuées par le biais du serveur Hyper-V à l'aide des informations d'identification de l'utilisateur VMM.

Lorsque vous utilisez SMB comme stockage, activez Authentication Credential Security Support Provider (CredSSP) du Controller sur différentes machines Hyper-V individuelles lors de l'utilisation de VMM 2012 SP1 avec Hyper-V sur Windows Server 2012. Pour obtenir davantage d'informations, veuillez consulter la section CTX137465.

À l'aide d'une session à distance PowerShell V3 standard, le HCL utilise CredSSP pour ouvrir une connexion à la machine Hyper-V. Cette fonctionnalité transmet des informations d'identification de l'utilisateur cryptées avec Kerberos à la machine Hyper-V, et les commandes PowerShell dans la session sur la machine Hyper-V distante exécutée avec les informations d'identification fournies (dans ce cas, celles de l'utilisateur VMM), de façon à ce que les commandes de communication vers le stockage fonctionnent correctement.

Les tâches suivantes utilisent des scripts PowerShell constituées initialement dans le HCL et sont alors envoyées à la machine Hyper-V pour agir sur le stockage SMB 3.0.

- **Consolider l'image principale :** une image principale crée un nouveau schéma de provisioning MCS (catalogue de machines). Il clone et écrase la VM principale en préparation pour la création de nouvelles VM à partir du nouveau disque créé (et supprime une dépendance sur la VM principale originale).

  ConvertVirtualHardDisk sur l'espace de noms root\virtualization\v2

  Exemple :

  ```
  1  $ims = Get-WmiObject -class $class -namespace "root\
         virtualization\v2";
  2  $result = $ims.ConvertVirtualHardDisk($diskName, $vhdastext)
  3  $result
  ```

- **Créer un disque de différence :** crée un disque de différence à partir de l'image principale générée par la consolidation de l'image principale. Le disque de différence est alors attaché à une nouvelle VM.

CreateVirtualHardDisk sur l'espace de noms root\virtualization\v2

Exemple :

```
$ims = Get-WmiObject -class $class -namespace "root\
    virtualization\v2";
$result = $ims.CreateVirtualHardDisk($vhdastext);
$result
```

- **Charger des disques d'identité :** le HCL ne peut pas directement charger le disque d'identité sur le stockage SMB. Par conséquent, la machine Hyper-V doit télécharger et copier le disque d'identité vers le stockage. Étant donné que la machine Hyper-V ne peut pas lire le disque à partir du Controller, HCL doit tout d'abord copier le disque d'identité via la machine Hyper-V comme suit.

  1. HCL télécharge l'identité de la machine Hyper-V via le partage d'administrateur.
  2. La machine Hyper-V copie le disque vers le stockage SMB via un script PowerShell exécuté dans la session à distance PowerShell. Un dossier est créé sur la machine Hyper-V et les permissions sur ce dossier sont verrouillées pour l'utilisateur VMM uniquement (via la connexion PowerShell distante).
  3. HCL supprime le fichier à partir du partage de l'administrateur.
  4. Lorsque le HCL termine le téléchargement du disque d'identité vers la machine Hyper-V, la session PowerShell distante copie les disques d'identité vers le stockage SMB puis le supprime de la machine Hyper-V.

     Le dossier du disque d'identité est recréé s'il est supprimé de façon à ce qu'il soit disponible pour une éventuelle réutilisation.

- **Télécharger des disques d'identité :** comme pour les chargements, les disques d'identité transitent via la machine Hyper-V vers le HCL. Le processus suivant permet de créer un dossier qui ne possède que des permissions utilisateur VMM sur le serveur Hyper-V s'il n'existe pas.

  1. La machine Hyper-V copie le disque à partir du stockage SMB vers le stockage Hyper-V local au travers d'un script PowerShell en cours d'exécution dans la session à distance PowerShell V3.
  2. HCL lit le disque depuis le partage administrateur de la machine Hyper-V dans la mémoire.
  3. HCL supprime le fichier à partir du partage de l'administrateur.

- **Création de Personal vDisk :** si l'administrateur crée les VM dans un catalogue de machine Personal vDisk, vous devez créer un disque vide (PvD).

  L'appel pour créer un disque vide ne nécessite pas d'accès direct au stockage. Si vous possédez des disques PvD qui résident sur différents stockages que le disque du système d'exploitation ou le système d'exploitation principal, puis utiliser le PowerShell à distance pour créer le disque

PvD dans un dossier de répertoire qui a le même nom que la VM à partir de laquelle il a été créé. Pour CSV ou LocalStorage, n'utilisez pas de PowerShell à distance. La création du répertoire avant de créer un disque vide évite l'échec de la commande VMM.

À partir de la machine Hyper-V, réalisez un mkdir sur le stockage.

Environnements Microsoft System Center Configuration Manager

January 23, 2019

Les sites qui utilisent Microsoft System Center Configuration Manager (Configuration Manager) pour gérer l'accès aux applications et bureaux sur les machines physiques peuvent étendre cette utilisation à XenApp ou XenDesktop via ces options d'intégration.

- **Citrix Connector 7.5 pour Configuration Manager 2012 :** Citrix Connector offre un pont entre Configuration Manager et XenApp ou XenDesktop. Le Connector vous permet d'unifier les opérations quotidiennes sur les environnements physiques que vous gérez avec Configuration Manager et les environnements virtuels que vous gérez avec XenApp ou XenDesktop. Pour de plus amples informations sur Connector, consultez Citrix Connector 7.5 pour System Center Configuration Manager 2012.
- **Fonctionnalité Configuration Manager Wake Proxy :** l'utilisation de la fonctionnalité Remote PC Access Wake on LAN requiert Configuration Manager. Pour de plus amples informations, consultez la section ci-dessous.
- **Propriété XenApp et XenDesktop :** les propriétés XenApp et XenDesktop vous permettent d'identifier les bureaux virtuels Citrix pour la gestion au travers de Configuration Manager. Ces propriétés sont automatiquement utilisées par Citrix Connector, mais elles peuvent également être configurées manuellement, comme décrit dans la section suivante.

Propriétés

Propriétés disponibles pour Microsoft System Center Configuration Manager pour gérer des bureaux virtuels.

Les propriétés booléennes affichées dans Configuration Manager peuvent apparaître sous la forme de 1 ou 0 au lieu de true ou false.

Les propriétés sont disponibles pour la classe Citrix_virtualDesktopInfo dans l'espace de noms Root\Citrix\DesktopInformation. Les noms des propriétés proviennent du fournisseur WMI (Windows Management Instrumentation) :

Propriété	Description
AssignmentType	Définit la valeur de IsAssigned. Les valeurs valides sont les suivantes : ClientIP, ClientName, None et User (définit *IsAssigned* sur True)
BrokerSiteName	Site ; renvoie la même valeur que HostIdentifier.
DesktopCatalogName	Catalogue de machines associé au bureau.
DesktopGroupName	Groupe de mise à disposition associé au bureau.
HostIdentifier	Site ; renvoie la même valeur que BrokerSiteName.
IsAssigned	True pour attribuer le bureau à un utilisateur, False pour un bureau aléatoire
IsMasterImage	Permet de prendre des décisions sur l'environnement. Par exemple, vous pouvez installer des applications sur l'image principale et non sur les machines provisionnées, particulièrement si ces machines sont dans un état propre au démarrage des machines. Les valeurs valides sont les suivantes : **True** sur une VM qui est utilisé comme une image principale (cette valeur est définie lors de l'installation basée sur une sélection) ; **Cleared** sur une VM qui est provisionnée à partir de cette image.
IsVirtualMachine	True pour une machine virtuelle, False pour une machine physique.
OSChangesPersist	False si l'image du système d'exploitation du bureau est réinitialisée à un nouvel état chaque fois qu'elle est redémarrée, sinon True.
PersistentDataLocation	Emplacement dans lequel le Gestionnaire de configuration stocke les données permanentes. Ceci n'est pas accessible aux utilisateurs.

Propriété	Description
PersonalvDiskDriveLetter	Pour un bureau comprenant un Personal vDisk, la lettre de lecteur que vous attribuez au Personal vDisk.
BrokerSiteName, DesktopCatalogName, DesktopGroupName et HostIdentifier	Déterminé lorsque le bureau s'enregistre auprès du Controller, ils ont la valeur de Null pour un bureau qui ne s'est pas complètement enregistré.

Pour collecter les propriétés, exécutez un inventaire matériel dans Configuration Manager. Pour afficher les propriétés, utilisez l'Explorateur de ressources Configuration Manager. Dans ce cas, il se peut que les noms incluent des espaces ou varient légèrement des noms de propriété. Par exemple, il se peut que **BrokerSiteName** s'affiche en tant que Broker Site Name.

- Configurer Configuration Manager pour collecter les propriétés Citrix WMI du VDA Citrix
- Créer des collections de machines basées sur une requête à l'aide des propriétés Citrix WMI
- Créer des conditions globales basées sur les propriétés Citrix WMI
- Utilisez les conditions globales pour définir les spécifications du type de déploiement de l'application

Vous pouvez également utiliser les propriétés Microsoft dans la classe Microsoft CCM_DesktopMachine dans l'espace de noms Root\ccm_vdi. Pour plus d'informations, veuillez consulter la documentation Microsoft.

Configuration Manager et Remote PC Access Wake on LAN

Pour configurer la fonctionnalité Remote PC Access Wake on LAN, procédez comme suit avant d'installer un VDA sur le PC de bureau et utilisez Studio pour créer ou mettre à jour le déploiement Remote PC Access :

- Configurez ConfigMgr 2012, 2012 R2 ou 2016 au sein de l'organisation. Déployez ensuite le client ConfigMgr sur toutes les machines Remote PC Access, tout en allouant un délai suffisant pour l'exécution du cycle d'inventaire SCCM programmé (ou en forcer un manuellement, si nécessaire). Les informations d'identification d'accès que vous avez spécifiées dans Studio pour configurer la connexion à ConfigMgr doivent inclure des collections dans l'étendue et le rôle d'opérateur des outils à distance.
- Pour activer la prise en charge d'Intel Active Management Technology (AMT) :
  - La version minimale prise en charge sur le PC doit être AMT 3.2.1.
  - Configurez le PC pour l'utilisation d'AMT avec des certificats et des processus de provisioning associés.

  - Seuls ConfigMgr 2012 et 2012 R2 peuvent être utilisés, et non ConfigMgr 2016.
- Pour ConfigMgr Wake Proxy et/ou la prise en charge de paquet magique :
  - Configurez Wake on LAN dans chacun des paramètres BIOS du PC.
  - Pour la prise en charge de Wake Proxy, activez l'option dans ConfigMgr. Pour chaque sous-réseau de l'organisation contenant les PC qui utiliseront la fonctionnalité Remote PC Access Wake on LAN, vérifiez que trois machines ou plus peuvent servir de machines sentinelles.
  - Pour une prise en charge de paquet magique, configurez des routeurs réseau et des pare-feu pour autoriser l'envoi des paquets magiques, en utilisant soit une diffusion dirigée vers un sous-réseau, soit une monodiffusion.

Une fois que vous avez installé le VDA sur les PC de bureau, activez ou désactivez la gestion de l'alimentation lorsque vous créez le déploiement Remote PC Access dans Studio.

- Si vous activez la gestion de l'alimentation, spécifiez les détails de connexion : l'adresse ConfigMgr et les informations d'identification d'accès et un nom.
- Si vous n'activez pas la gestion de l'alimentation, vous pouvez ajouter une connexion de gestion de l'alimentation (Configuration Manager) ultérieurement, puis modifier un catalogue de machines Remote PC Access pour activer la gestion de l'alimentation et spécifier la nouvelle connexion de gestion de l'alimentation.

Vous pouvez modifier la connexion de gestion de l'alimentation pour configurer l'utilisation de ConfigMgr Wake Proxy et des paquets magiques, ainsi que modifier la méthode de transmission des paquets.

Consultez Remote PC Access pour plus d'informations.

Environnements de virtualisation VMware

January 23, 2019

Suivez ce guide si vous utilisez VMware pour fournir des machines virtuelles.

Installez vCenter Server et les outils de gestion appropriés. (Aucune prise en charge n'est fournie pour l'opération vSphere vCenter Linked Mode.)

Si vous prévoyez d'utiliser MCS, ne désactivez pas la fonctionnalité de navigateur de banque de données dans vCenter Server (décrite dans https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2101567). Si vous désactivez cette fonctionnalité, MCS ne fonctionne pas correctement.

Privilèges requis

Créez un compte d'utilisateur VMware et un ou plusieurs rôles VMware avec un ensemble, ou la totalité, des privilèges répertoriés ci-dessous. Basez la création de rôles sur le niveau de granularité requis pour demander les diverses opérations de XenApp ou XenDesktop à tout moment. Pour accorder des permissions d'utilisateur spécifiques à tout moment, associez-les au rôle respectif, au niveau du centre de données au minimum.

Les tableaux suivants répertorient les correspondances entre les opérations XenApp and XenDesktop et les privilèges VMware requis au minimum.

Ajouter des connexions et des ressources

Kit de développement	Interface utilisateur
System.Anonymous, System.Read et System.View	Ajouté automatiquement. Peut utiliser le rôle lecture seule intégré.

Provisionner des machines (Machine Creation Services)

Kit de développement	**Interface utilisateur**
Datastore.AllocateSpace	Datastore > Allocate space
Datastore.Browse	Datastore > Browse datastore
Datastore.FileManagement	Datastore > Low level file operations
Network.Assign	Network > Assign network
Resource.AssignVMToPool	Resource > Assign virtual machine to resource pool
VirtualMachine.Config.AddExistingDisk	Virtual machine > Configuration > Add existing disk
VirtualMachine.Config.AddNewDisk	Virtual machine > Configuration > Add new disk
VirtualMachine.Config.AdvancedConfig	Virtual machine > Configuration > Advanced
VirtualMachine.Config.RemoveDisk	Virtual machine > Configuration > Remove disk
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Interact.PowerOn	Virtual machine > Interaction > Power On
VirtualMachine.Inventory.CreateFromExisting	Virtual machine > Inventory > Create from existing

Kit de développement	Interface utilisateur
VirtualMachine.Inventory.Create	Virtual machine > Inventory > Create new
VirtualMachine.Inventory.Delete	Virtual machine > Inventory > Remove
VirtualMachine.Provisioning.Clone	Virtual machine > Provisioning > Clone virtual machine
VirtualMachine.State.CreateSnapshot	vSphere 5.0, Update 2 and vSphere 5.1, Update 1: Virtual machine > State > Create snapshot. vSphere 5.5: Virtual machine > Snapshot management > Create snapshot

Si vous voulez que les VM que vous créez soient balisées, ajoutez les permissions suivantes pour le compte d'utilisateur.

Pour vous assurer que vous utilisez une nouvelle image de base pour créer de nouvelles VM, identifiez les VM créées avec Machine Creation Services pour les exclure de la liste des VM disponibles à utiliser en tant qu'images de base.

Kit de développement	Interface utilisateur
Global.ManageCustomFields	Global > Manage custom attributes
Global.SetCustomField	Global > Set custom attribute

Provisionner des machines (Provisioning Services)

Tous les privilèges de **Provisionner des machines (Machine Creation Services)** et ce qui suit.

Kit de développement	Interface utilisateur
VirtualMachine.Config.AddRemoveDevice	Virtual machine > Configuration > Add or remove device
VirtualMachine.Config.CPUCount	Virtual machine > Configuration > Change CPU Count
VirtualMachine.Config.Memory	Virtual machine > Configuration > Memory
VirtualMachine.Config.Settings	Virtual machine > Configuration > Settings
VirtualMachine.Provisioning.CloneTemplate	Virtual machine > Provisioning > Clone template

Kit de développement	Interface utilisateur
VirtualMachine.Provisioning.DeployTemplate	Virtual machine > Provisioning > Deploy template

Gestion de l'alimentation

Kit de développement	Interface utilisateur
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Interact.PowerOn	Virtual machine > Interaction > Power On
VirtualMachine.Interact.Reset	Virtual machine > Interaction > Reset
VirtualMachine.Interact.Suspend	Virtual machine > Interaction > Suspend

Mise à jour et restauration de l'image

Kit de développement	Interface utilisateur
Datastore.AllocateSpace	Datastore > Allocate space
Datastore.Browse	Datastore > Browse datastore
Datastore.FileManagement	Datastore > Low level file operations
Network.Assign	Network > Assign network
Resource.AssignVMToPool	Resource > Assign virtual machine to resource pool
VirtualMachine.Config.AddExistingDisk	Virtual machine > Configuration > Add existing disk
VirtualMachine.Config.AddNewDisk	Virtual machine > Configuration > Add new disk
VirtualMachine.Config.AdvancedConfig	Virtual machine > Configuration > Advanced
VirtualMachine.Config.RemoveDisk	Virtual machine > Configuration > Remove disk
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Interact.PowerOn	Virtual machine > Interaction > Power On
VirtualMachine.Interact.Reset	Virtual machine > Interaction > Reset
VirtualMachine.Inventory.CreateFromExisting	Virtual machine > Inventory > Create from existing

Kit de développement	Interface utilisateur
VirtualMachine.Inventory.Create	Virtual machine > Inventory > Create new
VirtualMachine.Inventory.Delete	Virtual machine > Inventory > Remove
VirtualMachine.Provisioning.Clone	Virtual machine > Provisioning > Clone virtual machine

Supprimer des machines provisionnées

Kit de développement	Interface utilisateur
Datastore.Browse	Datastore > Browse datastore
Datastore.FileManagement	Datastore > Low level file operations
VirtualMachine.Config.RemoveDisk	Virtual machine > Configuration > Remove disk
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Inventory.Delete	Virtual machine > Inventory > Remove

Créer des AppDisk

Valide pour VMware vSphere version 5.5 au minimum et XenApp et XenDesktop version 7.8 au minimum

Kit de développement	Interface utilisateur
Datastore.AllocateSpace	Datastore > Allocate space
Datastore.Browse	Datastore > Browse datastore
Datastore.FileManagement	Datastore > Low level file operations
VirtualMachine.Config.AddExistingDisk	Virtual machine > Configuration > Add existing disk
VirtualMachine.Config.AddNewDisk	Virtual machine > Configuration > Add new disk
VirtualMachine.Config.AdvancedConfig	Virtual machine > Configuration > Advanced
VirtualMachine.Config.EditDevice	Virtual machine > Configuration > Modify Device Settings
VirtualMachine.Config.RemoveDisk	Virtual machine > Configuration > Remove disk
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off

Kit de développement	Interface utilisateur
VirtualMachine.Interact.PowerOn	Virtual machine > Interaction > Power On

Supprimer des AppDisk

Valide pour VMware vSphere version 5.5 au minimum et XenApp et XenDesktop version 7.8 au minimum

Kit de développement	Interface utilisateur
Datastore.Browse	Datastore > Browse datastore
Datastore.FileManagement	Datastore > Low level file operations
VirtualMachine.Config.RemoveDisk	Virtual machine > Configuration > Remove disk
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off

Obtenir et importer un certificat

Pour protéger les communications vSphere, Citrix vous recommande d'utiliser HTTPS plutôt que HTTP. HTTPS requiert des certificats numériques. Citrix vous recommande d'utiliser un certificat numérique émis par une autorité de certification conformément à la stratégie de sécurité de votre organisation.

Si vous ne pouvez pas utiliser un certificat numérique émis par une autorité de certification et que la stratégie de sécurité de votre organisation le permet, vous pouvez utiliser le certificat auto-signé installé par VMware. Ajoutez le certificat VMware vCenter à chaque Controller.

ÉTAPE 1. Ajoutez le nom de domaine complet (FQDN) de l'ordinateur exécutant vCenter Server dans le fichier hôtes de ce serveur, situé à l'emplacement %SystemRoot%/WINDOWS/system32/Drivers/etc/. Cette étape est uniquement nécessaire que si le nom de domaine complet de l'ordinateur exécutant vCenter Server n'est pas déjà présent dans le DNS.

STEP 2. Obtenez le certificat vCenter à l'aide de l'une des trois méthodes suivantes :

Depuis le serveur vCenter :

1. Copiez le fichier rui.crt depuis le serveur vCenter vers un emplacement accessible sur vos Delivery Controller.
2. Sur le Controller, naviguez vers l'emplacement du certificat exporté et ouvrez le fichier rui.crt.

Téléchargez le certificat à l'aide d'un navigateur Web : si vous utilisez Internet Explorer, selon votre

compte utilisateur, il se peut que vous deviez cliquer avec le bouton droit de la souris sur Internet Explorer et choisir **Exécuter en tant qu'administrateur** pour pouvoir télécharger et installer le certificat.

1. Ouvrez votre navigateur Web et créez une connexion Web sécurisée vers le serveur vCenter (par exemple `https://server1.domain1.com`).
2. Acceptez les avertissements relatifs à la sécurité.
3. Cliquez sur la barre d'adresse sur laquelle l'erreur de certificat est affichée.
4. Affichez le certificat puis cliquez sur l'onglet Détails.
5. Sélectionnez **Copier dans un fichier puis effectuez l'exportation au format .CER**, en fournissant un nom lorsque vous êtes invité à le faire.
6. Enregistrez le certificat exporté.
7. Naviguez vers l'emplacement du certificat exporté et ouvrez le fichier .CER.

Importez directement depuis Internet Explorer exécuté en tant qu'administrateur :

1. Ouvrez votre navigateur Web et créez une connexion Web sécurisée vers le serveur vCenter (par exemple `https://server1.domain1.com`).
2. Acceptez les avertissements relatifs à la sécurité.
3. Cliquez sur la barre d'adresse sur laquelle l'erreur de certificat est affichée.
4. Affichez le certificat.

ÉTAPE 3. Importez le certificat dans le magasin de certificats sur chacun de vos Controller.

1. Cliquez sur **Installer le certificat**, sélectionnez **Machine locale**, puis cliquez sur **Suivant**.
2. Sélectionnez **Placer tous les certificats dans le magasin suivant**, puis cliquez sur **Parcourir**.

Sur Windows Server 2008 R2 : cochez la case **Afficher les magasins physiques**. Développez **Personnes autorisées**. Sélectionnez **Ordinateur local**. Cliquez sur **Suivant**, puis cliquez sur **Terminer**.

Sur une version ultérieure prise en charge : sélectionnez **Personnes autorisées** et cliquez sur **OK**. Cliquez sur **Suivant**, puis cliquez sur **Terminer**.

Important : si vous modifiez le nom du serveur vSphere après l'installation, vous devez générer un nouveau certificat auto-signé sur ce serveur avant d'importer le nouveau certificat.

Considérations liées à la configuration

Créer une VM principale :

Utilisez une VM principale pour fournir les bureaux et les applications des utilisateurs dans un catalogue de machines. Sur votre hyperviseur :

1. Installez un VDA sur la VM principale, en sélectionnant l'option d'optimisation du bureau, ce qui améliore les performances.
2. Réalisez un instantané de la MV principale à utiliser comme sauvegarde.

Créer une connexion :

Dans l'assistant de création de connexion :

- Sélectionnez le type de connexion VMware.
- Entrez l'adresse du point d'accès pour le kit de développement vCenter.
- Entrez les informations d'identification d'un compte d'utilisateur VMware configuré précédemment qui dispose des permissions nécessaires à la création de nouvelles VM. Spécifiez le nom d'utilisateur au format domaine/nomutilisateur.

Empreinte numérique SSL VMware

La fonctionnalité d'empreinte numérique SSL VMware résout une erreur fréquemment signalée lors de la création d'une connexion hôte sur un hyperviseur VMware vSphere. Précédemment, les administrateurs devaient créer manuellement une relation d'approbation entre les Delivery Controller du site et le certificat de l'hyperviseur avant de créer une connexion. La fonctionnalité d'empreinte numérique SSL VMware élimine cette opération manuelle : l'empreinte numérique du certificat non approuvé est stockée dans la base de données du site, de façon à ce que l'hyperviseur puisse être continuellement identifié comme approuvé par XenApp ou XenDesktop, même s'il ne l'est pas par les Controller.

Lors de la création d'une connexion hôte vSphere dans Studio, une boîte de dialogue vous permet d'afficher le certificat de la machine à laquelle vous vous connectez. Vous pouvez alors choisir de l'approuver.

Environnements de virtualisation Nutanix

November 6, 2018

Suivez ces instructions lors de l'utilisation de Nutanix Acropolis pour fournir des machines virtuelles dans votre déploiement XenApp ou XenDesktop. Le processus d'installation comprend les tâches suivantes :

- Installer et enregistrer le plug-in Nutanix dans votre environnement XenApp ou XenDesktop.
- Créer une connexion à l'hyperviseur Nutanix Acropolis.
- Créer un catalogue de machines qui utilise un instantané d'une image principale que vous avez créée sur l'hyperviseur Nutanix.

Pour de plus amples informations, consultez le Guide d'installation de plugin Nutanix Acropolix MCS, disponible sur le portail d'assistance Nutanix : https://portal.nutanix.com.

Pour plus d'informations sur la prise en charge de Nutanix et de Provisioning Services, consultez l'article du centre de connaissances CTX131239.

Installer et enregistrer le plug-in Nutanix

Après avoir installé les composants XenApp ou XenDesktop, complétez la procédure suivante pour installer et enregistrer le plug-in Nutanix sur les Delivery Controller. Vous pourrez ensuite utiliser Studio pour créer une connexion à l'hyperviseur Nutanix, puis créer un catalogue de machines qui utilise un instantané de l'image principale que vous avez créée dans l'environnement Nutanix.

1. Obtenez le plug-in Nutanix auprès de Nutanix, et installez-le sur les Delivery Controller.
2. Vérifiez qu'un dossier Nutanix Acropolis a été créé dans C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0.
3. Exécutez **C:\Program Files\Common Files\Citrix\HCLPlugins\RegisterPlugins.exe –PluginsRoot "C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0"**.
4. Redémarrez les services suivants : Citrix Host Service, Citrix Broker Service et Citrix Machine Creation Service.
5. Exécutez les applets de commande PowerShell suivantes pour vérifier que le plug-in Nutanix Acropolis a bien été enregistré :

   Add-PSSnapin Citrix*

   Get-HypHypervisorPlugin

Créer une connexion à Nutanix

Consultez les articles Créer un site et Connexions et ressources pour des informations complètes sur les pages dans les assistants de création d'une connexion.

Dans l'assistant Création d'un site ou Ajouter une connexion et des ressources, sélectionnez le type de connexion **Nutanix** sur la page **Connexion**, puis spécifiez l'adresse et les informations d'identification de l'hyperviseur, ainsi qu'un nom pour la connexion. Sur la page **Réseau**, sélectionnez un réseau pour l'unité d'hébergement.

Créer un catalogue de machines à l'aide d'un instantané Nutanix

Ces informations étayent les instructions disponibles dans l'article Créer des catalogues de machines. Elles décrivent uniquement les champs qui sont uniques à Nutanix.

L'instantané que vous sélectionnez représente le modèle qui sera utilisé pour créer les machines virtuelles dans le catalogue de machines. Avant de créer le catalogue de machines, créez des images et des instantanés dans Nutanix.

- Pour de plus amples informations sur les images principales en général, consultez l'article Créer des catalogues de machines.

- Pour consulter les procédures Nutanix de création d'images et d'instantanés, reportez-vous à la documentation Nutanix référencée ci-dessus.

Les pages **Système d'exploitation** et **Gestion des machines** ne contiennent aucune information spécifique à Nutanix. Suivez les instructions de l'article Créer des catalogues de machines.

Sur la page **Conteneur**, qui est unique Nutanix, sélectionnez le conteneur où les disques des VM seront placés.

Sur la page **Image principale**, sélectionnez l'instantané d'image. Les noms des instantanés Acropolis doivent être précédés de « XD_ » pour pouvoir être utilisés dans XenApp et XenDesktop Utilisez la console Acropolis pour renommer vos instantanés, le cas échéant. Si vous renommez des instantanés, redémarrez l'assistant de création de catalogues pour afficher une liste actualisée.

Sur la page **Machines virtuelles**, indiquez le nombre de processeurs virtuels et le nombre de cœurs par vCPU.

Les pages **Cartes réseau**, **Comptes d'ordinateurs** et **Résumé** ne contiennent aucune information spécifique à Nutanix. Suivez les instructions de l'article Créer des catalogues de machines.

Environnements de virtualisation Microsoft Azure

January 23, 2019

Configuration des connexions

Lorsque vous utilisez Studio pour créer une connexion Microsoft Azure, vous devez disposer d'informations contenues dans le fichier des paramètres de publication Microsoft Azure. Les informations contenues dans ce fichier XML pour chaque abonnement sont similaires à l'exemple ci-dessous (votre certificat de gestion sera beaucoup plus long) :

```
<Subscription
ServiceManagementUrl="https://management.core.windows.net"
Id="o1455234-0r10-nb93-at53-21zx6b87aabb7p"
Name="Test1"
ManagementCertificate=";alkjdflaksdjfl;akjsdfl;akjsdfl;
    sdjfklasdfilaskjdfkluqweiopruaiopdfaklsdjfjsdilfasdkl;fjerioup" />
```

La procédure ci-dessous suppose que vous créez une connexion à partir de Studio, et que vous avez démarré l'assistant de création de site ou l'assistant de création de connexion.

1. Dans un navigateur, accédez à https://manage.windowsazure.com/publishsettings/index.
2. Téléchargez le fichier de paramètres de publication.

3. Dans Studio, sur la page **Connexion** de l'assistant, lorsque vous sélectionnez le type de connexion Microsoft Azure, cliquez sur Importer.
4. Si vous disposez de plusieurs abonnements, vous êtes invité à sélectionner l'abonnement.

L'ID et le certificat sont automatiquement et de manière silencieuse importés dans Studio.

Les actions d'alimentation utilisant une connexion sont soumises à des seuils. En général, les valeurs par défaut sont appropriées et ne devraient pas être modifiées. Toutefois, vous pouvez modifier une connexion et les modifier (vous ne pouvez pas modifier ces valeurs lorsque vous créez la connexion). Pour de plus amples informations, consultez la section Modifier une connexion.

Machines virtuelles

Lors de la création d'un catalogue de machines dans Studio, la sélection de la taille de chaque machine virtuelle dépend des options présentées par Studio, du coût et des performances du type d'instance de VM sélectionné et de la capacité à monter en charge.

Studio affiche toutes les options d'instance de VM que Microsoft Azure met à disposition dans une région sélectionnée ; Citrix ne peut pas les modifier. Par conséquent, vous devez bien connaître vos applications et leurs besoins en UC, en mémoire et en E/S. Plusieurs options sont disponibles à des niveaux de prix et de performance différents ; veuillez consulter les articles Microsoft suivants afin de mieux comprendre les options.

- MSDN – Tailles des machines virtuelles et du service cloud pour Azure : https://msdn.microsoft.com/en-us/library/azure/dn197896.aspx
- Tarif des machines virtuelles : https://azure.microsoft.com/en-us/pricing/details/virtual-machines

Niveau de base : les machines virtuelles portant le préfixe « Basic » représentent le disque de base. Elles sont limitées principalement par le niveau IOPS Microsoft de 300. Elles ne sont pas recommandées pour les charges de travail OS de serveur (RDSH) ou OS de bureau (VDI).

Niveau standard : les VM de niveau standard apparaissent dans quatre séries : A, D, DS et G.

Série	Affichage dans Studio
Une	Très petite, petite, moyenne, grande, très grande, A5, A6, A7, A8, A9, A10, A11. « moyenne » et « grande » sont les options recommandées pour tester les charges de travail avec OS de bureau (VDI) ou OS de serveur (RDSH), respectivement.

Série	Affichage dans Studio
D	Standard_D1, D2, D3, D4, D11, D12, D13, D14. Ces machines virtuelles proposent un SSD pour le stockage temporaire.
DS	Standard_DS1, DS2, DS3, DS4, DS11, DS12, DS13, DS14. Ces machines virtuelles proposent un stockage SSD local pour tous les disques.
G	Standard_G1 – G5. Ces machines virtuelles sont destinées à des opérations informatiques haute performance.

Lors du provisioning de machines dans un stockage Premium Azure, veillez à sélectionner une taille de machine qui est prise en charge dans un compte de stockage Premium.

Coût et performance des types d'instance de VM

Pour la tarification aux États-Unis, le coût de chaque type d'instance VM par heure est disponible sur https://azure.microsoft.com/en-us/pricing/details/virtual-machines/.

Lorsque vous travaillez avec des environnements de cloud, il est important de bien comprendre vos besoins informatiques réels. Pour les déploiements de preuve de concept ou autres activités de test, il peut être tentant d'avoir recours à des types d'instance de VM haute performance. Il peut également être tentant d'utiliser des VM de moindre performance pour réduire les coûts. La meilleure option est d'utiliser une VM appropriée pour la tâche. Démarrer avec les machines les plus performantes peut ne pas donner les résultats escomptés et s'avérer coûteux dans le temps, au bout d'une semaine dans certains cas. Avec les types d'instance de VM moins performants et moins coûteux, les performances et la convivialité peuvent ne pas être appropriées pour la tâche.

Pour les charges de travail avec OS de bureau (VDI) ou OS de serveur (RDSH), des tests effectués avec LoginVSI et sa charge de travail moyenne ont révélé que les types d'instance Moyenne (A2) et Grande (A3) offraient le meilleur équilibre entre le prix et les performances.

Moyenne (A2) et Grande (A3 ou A5) représentent le meilleur équilibre coût/performances pour les charges de travail d'évaluation. Les niveaux inférieurs ne sont pas recommandés. Des séries de VM plus performantes peuvent proposer à vos applications ou à vos utilisateurs les performances et la convivialité dont ils ont besoin ; cependant, il est préférable de se baser sur l'un de ces trois types d'instance pour déterminer si le coût plus élevé d'une instance de VM plus performante est justifié.

Capacité à monter en charge

Plusieurs contraintes affectent la capacité à monter en charge des catalogues d'une unité d'hébergement. Certaines contraintes, telles que le nombre de cœurs d'UC dans un abonnement Azure, peuvent être éliminées en contactant l'assistance Microsoft Azure pour augmenter la valeur par défaut (20). D'autres, telles que le nombre de machines virtuelles dans un réseau virtuel par abonnement (2048), ne peuvent pas être modifiées.

Actuellement, Citrix prend en charge 40 VM dans un catalogue.

Pour augmenter le nombre de VM dans un catalogue ou un hôte, contactez l'assistance Microsoft Azure. Les limites par défaut de Microsoft Azure empêchent l'extension au-delà d'un certain nombre de machines virtuelles ; cependant, ces limites changent souvent, il est donc recommandé de vérifier les dernières informations : https://azure.microsoft.com/en-us/documentation/articles/azure-subscription-service-limits/.

Un réseau virtuel Microsoft Azure prend en charge jusqu'à 2 048 VM.

Microsoft recommande une limite de 40 images de VM avec disque standard par service cloud. Lors d'une extension, prenez en compte le nombre de services de cloud requis pour le nombre de VM de l'ensemble de la connexion. Prenez aussi en compte les VM nécessaires pour fournir les applications hébergées.

Contactez l'assistance Microsoft Azure pour déterminer si les limitations par défaut d'UC doivent être augmentées pour vos charges de travail.

Installer les composants principaux

February 28, 2019

Les composants principaux sont le Delivery Controller, Studio, Director, StoreFront et le serveur de licences.

Important : avant de commencer l'installation, consultez l'article Préparer l'installation. Consultez aussi cet article avant une installation.

Cet article décrit la séquence de l'assistant d'installation lors de l'installation des composants principaux. Des lignes de commande équivalentes sont fournies. Pour de plus amples informations, consultez la section Installer à l'aide de la ligne de commande.

Étape 1 – Télécharger le logiciel du produit et démarrer l'assistant

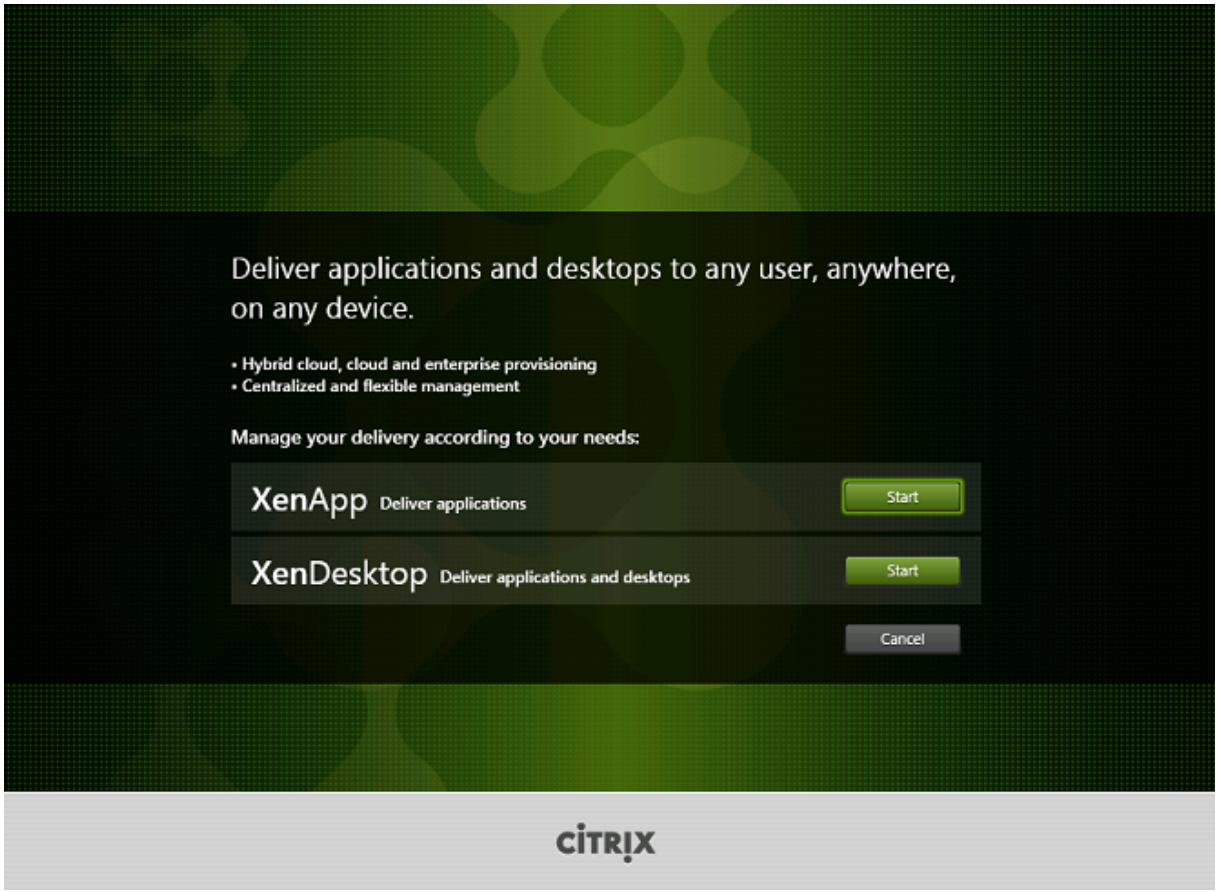
Utilisez vos informations d'identification de compte Citrix pour accéder à la page de téléchargement de XenApp et XenDesktop. Téléchargez le fichier ISO du produit.

Décompressez le fichier. Éventuellement, gravez un DVD du fichier ISO.

Ouvrez une session sur la machine sur lequel vous installez les composants principaux, à l'aide d'un compte d'administrateur local.

Insérez le DVD dans le lecteur ou montez le fichier ISO. Si le programme d'installation ne se lance pas automatiquement, double-cliquez sur l'application **AutoSelect** ou sur le lecteur monté.

Étape 2 – Choisir le produit à installer

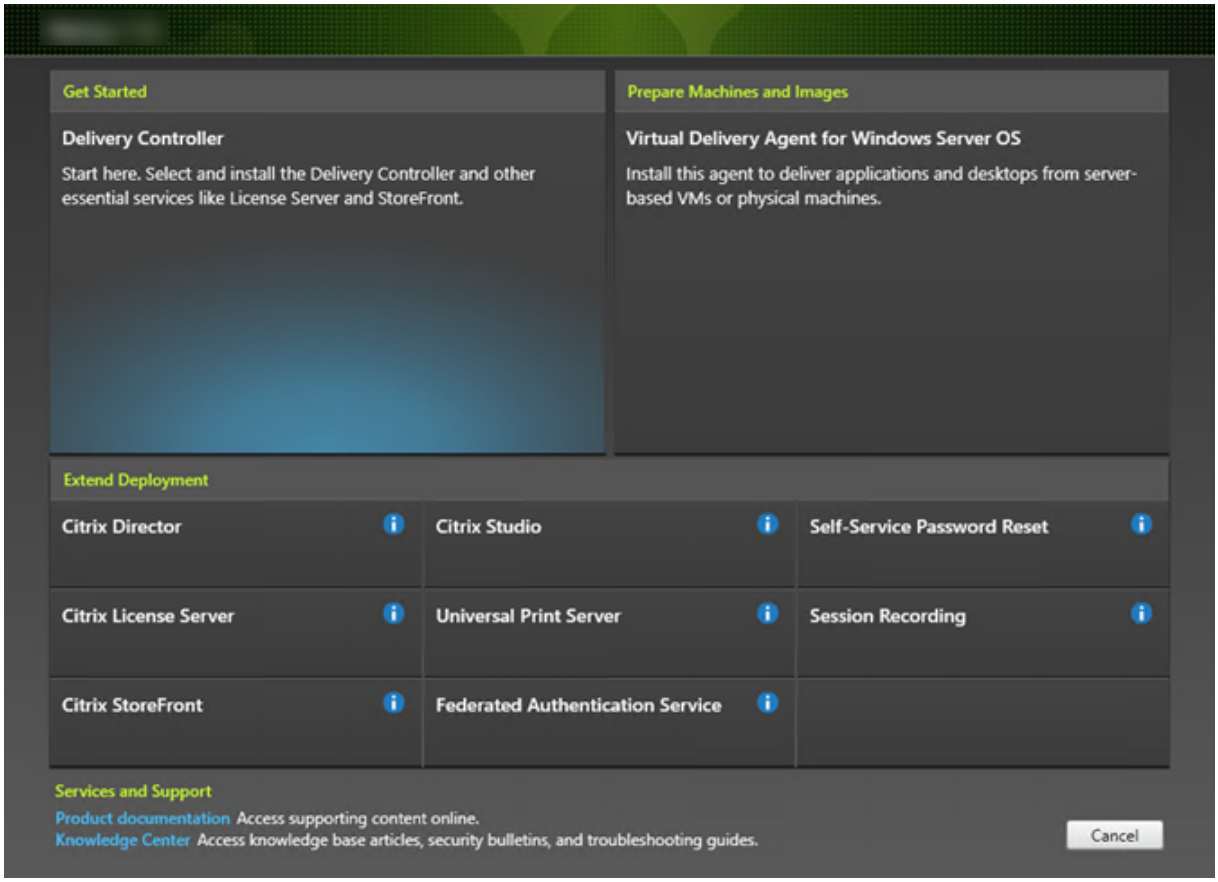


Cliquez sur **Démarrer** en regard du produit à installer : XenApp ou XenDesktop.

(si la machine dispose déjà d'un composant XenApp ou XenDesktop, cette page ne s'affiche pas).

Option de ligne de commande : /xenapp pour installer XenApp ; XenDesktop est installé si l'option est omise

Étape 3 – Choisir les composants à installer

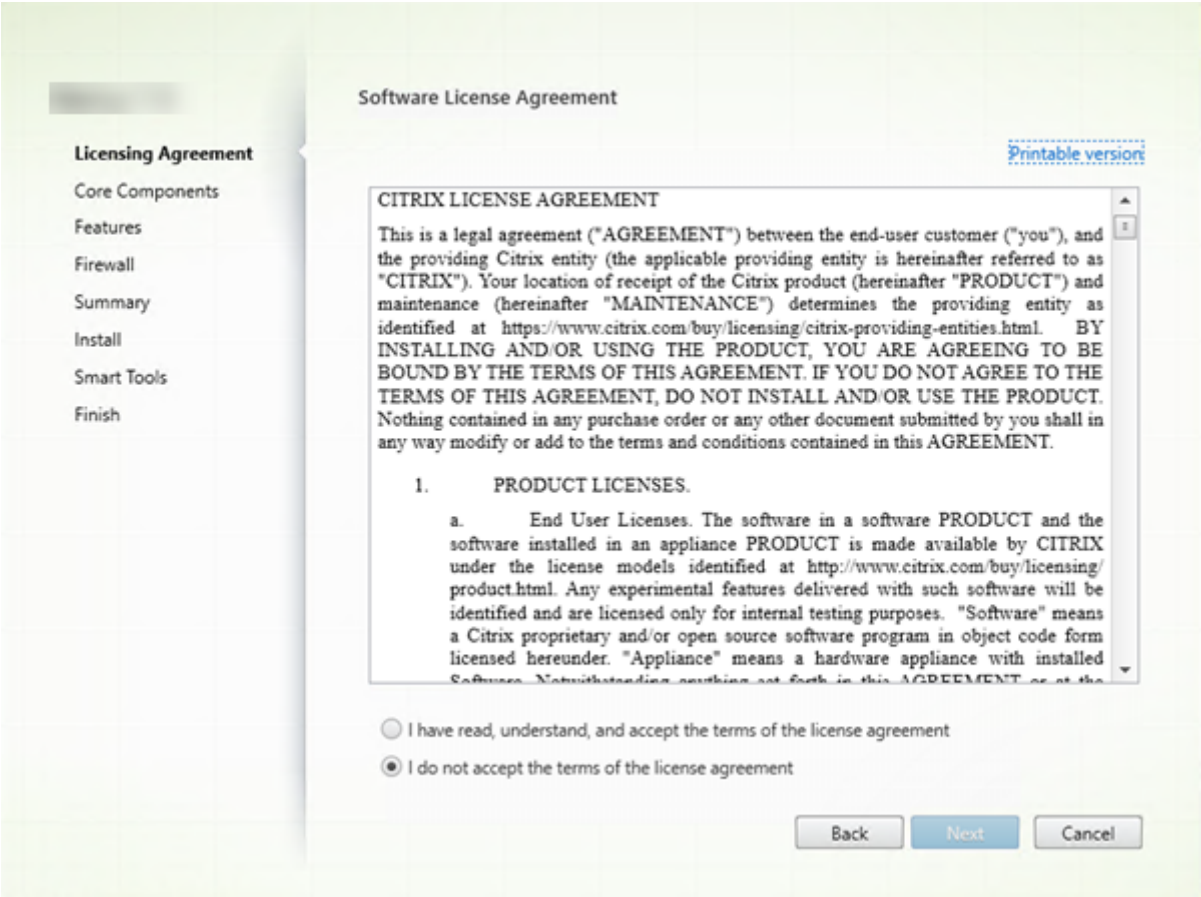


Si vous venez juste de démarrer, sélectionnez **Delivery Controller**. (vous sélectionnerez les composants spécifiques à installer sur cette machine dans une page ultérieure).

Si vous avez déjà installé un Controller (sur cette machine ou une autre) et souhaitez installer un autre composant, sélectionnez le composant dans la section Étendre le déploiement.

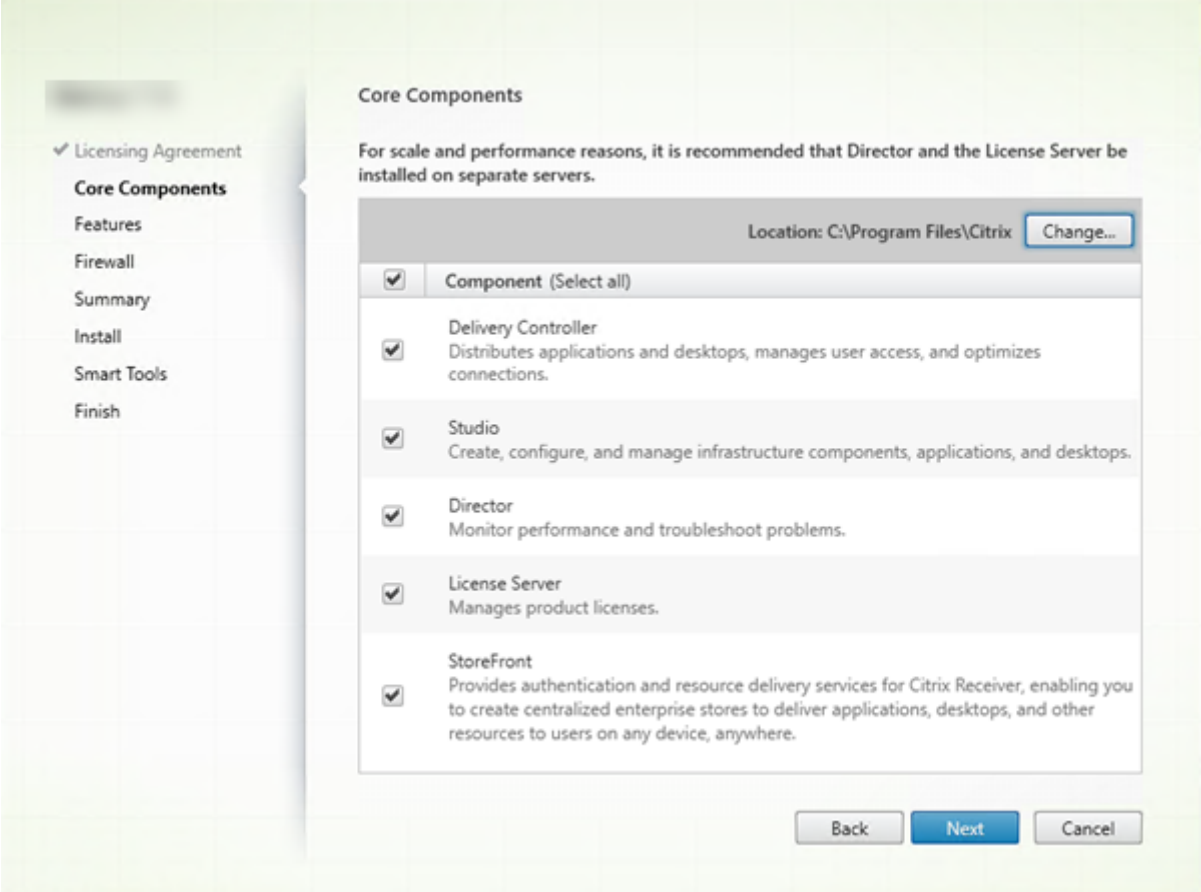
Option de ligne de commande : /components

Étape 4 – Lire puis accepter le contrat de licence



Sur la page **Contrat de licence**, après avoir lu le contrat de licence, indiquez que vous l'avez lu et accepté. Cliquez ensuite sur **Suivant**.

Étape 5 – Sélectionner les composants à installer et l'emplacement d'installation



Sur la page **Composants principaux** :

- **Emplacement :** par défaut, les composants sont installés dans C:\Program Files\Citrix. Le paramètre par défaut convient à la plupart des déploiements. Si vous spécifiez un autre emplacement, ce dernier doit disposer d'autorisations d'exécution pour le service réseau.
- **Composants :** par défaut, les cases à cocher pour tous les composants principaux sont sélectionnées. L'installation de tous les composants principaux sur un seul serveur convient aux déploiements d'évaluation, de test ou de production de petite taille. Pour les environnements de production, Citrix vous recommande d'installer Director, StoreFront et le serveur de licences sur des serveurs distincts.

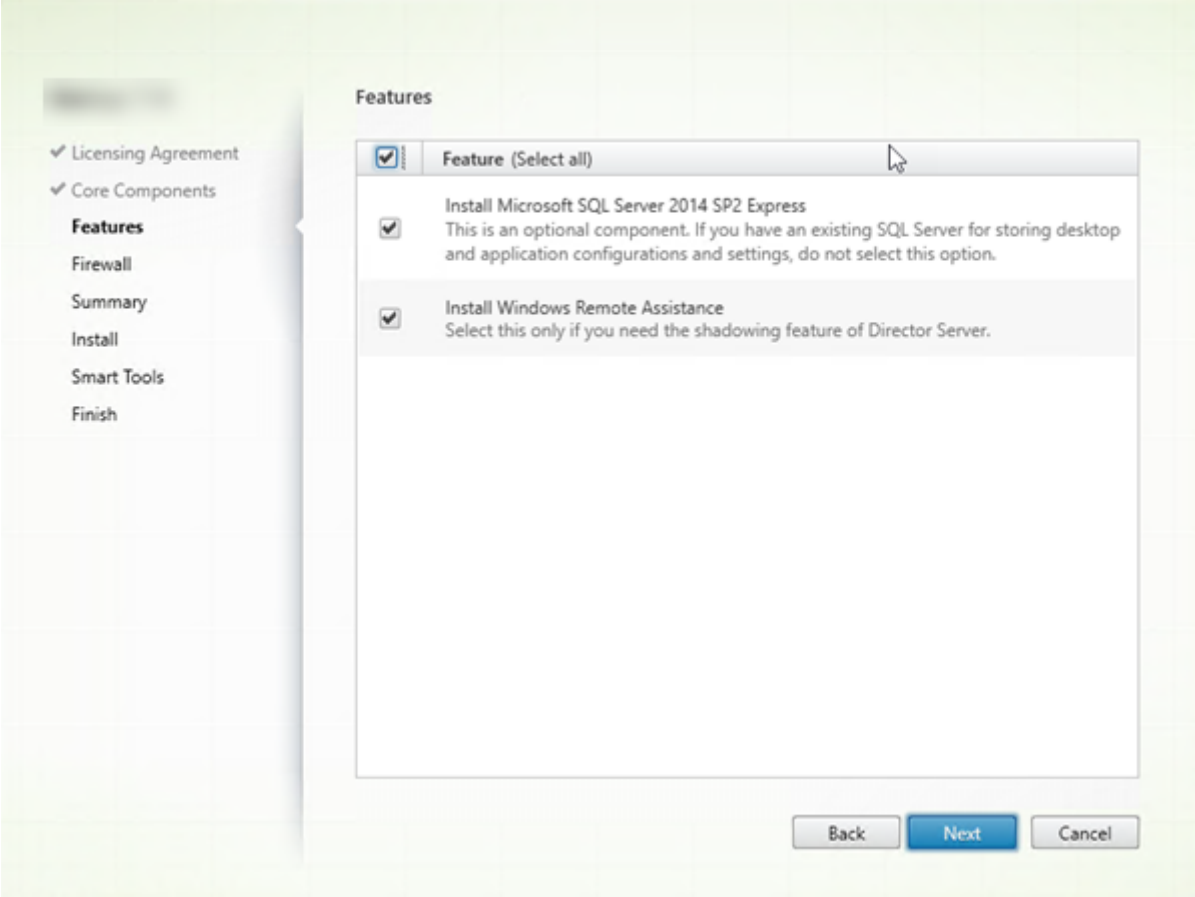
Sélectionnez uniquement les composants que vous voulez installer sur cette machine. (une fois que vous avez installé les composants sur cette machine, vous pouvez exécuter de nouveau le programme d'installation sur d'autres machines pour installer d'autres composants).

Une icône vous avertit lorsque vous choisissez de ne pas installer des composants principaux requis sur cette machine. Cette alerte vous rappelle d'installer ce composant, mais pas nécessairement sur cette machine.

Cliquez sur **Suivant**.

Options de ligne de commande : /installdir, /components, /exclude

Étape 6 – Activer ou désactiver des fonctionnalités



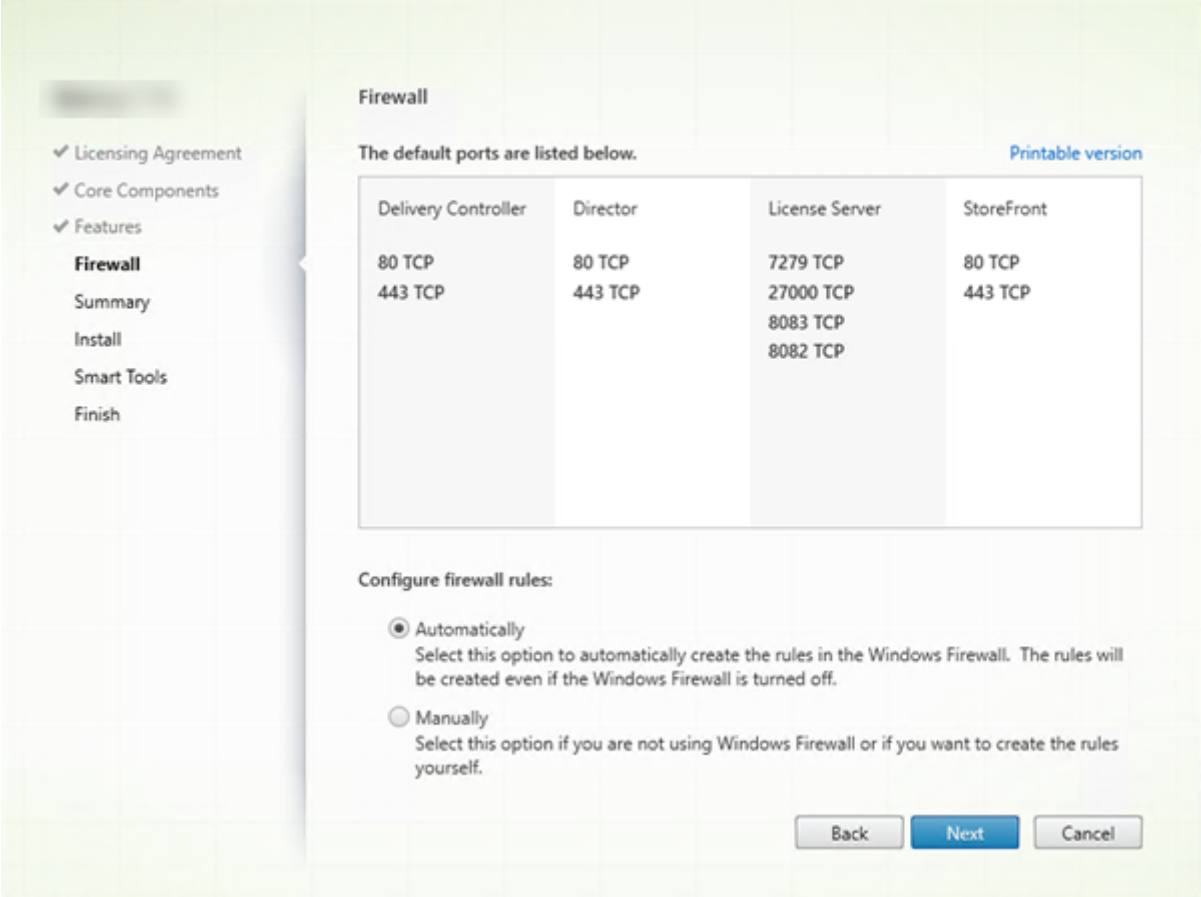
Sur la page **Fonctionnalités** :

- Sélectionnez si vous souhaitez installer Microsoft SQL Server Express pour l'utiliser en tant que base de données du site. Par défaut, cette option est activée. Si vous n'avez pas d'expérience avec les bases de données XenApp et XenDesktop, consultez la section Bases de données.
- Lorsque vous installez Director, l'Assistance à distance Windows est installée automatiquement. Vous pouvez choisir d'activer l'observation dans l'Assistance à distance Windows pour l'utiliser avec l'observation utilisateur de Director. L'activation de l'observation ouvre le port TCP 3389. Cette fonctionnalité est activée par défaut. Le paramètre par défaut convient à la plupart des déploiements. Cette fonction s'affiche uniquement lors de l'installation de Director.

Cliquez sur **Suivant**.

Options de ligne de commande : /nosql (pour empêcher l'installation), /no_remote_assistance (pour empêcher l'activation)

Étape 7 – Ouvrir automatiquement les ports de pare-feu Windows



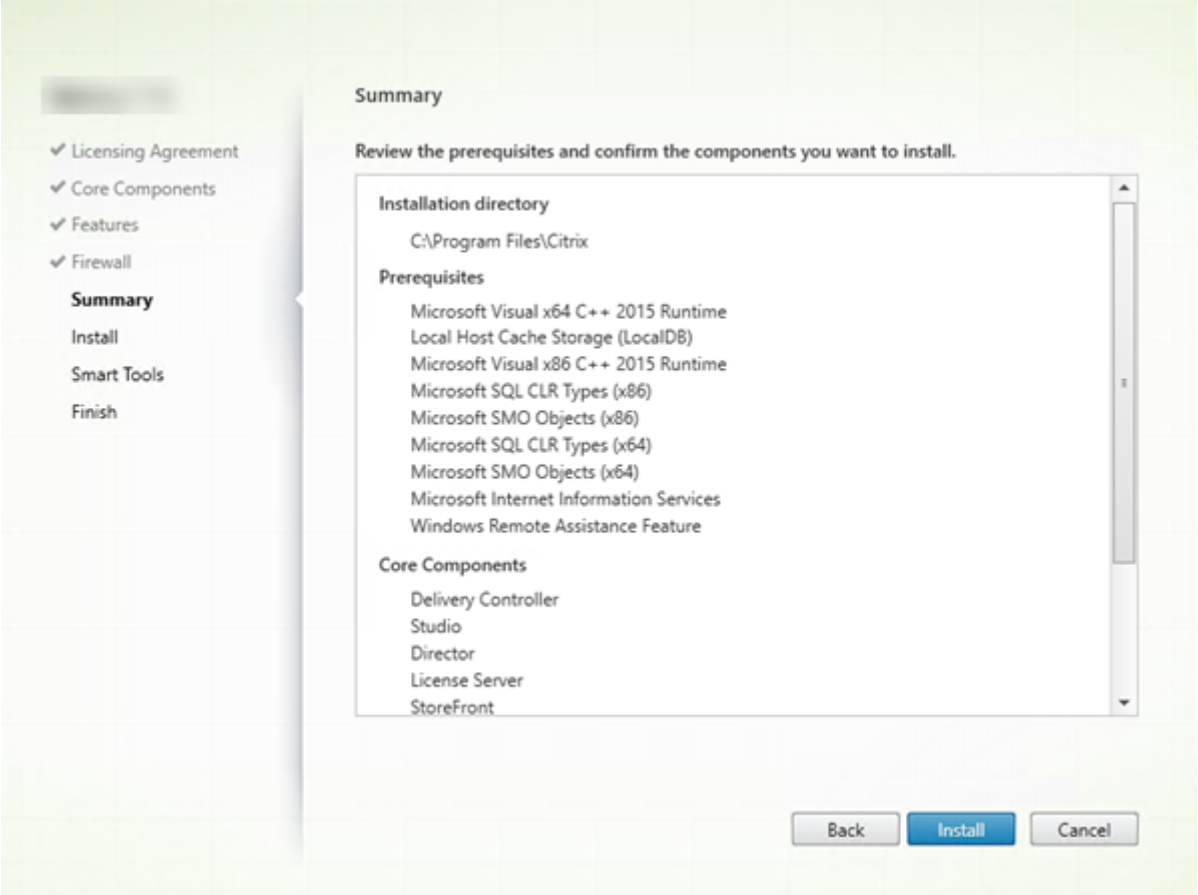
Par défaut, les ports répertoriés sur la page **Pare-feu** sont ouverts automatiquement si le service Pare-feu Windows est en cours d'exécution, même si le pare-feu n'est pas activé. Le paramètre par défaut convient à la plupart des déploiements. Pour obtenir des informations sur le port, consultez la section Ports réseau.

Cliquez sur **Suivant**.

(Le graphique présente la liste des ports si vous avez choisi d'installer tous les composants principaux sur cette machine. Ce type d'installation est généralement effectué uniquement pour les déploiements test.)

Option de ligne de commande : /configure_firewall

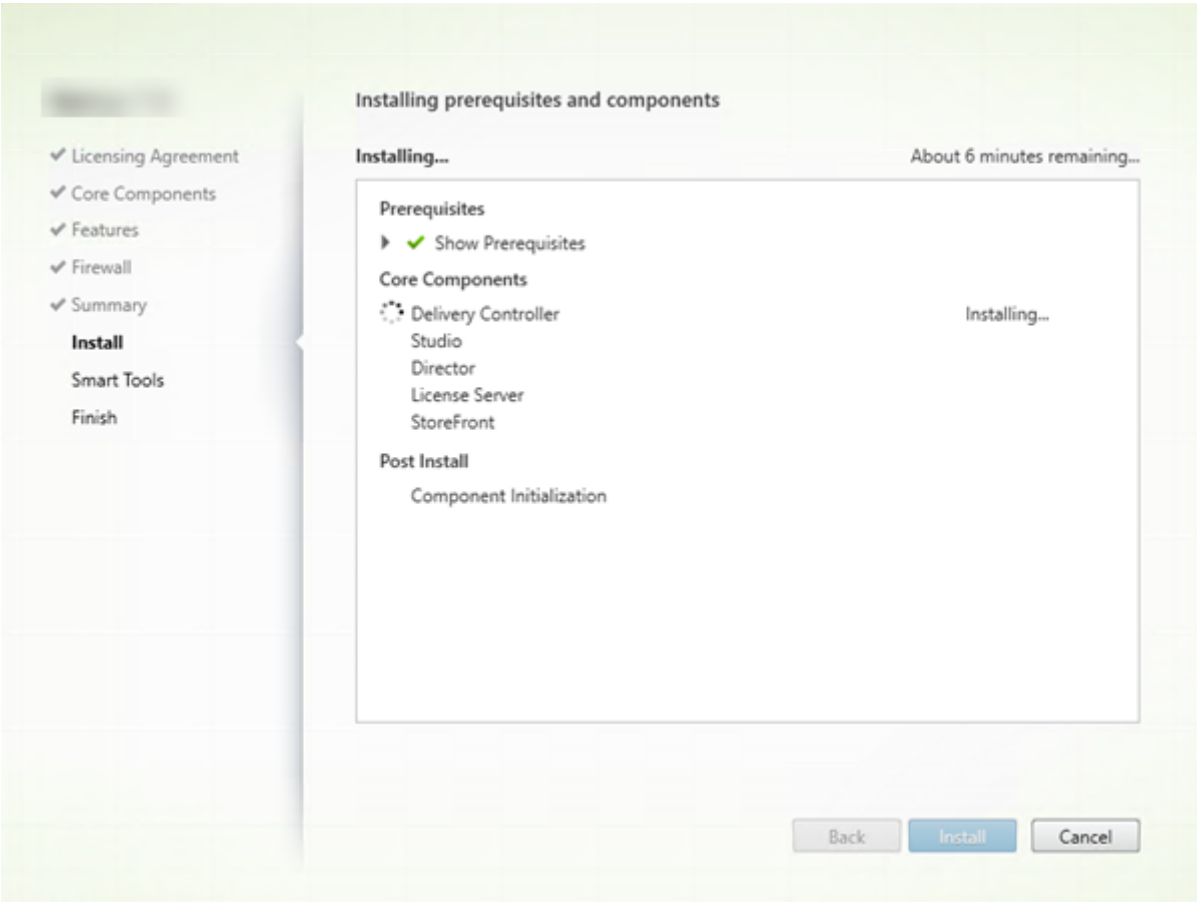
Étape 8 – Vérifier les composants requis et confirmer l'installation



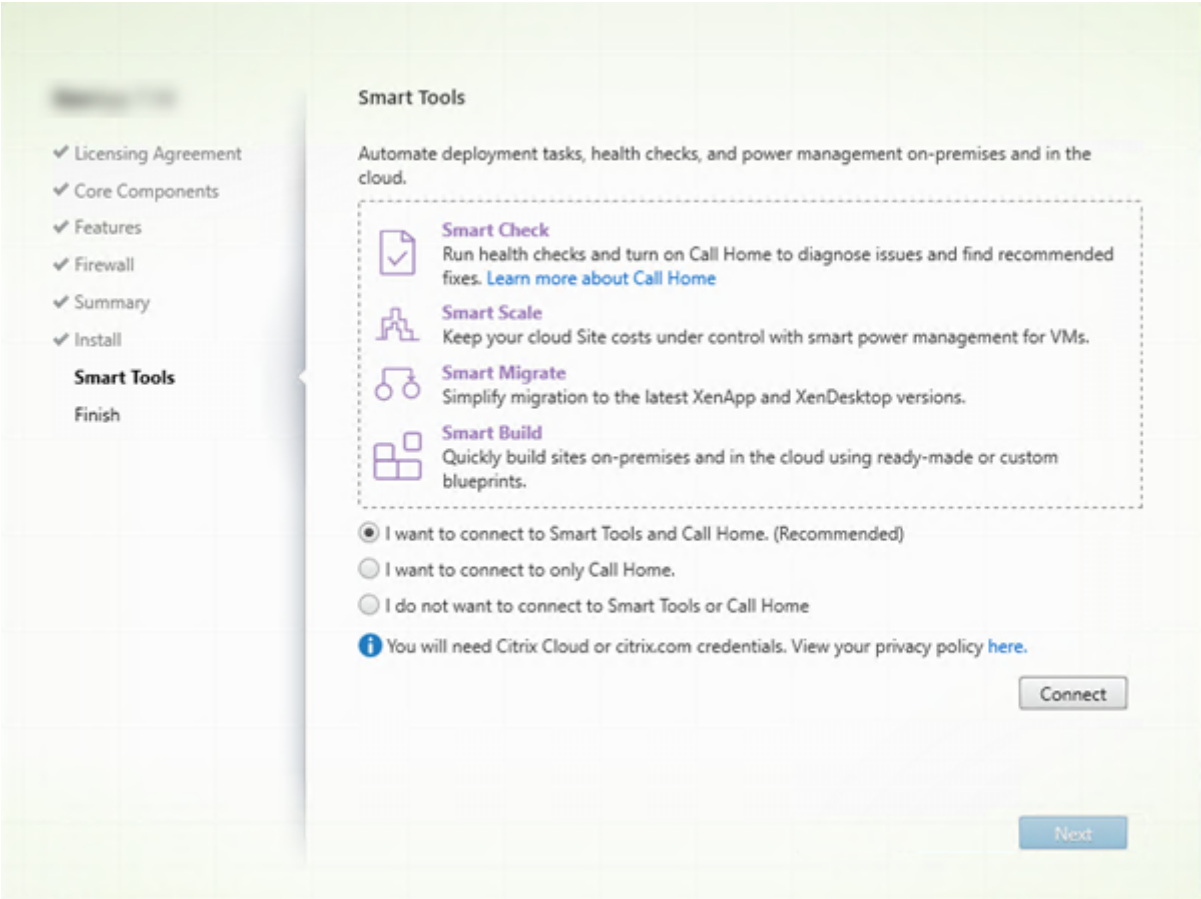
La page **Résumé** répertorie les éléments qui seront installés. Utilisez le bouton Précédent pour revenir sur les pages précédentes de l'assistant et modifier les réglages, le cas échéant.

Lorsque vous êtes prêt, cliquez sur **Installer**.

L'écran indique la progression de l'installation :



Étape 9 – Se connecter à Smart Tools et à Call Home



Lorsque vous installez ou effectuez la mise à niveau d'un Delivery Controller, la page Smart Agent propose plusieurs options :

- Activer les connexions à Smart Tools et à Call Home. Il s'agit de la sélection recommandée.
- Activer les connexions à Call Home. Durant une mise à niveau, cette option ne s'affiche pas si Call Home est déjà activé ou si le programme d'installation rencontre une erreur liée au service de télémétrie Citrix (Citrix Telemetry Service).
- Ne pas activer les connexions à Smart Tools ou à Call Home.

Si vous installez StoreFront (mais pas un Controller), l'assistant affiche la page **Smart Tools**. Si vous installez d'autres composants principaux (mais pas un Controller ou StoreFront), l'Assistant n'affiche pas les pages **Smart Tools** ou **Call Home**.

Si vous choisissez une option activant les connexions à Smart Tools et/ou à Call Home :

1. Cliquez sur **Connect**.
2. Fournissez vos informations d'identification Citrix ou Citrix Cloud.
3. Une fois que vos informations d'identification ont été validées, le processus télécharge un certificat Smart Agent. Une fois ce téléchargement terminé, une coche verte s'affiche à côté du

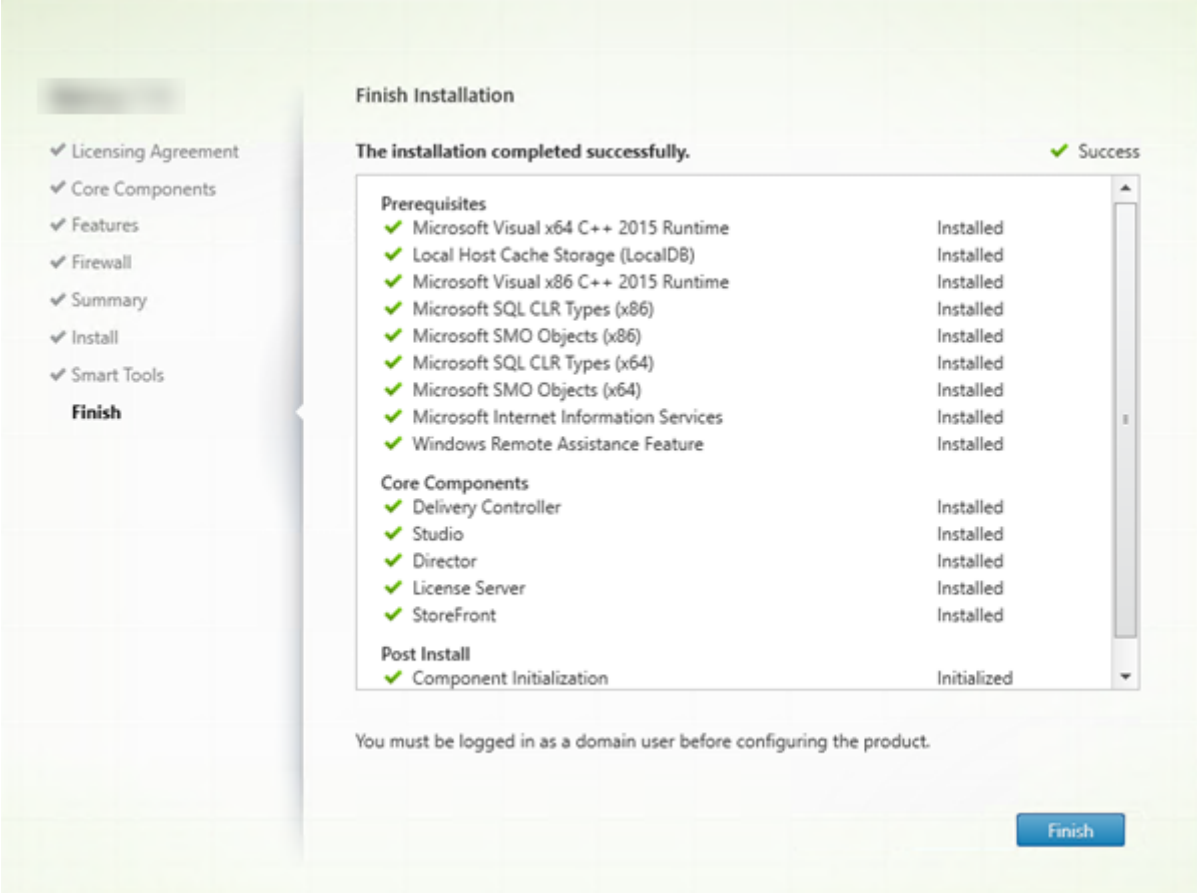
bouton **Connecter**. Si une erreur se produit lors de ce processus, modifiez la sélection (« **Je ne souhaite pas …**»). Vous pouvez vous inscrire ultérieurement.

4. Cliquez sur **Suivant** pour continuer avec l'assistant d'installation.

Si vous choisissez de ne pas participer, cliquez sur **Suivant**.

Option de ligne de commande : /exclude "Smart Tools Agent" (pour empêcher l'installation)

Étape 10 – Fin de l'installation



La page **Terminer** contient des coches vertes pour tous les éléments pré-requis et composants installés et initialisés avec succès.

Cliquez sur **Terminer**.

Étape 11 : Installer les autres composants principaux sur d'autres machines

Si vous avez installé tous les composants principaux sur une machine, passez aux étapes suivantes. Sinon, exécutez le programme d'installation sur d'autres machines pour installer d'autres composants principaux. Vous pouvez également installer des Controller supplémentaires sur d'autres serveurs.

Étapes suivantes

Une fois que vous avez installé tous les composants principaux, utilisez Studio pour créer un site.

Après avoir créé le site, installez les VDA.

À tout moment, vous pouvez utiliser le programme d'installation du produit entier pour étendre votre déploiement avec les composants suivants :

- Composant serveur d'impression universelle : exécutez le programme d'installation sur le serveur d'impression. Sélectionnez **Serveur d'impression universelle** dans la section Étendre le déploiement. Acceptez le contrat de licence, puis passez à la fin de l'assistant. Il ne reste plus rien à spécifier ou à sélectionner. Pour installer ce composant à partir de la ligne de commande, consultez la section Installer à l'aide de la ligne de commande.
- Service d'authentification fédérée : consultez la section Service d'authentification fédérée
- Réinitialisation en libre-service des mots de passe : consultez la documentation Service de réinitialisation en libre-service des mots de passe.

Installer des VDA

February 28, 2019

Il existe deux types de VDA pour machines Windows : VDA pour OS de serveur et VDA pour OS de bureau (pour de plus amples informations sur les VDA pour machines Linux, consultez la documentation Virtual Delivery Agent Linux).

> **Important :**
>
> Avant de commencer l'installation, consultez l'article Préparer l'installation. Par exemple, les dernières mises à jour Windows doivent avoir été installées sur la machine. Si les mises à jour requises ne sont pas présentes (par exemple, KB2919355), l'installation échoue.

Avant l'installation de VDA, vous devez avoir déjà installé les composants principaux. Vous pouvez également créer le site avant d'installer les VDA.

Cet article décrit la séquence de l'assistant d'installation lors de l'installation d'un VDA. Des lignes de commande équivalentes sont fournies. Consultez la section Installer à l'aide de la ligne de commande pour plus de détails.

Étape 1 – Télécharger le logiciel du produit et démarrer l'assistant

Si vous utilisez le programme d'installation du produit entier :

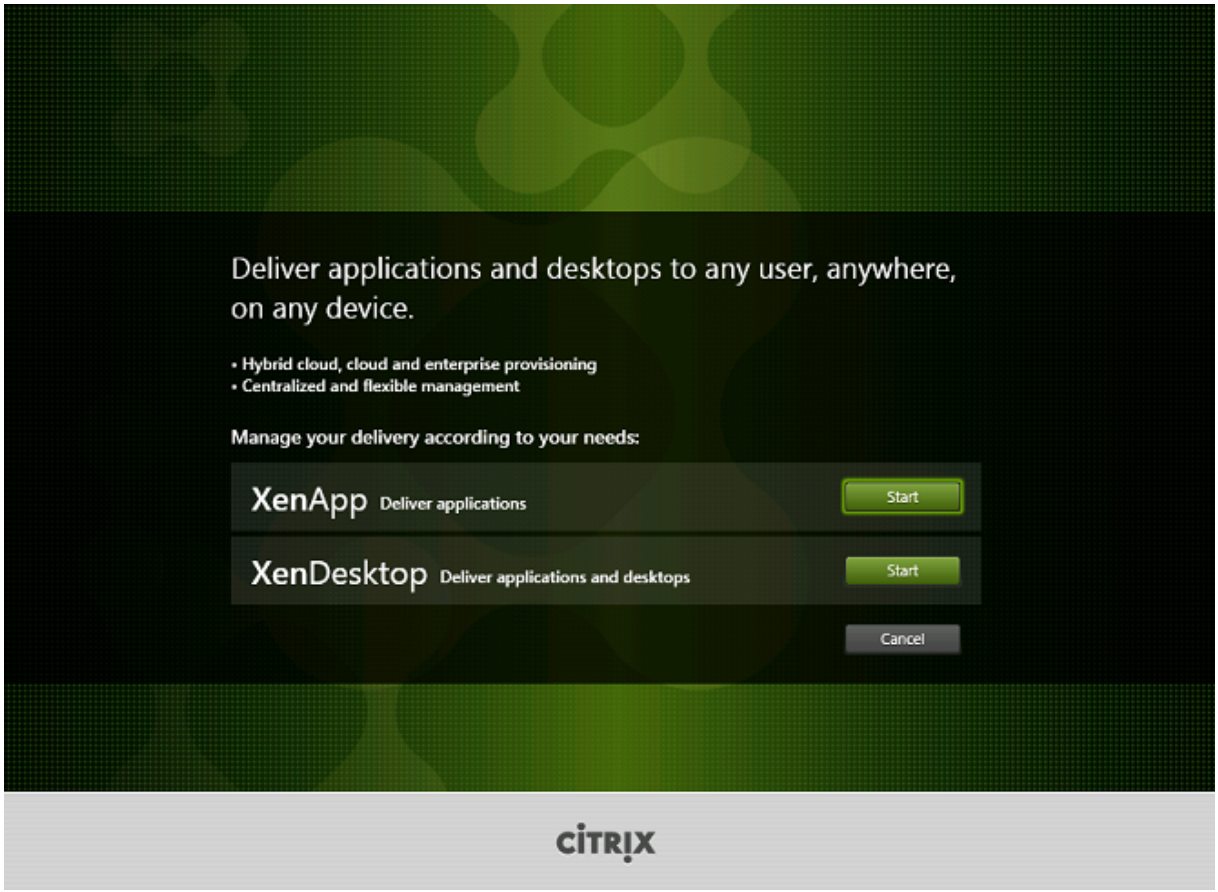
- Si vous n'avez pas encore téléchargé l'image ISO de XenApp et XenDesktop :

  - Utilisez vos informations d'identification de compte Citrix pour accéder à la page de téléchargement de XenApp et XenDesktop. Téléchargez le fichier ISO du produit.
  - Décompressez le fichier. Éventuellement, gravez un DVD du fichier ISO.
- Utilisez un compte d'administrateur local sur l'image ou la machine sur laquelle vous installez le VDA. Insérez le DVD dans le lecteur ou montez le fichier ISO. Si le programme d'installation ne se lance pas automatiquement, double-cliquez sur l'application **AutoSelect** ou sur le lecteur monté.
- L'assistant d'installation démarre.

Si vous utilisez un pack autonome :

- Utilisez vos informations d'identification de compte Citrix pour accéder à la page de téléchargement de XenApp et XenDesktop. Téléchargez le pack approprié :
  - VDAServerSetup.exe : VDA avec OS de serveur <version>
  - VDAWorkstationSetup.exe : VDA avec OS de bureau <version>
  - VDAWorkstationCoreSetup.exe: VDA avec Services de base OS de bureau <version>
- Cliquez avec le bouton droit sur le pack et choisissez **Exécuter en tant qu'administrateur**.
- L'assistant d'installation démarre.

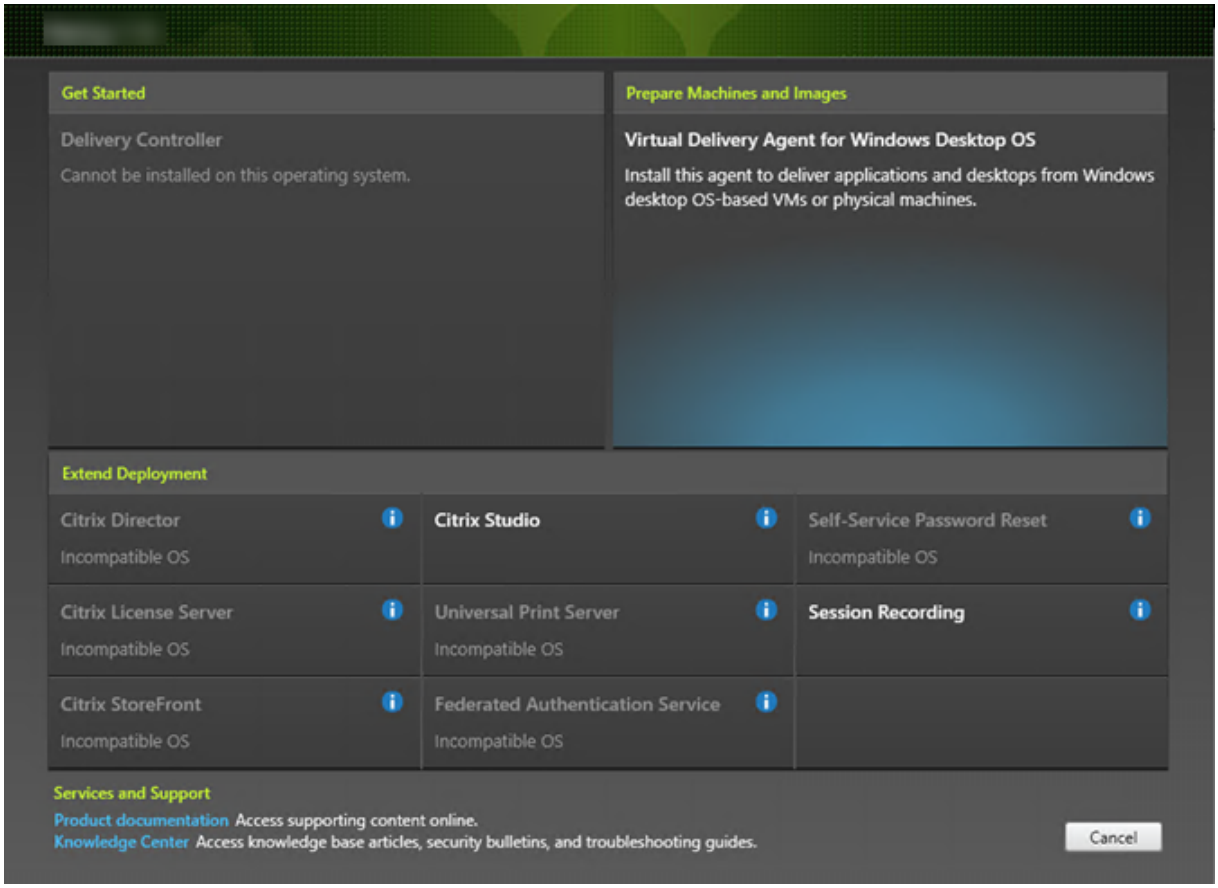
Étape 2 – Choisir le produit à installer



Cliquez sur **Démarrer** en regard du produit à installer : XenApp ou XenDesktop. (si la machine dispose déjà d'un composant XenApp ou XenDesktop, cette page ne s'affiche pas).

Option de ligne de commande : /xenapp pour installer XenApp ; XenDesktop est installé si l'option est omise

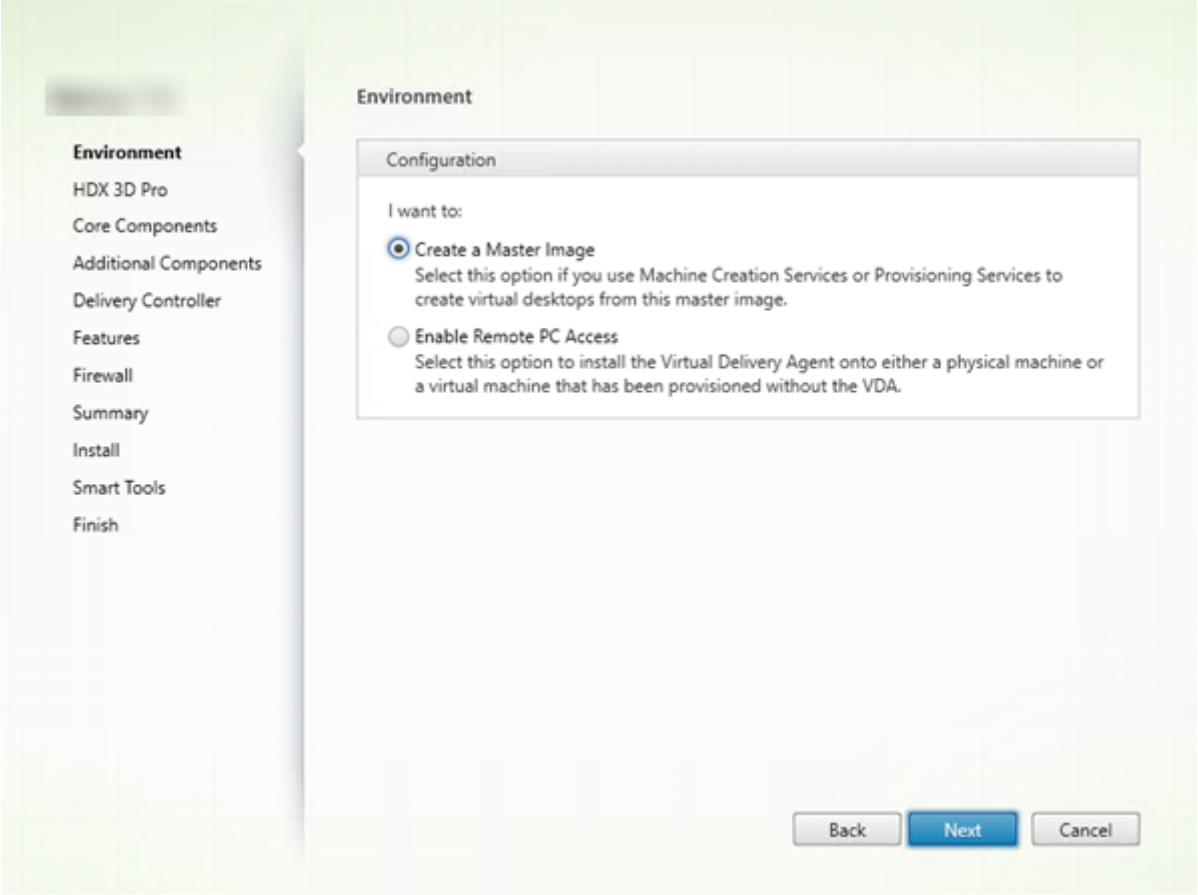
Étape 3 – Sélectionner le VDA



Sélectionnez l'entrée Virtual Delivery Agent. Le programme d'installation sait s'il s'exécute sur un OS de bureau ou de serveur, il présente donc uniquement le type de VDA approprié.

Par exemple, lorsque vous exécutez le programme d'installation sur une machine Windows 10, l'option VDA pour OS de bureau est disponible. L'option VDA pour OS de serveur n'est pas disponible.

Étape 4 – Spécifier comment le VDA sera utilisé



Sur la page **Environnement**, spécifiez la manière dont vous utiliserez le VDA. Sélectionnez l'une des options suivantes :

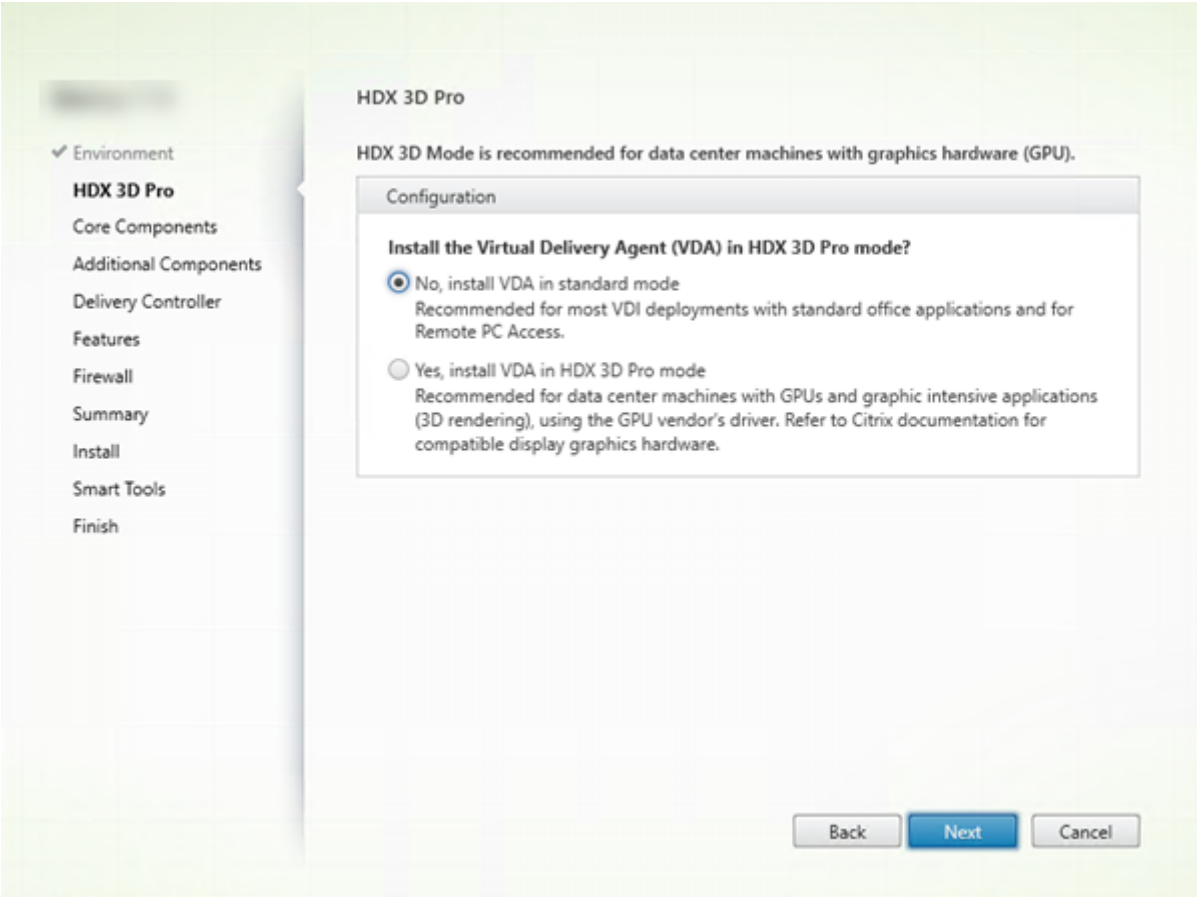
- **Image principale :** (par défaut) vous installez le VDA sur une image de la machine. Vous prévoyez d'utiliser les outils Citrix (Machine Creation Services ou Provisioning Services) pour créer des VM à partir de cette image principale.
- **Activer les connexions à une machine de serveur** (installation sur un serveur) ou **Remote PC Access** (installation sur une machine de bureau) : vous installez le VDA sur une machine physique ou sur une VM qui a été provisionnée sans VDA. Lorsque vous sélectionnez l'option Remote PC Access, les composants suivants ne sont pas installés/activés :
  - App-V
  - Profile Management
  - Machine Identity Service
  - Personal vDisk

Cliquez sur **Next**.

Options de ligne de commande : /masterimage, /remotepc

Si vous utilisez le programme d'installation VDAWorkstationCoreSetup.exe, cette page ne s'affiche pas dans l'assistant et les options de ligne de commande ne sont pas valides.

Étape 5 – Choisir si le mode HDX 3D Pro est activé



La page **HDX 3D Pro** apparaît uniquement lors de l'installation d'un VDA pour OS de bureau.

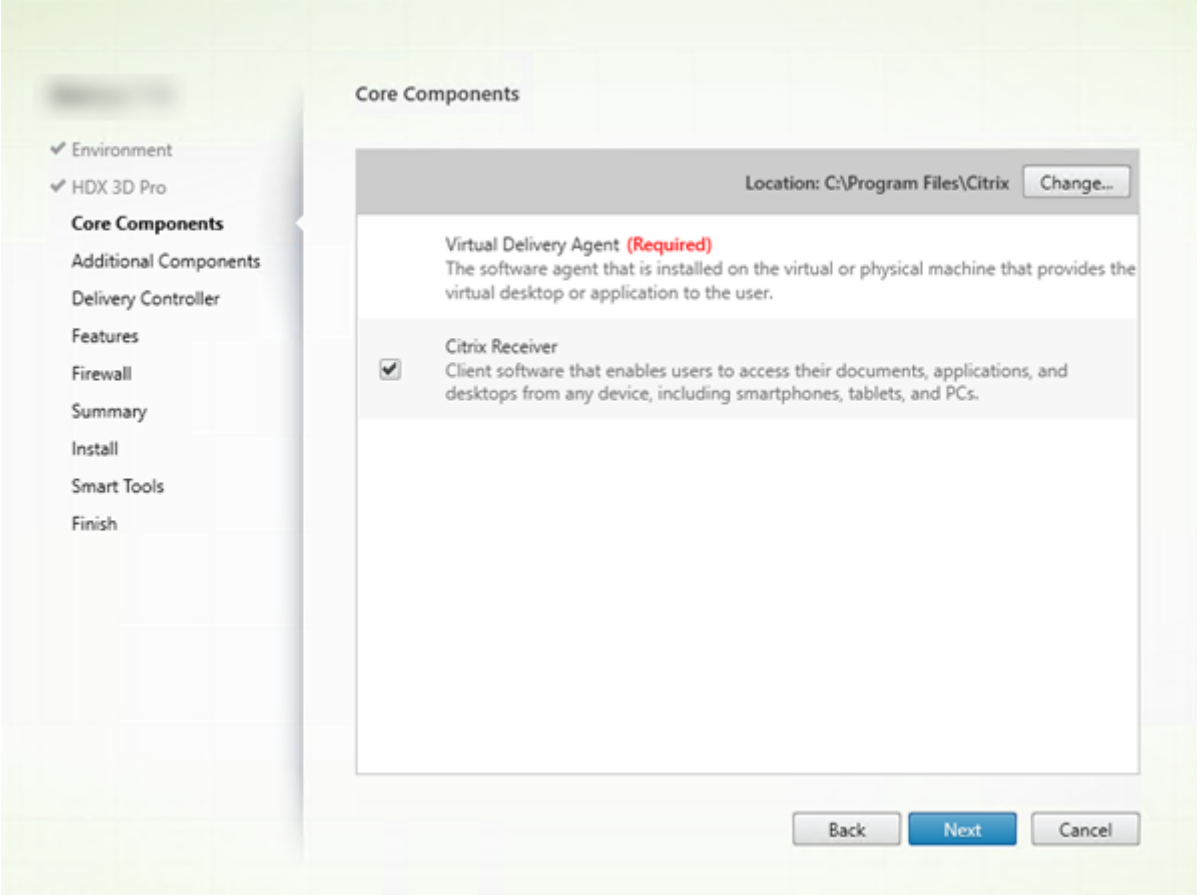
- Le mode de VDA standard est recommandé pour la plupart des bureaux, y compris ceux activés avec Microsoft RemoteFX. Le mode VDA standard est la valeur par défaut.
- Le mode de VDA HDX 3D Pro optimise les performances des programmes gourmands en graphique et des applications riches en multimédia. Le mode HDX 3D Pro VDA est recommandé si la machine accède au processeur graphique pour la restitution 3D.
- Pour Remote PC Access, le VDA est généralement configuré avec le mode VDA standard. Pour Remote PC Access configuré avec HDX 3D Pro, le vidage de l'écran est pris en charge avec
  - Intel Iris Pro Graphics et Intel HD Graphics 5300 et version supérieure (processeurs Intel Core 5ème génération et Intel Core i5 6ème génération)
  - Cartes graphiques NVIDIA Quadro et NVIDIA GRID
  - AMD RapidFire

Mode standard	Mode HDX 3D Pro
Recommandé en général pour les bureaux virtuels sans accélération graphique matérielle et pour Remote PC Access.	Recommandé en général pour les bureaux de centre de données avec accélération graphique matérielle, sauf si plus de quatre moniteurs sont requis.
Tout GPU peut être utilisé pour Remote PC Access, avec certaines limitations de compatibilité de l'application : **sur Windows 7, 8 et 8.1**, accélération GPU pour niveaux de fonctionnalité DirectX jusqu'à 9.3. Certaines applications DirectX 10, 11 et 12 risquent de ne pas s'exécuter si elles ne gèrent pas le retour sur DirectX 9; **sur Windows 10**, l'accélération GPU est fournie pour les applications DirectX 10, 11 et 12 fenêtrées. Les applications DX 9 sont restituées par WARP. Les applications DX ne peuvent pas être utilisées en mode plein écran ; **Accélération des applications OpenGL** dans les sessions distantes si prise en charge par le fournisseur GPU (NVIDIA uniquement pour le moment).	Prend en charge l'accélération GPU avec n'importe quel processeur. Toutefois l'occultation de console, les résolutions d'écran non standard et la prise en charge de moniteurs multiples réelle requièrent des graphiques NVIDIA GRID, Intel Iris Pro ou AMD RapidFire. Utilise le pilote du fournisseur de graphiques pour une compatibilité applicative optimale : **toutes les API 3D (DirectX ou OpenGL)** que le processeur graphique prend en charge ; **prise en charge d'applications 3D plein écran** avec Intel Iris Pro (Win10 uniquement), NVIDIA GRID et AMD RapidFire ; **prise en charge d'API et d'extensions de pilote personnalisées**. Par exemple, CUDA ou OpenCL.
Résolutions de moniteur arbitraires (limite déterminée par le système d'exploitation Windows et les performances) et jusqu'à huit moniteurs.	Prend en charge jusqu'à quatre moniteurs.
Encodage matériel H.264 disponible avec les processeurs graphiques Intel Iris Pro.	Encodage matériel H.264 disponible avec les processeurs graphiques Intel Iris Pro et les cartes NVIDIA.

Cliquez sur **Suivant**.

Option de ligne de commande : /enable_hdx_3d_pro

Étape 6 – Sélectionner les composants à installer et l'emplacement d'installation



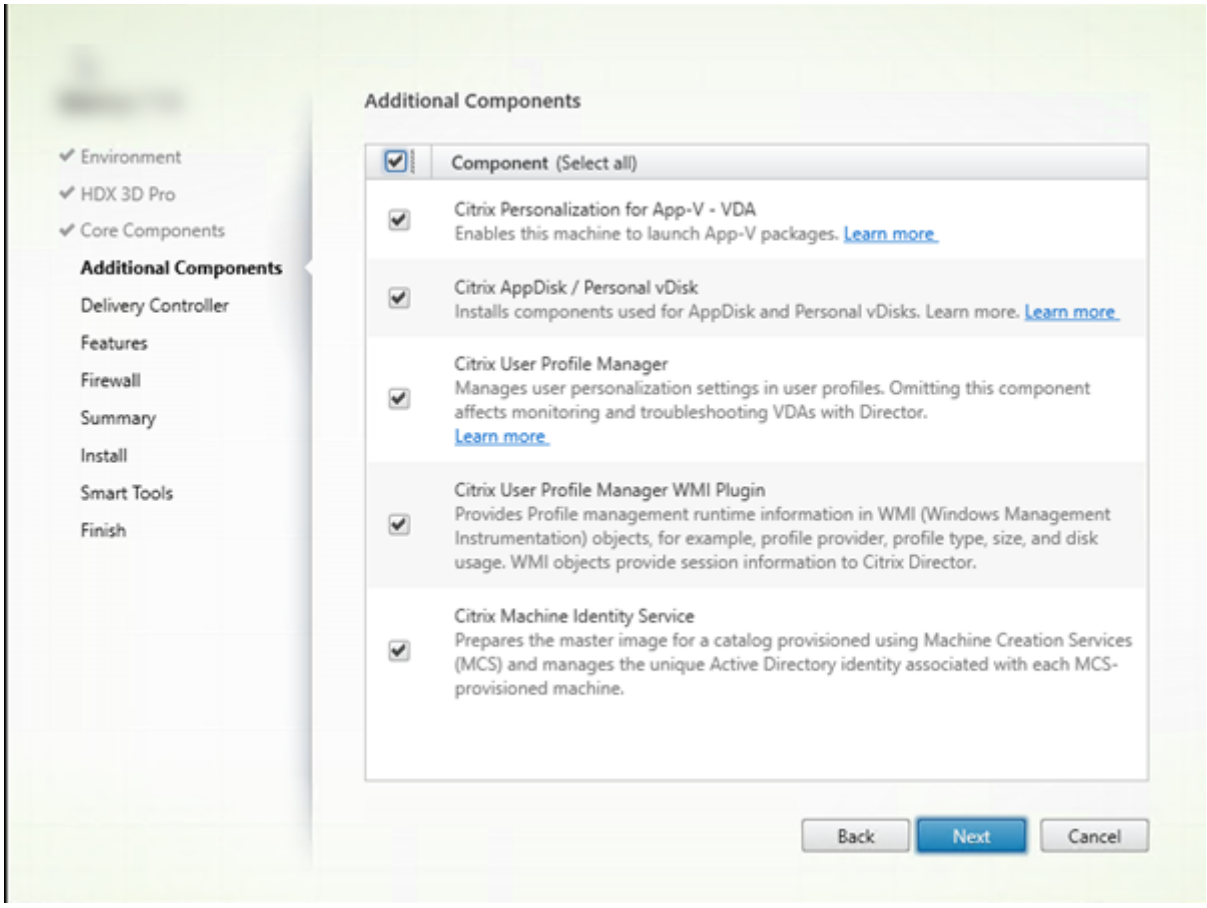
Sur la page **Composants principaux** :

- **Emplacement :** par défaut, les composants sont installés dans C:\Program Files\Citrix. Ce paramètre par défaut convient à la plupart des déploiements. Si vous spécifiez un autre emplacement, ce dernier doit disposer d'autorisations d'exécution pour le service réseau.
- **Composants** : par défaut, Citrix Receiver pour Windows est installé avec le VDA (sauf si vous utilisez le programme d'installation VDAWorkstationCoreSetup.exe). Désactivez la case à cocher si vous ne souhaitez pas que Citrix Receiver soit installé. Si vous utilisez le programme d'installation VDAWorkstationCoreSetup.exe, Citrix Receiver pour Windows n'est jamais installé, donc cette case à cocher n'est pas affichée.

Cliquez sur **Next**.

Options de ligne de commande : /installdir, /components vda pour empêcher l'installation de Citrix Receiver pour Windows

Étape 7 – Installer des composants supplémentaires



La page **Composants supplémentaires** contient des cases à cocher permettant d'activer ou de désactiver l'installation de fonctions et technologies supplémentaires avec le VDA. Cette page ne s'affiche pas si :

- Vous utilisez le programme d'installation VDAWorkstationCoreSetup.exe. Par ailleurs, les options de ligne de commande des composants supplémentaires ne sont pas valides avec ce programme d'installation.
- Vous mettez à niveau un VDA et tous les composants supplémentaires sont déjà installés. (Si certains des composants supplémentaires sont déjà installés, la page répertorie uniquement ceux qui ne sont pas installés.)

Citrix Personalization pour AppV :

Installez ce composant si vous prévoyez d'utiliser des applications à partir de packages Microsoft App-V. Pour plus d'informations, consultez App-V.

Option de ligne de commande : /exclude "Citrix Personalization for App-V – VDA" pour empêcher l'installation du composant

Citrix AppDisk / Personal vDisk :

valide uniquement lors de l'installation d'un VDA pour OS de bureau sur une VM. Installe les composants utilisés pour AppDisk et Personal vDisk. Pour de plus amples informations, consultez les sections AppDisks et Personal vDisks.

Option de ligne de commande : /exclude "Personal vDisk" pour empêcher l'installation du composant AppDisk et Personal vDisk

Citrix Profile Management :

Ce composant permet de gérer les paramètres de personnalisation utilisateur dans les profils utilisateur. Pour de plus amples informations, consultez la section Profile Management.

L'exclusion de Citrix Profile Management à partir de l'installation de ces paramètres affecte la surveillance et la résolution des problèmes des VDA avec Citrix Director. Sur les pages Détails de l'utilisateur et Point de terminaison, les panneaux Personnalisation et Durée de l'ouverture de session échouent. Sur les pages Tableau de bord et Tendances, le panneau Durée moyenne d'ouverture de session affiche les données uniquement pour les machines sur lesquelles Profile Management est installé.

Même si vous n'utilisez pas une solution de gestion de profils utilisateur tierce, Citrix vous recommande d'installer et d'exécuter Citrix Profile Management Service. L'activation de Citrix Profile Management Service n'est pas nécessaire.

Option de ligne de commande : /exclude "Citrix User Profile Manager" pour empêcher l'installation du composant

Citrix Profile Management WMI Plugin :

Ce plug-in fournit des informations d'exécution sur Profile Management dans les objets WMI (Infrastructure de gestion Windows), par exemple le fournisseur de profils, le type de profil, la taille et l'utilisation du disque. Les objets WMI fournissent des informations sur les sessions à Director.

Option de ligne de commande : /exclude "Citrix User Profile Manager WMI Plugin" pour empêcher l'installation du composant

Citrix Machine Identity Service :

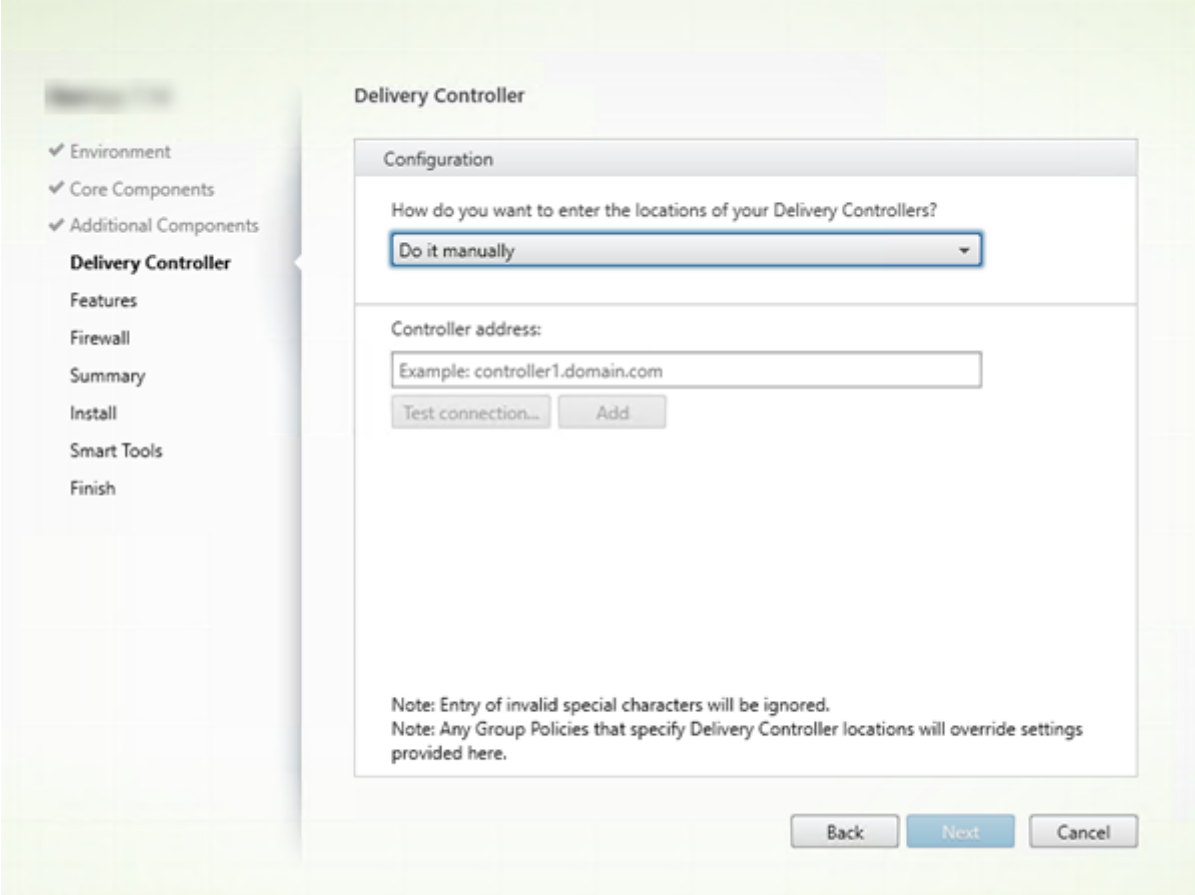
Ce service prépare l'image principale pour un catalogue provisionné par MCS. Le service gère également l'identité Active Directory unique de chaque machine provisionnée.

Option de ligne de commande : /exclude "Machine Identity Service" pour empêcher l'installation du composant

Valeurs par défaut dans l'interface graphique :

- Si vous sélectionnez l'option « Créer une image principale » sur la page **Environnement** (étape 4), les éléments de la page **Composants supplémentaires** sont activés par défaut.
- Si vous sélectionnez « Activer Remote PC Access » ou « Activer les connexions à une machine de serveur » sur la page **Environnement**, les éléments de la page **Composants supplémentaires** sont désactivés par défaut.

Étape 8 – Adresses Delivery Controller



Sur la page **Delivery Controller**, choisissez la manière dont vous souhaitez entrer les adresses des Controller installés. Citrix vous recommande de spécifier les adresses pendant que vous installez le VDA (« Effectuer manuellement »). Le VDA ne peut pas s'enregistrer auprès d'un Controller sans ces informations. Si un VDA ne peut pas s'enregistrer, les utilisateurs ne peuvent pas accéder aux applications et aux bureaux sur ce VDA.

- **Effectuer manuellement :** (valeur par défaut) entrez le nom de domaine complet d'un Controller installé, puis cliquez sur **Ajouter**. Si vous avez installé des Controller supplémentaires, ajoutez leurs adresses.
- **Le faire plus tard (avancé) :** si vous choisissez cette option, l'assistant vous demande de confirmer avant de continuer. Pour spécifier des adresses ultérieurement, vous pouvez soit exécuter de nouveau le programme d'installation ultérieurement soit utiliser la stratégie de groupe Citrix. L'assistant vous le rappelle également sur la page **Résumé**.
- **Choisir les emplacements d'Active Directory :** valide uniquement lorsque la machine est associée à un domaine et que l'utilisateur est un utilisateur de domaine.
- **Laisser Machine Creation Services effectuer ceci automatiquement :** valide uniquement si vous utilisez MCS pour provisionner des machines.

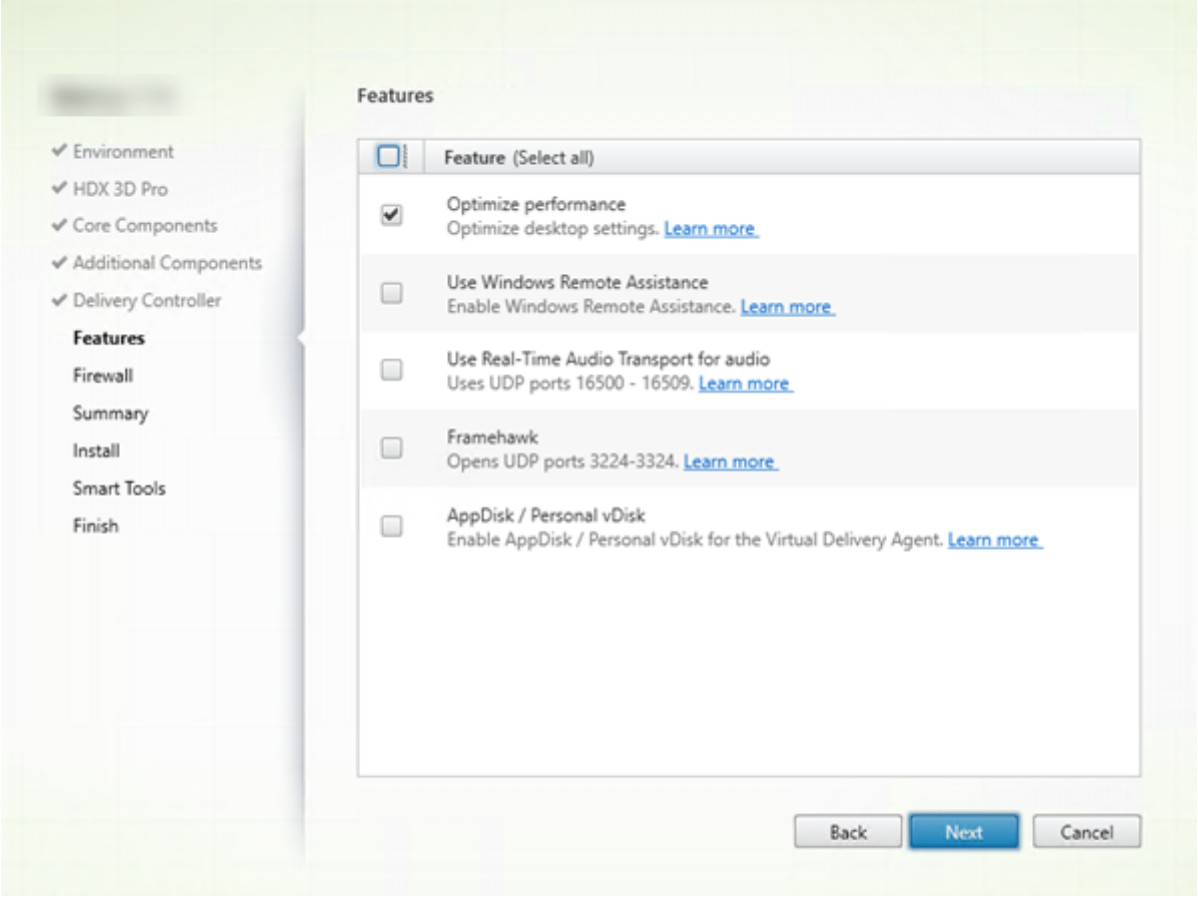
Cliquez sur **Next**. Si vous avez sélectionné l'option « Le faire plus tard (avancé) », vous êtes invité à confirmer que vous devrez spécifier des adresses de Controller ultérieurement.

Autres considérations :

- L'adresse ne peut pas contenir les caractères { | } ~ [\ ] ^ ‘ : ; < = > ? & @ ! “ # $ % ( ) + / ,
- Si vous spécifiez les adresses lors de l'installation du VDA et dans la stratégie de groupe, les paramètres de la stratégie remplacent les paramètres fournis au cours de l'installation.
- L'enregistrement du VDA requiert également que les ports de pare-feu utilisés pour les communications avec le Controller soient ouverts. Ce paramètre est activé par défaut sur la page **Pare-feu** de l'assistant.
- Une fois que vous avez spécifié l'emplacement des Controller (au cours de l'installation du VDA ou ultérieurement), vous pouvez utiliser la fonctionnalité de mise à jour automatique pour mettre les VDA à jour lorsque des Controller sont ajoutés ou supprimés. Pour de plus amples informations sur la façon dont les VDA découvrent et s'enregistrent auprès de Controller, consultez Delivery Controller.

Options de ligne de commande : /controllers

Étape 9 – Activer ou désactiver des fonctionnalités



Sur la page **Fonctionnalités**, utilisez les cases à cocher pour activer ou désactiver les fonctionnalités que vous souhaitez utiliser.

Optimiser les performances :

valide uniquement lors de l'installation d'un VDA sur une VM, pas une machine physique. Lorsque cette fonctionnalité est activée (valeur par défaut), l'outil d'optimisation est utilisé pour les VDA exécutés sur une machine virtuelle d'un hyperviseur. L'optimisation de VM comprend la désactivation des fichiers en mode déconnecté, la désactivation de la défragmentation en arrière-plan et la réduction de la taille du journal d'événements. Pour plus d'informations, veuillez consulter CTX125874.

Option de ligne de commande : /optimize

Si vous utilisez le programme d'installation VDAWorkstationCoreSetup.exe, cette fonctionnalité ne s'affiche pas dans l'assistant et l'option de ligne de commande n'est pas valide. Si vous utilisez un autre programme d'installation dans un environnement Remote PC Access, désactivez cette fonctionnalité.

Utiliser Assistance à distance Windows :

Lorsque cette option est activée, l'Assistance à distance Windows est utilisée avec la fonctionnalité d'observation utilisateur de Director. L'Assistance à distance Windows ouvre les ports dynamiques dans le pare-feu. (Valeur par défaut = désactivé)

Option de ligne de commande : /enable_remote_assistance

Utiliser le transport audio en temps réel pour l'audio :

activez cette fonctionnalité si la fonctionnalité VoIP est largement utilisée dans votre réseau. Cette fonctionnalité réduit la latence et améliore la résilience audio sur les réseaux avec perte. Elle permet aux données audio d'être transmises à l'aide du protocole de transport RTP via UDP. (Valeur par défaut = désactivé)

Option de ligne de commande : /enable_real_time_transport

Framehawk :

lorsque cette fonctionnalité est activée, les ports UDP bidirectionnels 3224-3324 sont ouverts. (Valeur par défaut = désactivé)

Vous pouvez modifier la plage de ports ultérieurement avec le paramètre de stratégie Citrix « Plage de ports du canal d'affichage Framehawk ». Vous devez ensuite ouvrir les ports du pare-feu local. Un chemin d'accès réseau UDP doit être ouvert sur les pare-feux internes (VDA vers Citrix Receiver ou NetScaler Gateway) et externes (NetScaler Gateway vers Citrix Receiver). Si NetScaler Gateway est déployé, les datagrammes Framehawk sont cryptés à l'aide de DTLS (port UDP 443 par défaut). Pour de plus amples informations, veuillez consulter l'article Framehawk.

Option de ligne de commande : /enable_framehawk_port

AppDisk / Personal vDisk :

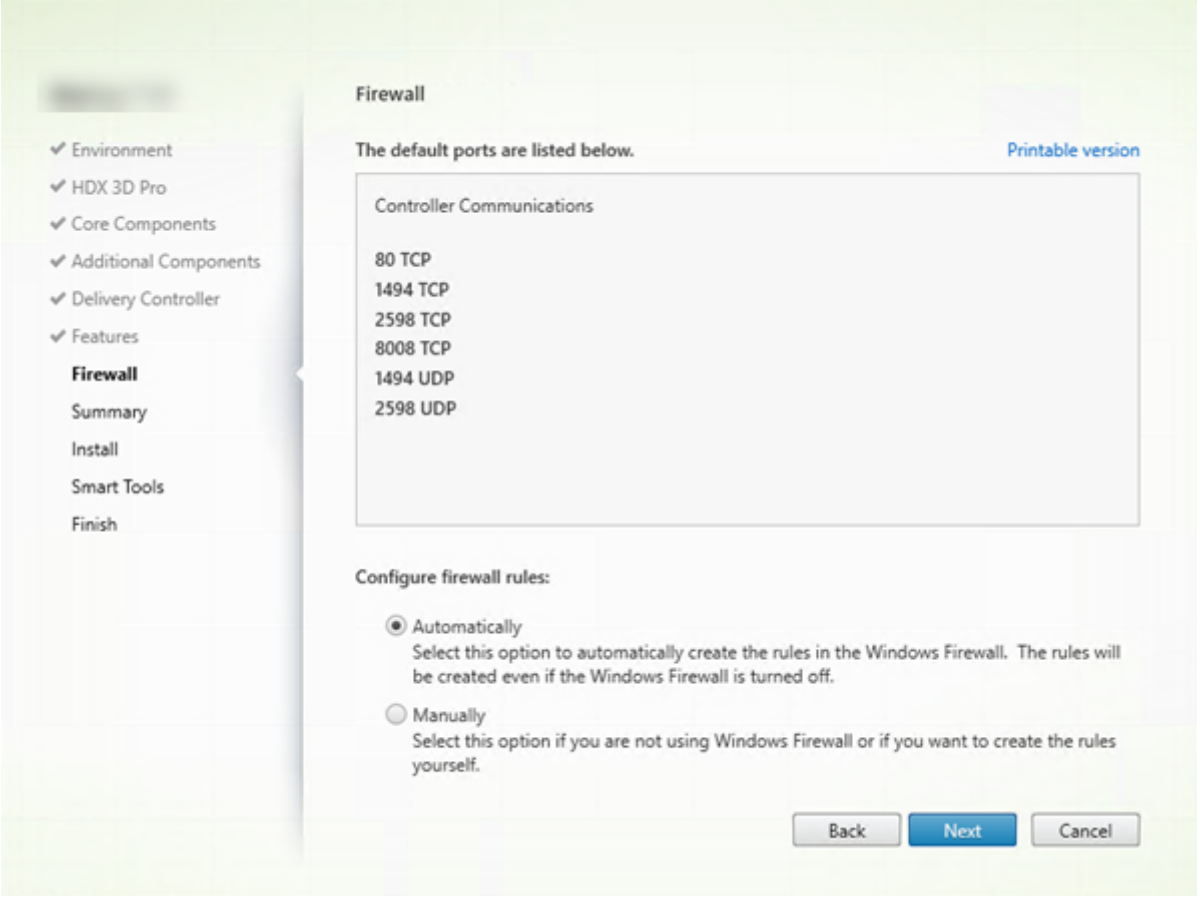
valide uniquement lors de l'installation d'un VDA pour OS de bureau sur une VM. Cette case à cocher est disponible uniquement si la case Citrix AppDisk / Personal vDisk est sélectionnée sur la page **Composants supplémentaires**. Lorsque cette case à cocher est activée, les AppDisks et Personal vDisks peuvent être utilisés. Pour de plus amples informations, consultez les sections AppDisks et Personal vDisks.

Option de ligne de commande : /baseimage

Si vous utilisez le programme d'installation VDAWorkstationCoreSetup.exe, cette fonctionnalité ne s'affiche pas dans l'assistant et l'option de ligne de commande n'est pas valide.

Cliquez sur **Next**.

Étape 10 – Ports du pare-feu

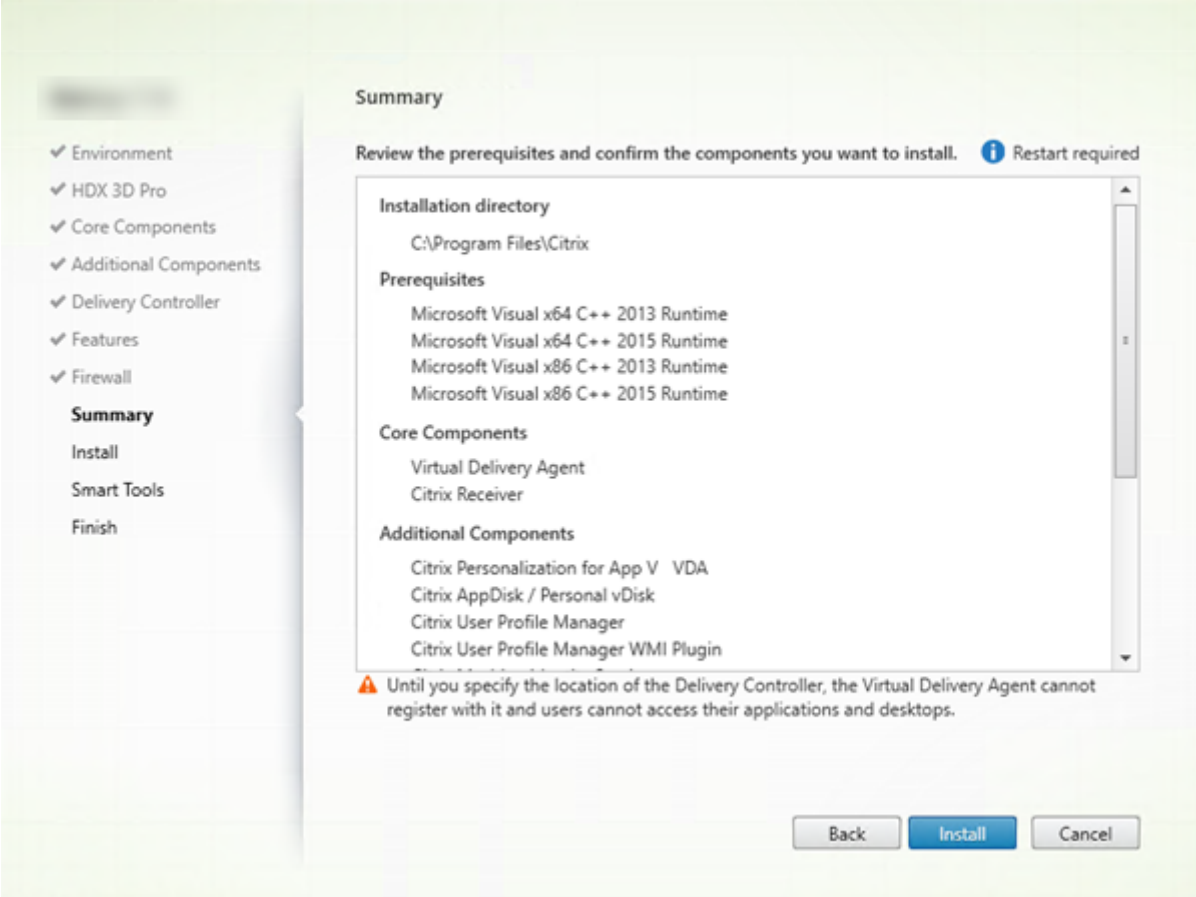


Sur la page **Pare-feu**, par défaut, les ports sont ouverts automatiquement si le service Pare-feu Windows est en cours d'exécution, même si le pare-feu n'est pas activé. Ce paramètre par défaut convient à la plupart des déploiements. Pour obtenir des informations sur le port, consultez la section Ports réseau.

Cliquez sur **Next**.

Option de ligne de commande : /enable_hdx_ports

Étape 11 – Vérifier les composants requis et confirmer l'installation

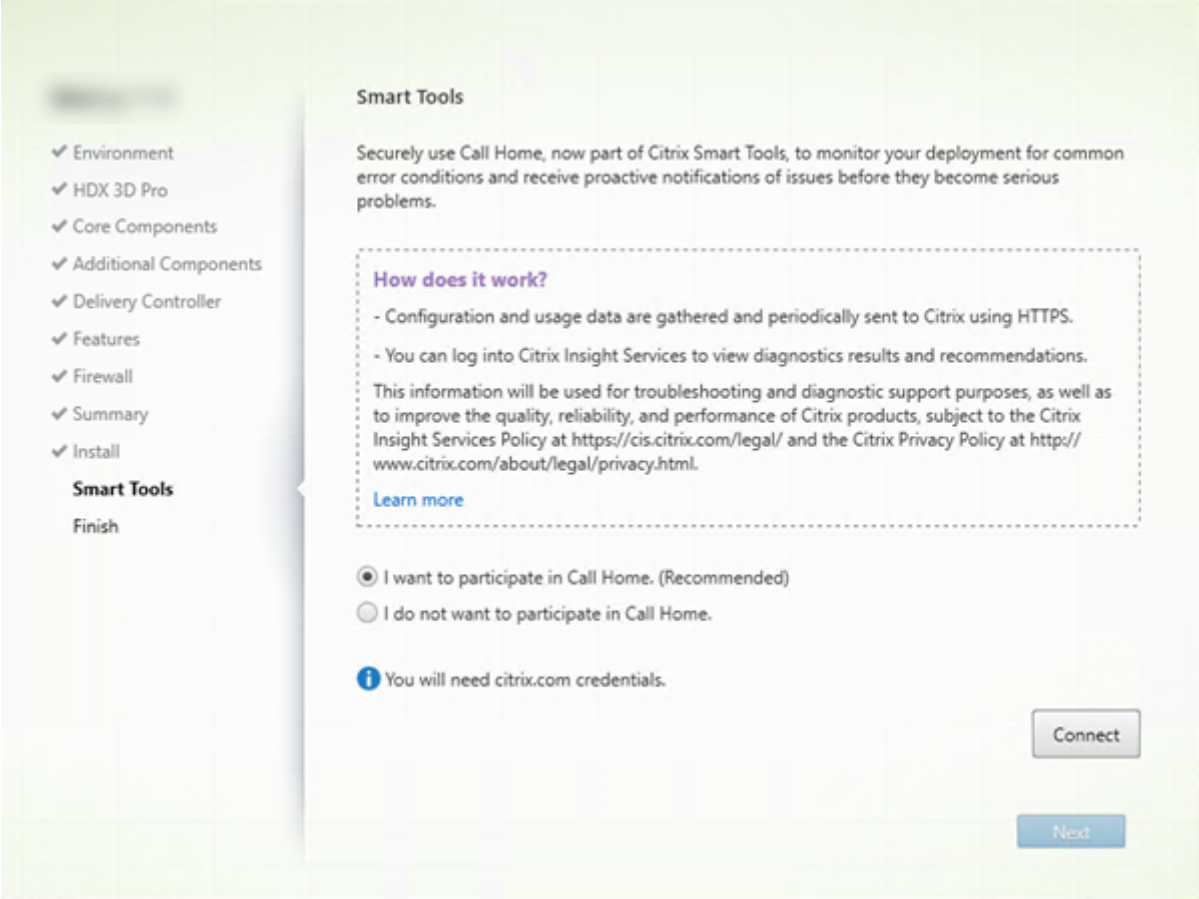


La page **Résumé** répertorie les éléments qui seront installés. Utilisez le bouton Précédent pour revenir sur les pages précédentes de l'assistant et modifier les réglages.

Lorsque vous êtes prêt, cliquez sur **Installer**.

Si des composants requis ne sont pas déjà installés/activés, la machine peut redémarrer une ou deux fois. Consultez la section Préparer l'installation.

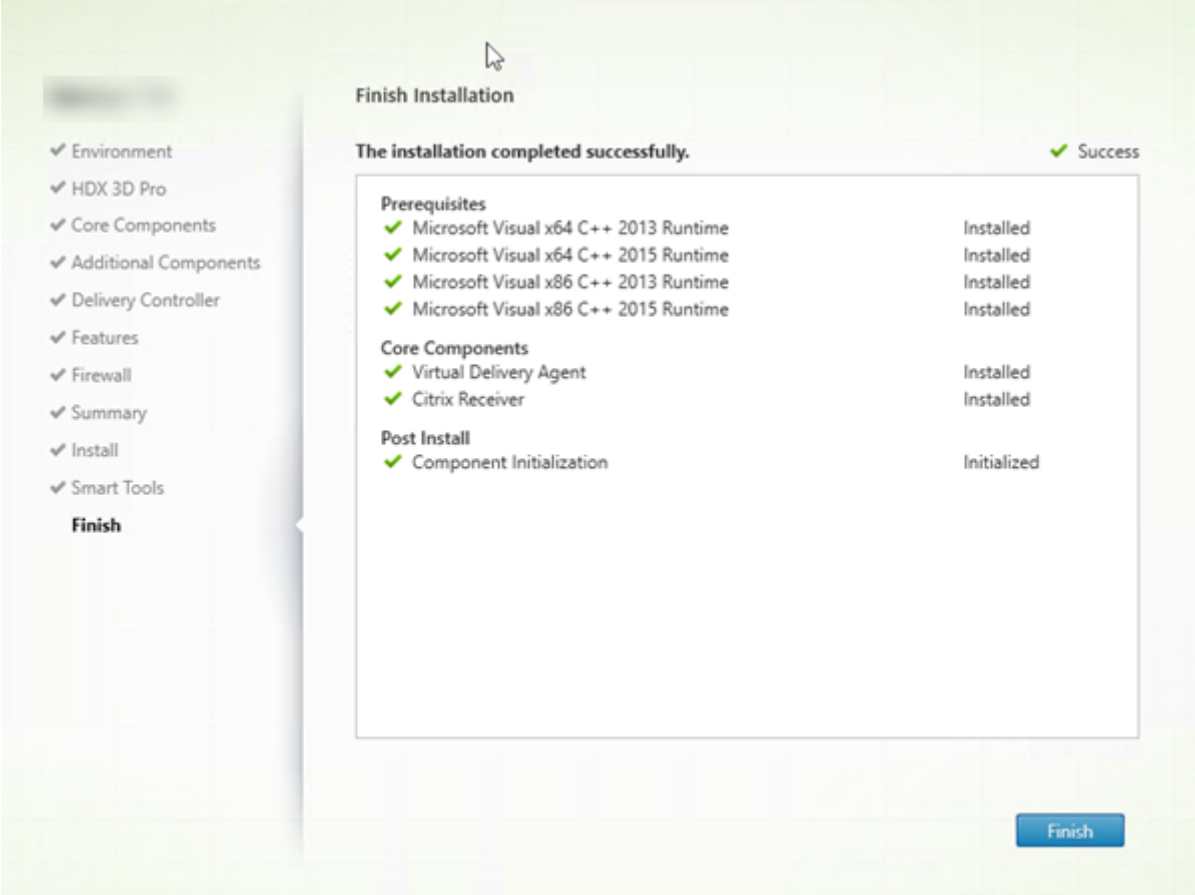
Étape 12 – Participer à Smart Tools



Sur la page **Smart Tools**, indiquez si vous souhaitez participer à Citrix Call Home, qui fait désormais partie de Citrix Smart Tools. Si vous choisissez de participer (valeur par défaut), cliquez sur **Connecter**. Lorsque vous y êtes invité, entrez vos informations d'identification de compte Citrix.

Une fois que vos informations d'identification sont validées (ou si vous choisissez de ne pas participer au programme), cliquez sur **Suivant**.

Étape 13. Terminer cette installation



La page **Terminer** contient des coches vertes pour tous les éléments pré-requis et composants installés et initialisés avec succès.

Cliquez sur **Terminer**. Par défaut, la machine redémarre automatiquement (bien que vous puissiez désactiver le redémarrage automatique, le VDA ne peut pas être utilisé jusqu'à ce que la machine redémarre).

Étape suivante : Installer d'autres VDA et continuer la configuration

Répétez les étapes ci-dessus pour installer des VDA sur d'autres machines ou images, si nécessaire.

Après avoir installé tous les VDA, démarrez Studio. Si vous n'avez pas encore créé de site, Studio vous guide dans cette tâche. Lorsque vous avez terminé, Studio vous guide dans la création d'un catalogue de machines, puis d'un groupe de mise à disposition. Voir :

- Créer un site
- Créer des catalogues de machines
- Créer des groupes de mise à disposition

Plus tard, si vous voulez personnaliser un VDA installé :

1. À partir de la fonctionnalité Windows de suppression ou modification des programmes, sélectionnez **Citrix Virtual Delivery Agent** ou **Citrix Remote PC Access/VDI Core Services VDA**. Cliquez ensuite avec le bouton droit sur **Modifier**.
2. Sélectionnez **Personnaliser les paramètres Virtual Delivery Agent**. Lorsque le programme d'installation démarre, vous pouvez modifier :

- les adresses de Controller
- le numéro du port TCP/IP à enregistrer auprès du Controller (valeur par défaut = 80)
- si les ports de pare-feu Windows doivent s'ouvrir automatiquement

Dépannage

Si votre déploiement utilise Microsoft System Center Configuration Manager, l'installation d'un VDA peut sembler avoir échoué avec le code de sortie 3, bien que le VDA ait été installé avec succès. Pour éviter ce message erroné, vous pouvez wrapper votre installation dans un script CMD ou modifier les codes de réussite dans votre pack Configuration Manager. Pour de plus amples informations, consultez le forum de discussion sur https://discussions.citrix.com/topic/350000-sccm-install-of-vda-71-fails-with-exit-code-3/.

Dans l'écran Studio d'un groupe de mise à disposition, l'entrée « Version de VDA installée » dans le panneau Détails peut ne pas être la version installée sur les machines. Les programmes et fonctionnalités Windows de la machine affichent la version actuelle du VDA.

Installer à l'aide de la ligne de commande

February 28, 2019

Cet article s'applique à l'installation de composants sur des machines avec systèmes d'exploitation Windows. Pour de plus amples informations sur les VDA pour systèmes d'exploitation Linux, consultez la documentation Virtual Delivery Agent Linux.

> **Important :**
>
> Cet article explique comment émettre des commandes d'installation du produit. Avant de procéder à une installation, consultez l'article Préparer l'installation. Cet article contient des descriptions des programmes d'installation disponibles.

Pour pouvoir suivre la progression de l'exécution de la commande en cours et des valeurs de retour, vous devez être l'administrateur d'origine ou utiliser l'option **Exécuter en tant qu'administrateur**. Pour plus d'informations, veuillez consulter la documentation des commandes Microsoft.

En complément des commandes d'installation directes, des exemples de scripts sont fournis sur le fichier ISO du produit que vous pouvez utiliser pour installer, mettre à niveau ou supprimer des VDA dans Active Directory. Pour de plus amples informations, consultez Installer les VDA à l'aide de scripts.

Utiliser le programme d'installation du produit entier

Pour accéder à l'interface de la ligne de commande du programme d'installation du produit complet :

1. Téléchargez le pack du produit auprès de Citrix. Des informations d'identification de compte Citrix sont requises pour accéder au site de téléchargement.
2. Décompressez le fichier. Éventuellement, gravez un DVD du fichier ISO.
3. Ouvrez une session sur le serveur sur lequel vous installez les composants, à l'aide d'un compte d'administrateur local.
4. Insérez le DVD dans le lecteur ou montez le fichier ISO.
5. À partir du répertoire \x64\XenDesktop Setup du support d'installation, exécutez la commande appropriée.

Pour installer les composants principaux

Exécutez la commande **XenDesktopServerSetup.exe** avec les options répertoriées dans la section Options de ligne de commande pour l'installation des composants principaux.

Pour installer un VDA

Exécutez la commande **XenDesktopVDASetup.exe** avec les options répertoriées dans la section Options de ligne de commande pour l'installation d'un VDA.

Pour installer le Serveur d'impression universelle

Suivez les instructions de la section Installer le Serveur d'impression universelle à l'aide de la ligne de commande.

Pour installer le service d'authentification fédérée

Citrix vous recommande d'utiliser l'interface graphique.

Pour installer le service de réinitialisation en libre-service des mots de passe

Suivez les instructions de la documentation du service de réinitialisation en libre-service des mots de passe.

Utiliser le programme d'installation de VDA autonome

Des informations d'identification de compte Citrix sont requises pour accéder au site de téléchargement. vous devez soit disposer de privilèges d'administrateur avant de démarrer l'installation, soit utiliser l'option **Exécuter en tant qu'administrateur**.

- Téléchargez le pack approprié auprès de Citrix :

Nom du composant sur la page de téléchargement	Nom de fichier du programme d'installation
Virtual Delivery Agent <*version*> OS de serveur	VDAServerSetup.exe
Virtual Delivery Agent <*version*> OS de bureau	VDAWorkstationSetup.exe
Virtual Delivery Agent <*version*> OS de bureau - Services de base	VDAWorkstationCoreSetup.exe

- Vous pouvez extraire les fichiers du pack dans un répertoire existant, puis exécuter la commande d'installation, ou uniquement exécuter le pack.

Pour extraire les fichiers avant l'installation, utilisez **/extract** avec le chemin d'accès absolu ; par exemple, .\VDAWorkstationCoreSetup.exe /extract %temp%\CitrixVDAInstallMedia. (Le répertoire doit exister. Sinon, l'extraction échoue.) Ensuite, dans une commande séparée, exécutez **XenDesktopVdaSetup.exe** à partir du répertoire contenant le contenu extrait (dans l'exemple ci-dessus, CitrixVDAInstallMedia). Utilisez les options valides répertoriées dans la section Options de ligne de commande pour l'installation d'un VDA.

Pour exécuter le pack téléchargé, exécutez son nom : **VDAServerSetup.exe**, **VDAWorkstationSetup.exe** ou **VDAWorkstationCoreSetup.exe**. Utilisez les options valides répertoriées dans la section Options de ligne de commande pour l'installation d'un VDA.

Si vous connaissez le programme d'installation de la version complète du produit :

- Exécutez le programme d'installation autonome VDAServerSetup.exe ou VDAWorkstationSetup.exe comme s'il s'agissait de la commande XenDesktopVdaSetup.exe sauf pour le nom.
- Le programme d'installation VDAWorkstationCoreSetup.exe est différent, car il prend en charge un sous-ensemble des options disponibles avec les autres programmes d'installation.

Options de ligne de commande pour l'installation des composants principaux

Les options suivantes sont valides lors de l'installation des composants principaux à l'aide de la commande **XenDesktopServerSetup.exe**. Pour de plus amples informations sur les options disponibles, consultez la section Installer les composants principaux.

/components <*composant*> [,<*composant*>] ...

Liste séparée par des virgules des composants à installer ou supprimer. Les valeurs autorisées sont :

CONTROLLER : Controller

DESKTOPSTUDIO : Studio

DESKTOPDIRECTOR : Director

LICENSESERVER : Serveur de licences Citrix

STOREFRONT : StoreFront

Si cette option est omise, tous les composants sont installés (ou supprimés, si l'option /remove est également spécifiée).

/configure_firewall

Ouvre tous les ports du pare-feu Windows utilisés par les composants installés, si le service Pare-feu Windows est en cours d'exécution, même si le pare-feu n'est pas activé. Si vous utilisez un pare-feu tiers ou aucun pare-feu, vous devez ouvrir les ports manuellement.

/disableexperiencemetrics

Empêche l'envoi automatique des analyses collectées au cours de l'installation, de la mise à niveau ou de la suppression à Citrix.

/exclude

Empêche l'installation de fonctions, services ou technologies séparés par des virgules, entourés de guillemets droits. Les valeurs autorisées sont :

"Stockage du cache d'hôte local (LocalDB)" : empêche l'installation de la base de données utilisée pour le cache d'hôte local. Cette option n'a aucun effet sur l'installation de SQL Server Express pour une utilisation en tant que base de données du site.

« Smart Tools Agent » : empêche l'installation de l'agent Citrix Smart Tools.

/help ou/h

Affiche la commande d'aide.

/installdir <*directory*>

Répertoire vide existant où les composants seront installés. Valeur par défaut : c:\Program Files\Citrix.

/logpath <*path*>

Emplacement du fichier journal. Le dossier spécifié doit exister. Le programme d'installation ne le crée pas. Valeur par défaut = "%TEMP%\Citrix\XenDesktop Installer"

/no_remote_assistance

(Valide uniquement lors de l'installation de Director.) Désactive la fonctionnalité d'observation utilisateur qui utilise l'Assistance à distance Windows.

/noreboot

Empêche un redémarrage après l'installation. (Pour la plupart des composants principaux, aucun redémarrage n'est activé par défaut).

/nosql

Empêche l'installation de Microsoft SQL Server Express sur le serveur sur lequel vous installez le Controller. Si cette option est omise, SQL Server Express est installé pour être utilisé en tant que base de données du site. (Cette option n'a aucun effet sur l'installation de SQL Server Express LocalDB utilisé pour le cache d'hôte local).

/quiet ou /passive

Aucune interface utilisateur ne s'affiche lors de l'installation. La seule preuve de l'installation est dans le Gestionnaire des tâches Windows. Si cette option n'est pas utilisée, l'interface graphique démarre.

/remove

Supprime les principaux composants spécifiés avec l'option /components.

/removeall

Supprime tous les principaux composants installés.

/sendexperiencemetrics

Envoie automatiquement les analyses collectées au cours de l'installation, de la mise à niveau ou de la suppression à Citrix. Si cette option est omise (ou que /disableexperiencemetrics est spécifié), les analyses sont collectées localement, mais pas envoyées automatiquement.

/tempdir <*répertoire*>

Répertoire qui contient les fichiers temporaires durant l'installation. Valeur par défaut = c:\Windows\Temp.

/xenapp

Installe XenApp. Si cette option est omise, XenDesktop est installé.

Exemples : Installer les composants principaux

La commande suivante installe un Controller XenDesktop, Studio, le système de licences Citrix et SQL Server Express sur un serveur. Les ports de pare-feu requis pour les communications de composants sont ouverts automatiquement.

```
1 \x64\XenDesktop Setup\XenDesktopServerSetup.exe /components controller,
     desktopstudio,licenseserver /configure_firewall
```

La commande suivante installe un contrôleur XenApp, Studio, et SQL Server Express sur le serveur. Les ports de pare-feu requis pour les communications de composants seront ouverts automatiquement.

```
1 \x64\XenDesktop Setup\XenDesktopServerSetup.exe /xenapp /components
     controller,desktopstudio /configure_firewall
```

Options de ligne de commande pour l'installation d'un VDA

Les options suivantes sont valides avec une ou plusieurs des commandes suivantes : **XenDesktopVDASetup.exe**, **VDAServerSetup.exe**, **VDAWorkstationSetup.exe** ou **VDAWorkstationCoreSetup.exe**.

/baseimage

valide uniquement lors de l'installation d'un VDA pour OS de bureau sur une VM. Permet d'utiliser des Personal vDisk avec une image principale. Pour plus d'informations, consultez la section Personal vDisk.

Cette option n'est pas valide lors de l'utilisation du programme d'installation **VDAWorkstationCoreSetup.exe**.

/components <*composant*>[,<*composant*>]

Liste séparée par des virgules des composants à installer ou supprimer. Les valeurs autorisées sont :

VDA : Virtual Delivery Agent

PLUGINS : Citrix Receiver pour Windows (CitrixReceiver.exe)

Par exemple, pour installer le VDA, mais pas Citrix Receiver, spécifiez l'option /components vda.

Si cette option est omise, tous les composants sont installés.

Cette option n'est pas valide lors de l'utilisation du programme d'installation **VDAWorkstationCoreSetup.exe**. Ce programme d'installation ne peut pas installer Citrix Receiver.

/controllers "<*contrôleur*> [<*contrôleur*>] [...]"

Noms de domaines complets (FQDN) des Controller avec lesquels le VDA peut communiquer, séparés par des espaces et entourés de guillemets droits. Ne spécifiez pas à la fois les options /site_guid et /controllers.

/disableexperiencemetrics

Envoie automatiquement les analyses collectées au cours de l'installation, de la mise à niveau ou de la suppression à Citrix.

/enable_framehawk_port

Ouvre les ports UDP utilisés par Framehawk. Valeur par défaut = false

/enable_hdx_3d_pro

Installe le VDA en mode HDX 3D Pro.

/enable_hdx_ports

Ouvre les ports du pare-feu Windows requis par le Controller et les fonctionnalités activées (sauf l'assistance à distance Windows), si le service Pare-feu Windows est détecté, même si le pare-feu n'est pas activé. Si vous utilisez un autre pare-feu ou aucun pare-feu, vous devez configurer le pare-feu manuellement. Pour obtenir des informations sur le port, consultez la section Ports réseau.

> **Conseil :**
>
> Pour ouvrir les ports UDP que le transport adaptatif HDX utilise pour communiquer avec le Controller, spécifiez l'option /enable_hdx_udp_ports, en plus de l'option /enable_hdx_ports.

/enable_hdx_udp_ports

Ouvre les ports UDP, dans le pare-feu Windows, qui sont requis par le transport adaptatif HDX, si le Service pare-feu Windows est détecté, même si le pare-feu n'est pas activé. Si vous utilisez un autre pare-feu ou aucun pare-feu, vous devez configurer le pare-feu manuellement. Pour obtenir des informations sur le port, consultez la section Ports réseau.

> **Conseil :**
>
> Pour ouvrir les ports supplémentaires que le VDA utilise pour communiquer avec le Controller et les fonctionnalités activées, spécifiez l'option /enable_hdx_ports, en plus de l'option /enable_hdx_udp_ports.

/enable_real_time_transport

Active ou désactive l'utilisation d'UDP pour les paquets audio (Real-Time Audio Transport pour l'audio). L'activation de cette fonctionnalité peut améliorer les performances audio. Incluez l'option /enable_hdx_ports si vous souhaitez que les ports UDP soient ouverts automatiquement si le service Pare-feu Windows est détecté.

/enable_remote_assistance

Active la fonctionnalité d'observation dans l'Assistance à distance Windows pour l'utiliser avec Director. Si vous spécifiez cette option, l'Assistance à distance Windows ouvre les ports dynamiques dans le pare-feu.

/exclude "*<component>*"[,"*<component>*"]

Empêche l'installation d'un ou de plusieurs composants facultatifs séparés par des virgules, entourés de guillemets droits. Par exemple, l'installation ou la mise à niveau d'un VDA sur une image qui n'est

pas gérée par MCS ne nécessite pas les composants Personal vDisk ou Machine Identity Service. Les valeurs autorisées sont :

- Personal vDisk
- Machine Identity Service
- Citrix User Profile Manager
- Citrix User Profile Manager WMI Plugin
- Client d'impression universelle Citrix
- Citrix Telemetry Service
- Citrix Personalization pour AppV : VDA

L'exclusion de Citrix Profile Management de l'installation (à l'aide de l'option /exclude "Citrix User Profile Manager") affecte la surveillance et la résolution des problèmes des VDA avec Citrix Director. Sur les pages Détails de l'utilisateur et Point de terminaison, les panneaux Personnalisation et Durée de l'ouverture de session échouent. Sur les pages Tableau de bord et Tendances, le panneau Durée moyenne d'ouverture de session affiche les données uniquement pour les machines sur lesquelles Profile Management est installé.

Même si vous n'utilisez pas une solution de gestion de profils utilisateur tierce, Citrix vous recommande d'installer et d'exécuter Citrix Profile Management Service. L'activation de Citrix Profile Management Service n'est pas nécessaire.

Cette option n'est pas valide lors de l'utilisation du programme d'installation VDAWorkstationCoreSetup.exe. Ce programme d'installation exclut automatiquement un grand nombre de ces éléments.

/h ou /help

Affiche la commande d'aide.

/hdxflashv2only

Empêche l'installation des fichiers binaires d'ancienne génération de la redirection Flash, pour une sécurité accrue.

Cette option n'est pas disponible dans l'interface graphique.

/installdir <*directory*>

Répertoire vide existant où les composants seront installés. Valeur par défaut : c:\Program Files\Citrix.

/logpath <*path*>

Emplacement du fichier journal. Le dossier spécifié doit exister. Le programme d'installation ne le crée pas. Valeur par défaut = "%TEMP%\Citrix\XenDesktop Installer"

Cette option n'est pas disponible dans l'interface graphique.

/masterimage

Valide uniquement lors de l'installation de VDA sur une VM. Définit le VDA comme image principale.

Cette option n'est pas valide lors de l'utilisation du programme d'installation VDAWorkstationCoreSetup.exe.

/no_mediafoundation_ack

Reconnaît que Microsoft Media Foundation n'est pas installé, et que plusieurs fonctionnalités multimédias de HDX ne seront pas installées et ne fonctionneront pas. Si cette option est omise et Media Foundation n'est pas installé, l'installation de VDA échoue. La plupart des éditions Windows prises en charge sont fournies avec Media Foundation, à l'exception des éditions N.

/nocitrixwddm

Valide uniquement sur les machines Windows 7 qui ne contiennent pas un pilote WDDM. Désactive l'installation du pilote Citrix WDDM.

Cette option n'est pas disponible dans l'interface graphique.

/nodesktopexperience

Valide uniquement lors de l'installation d'un VDA pour OS de serveur. Empêche l'activation de la fonctionnalité Expérience de bureau améliorée. Cette fonctionnalité est contrôlée par le paramètre de stratégie Citrix Expérience de bureau améliorée.

/noreboot

Empêche un redémarrage après l'installation. Le VDA ne peut être utilisé qu'après un redémarrage.

/noresume

Par défaut, lorsqu'un redémarrage de la machine est nécessaire pendant une installation, le programme d'installation reprend automatiquement une fois le redémarrage terminé. Pour remplacer la valeur par défaut, spécifiez /noresume. Cela peut être utile si vous devez réinstaller le support ou si vous souhaitez capturer des informations lors d'une installation automatisée.

/optimize

Valide uniquement lors de l'installation de VDA sur une VM. Permet l'optimisation des VDA exécutés dans une VM sur un hyperviseur. L'optimisation de VM comprend la désactivation des fichiers en mode déconnecté, la désactivation de la défragmentation en arrière-plan et la réduction de la taille du journal d'événements. Ne spécifiez pas cette option pour les déploiements Remote PC Access. Pour obtenir davantage d'informations, veuillez consulter l'article CTX125874.

/portnumber <*port*>

Valide uniquement si l'option /reconfig est spécifiée. Numéro de port à activer pour les communications entre le VDA et le Controller. Le port configuré précédemment est désactivé, à moins qu'il s'agisse du port 80.

/quiet ou /passive

Aucune interface utilisateur ne s'affiche lors de l'installation. La seule preuve de l'installation et de la configuration est dans le Gestionnaire des tâches Windows. Si cette option n'est pas utilisée, l'interface graphique démarre.

/reconfigure

Personnalise les paramètres VDA précédemment configurés lorsqu'il est utilisé avec les options /portnumber, /controllers ou /enable_hdx_ports. Si vous spécifiez cette option sans spécifier également l'option/quiet, l'interface graphique de personnalisation de VDA démarre.

/remotepc

Valide uniquement pour les déploiements Remote PC Access. Exclut l'installation des composants suivants sur un OS de bureau :

- Citrix Personalization pour AppV

- Citrix User Profile Manager
- Citrix User Profile Manager WMI Plugin
- Machine Identity Service
- Personal vDisk

Cette option n'est pas valide lors de l'utilisation du programme d'installation VDAWorkstationCoreSetup.exe. Ce programme d'installation exclut automatiquement l'installation de ces composants.

/remove

Supprime les composants spécifiés avec l'option /components.

/removeall

Supprime tous les composants VDA installés.

/sendexperiencemetrics

Envoie automatiquement les analyses collectées au cours de l'installation, de la mise à niveau ou de la suppression à Citrix. Si cette option est omise (ou que /disableexperiencemetrics est spécifié), les analyses sont collectées localement, mais pas envoyées automatiquement.

/servervdi

Installe un VDA pour OS de bureau sur un serveur Windows pris en charge. Évitez cette option lors de l'installation d'un VDA pour OS de serveur sur un serveur Windows. Avant d'utiliser cette option, consultez la section Server VDI.

Cette option doit uniquement être utilisée avec le programme d'installation du produit entier VDA. Cette option n'est pas disponible dans l'interface graphique.

/site_guid <*guid*>

Identificateur global unique (GUID) de l'unité d'organisation Active Directory du site. Associe un bureau virtuel à un site lorsque vous utilisez Active Directory pour la découverte (la mise à jour automatique est la méthode recommandée et la méthode de découverte par défaut). Le GUID du site est une propriété de site affichée dans Studio. Ne spécifiez pas à la fois les options /site_guid et /controllers.

/tempdir <*répertoire*>

Répertoire sur lequel stocker les fichiers temporaires durant l'installation. Valeur par défaut = c:\Windows\Temp.

Cette option n'est pas disponible dans l'interface graphique.

/virtualmachine

Valide uniquement lors de l'installation de VDA sur une VM. Remplace la détection par le programme d'installation d'une machine physique, où les informations du BIOS transmises aux VM les font passer pour des machines physiques.

Cette option n'est pas disponible dans l'interface graphique.

Exemples : Installer un VDA

Installer un VDA avec le programme d'installation complet du produit

La commande suivante installe un VDA pour OS de bureau et Citrix Receiver à l'emplacement par défaut sur une VM. Ce VDA sera utilisé comme une image principale. Le VDA s'enregistrera initialement auprès du Controller sur le serveur appelé « Contr-Main » dans le domaine « mondomaine ». Le VDA utilisera des Personal vDisks, la fonctionnalité d'optimisation et l'Assistance à distance Windows.

```
1 \x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /components vda,
    plugins /controllers "Contr-Main.mydomain.local" /enable_hdx_ports /
    optimize /masterimage /baseimage /enable_remote_assistance
```

Installer un VDA pour OS de bureau avec le programme d'installation autonome VDAWorkstationCoreSetup

La commande suivante installe un VDA Core Services sur un OS de bureau à utiliser dans un déploiement VDI ou Remote PC Access. Citrix Receiver et les autres services non fondamentaux ne sont pas installés. L'adresse d'un Controller est spécifiée, et les ports du Service de pare-feu Windows seront automatiquement ouverts. L'administrateur doit gérer les redémarrages.

```
1 VDAWorkstationCoreSetup .exe /quiet /controllers "Contr-East.domain.com
    " /enable_hdx_ports /noreboot
```


Personnaliser un VDA à l'aide de la ligne de commande

Une fois que vous avez installé un VDA, vous pouvez personnaliser plusieurs paramètres. À partir du répertoire \x64\XenDesktop Setup du support du produit, exécutez la commande `XenDesktopVdaSetup.exe`, à l'aide d'une ou plusieurs des options suivantes, qui sont décrites dans la section Options de ligne de commande pour l'installation d'un VDA.

- /reconfigure (option requise lors de la personnalisation d'un VDA)
- /h ou /help
- /quiet
- /noreboot
- /controllers
- /portnumber port
- /enable_hdx_ports

Installer le Serveur d'impression universelle à l'aide de la ligne de commande

Exécutez l'une des commandes suivantes sur chaque serveur d'impression :

- Sur un système d'exploitation 32 bits pris en charge : à partir du répertoire \x86\Universal Print Server\ sur le support d'installation Citrix, exécutez **UpsServer_x86.msi**.
- Sur un système d'exploitation 64 bits pris en charge : à partir du répertoire \x64\Universal Print Server\ sur le support d'installation Citrix, exécutez **UpsServer_x64.msi**.

Après avoir installé le composant du serveur d'impression universelle sur vos serveurs d'impression, configurez ce dernier à l'aide des instructions de la section Provisionner les imprimantes.

Installer les VDA à l'aide de scripts

January 23, 2019

Cet article s'applique à l'installation de VDA sur des machines avec systèmes d'exploitation Windows. Pour de plus amples informations sur les VDA pour systèmes d'exploitation Linux, consultez la documentation Virtual Delivery Agent Linux.

Le support d'installation contient des exemples de scripts qui permettent d'installer, mettre à niveau ou supprimer les VDA pour des machines dans Active Directory. Vous pouvez également appliquer les scripts à des machines individuelles, et les utiliser pour gérer les images principales utilisées par Machine Creation Services et Provisioning Services.

Accès requis :

- Les scripts doivent disposer d'un accès en lecture Tout le monde sur le partage réseau sur lequel figure la commande d'installation. La commande d'installation est XenDesktopVdaSetup.exe dans l'image ISO du produit complet ou VDAWorkstationSetup.exe ou VDAServerSetup.exe dans un programme d'installation autonome.
- Les informations de journalisation sont stockées sur chaque machine locale. Pour consigner les résultats de manière centralisée à des fins de vérification et d'analyse, les scripts doivent disposer d'un accès en lecture et écriture Tout le monde sur le partage réseau approprié.

Pour vérifier les résultats de l'exécution d'un script, examinez le partage du journal central. Les journaux consignés incluent le journal du script, le journal du programme d'installation et les journaux d'installation MSI. Chaque tentative d'installation ou de suppression est enregistrée dans un dossier horodaté. Le titre du dossier indique le résultat de l'opération avec le préfixe PASS ou FAIL. Vous pouvez utiliser les outils de recherche d'annuaire standard pour trouver une installation ayant échoué ou une suppression dans le journal central. Cela vous évite d'effectuer une recherche locale sur les machines cibles.

> **Important :**
>
> Avant de commencer l'installation, lisez et complétez les tâches décrites dans la section Préparer l'installation.

Installer ou mettre à niveau des VDA à l'aide du script

1. Obtenez le script exemple InstallVDA.bat à partir de \Support\AdDeploy\ sur le support d'installation. Citrix vous recommande d'effectuer une sauvegarde du script d'origine avant de le personnaliser.
2. Modifiez le script :
   - Spécifiez la version du VDA à installer : SET DESIREDVERSION. Par exemple, la version 7 peut être spécifiée comme 7.0. La valeur complète est disponible sur le support d'installation dans le fichier ProductVersion.txt (par exemple, 7.0.0.3018). Toutefois, une correspondance complète n'est pas nécessaire.
   - Spécifiez l'emplacement du partage réseau où le programme d'installation va être appelé. Pointez sur la racine de la structure (point le plus élevé de l'arborescence). La version appropriée du programme d'installation (32 bits ou 64 bits) est automatiquement appelée lorsque le script s'exécute. Par exemple : SET DEPLOYSHARE =\\\fileserver1 share1.
   - Si vous le souhaitez, vous pouvez spécifier un emplacement de partage réseau pour le stockage des journaux centralisés. Par exemple : SET LOGSHARE=\\fileserver1\log1.
   - Spécifiez les options de configuration VDA comme décrit dans la section Installer à l'aide de la ligne de commande. Les options /quiet et /noreboot sont incluses par défaut dans le script et sont requises : SET COMMANDLINEOPTIONS =/QUIET/NOREBOOT.
3. À l'aide de scripts de démarrage de stratégie de groupe, attribuez le script à l'unité

d'organisation contenant vos machines. Cette unité d'organisation doit uniquement contenir les machines sur lesquelles vous souhaitez installer le VDA. Lorsque les machines dans l'unité d'organisation sont redémarrées, le script s'exécute sur toutes ces machines. Un VDA est installé sur chaque machine qui dispose d'un système d'exploitation pris en charge.

Supprimer des VDA à l'aide du script

1. Obtenez le script exemple UninstallVDA.bat à partir de \Support\AdDeploy\ sur le support d'installation. Citrix vous recommande d'effectuer une sauvegarde du script d'origine avant de le personnaliser.
2. Modifiez le script.
   - Spécifiez la version du VDA à supprimer : SET CHECK_VDA_VERSION. Par exemple, la version 7 peut être spécifiée comme 7.0. La valeur complète est disponible sur le support d'installation dans le fichier ProductVersion.txt (par exemple, 7.0.0.3018). Toutefois, une correspondance complète n'est pas nécessaire.
   - Si vous le souhaitez, vous pouvez spécifier un emplacement de partage réseau pour le stockage des journaux centralisés.
3. À l'aide de scripts de démarrage de stratégie de groupe, attribuez le script à l'unité d'organisation contenant vos machines. Cette unité d'organisation doit uniquement contenir les machines sur lesquelles vous souhaitez supprimer le VDA. Lorsque les machines dans l'unité d'organisation sont redémarrées, le script s'exécute sur toutes ces machines et supprime un VDA de chaque machine. Le VDA est supprimé de chaque machine.

Dépannage

Le script génère des fichiers journaux internes qui décrivent la progression de l'exécution du script. Le script copie un journal Kickoff_VDA_Startup_Script sur le partage de journal central quelques secondes après le démarrage du déploiement sur la machine. Vous pouvez vérifier que le processus fonctionne. Si ce journal n'est pas copié dans le partage de journaux central comme prévu, corrigez le problème en inspectant la machine locale. Le script place deux fichiers journaux de débogage dans le dossier %temp% sur chaque machine :

- Kickoff_VDA_Startup_Script_<horodatage>.log
- VDA_Install_ProcessLog_<horodatage>.log

Vérifiez ces journaux pour vous assurer que le script :

- S'exécute comme prévu.
- Détecte correctement le système d'exploitation cible.
- Est correctement configuré pour pointer vers le ROOT du partage DEPLOYSHARE (contient le fichier appelé AutoSelect.exe).

- Est capable de s'authentifier auprès des partages DEPLOYSHARE et LOG.

Créer un site

February 28, 2019

Un *site* est le nom que vous donnez à un déploiement XenApp ou XenDesktop. Il comprend les Delivery Controller et autres composants principaux, les VDA, les connexions aux hôtes, les catalogues de machines et les groupes de mise à disposition. Vous créez le site après avoir installé les composants et avant la création du premier catalogue de machines et groupe de mise à disposition.

Lorsque vous créez un site, vous êtes automatiquement inscrit au Programme d'amélioration de l'expérience utilisateur Citrix (CEIP). CEIP recueille des informations d'utilisation et des statistiques anonymes, puis les envoie à Citrix. Le premier package de données est envoyé à Citrix approximativement sept jours après la création du site. Vous pouvez modifier votre inscription à tout moment après la création du site. Sélectionnez **Configuration** dans le volet de navigation Studio, puis l'onglet Assistance produit et suivez les instructions. Pour plus de détails, consultez https://more.citrix.com/XD-CEIP.

L'utilisateur qui crée un site devient un administrateur complet ; pour de plus amples informations, consultez la section Délégation de l'administration.

Lisez cet article avant de démarrer l'Assistant Création de site.

Pour créer un site

Ouvrez Studio, s'il n'est pas déjà ouvert. Vous êtes automatiquement dirigé vers l'action qui lance l'assistant de création de site. Les pages de l'assistant couvrent la configuration suivante :

Type et nom du site

Il existe deux types de site ; choisissez-en un :

- **Site de mise à disposition d'applications et de bureaux**. Si vous créez un site de mise à disposition d'applications et de bureaux, vous pouvez également choisir de créer un site de déploiement complet (recommandé) ou un site vide. Un site vide est uniquement partiellement configuré et il est généralement créé par des administrateurs expérimentés.
- **Site Remote PC Access**. Un site Remote PC Access autorise les utilisateurs désignés à accéder à distance à leurs ordinateurs de bureau via une connexion sécurisée.

Si vous créez maintenant un déploiement de mise à disposition d'applications et de bureaux, vous pouvez ajouter un déploiement Remote PC Access plus tard. Inversement, si vous créez

un déploiement Remote PC Access maintenant, vous pouvez ajouter un déploiement complet ultérieurement.

Tapez un nom pour le site. Une fois le site créé, son nom apparaît en haut du volet de navigation Studio : **Citrix Studio** (*nom du site*).

Bases de données

La page **Bases de données** contient des sélections permettant de configurer les bases de données Site, Surveillance et Journalisation de la configuration. Pour de plus amples informations sur les choix et les exigences de configuration de base de données, consultez la section Bases de données.

Si vous choisissez d'installer le logiciel SQL Server Express en tant que base de données du site (paramètre par défaut), un redémarrage se produit après l'installation du logiciel. Ce redémarrage ne se produit pas si vous choisissez de ne pas installer le logiciel SQL Server Express en tant que base de données du site.

Si vous n'utilisez pas la valeur par défaut SQL Server Express, assurez-vous que le logiciel SQL Server est installé sur les machines avant de créer un site. La section Configuration système requise répertorie les versions prises en charge.

Si vous souhaitez ajouter plusieurs Controller au site, et que vous avez déjà installé le logiciel du Controller sur d'autres serveurs, vous pouvez ajouter ces Controller au site à partir de cette page. Si vous souhaitez générer des scripts qui configurent les bases de données, ajoutez les Controller avant de générer les scripts.

Licences

Posez-vous la question de savoir si vous allez utiliser des licences existantes ou l'évaluation gratuite de 30 jours qui vous permet d'ajouter des fichiers de licences ultérieurement. Vous pouvez aussi ajouter ou télécharger des fichiers de licences à partir de l'assistant de création de site. Consultez la documentation relative au système de licences pour plus d'informations.

Indiquez l'adresse du serveur de licences sous la forme *nom*:[*port*]. Le nom doit être un nom de domaine complet, NetBIOS ou une adresse IP. Un nom de domaine complet est recommandé. Si vous omettez le numéro de port, la valeur par défaut est 27000. Cliquez sur **Connect**. Vous ne pouvez pas passer à la page suivante de l'assistant tant qu'une connexion n'a pas été établie avec le serveur de licences.

Gestion de l'alimentation (Remote PC Access uniquement)

Consultez la section Remote PC Access.

Connexion hôte, réseau et stockage

Si vous utilisez des machines virtuelles sur un hyperviseur ou service de cloud pour fournir des bureaux et des applications, vous pouvez éventuellement créer la première connexion à cet hôte. Vous pouvez également spécifier des ressources réseau et de stockage pour cette connexion. Après avoir créé le site, vous pouvez modifier cette connexion et les ressources et créer davantage de connexions. Pour de plus amples informations, veuillez consulter la section Connexions et ressources.

Page de connexion : voir Sources d'informations du type de connexion.

- Si vous n'utilisez pas de VM sur un hyperviseur où un service de cloud (ou si vous utilisez Studio pour gérer les bureaux sur des PC lames dédiés), sélectionnez le type de connexion **Aucun**.
- Si vous configurez un site Remote PC Access et prévoyez d'utiliser la fonctionnalité Wake on LAN, sélectionnez le type **Microsoft System Center Configuration Manager**.

Outre le type de connexion, spécifiez également si vous allez utiliser les outils Citrix (tels que Machine Creation Services) ou d'autres outils pour créer des VM.

Pages stockage et réseau : voir Stockage hôte, Gestion du stockage et Sélection du stockage pour plus d'informations sur les types de stockage et les méthodes de gestion.

Fonctionnalités supplémentaires

Vous pouvez sélectionner des fonctionnalités pour personnaliser votre site. Lorsque vous sélectionnez la case à cocher d'un élément qui requiert des informations, une boîte de dialogue de configuration s'affiche.

Intégration de AppDNA

Valable si vous utilisez des AppDisk et avez installé AppDNA. L'intégration AppDNA permet une analyse des applications dans les AppDisk. Vous pouvez ensuite passer en revue les problèmes de compatibilité et prendre les actions correctives pour résoudre ces problèmes. Pour plus d'informations, veuillez consulter la section AppDisks.

App-V Publishing

Sélectionnez cette fonctionnalité si vous utilisez des applications à partir de packages Microsoft App-V sur des serveurs App-V. Fournissez l'URL du serveur de gestion App-V ainsi que l'URL et le numéro de port du serveur de publication App-V.

Si vous utilisez des applications depuis les packages App-V sur des emplacements de partage réseau uniquement, vous n'avez pas besoin d'activer cette fonctionnalité.

Vous pouvez également activer/désactiver et configurer cette fonctionnalité ultérieurement dans Studio. Pour obtenir davantage d'informations, veuillez consulter la section App-V.

Remote PC Access

Pour de plus amples informations sur les déploiements Remote PC Access, consultez la section Remote PC Access.

Si vous utilisez la fonctionnalité Wake on LAN, suivez les étapes de configuration sur la console Microsoft System Center Configuration Manager avant de créer le site. Pour de plus amples informations, veuillez consulter la section Microsoft System Center Configuration Manager.

Lorsque vous créez un site Remote PC Access :

- Si vous utilisez la fonctionnalité Wake on LAN, spécifiez l'adresse, les informations d'identification et les informations de connexion Microsoft System Center Configuration Manager sur la page **Gestion de l'alimentation**.
- Spécifiez les utilisateurs ou les groupes d'utilisateurs sur la page **Utilisateurs**. Il n'y a aucune action par défaut qui ajoute automatiquement tous les utilisateurs. Vous pouvez également spécifier des comptes de machines (domaine et unité d'organisation (UO)) sur la page **Comptes de machines**.

  Pour ajouter des informations utilisateur, cliquez sur **Ajouter des utilisateurs**. Sélectionnez des utilisateurs et des groupes d'utilisateurs, puis cliquez sur **Ajouter des utilisateurs**.

  Pour ajouter des informations sur les comptes d'ordinateur, cliquez sur **Ajouter des comptes de machines**. Sélectionnez les comptes de machines, puis cliquez sur **Ajouter des comptes de machines**. Cliquez sur **Ajouter des unités d'organisation**. Sélectionnez le domaine et les unités d'organisation et indiquez si les éléments des sous-dossiers doivent être inclus. Cliquez sur **Ajouter des unités d'organisation**.

Lorsque vous créez un site Remote PC Access, un catalogue de machines appelé Remote PC User Machine Accounts est créé automatiquement. Le catalogue contient tous les comptes de machine que vous avez ajoutés dans l'Assistant Création de site. Un groupe de mise à disposition appelé Remote PC User Desktops est créé automatiquement. Le groupe contient tous les utilisateurs et les groupes d'utilisateurs que vous avez ajoutés.

Synthèse

La dernière page de l'assistant de création de site présente les informations que vous avez spécifiées. Utilisez le bouton **Précédent** si vous souhaitez modifier quoi que ce soit. Lorsque vous avez terminé, cliquez sur **Créer** ; la création de site commence.

Tester une configuration de site

Pour exécuter des tests après avoir créé le site, sélectionnez **Citrix Studio (*Sitenom* site)** dans la partie supérieure du panneau de navigation. Cliquez ensuite sur **Tester le site** dans le panneau central. Vous pouvez afficher un rapport HTML des résultats de test du site.

La fonctionnalité de test de site peut échouer pour un Controller installé sur Windows Server 2016. L'échec se produit lorsqu'un SQL Server Express local est utilisé pour la base de données de site et que le service SQL Server Browser n'est pas démarré. Pour éviter cet échec, effectuez les tâches suivantes.

1. Activez le service SQL Server Browser (si nécessaire), puis démarrez-le.
2. Redémarrez le service SQL Server (SQLEXPRESS).

Dépannage

Après avoir configuré le site, vous pouvez installer Studio et l'ajouter par l'intermédiaire de la console MMC sous la forme d'un composant logiciel enfichable sur une machine distante. Si vous essayez de supprimer ce composant logiciel enfichable plus tard, MMC peut cesser de répondre. Pour contourner le problème, redémarrez MMC.

Créer des catalogues de machines

February 28, 2019

Des collections de machines virtuelles ou physiques sont gérées comme une seule entité appelée catalogue de machines. Toutes les machines d'un catalogue ont le même type de système d'exploitation : serveur ou bureau. Un catalogue contenant des machines avec OS de serveur peut contenir des machines Windows ou Linux, mais pas les deux.

Studio vous guide dans le processus de création du premier catalogue de machines après la création du site. Après la création du premier catalogue, Studio vous guide dans le processus de création du premier groupe de mise à disposition. Plus tard, vous pourrez modifier le catalogue que vous avez créé et créer des catalogues supplémentaires.

Généralités

Lorsque vous créez un catalogue de machines virtuelles, vous spécifiez comment provisionner ces ordinateurs virtuels. Vous pouvez utiliser des outils Citrix, tels que Machine Creation Services (MCS) ou Provisioning Services (PVS). Ou vous pouvez utiliser vos propres outils pour fournir des machines.

- Si vous utilisez PVS pour créer des machines, consultez la documentation Provisioning Services pour obtenir des instructions.

- Si vous utilisez MCS pour provisionner des VM, vous devez fournir une image principale (ou un instantané) pour créer des machines virtuelles identiques dans le catalogue. Avant de créer le catalogue, vous devez utiliser des outils d'hyperviseur ou de service de cloud pour créer et configurer l'image principale. Ce processus comprend l'installation d'un Virtual Delivery Agent (VDA) sur l'image. Vous créez ensuite le catalogue de machines dans Studio. Vous sélectionnez cette image (ou un instantané de cette image), spécifiez le nombre de machines virtuelles à créer dans le catalogue et configurez les informations supplémentaires.
- Si vos machines sont déjà disponibles (et vous n'avez pas besoin d'images principales), vous devez quand même créer un ou plusieurs catalogues pour ces machines.

Lorsque vous utilisez MCS ou PVS pour créer le premier catalogue, vous pouvez utiliser la connexion hôte que vous avez configurée lors de la création du site. Plus tard (après avoir créé votre premier catalogue et groupe de mise à disposition), vous pouvez modifier les informations concernant cette connexion ou créer d'autres connexions.

Une fois que vous avez créé un catalogue à l'aide de l'assistant, des tests sont exécutés automatiquement pour vous assurer qu'il est correctement configuré. Lorsque les tests sont terminés, vous pouvez afficher un rapport de test. Vous pourrez exécuter des tests à tout moment à partir de Studio.

Pour les déploiements locaux uniquement : lorsque vous utilisez MCS ou PVS pour créer le premier catalogue, vous pouvez utiliser la connexion hôte que vous avez configurée lors de la création du site. Plus tard (après avoir créé votre premier catalogue et groupe de mise à disposition), vous pouvez modifier les informations concernant cette connexion ou créer d'autres connexions.

Si vous créez un catalogue directement à l'aide du SDK du PowerShell, vous pouvez spécifier un modèle d'hyperviseur (VMTemplates), plutôt qu'une image ou un instantané.

Enregistrement de VDA

Un VDA doit être enregistré auprès d'un Delivery Controller (pour les déploiements locaux) ou Cloud Connector (pour les déploiements Citrix Cloud) pour être pris en compte lors du lancement de sessions négociées. Des VDA non enregistrés peuvent entraîner une sous-utilisation des ressources disponibles. Il existe un certain nombre de raisons pour lesquelles un VDA peut ne pas être enregistré, un grand nombre d'entre elles pouvant être résolues par un administrateur. Studio fournit des informations de dépannage dans l'assistant de création de catalogue, et après l'ajout de machines depuis un catalogue à un Delivery Group.

Dans l'assistant Créer un catalogue de machines, lorsque vous ajoutez des machines existantes, la liste des noms de compte d'ordinateur indique si chaque machine peut être ajoutée au catalogue. Placez le pointeur de la souris sur l'icône située en regard de chaque machine pour afficher un message informatif sur cette machine.

Si le message identifie une machine problématique, vous pouvez supprimer cette machine (à l'aide du

bouton **Supprimer**) ou ajouter la machine. Par exemple, si un message indique qu'il est impossible d'obtenir des informations sur une machine (peut-être parce qu'elle n'a jamais été enregistrée), vous pouvez quand même choisir d'ajouter la machine.

Pour les messages sur le niveau fonctionnel, consultez la section Versions VDA et niveaux fonctionnels.

Pour plus d'informations sur le dépannage de l'enregistrement de VDA, voir l'article CTX136668.

Résumé de la création d'un catalogue MCS

Vous trouverez ci-après une brève présentation des actions MCS par défaut à exécuter après avoir fourni les informations dans l'assistant de création d'un catalogue.

- Si vous avez sélectionné une image principale (plutôt qu'un instantané), MCS crée un instantané.
- MCS crée une copie complète de l'instantané et la place sur chaque emplacement de stockage défini dans la connexion hôte.
- MCS ajoute les machines à Active Directory, qui crée des identités uniques.
- MCS crée le nombre de VM spécifiées dans l'assistant, avec deux disques pour chaque VM. Outre les deux disques par VM, une image principale est également stockée dans le même emplacement de stockage. Si vous avez défini plusieurs emplacements de stockage, chacun obtient les types de disque suivants :
  - La copie complète de l'instantané (mentionnée ci-dessus), qui est en lecture seule et partagée entre les VM qui viennent d'être créées.
  - Un disque d'identité 16 Mo unique qui attribue à chaque VM une identité unique. Chaque VM dispose d'un disque d'identité.
  - Un disque de différence unique pour stocker les écritures effectuées sur la VM. Ce disque est provisionné par allocation dynamique (si elle est prise en charge par le stockage hôte) et augmente la taille maximale de l'image principale, si nécessaire. Chaque VM dispose d'un disque de différence. Le disque de différence conserve les modifications apportées au cours de sessions. Il est permanent pour les postes de travail dédiés. Pour les postes de travail regroupés, il est supprimé et un autre est créé après chaque redémarrage.

Éventuellement, lors de la création de machines virtuelles pour mettre à disposition des bureaux statiques, vous pouvez spécifier (sur la page **Machines** de l'assistant de création d'un catalogue de machines) des clones de VM lourds (copie complète). Les clones complets ne requièrent pas la rétention de l'image principale sur chaque magasin de données. Chaque VM dispose de son propre fichier.

Préparer une image principale sur l'hyperviseur ou le service de cloud

Pour de plus amples informations sur la création de connexions à des hyperviseurs et à des fournisseurs de cloud, consultez l'article Connexions et ressources.

L'image principale contient le système d'exploitation, les applications non virtualisées, le VDA, et d'autres logiciels.

À savoir

- Une image principale peut également être appelée image clone, image principale, VM de base ou image de base. Les fournisseurs d'hôte et les fournisseurs de service cloud peuvent utiliser des termes différents.
- Lors de l'utilisation de PVS, vous pouvez utiliser une image principale ou un ordinateur physique comme machine cible principale. PVS utilise une terminologie différente de MCS pour faire référence aux images ; consultez la documentation Provisioning Services pour plus de détails.
- Assurez-vous que l'hyperviseur ou le service cloud a suffisamment de processeurs, de mémoire et de stockage pour accueillir le nombre de machines créées.
- Configurez la bonne taille d'espace disque dur nécessaire pour les ordinateurs de bureau et les applications. Cette valeur ne peut pas être modifiée ultérieurement ou dans le catalogue de machines.
- Les catalogues de machines Remote PC Access ne requièrent pas d'images principales.
- Considérations liées à l'activation de Microsoft KMS lors de l'utilisation de MCS : si votre déploiement comprend un VDA 7.x avec XenServer 6.1 ou 6.2, vSphere ou hôte Microsoft System Center Virtual Machine Manager, vous n'avez pas à réarmer manuellement Microsoft Windows ou Microsoft Office. Si votre déploiement comprend un VDA 5.x avec un hôte XenServer 6.0.2, consultez l'articleCTX128580.
- Installez et configurez le logiciel suivant sur l'image principale :
  - Intégration des outils pour votre hyperviseur (tels que les outils XenServer, Services d'intégration Hyper-V ou outils VMware). Si vous ignorez cette étape, vos applications et bureaux risquent de ne pas fonctionner correctement.
  - Un VDA. Citrix recommande d'installer la version la plus récente pour autoriser l'accès aux dernières fonctionnalités. Si vous ne parvenez pas à installer un VDA sur l'image principale, la création du catalogue échoue.
  - Outils tiers en fonction de vos besoins, tels que le logiciel antivirus ou les agents électroniques de distribution de logiciels. Configurez les services avec les paramètres appropriés pour vos utilisateurs et le type de machine (tels que la mise à jour des fonctionnalités).
  - Les applications tierces qui ne sont pas virtualisées. Citrix recommande de virtualiser les applications. Virtualiser les applications réduit de manière significative les coûts en éliminant le besoin de mettre à jour l'image principale après l'ajout ou la reconfiguration d'une application. En outre, moins d'applications installées réduisent la taille des disques durs de l'image principale, ce qui économise les coûts de stockage.
  - Les clients App-V avec les paramètres recommandés, si vous souhaitez publier des applications App-V. Le client App-V est disponible auprès de Microsoft.
  - Lors de l'utilisation de MCS, si vous localisez Microsoft Windows, installez les paramètres régionaux et les packs de langue. Lors du provisioning, lorsqu'un instantané est créé, les

VM provisionnées utilisent les variables locales installées et les packs de langue.

> **Important :**
>
> Si vous utilisez PVS ou MCS, n'exécutez pas Sysprep sur les images principales.

Pour préparer une image principale

1. À l'aide de l'outil de gestion de votre hyperviseur, créez une image principale, puis installez le système d'exploitation, ainsi que tous les service packs et mises à jour. Indiquez le nombre de processeurs virtuels. Vous pouvez également spécifier le nombre de processeurs virtuels si vous créez le catalogue de machines à l'aide de PowerShell. Vous ne pouvez pas spécifier le nombre de processeurs virtuels lors de la création d'un catalogue à l'aide de Studio. Configurez la taille d'espace disque dur nécessaire pour les ordinateurs de bureau et les applications. Cette valeur ne peut pas être modifiée ultérieurement ou dans le catalogue.
2. Assurez-vous que le disque dur de votre ordinateur est connecté à l'emplacement de périphérique 0. La plupart des modèles d'image principale standard configurent cet emplacement par défaut, mais ce n'est peut-être pas le cas de certains modèles personnalisés.
3. Installez et configurez les logiciels répertoriés ci-dessus sur l'image principale.
4. Lors de l'utilisation de PVS, créez un fichier VHD pour le vDisk à partir de votre machine cible principale avant de joindre la machine cible principale à un domaine. Pour plus d'informations, veuillez consulter la documentation relative à Provisioning Services.
5. Si vous n'utilisez pas MCS, joignez l'image principale au domaine dont les ordinateurs de bureau et les applications sont membres. Assurez-vous que l'image principale est disponible sur l'hôte sur lequel les machines sont créées. Si vous utilisez MCS, joindre l'image principale à un domaine n'est pas nécessaire. Les machines provisionnées rejoignent le domaine spécifié dans l'assistant de création de catalogue.
6. Citrix vous recommande de créer et de nommer un instantané de l'image principale afin qu'il puisse être identifié. Si vous spécifiez une image principale plutôt qu'un instantané lors de la création d'un catalogue, Studio crée un instantané, mais vous ne pouvez pas le renommer.

Préparer une image principale pour des machines compatibles GPU sur XenServer

Lorsque vous utilisez XenServer pour votre infrastructure d'hébergement, les machines compatibles GPU requièrent une image principale dédiée. Ces machines virtuelles requièrent des pilotes de carte vidéo qui prennent en charge les processeurs graphiques. Configurez des machines prenant en charge les processeurs graphiques pour permettre à la machine virtuelle de fonctionner avec un logiciel qui utilise le processeur graphique pour les opérations.

1. Dans XenCenter, créez une VM avec un VGA, des réseaux et un processeur virtuel standard.
2. Mettez à jour la configuration de la VM pour activer l'utilisation du GPU (Passthough ou vGPU).

3. Installez un système d'exploitation pris en charge et activez RDP.
4. Installez XenServer Tools et les pilotes NVIDIA.
5. Désactiver la console Administrateur VNC (Virtual Network Computing) pour optimiser les performances, puis redémarrez la VM.
6. Vous êtes invité à utiliser le logiciel RDP (Connexion Bureau à distance). À l'aide de RDP, installez le VDA, puis redémarrez la machine virtuelle.
7. Si vous le souhaitez, vous pouvez créer un instantané de la VM en tant que modèle de la ligne de base pour d'autres images principales GPU.
8. À l'aide de RDP, installez des applications spécifiques au client qui sont configurées dans XenCenter et utilisent les capacités de processeur graphique.

Créer un catalogue de machines à l'aide de Studio

Avant de démarrer l'Assistant de création du catalogue, consultez cette section pour en savoir plus sur les choix que vous effectuerez et les informations que vous devez fournir.

Si vous utilisez une image principale, assurez-vous que vous avez installé un VDA sur l'image avant de créer le catalogue.

À partir de Studio :

- si vous avez créé un site, mais n'avez pas encore créé un catalogue de machines, Studio vous guide au bon emplacement de départ pour créer un catalogue.
- Si vous avez déjà créé un catalogue et souhaitez en créer un autre, sélectionnez **Catalogues de machines** dans le volet de navigation Studio. Sélectionnez ensuite **Créer un catalogue de machines** dans le volet Actions.

L'Assistant va vous guider au travers des éléments ci-dessous. Les pages de l'assistant qui s'affichent peuvent être différentes selon les sélections que vous effectuez.

Système d'exploitation

Chaque catalogue contient des machines d'un seul type :

- **OS de serveur :** un catalogue de machines avec OS de serveur fournit des bureaux et des applications partagés hébergés. Les machines peuvent exécuter des versions prises en charge des systèmes d'exploitation Windows ou Linux, mais le catalogue ne peut pas contenir les deux. (Consultez la documentation VDA Linux pour de plus amples informations sur ce système d'exploitation.)
- **OS de bureau :** un catalogue avec OS de bureau fournit des bureaux et des applications VDI qui peuvent être affectés à différents utilisateurs.

- **Remote PC Access :** un catalogue Remote PC Access permet aux utilisateurs d'accéder à distance à leurs machines de bureau de bureau physique. Remote PC Access ne requiert pas de VPN pour fournir la sécurité.

Gestion de machine

Cette page ne s'affiche pas lorsque vous créez des catalogues Remote PC Access.

La page **Gestion des machines** indique la manière dont les machines sont gérées et l'outil que vous utilisez pour déployer les machines.

Indiquez si la gestion de l'alimentation des machines du catalogue sera effectuée au travers de Studio.

- Machines dont la gestion de l'alimentation est effectuée au travers de Studio ou provisionnées via un environnement de cloud, des VM ou des PC lames par exemple. Cette option est disponible uniquement si vous avez déjà configuré une connexion à un hyperviseur ou un service de cloud.
- La gestion de l'alimentation des machines n'est pas effectuée au travers de Studio, les machines physiques par exemple.

Si vous avez indiqué que l'alimentation des machines est gérée au travers de Studio ou que les machines sont provisionnées via un environnement de cloud, choisissez l'outil à utiliser pour créer des machines virtuelles.

- **Citrix Machine Creation Services (MCS) :** utilise une image principale pour créer et gérer les machines virtuelles. Les catalogues de machine dans les environnements de cloud utilisent MCS. MCS n'est pas disponible pour les machines physiques.
- **Citrix Provisioning Services (PVS) :** vous permet de gérer des machines cibles en tant que collection de machines. Une image vDisk PVS créée à partir d'une machine cible principale permet de mettre à disposition des bureaux et des applications. Cette option n'est pas disponible pour les déploiements de cloud.
- **Autres :** un outil qui permet de gérer les machines se trouvant déjà dans le centre de données. Citrix vous recommande d'utiliser Microsoft System Center Configuration Manager ou une autre application tierce pour vous assurer que les machines du catalogue sont cohérentes.

Types de bureau (expérience de bureau)

Cette page s'affiche uniquement lors de la création d'un catalogue de machines contenant des machines avec OS de bureau.

La page **Expérience de bureau** détermine ce qui se produit chaque fois qu'un utilisateur ouvre une session. Sélectionnez l'une des options suivantes :

- Les utilisateurs se connectent à un nouveau bureau (aléatoire) chaque fois qu'ils ouvrent une session
- Les utilisateurs se connectent au même bureau (statique) chaque fois qu'ils ouvrent une session.

Si vous choisissez la deuxième option et que vous utilisez PVS pour provisionner les machines, vous pouvez configurer la manière dont les modifications apportées par l'utilisateur au bureau doivent être gérées :

- Enregistrer les modifications apportées par l'utilisateur au bureau sur un Personal vDisk distinct.
- Enregistrer les modifications apportées par l'utilisateur au bureau sur un disque local.
- Supprimer toutes les modifications et effacer le bureau virtuel à la fermeture de session.

Image principale

Cette page s'affiche uniquement lorsque vous utilisez MCS pour créer des VM.

Sélectionnez la connexion à l'hyperviseur ou au service de cloud hôte, puis sélectionnez la machine virtuelle ou l'instantané créé(e) précédemment. Si vous créez le premier catalogue, la seule connexion disponible est celle que vous avez configurée lors de la création du site.

Rappel :

- Lorsque vous utilisez MCS (ou PVS), n'exécutez pas Sysprep sur les images principales.
- Si vous spécifiez une image principale plutôt qu'un instantané, Studio crée un instantané, mais vous ne pouvez pas le renommer.

Pour pouvoir utiliser les dernières fonctionnalités des produits, assurez-vous que la dernière version de VDA est installée sur l'image principale. Ne modifiez pas la sélection de VDA minimale par défaut. Toutefois, si vous devez utiliser une version de VDA antérieure, consultez Versions VDA et niveaux fonctionnels.

Un message d'erreur s'affiche si vous sélectionnez un instantané ou une VM qui n'est pas compatible avec la technologie de gestion de machines que vous avez sélectionnée précédemment dans l'assistant.

Plate-forme cloud et environnements de service

Lorsque vous utilisez un service ou une plate-forme cloud pour héberger des machines virtuelles (telles que Azure Resource Manager, Nutanix ou Amazon Web Services), l'assistant de création d'un catalogue de machines peut contenir des pages spécifiques à cet hôte.

Pour de plus amples informations, consultez la section Où trouver des informations sur les types de connexion.

Collection de machines

Cette page s'affiche uniquement lorsque vous utilisez PVS pour créer des VM. Elle affiche les collections de machines et les machines qui n'ont pas encore été ajoutées aux catalogues.

Sélectionnez les collections de machines à utiliser. Pour plus d'informations, veuillez consulter la documentation relative à Provisioning Services.

Machines

Cette page ne s'affiche pas lorsque vous créez des catalogues Remote PC Access.

Le titre de cette page dépend de ce que vous avez sélectionné sur la page **Gestion des machines** : **Machines**, **Machines virtuelles** ou **VM et utilisateurs**.

Lorsque vous utilisez MCS pour créer des machines :

- Spécifiez le nombre de machines virtuelles à créer.
- Choisissez la quantité de mémoire (Mo) pour chaque machine.
- **Important :** chaque machine virtuelle créée doit disposer d'un disque dur. Leur taille est définie dans l'image principale ; vous ne pouvez pas modifier la taille du disque dur dans le catalogue.
- Si vous avez indiqué sur la page **Expérience de bureau** que les modifications apportées par l'utilisateur aux bureaux statiques doivent être enregistrées sur un Personal vDisk distinct, spécifiez la taille de vDisk en gigaoctets et la lettre de lecteur.
- Si votre déploiement contient plusieurs zones, vous pouvez sélectionner une zone pour le catalogue.
- Si vous créez des machines virtuelles de bureau statique, sélectionnez le mode de copie de la machine virtuelle. Voir Mode de copie des machines virtuelles.
- Si vous créez des machines virtuelles de bureau aléatoire qui n'utilisent pas de Personal vDisks, vous pouvez configurer un cache à utiliser pour les données temporaires sur chaque machine. Voir Configurer un cache pour les données temporaires.

Lorsque vous utilisez PVS pour créer des machines :

La page **Périphériques** dresse la liste des machines de la collection que vous avez sélectionnée sur la page précédente de l'assistant. Vous ne pouvez pas ajouter ou supprimer des machines sur cette page.

Lorsque vous utilisez d'autres outils pour fournir des machines virtuelles :

Ajoutez (ou importez une liste) les noms de compte de machine Active Directory. Vous pouvez modifier le nom de compte Active Directory pour une VM après l'avoir ajoutée/importée. Si vous avez spécifié des machines statiques sur la page de l'assistant **Expérience de bureau**, vous pouvez également spécifier le nom de l'utilisateur Active Directory pour chaque VM que vous ajoutez.

Une fois que vous avez ajouté ou importé les noms, vous pouvez utiliser le bouton **Supprimer** pour supprimer les noms de la liste lorsque vous vous trouvez encore sur cette page de l'assistant.

Lors de l'utilisation de PVS ou d'autres outils (mais pas MCS) :

Une icône et une info-bulle pour chaque machine ajoutée (ou importée, ou d'une collection de machines PVS) vous aident à identifier les machines qu'il peut ne pas être possible d'ajouter au catalogue, ou d'enregistrer auprès d'un Delivery Controller. Pour de plus amples informations, consultez la section Versions VDA et niveaux fonctionnels.

Mode de copie des machines virtuelles

Le mode de copie que vous spécifiez sur la page **Machines** détermine si MCS crée des clones légers (copie rapide) ou lourds (copie complète) de l'image principale. (Valeur par défaut=clones légers)

- Utilisez le clonage rapide pour créer des machines plus rapidement et utiliser le stockage de manière plus efficace.
- Utilisez la copie complète pour profiter de meilleures performances en matière de recouvrement et de migration des données, tout en réduisant les opérations E/S par seconde une fois que les machines sont créées.

Versions VDA et niveaux fonctionnels

Le niveau fonctionnel d'un catalogue détermine les fonctionnalités du produit qui sont disponibles pour les machines du catalogue. L'utilisation de fonctionnalités introduites dans les nouvelles versions de produit peut nécessiter un nouveau VDA. Définir un niveau fonctionnel met toutes les fonctionnalités introduites dans cette version (et les versions ultérieures, si le niveau fonctionnel ne change pas) à disposition des machines du catalogue. Toutefois, les machines de ce catalogue avec une version antérieure de VDA ne pourront pas s'enregistrer.

Une liste déroulante dans la partie inférieure de la page **Machines** (ou **Périphériques**) vous permet de sélectionner le niveau minimum de VDA qui pourra s'enregistrer avec succès ; cela définit le niveau fonctionnel minimal du catalogue. Par défaut, le niveau fonctionnel le plus courant est sélectionné pour les déploiements locaux. Si vous observez les recommandations de Citrix pour installer et mettre à niveau les composants principaux et les VDA vers la version la plus récente, vous n'avez pas besoin de modifier cette sélection. Toutefois, si vous devez continuer à utiliser des versions antérieures de VDA, sélectionnez la valeur appropriée.

Il est possible qu'une version de XenApp et XenDesktop ne comprenne pas une nouvelle version du VDA, ou que le nouveau VDA n'affecte pas le niveau fonctionnel. Dans de tels cas, le niveau fonctionnel peut indiquer une version du VDA antérieure aux composants installés ou mis à niveau. À titre d'exemple, bien que XenApp et XenDesktop 7.15 LTSR contienne un VDA 7.15, le niveau fonctionnel par

défaut (7.9 ou ultérieur) reste le niveau actuel. Par conséquent, après l'installation ou la mise à niveau des composants de 7.9-7.14 à 7.15 LTSR, vous n'avez pas besoin de modifier le niveau fonctionnel par défaut.

Dans les déploiements Citrix Cloud, Studio utilise un niveau fonctionnel par défaut qui peut être antérieur à la version la plus récente.

Le niveau fonctionnel sélectionné affecte la liste des machines. Dans la liste, une info-bulle en regard de chaque entrée indique si le VDA de la machine est compatible avec le catalogue à ce niveau fonctionnel.

Des messages sont publiés sur la page si le VDA de chaque machine ne correspond pas ou est supérieur au numéro minimal de niveau fonctionnel sélectionné. Vous pouvez continuer avec l'assistant, mais veuillez noter que ces machines sont susceptibles de ne pas être en mesure de s'enregistrer auprès d'un Controller ultérieurement. Vous pouvez également effectuer les opérations suivantes :

- Supprimer de la liste les machines contenant une version plus ancienne de VDA, mettre à niveau leurs VDA et les ajouter de nouveau au catalogue.
- Choisissez un niveau fonctionnel bas ; cependant, cela empêchera l'accès aux dernières fonctionnalités du produit.

Un message est également affiché si une machine n'a pas été ajoutée au catalogue car il ne s'agit pas d'un type de machine correct. Cela peut se produire lors de la tentative d'ajout d'un serveur à un catalogue avec OS de bureau ou d'ajout d'une machine avec OS de bureau créée initialement pour une allocation aléatoire à un catalogue de machines statiques.

Configurer un cache pour les données temporaires

La mise en cache locale des données temporaires sur la VM est facultative. Vous pouvez activer le stockage des données temporaires sur le cache de la machine lorsque vous utilisez MCS pour gérer les machines regroupées (non dédiées) dans un catalogue. Si le catalogue utilise une connexion qui spécifie un stockage des données temporaires, vous pouvez activer et configurer les informations de mise en cache des données temporaires lorsque vous créez le catalogue.

Pour activer la mise en cache des données temporaires, le VDA de chaque machine dans le catalogue doit être à la version minimale 7.9.

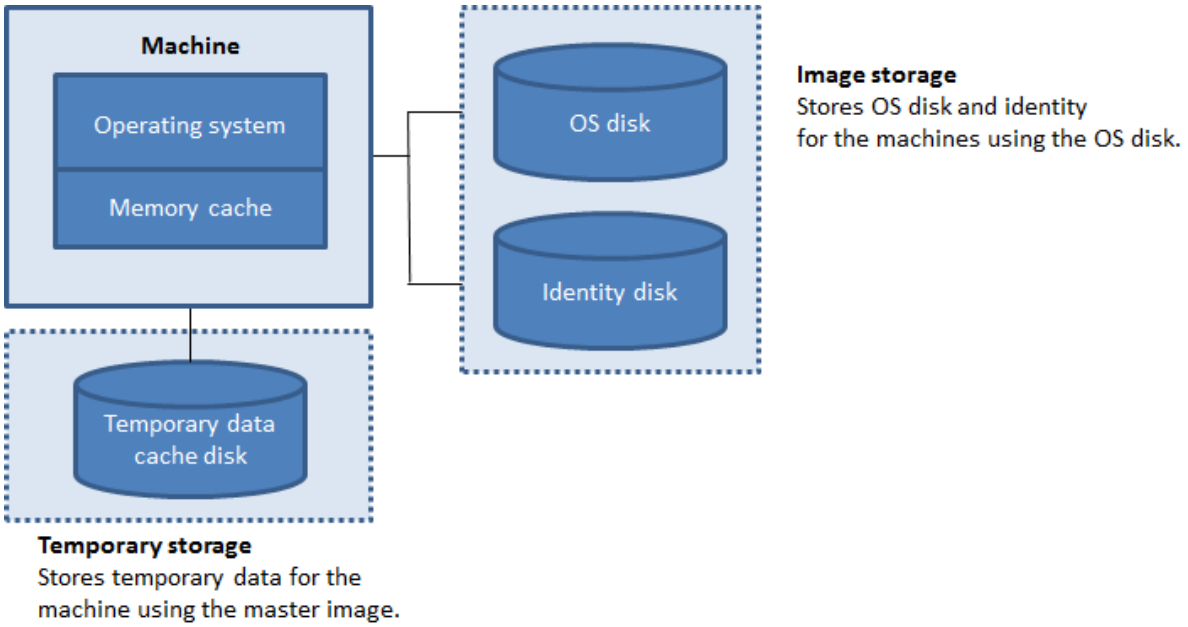
Vous spécifiez si les données temporaires utilisent le stockage local ou partagé lorsque vous créez la connexion que le catalogue utilise ; pour de plus amples informations, veuillez consulter la section Connexions et ressources. L'activation et la configuration du cache temporaire dans le catalogue contient deux cases à cocher : **Mémoire allouée au cache (Mo)** et **Taille du cache disque (Go)**. Les valeurs par défaut diffèrent selon le type de connexion. En général, les valeurs par défaut suffisent à la plupart des cas, cependant, tenez compte de l'espace nécessaire pour les :

- Fichiers de données temporaires créés par Windows, y compris le fichier de pages Windows.

- Données du profil utilisateur.
- Données ShareFile qui sont synchronisées sur les sessions des utilisateurs.
- Données qui peuvent être créées ou copiées par un utilisateur de session ou toute application que les utilisateurs peuvent installer dans la session.

Windows n'autorisera pas une session à utiliser une quantité de cache disque plus importante que la quantité d'espace disponible sur l'image principale originale à partir de laquelle les machines dans le catalogue de machines sont provisionnées. Par exemple, il n'existe aucun avantage à spécifier un disque de cache de 20 Go s'il existe uniquement 10 Go d'espace disponible sur l'image principale.

Si vous activez la case à cocher **Taille du cache disque**, les données temporaires sont initialement écrites dans la mémoire cache. Lorsque la mémoire cache atteint sa limite configurée (valeur **Mémoire allouée au cache**), les données les plus anciennes sont déplacées sur le disque de mise en cache des données temporaires.



La mémoire cache est prise en compte dans le calcul de la quantité totale de mémoire sur chaque machine ; par conséquent, si vous activez la case **Mémoire allouée au cache**, envisagez d'augmenter la quantité totale de mémoire sur chaque machine.

Si vous désactivez la case **Mémoire allouée au cache** et laissez la case **Taille du cache disque** activée, les données temporaires sont écrites directement sur le disque cache, ce qui utilise une quantité minimale de la mémoire cache.

La modification de la valeur par défaut **Taille du cache disque** peut affecter les performances. La taille doit correspondre aux besoins des utilisateurs et à la charge de travail placée sur la machine.

> **Important :**
>
> Si le cache disque vient à manquer d'espace, la session de l'utilisateur devient inutilisable.

Si vous désactivez la case **Taille du cache disque**, aucun disque cache n'est créé. Dans ce cas, spécifiez une valeur de **Mémoire allouée au cache** suffisante pour stocker toutes les données temporaires ; cela est uniquement possible si d'importantes quantités de RAM sont disponibles pour allocation à chaque machine virtuelle.

Si vous désactivez ces deux cases à cocher, les données temporaires ne sont pas mises en cache ; elles sont écrites sur le disque de différence (situé dans l'espace de stockage du système d'exploitation) pour chaque machine virtuelle. (Il s'agit de l'action de provisioning dans les versions antérieures à la version 7.9).

N'activez pas la mise en cache si vous avez l'intention d'utiliser ce catalogue pour créer des AppDisks.

Cette fonctionnalité n'est pas disponible lors de l'utilisation d'une connexion hôte Nutanix.

Vous ne pouvez pas modifier les valeurs de cache dans un catalogue de machines après sa création.

Cartes d'interface réseau (NIC)

Cette page ne s'affiche pas lorsque vous créez des catalogues Remote PC Access.

Si vous prévoyez d'utiliser plusieurs cartes d'interface réseau, vous devez associer un réseau virtuel avec chaque carte. Par exemple, vous pouvez attribuer une carte pour accéder à un réseau sécurisé spécifique, et une autre carte pour accéder à un réseau plus courant. Vous pouvez également ajouter ou supprimer les cartes d'interface réseau à partir de cette page.

Comptes de machines

Cette page s'affiche uniquement lors de la création de catalogues Remote PC Access.

Spécifiez les comptes de machines Active Directory ou des unités d'organisation (OU) à ajouter qui correspondent à des utilisateurs ou des groupes d'utilisateurs. N'utilisez pas de barre oblique (/) dans un nom d'unité d'organisation.

Vous pouvez choisir une connexion de gestion de l'alimentation configurée précédemment ou choisir de ne pas utiliser la gestion de l'alimentation. Si vous souhaitez utiliser la gestion de l'alimentation, mais une connexion adéquate n'a pas encore été configurée, vous pouvez créer cette connexion plus tard, puis modifiez le catalogue de machines pour mettre à jour les paramètres de gestion de l'alimentation.

Comptes d'ordinateurs

Cette page s'affiche uniquement lorsque vous utilisez MCS pour créer des VM.

Chaque machine du catalogue de machines a besoin d'un compte d'ordinateur Active Directory correspondant. Indiquez s'il faut créer de nouveaux comptes ou utiliser des comptes existants, ainsi que l'emplacement de ces comptes.

- Si vous créez de nouveaux comptes, vous devez disposer de l'accès à un compte d'administrateur de domaine pour le domaine dans lequel les machines se trouvent.

Spécifiez le schéma d'affectation de nom du compte pour les machines qui seront créées, en utilisant des marques de hachage pour indiquer l'emplacement où les lettres ou chiffres séquentiels apparaîtront. N'utilisez pas de barre oblique (/) dans un nom d'unité d'organisation. Un nom ne peut pas commencer par un chiffre. Par exemple, un principe de dénomination de PC-Sales-## (avec 0-9 sélectionné) dans les comptes d'ordinateur nommés PC-Sales-01, PC-Sales-02, PC-Sales-03, etc.

- Si vous utilisez des comptes existants, vous pouvez sélectionner les comptes ou cliquez sur **Importer** et spécifiez un fichier .csv contenant les noms de compte. Le contenu du fichier importé doit utiliser le format :

```
[ADComputerAccount]
ADcomputeraccountname.domain
...
```

Assurez-vous qu'il existe suffisamment de comptes pour toutes les machines que vous ajoutez. Étant donné que Studio gère ces comptes, soit autorisez Studio à réinitialiser les mots de passe de tous les comptes soit spécifiez le mot de passe de compte, qui doit être le même pour tous les comptes.

Pour les catalogues contenant des machines physiques ou des machines existantes, sélectionnez ou importez des comptes existants et attribuez chaque machine à un compte d'ordinateur Active Directory et à un compte d'utilisateur.

Pour les machines créées avec PVS, les comptes d'ordinateur pour les machines cibles sont gérés différemment ; consultez la documentation Provisioning Services.

Résumé, nom et description

Sur la page **Résumé** de l'assistant, vérifiez les paramètres que vous avez spécifiés. Entrez un nom et une description pour le catalogue ; les informations suivantes s'affichent dans Studio.

Une fois que vous avez vérifié les informations que vous avez spécifiées, cliquez sur **Terminer** pour lancer la création du catalogue.

Dépannage

Citrix recommande de collecter des journaux pour aider l'équipe de support à fournir des solutions. Utilisez la procédure suivante pour générer des fichiers journaux lors de l'utilisation de PVS :

1. Sur l'image principale, créez la clé de registre suivante avec la valeur 1 (pour valeur DWORD (32 bits)) :

   ```
   HKLM\Software\Citrix\MachineIdentityServiceAgent\LOGGING
   ```

2. Arrêtez l'image principale et créez un nouvel instantané.
3. Exécutez la commande suivante sur le Delivery Controller :

   ```
   Set-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown
    -Value $True
   ```

4. Créez un nouveau catalogue basé sur cet instantané.
5. Lorsque la VM de préparation est créée sur l'hyperviseur, connectez-vous et extrayez les fichiers suivants dans la racine du lecteur C:\:
   - Image-prep.log
   - PvsVmAgentLog.txt
6. Arrêtez la machine ; à ce stade, elle signale l'échec.
7. Exécutez la commande PowerShell suivante pour réactiver l'arrêt automatique des machines de préparation d'image :

   ```
   Remove-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown
   ```

Gérer des catalogues de machines

February 28, 2019

Introduction

Vous pouvez ajouter ou supprimer des machines dans un catalogue de machines, renommer, modifier la description ou gérer les comptes d'ordinateurs Active Directory d'un catalogue.

La gestion des catalogues peut également consister à s'assurer que chaque machine dispose des mises à jour de système d'exploitation, des mises à jour des logiciels antivirus, des mises à niveau de système d'exploitation ou des modifications apportées à la configuration les plus récentes.

- Pour les catalogues contenant des machines regroupées au hasard créées à l'aide de Machine Creation Services (MCS), vous pouvez gérer les machines en mettant à jour l'image principale utilisée dans le catalogue. Une fois les images principales mises à jour, mettez à jour les machines. Ce processus vous permet de mettre à jour de manière efficace un grand nombre de machines utilisateur. Pour les machines créées par le biais de Provisioning services, les mises à jour des machines sont propagées via le vDisk. Pour plus d'informations, veuillez consulter la documentation relative à Provisioning Services.
- Pour les catalogues contenant des machines statiques attribuées de façon permanente et pour les catalogues de machine Remote PC Access, vous devez gérer les mises à jour des machines des utilisateurs en dehors de Studio, soit individuellement, soit collectivement à l'aide d'outils de distribution de logiciels tiers.

Pour de plus amples informations sur la création et la gestion de connexions à des hyperviseurs hôtes et à des services de cloud, consultez l'article Connexions et ressources.

À propos des instances persistantes

Lors de la mise à jour d'un catalogue MCS créé à l'aide d'instances persistantes ou dédiées, toutes les nouvelles machines créées pour le catalogue utilisent l'image mise à jour. Les instances préexistantes continuent d'utiliser l'instance d'origine. Le processus de mise à jour d'une image se fait de la même manière pour tout autre type de catalogue. Tenez compte des considérations suivantes :

- Pour les catalogues de disques persistants, les machines préexistantes ne sont pas mises à jour vers la nouvelle image, mais toutes les nouvelles machines ajoutées au catalogue utilisent la nouvelle image.
- Pour les catalogues de disques non persistants, l'image de la machine est mise à jour lors de la prochaine réinitialisation de la machine.
- Pour les catalogues de machines persistantes, la mise à jour de l'image met également à jour les instances du catalogue qui l'utilisent.
- Pour les catalogues non persistants, si vous souhaitez des images différentes pour différentes machines, les images doivent résider dans des catalogues distincts.

Ajouter des machines à un catalogue de machines

Avant de commencer :

- Assurez-vous que l'ordinateur hôte de virtualisation ((hyperviseur ou fournisseur de service cloud) dispose de suffisamment de processeurs, de mémoire et de stockage pour prendre en charge les machines supplémentaires.
- Vérifiez que vous disposez de suffisamment de comptes d'ordinateurs Active Directory inutilisés. Si vous utilisez des comptes existants, le nombre de machines que vous pouvez ajouter

est limité par le nombre de comptes disponibles.
- Si vous utilisez Studio pour créer des comptes d'ordinateurs Active Directory pour les machines supplémentaires, vous devez disposer des droits d'administrateur de domaine.

Pour ajouter des machines à un catalogue :

1. Sélectionnez **Catalogues de machines** dans le volet de navigation **Studio**.
2. Sélectionnez un catalogue de machines, puis sélectionnez **Ajouter des machines** dans le volet **Actions**.
3. Sélectionnez le nombre de machines virtuelles à ajouter.
4. S'il n'y a pas suffisamment de comptes Active Directory pour le nombre de machines virtuelles que vous ajoutez, sélectionnez le domaine et l'emplacement où les comptes sont créés. Spécifiez un schéma d'affectation de nom du compte, à l'aide des marques de hachage pour indiquer l'emplacement où les numéros séquentiels ou les lettres apparaissent. N'utilisez pas de barre oblique (/) dans un nom d'unité d'organisation. Un nom ne peut pas commencer par un chiffre. Par exemple, un principe de dénomination de PC-Sales-## (avec 0-9 sélectionné) dans les comptes d'ordinateur nommés PC-Sales-01, PC-Sales-02, PC-Sales-03, etc.
5. Si vous utilisez des comptes Active Directory existants, vous pouvez sélectionner les comptes ou cliquer sur **Importer** et spécifier un fichier .csv contenant les noms de compte. Assurez-vous qu'il existe suffisamment de comptes pour toutes les machines que vous ajoutez. Studio gère ces comptes. Autorisez Studio à réinitialiser les mots de passe de tous les comptes ou spécifiez le mot de passe de compte (qui doit être le même pour tous les comptes).

Les machines sont créées en tant que processus en arrière-plan, qui peut être long lors de la création de plusieurs machines. La création de la machine se poursuit même si vous fermez Studio.

Supprimer des machines depuis un catalogue de machine

Lorsque vous supprimez une machine d'un catalogue de machines, les utilisateurs ne peuvent plus y accéder ; donc, avant de supprimer une machine, assurez-vous que :

- Les données utilisateur sont sauvegardées ou ne sont plus nécessaires.
- Tous les utilisateurs sont déconnectés. L'activation du mode maintenance empêche les nouvelles connexions à une machine.
- Les machines sont hors tension.

Pour supprimer des machines d'un catalogue :

1. Sélectionnez **Catalogues de machines** dans le volet de navigation **Studio**.
2. Sélectionner un catalogue, puis sélectionnez **Afficher les machines** dans le volet **Actions**.
3. Sélectionnez une ou plusieurs machines, puis sélectionnez **Supprimer** dans le volet **Actions**.

Choisissez si vous souhaitez supprimer les machines en cours de suppression. Si vous choisissez de

supprimer les machines, indiquez si les comptes Active Directory pour ces machines doivent être conservés, désactivés ou supprimés.

Modifier une description du catalogue de machine ou modifier les paramètres Remote PC Access

1. Sélectionnez **Catalogues de machines** dans le volet de navigation **Studio**.
2. Sélectionnez un catalogue, puis sélectionnez **Modifier le catalogue de machines** dans le volet **Actions**.
3. (Catalogues Remote PC Access uniquement) Sur la page **Gestion de l'alimentation**, vous pouvez modifier les paramètres de gestion de l'alimentation et sélectionner une connexion de gestion de l'alimentation. Sur la page **Unités d'organisation**, ajoutez ou supprimez des unités d'organisation Active Directory.
4. Sur la page **Description**, modifiez la description du catalogue.

Renommer un catalogue de machine

1. Sélectionnez **Catalogues de machines** dans le volet de navigation **Studio**.
2. Sélectionnez un catalogue, puis sélectionnez **Renommer le catalogue de machines** dans le volet **Actions**.
3. Entrez le nouveau nom.

Déplacer un catalogue de machines vers une autre zone

Si votre déploiement contient plusieurs zones, vous pouvez déplacer un catalogue d'une zone vers une autre.

Veuillez noter que le déplacement d'un catalogue vers une zone autre que l'hyperviseur ou le service de cloud contenant les VM de ce catalogue peut affecter les performances.

1. Sélectionnez **Catalogues de machines** dans le volet de navigation **Studio**.
2. Sélectionnez un catalogue, puis sélectionnez **Déplacer** dans le volet **Actions**.
3. Sélectionnez la zone vers laquelle vous souhaitez déplacer le catalogue.

Supprimer un catalogue de machines

Avant de supprimer un catalogue, vérifiez ce qui suit :

- Tous les utilisateurs ont fermé leur session et qu'aucune session déconnectée n'est en cours d'exécution.

- Le mode de maintenance est activé pour toutes les machines du catalogue, de sorte qu'il ne soit pas possible d'effectuer de nouvelles connexions.
- Toutes les machines des catalogues sont hors tension.
- Le catalogue n'est pas associé à un groupe de mise à disposition. En d'autres termes, le groupe de mise à disposition ne contient pas les machines du catalogue.

Pour supprimer un catalogue :

1. Sélectionnez **Catalogues de machines** dans le volet de navigation **Studio**.
2. Sélectionnez un catalogue, puis sélectionnez **Supprimer le catalogue de machines** dans le volet **Actions**.
3. Indiquez si les machines du catalogue doivent être supprimées. Si vous choisissez de supprimer les machines, indiquez si les comptes d'ordinateur Active Directory pour ces machines doivent être conservés, désactivés ou supprimés.

Gérer les comptes d'ordinateurs Active Directory dans un catalogue de machines

Pour gérer les comptes Active Directory dans un catalogue de machines, vous pouvez :

- Libérer des comptes de machines non utilisés en supprimant les comptes d'ordinateurs Active Directory des catalogues de machines avec OS de bureau et avec OS de serveur. Ces comptes peuvent ensuite être utilisés pour d'autres machines.
- Ajoutez des comptes de façon à ce que lorsque plus de machines sont ajoutées au catalogue, les comptes d'ordinateurs soient déjà en place N'utilisez pas de barre oblique (/) dans un nom d'unité d'organisation.

Pour gérer les comptes Active Directory :

1. Sélectionnez **Catalogues de machines** dans le volet de navigation **Studio**.
2. Sélectionnez un catalogue, puis sélectionnez **Gérer les comptes AD** dans le volet **Actions**.
3. Choisissez si vous souhaitez ajouter ou supprimer des comptes d'ordinateurs. Si vous ajoutez des comptes, indiquez la marche à suivre avec les mots de passe de compte : les réinitialiser ou entrer un mot de passe qui s'applique à tous les comptes. Vous pouvez réinitialiser les mots de passe si vous ne connaissez pas les mots de passe de compte actuels, vous devez avoir l'autorisation d'effectuer une réinitialisation du mot de passe. Si vous entrez un mot de passe, le mot de passe est modifié sur les comptes lors de leur importation. Si vous supprimez un compte, indiquez si le compte dans Active Directory doit être conservé, désactivé ou supprimé.

Vous pouvez également indiquer si les comptes Active Directory doivent être conservés, désactivés ou supprimés lorsque vous supprimez les machines d'un catalogue ou supprimez un catalogue.

Mettre un catalogue de machines à jour

Citrix vous recommande de sauvegarder des copies ou des instantanés des images principales avant de mettre à jour les machines dans le catalogue. La base de données conserve un enregistrement historique des images principales utilisées avec chaque catalogue de machines. Vous pouvez restaurer un catalogue afin d'utiliser la version précédente de l'image principale si les utilisateurs rencontrent des problèmes avec les mises à jour que vous avez déployé sur leurs bureaux, ce qui permet de réduire les temps d'arrêt des utilisateurs. Ne supprimez, déplacez ou renommez pas les images principales ; sinon, vous ne pourrez pas restaurer un catalogue pour les utiliser.

Pour les catalogues qui utilisent Provisioning Services, vous devez publier un nouveau vDisk pour appliquer les modifications au catalogue. Pour de plus amples informations, consultez la documentation Provisioning Services.

Après qu'une machine a été mise à jour, elle redémarre automatiquement.

Mettre à jour ou créer une image principale

Avant de mettre à jour le catalogue, mettez à jour une image principale existante ou créez une image sur votre hyperviseur hôte.

1. Sur votre hyperviseur ou fournisseur de services de cloud, prenez un instantané de la VM et donnez à l'instantané un nom significatif. Cet instantané peut être utilisé pour rétablir (restaurer) des machines dans le catalogue, si nécessaire.
2. Si nécessaire, démarrez l'image principale et ouvrez une session.
3. Installez les mises à jour ou apportez les modifications requises à l'image principale.
4. Si l'image principale utilise un Personal vDisk, mettez à jour l'inventaire.
5. Arrêtez la VM.
6. Prenez un instantané de la VM, puis donnez à l'instantané un nom significatif qui sera reconnu lorsque le catalogue est mis à jour dans Studio. Bien que Studio puisse créer un instantané, Citrix vous recommande de créer un instantané à l'aide de la console de gestion de l'hyperviseur, puis de sélectionner cet instantané dans Studio. Cette méthode vous permet de choisir un nom et une description significatifs plutôt qu'un nom généré automatiquement. Pour les images principales GPU, vous pouvez modifier l'image principale uniquement par le biais de la console XenCenter de XenServer.

Mettre le catalogue à jour

Pour préparer et distribuer la mise à jour à toutes les machines d'un catalogue :

1. Sélectionnez **Catalogues de machines** dans le volet de navigation **Studio**.
2. Sélectionnez un catalogue, puis sélectionnez **Mettre à jour les machines** dans le volet **Actions**.

3. Sur la page **Image principale**, sélectionnez l'hôte et l'image que vous voulez déployer.
4. Sur la page **Stratégie de déploiement**, indiquez lorsque les machines du catalogue de machines doivent être mises à jour avec la nouvelle image principale : lors de la prochaine fermeture de session ou immédiatement. Consultez la section ci-dessous pour plus de détails.
5. Sur la page **Résumé**, vérifiez les informations et cliquez sur **Terminer**. Chaque machine redémarre automatiquement après sa mise à jour.

Si vous mettez à jour un catalogue directement à l'aide du SDK du PowerShell, plutôt que dans Studio, vous pouvez spécifier un modèle d'hyperviseur (VMTemplates), comme alternative à une image ou un instantané de l'image.

Stratégie de déploiement

La mise à jour de l'image lors de la prochaine fermeture de session est effectuée lorsque vous utilisez Citrix Connector pour System Center Configuration Manager.

Si vous choisissez de mettre à jour l'image immédiatement, configurez une heure de distribution et des notifications.

- **Heure de distribution :** vous pouvez choisir de mettre à jour toutes les machines en même temps ou spécifier la durée totale du lancement de la mise à jour de toutes les machines du catalogue. Un algorithme interne détermine le moment où chaque machine est mise à jour et redémarrée pendant cet intervalle.
- **Notification :** dans la liste déroulante Notification de gauche, indiquez si un message de notification doit s'afficher sur les machines avant qu'une mise à jour commence. Par défaut, aucun message ne s'affiche. Si vous choisissez d'afficher un message 15 minutes avant que la mise à jour commence, vous pouvez choisir (dans la liste déroulante de droite) de répéter le message toutes les cinq minutes après le premier message. Par défaut, le message n'est pas répété. Si vous choisissez de mettre à jour toutes les machines en même temps, le message de notification s'affiche sur chaque machine à l'heure appropriée avant que la mise à jour ne commence, calculée par un algorithme interne.

Restaurer une mise à jour

Après avoir déployé une image principale mise à jour/nouvelle, vous pouvez la restaurer. Cette opération peut être nécessaire si des problèmes se produisent avec les machines mises à jour. Lors de la restauration, les machines du catalogue reviennent à la dernière image fonctionnelle. Les nouvelles fonctionnalités qui nécessitent la nouvelle image ne seront plus disponibles. Comme avec le déploiement, restaurer une machine implique un redémarrage.

1. Sélectionnez **Catalogues de machines** dans le volet de navigation **Studio**.

2. Sélectionnez le catalogue, puis sélectionnez **Restaurer la mise à jour de la machine** dans le volet **Actions**.
3. Spécifiez quand appliquer la version antérieure de l'image principale aux machines, comme décrit ci-dessus pour l'opération de déploiement.

La restauration n'est appliquée qu'aux machines qui doivent être rétablies. Pour les machines qui n'ont pas été mises à jour avec l'image principale nouvelle ou mise à jour (par exemple, des machines avec des utilisateurs qui n'ont pas fermé leur session), les utilisateurs ne reçoivent pas de messages de notification et ne sont pas forcés de fermer la session.

Mettre à niveau un catalogue de machines ou rétablir une mise à niveau

Mettez à niveau le catalogue de machine après avoir mis à niveau les VDA sur les machines vers une version plus récente. Citrix recommande de mettre à niveau tous les VDA vers la version la plus récente de façon à ce qu'ils puissent tous accéder à toutes les fonctionnalités les plus récentes.

Avant de procéder à la mise à niveau d'un catalogue :

- Si vous utilisez Provisioning Services, vous devez mettre à niveau la version du VDA dans la console Provisioning Services.
- Démarrez les machines mises à niveau afin qu'elles s'enregistrent auprès du Controller. Cela permet à Studio de déterminer si les machines du catalogue doivent être mises à niveau.

Pour mettre à niveau un catalogue :

1. Sélectionnez **Catalogues de machines** dans le volet de navigation **Studio**.
2. Sélectionnez le catalogue. L'onglet **Détails** dans le volet inférieur affiche les informations de version.
3. Sélectionnez **Mettre à niveau le catalogue**. Si Studio détecte que le catalogue a besoin de procéder à la mise à niveau, il affiche un message. Suivez les invites. Si une ou plusieurs machines ne peut pas être mise à niveau, un message explique pourquoi. Citrix vous recommande de résoudre les problèmes de machine avant d'effectuer une mise à niveau du catalogue pour vous assurer que toutes les machines fonctionnent correctement.

Une fois la mise à niveau du catalogue terminée, vous pouvez rétablir les machines vers leurs versions de VDA précédentes en sélectionnant le catalogue, puis en sélectionnant **Annuler** dans le volet **Actions**.

Dépannage

Pour les machines affichant un « état d'alimentation inconnu », consultez l'article CTX131267 pour plus d'informations.

Créer des groupes de mise à disposition

February 28, 2019

Un groupe de mise à disposition est une collection de machines sélectionnées à partir d'un ou de plusieurs catalogues de machines. Le groupe de mise à disposition indique quels utilisateurs peuvent utiliser ces machines et les applications et/ou les bureaux à la disposition des utilisateurs.

La création d'un groupe de mise à disposition est la prochaine étape de la configuration de votre déploiement après la création d'un site et la création d'un catalogue de machines. Plus tard, vous pourrez modifier les paramètres initiaux dans le premier groupe de mise à disposition et créer d'autres groupes de mise à disposition. Il existe également des fonctionnalités et paramètres que vous pouvez configurer uniquement lors de la modification d'un groupe de mise à disposition, et non pas lors de sa création.

Pour Remote PC Access, lorsque vous créez un site, un groupe de mise à disposition appelé **Bureaux Remote PC Access** est automatiquement créé.

Pour créer un groupe de mise à disposition :

1. si vous avez créé un site et un catalogue de machines, mais n'avez pas encore créé un groupe de mise à disposition, Studio vous guidera au bon emplacement de départ pour créer un groupe de mise à disposition. Si vous avez déjà créé un groupe de mise à disposition et souhaitez en créer un autre, sélectionnez **Groupes de mise à disposition** dans le volet de navigation Studio, puis sélectionnez **Créer un groupe de mise à disposition** dans le volet Actions.
2. L'assistant Créer un groupe de mise à disposition s'ouvre avec une page **Introduction**, que vous pouvez supprimer des lancements ultérieurs de cet assistant.
3. L'assistant vous guide ensuite au travers des pages décrites ci-dessous. Lorsque vous avez terminé chaque page, cliquez sur **Suivant** jusqu'à la page finale.

Étape 1 – Machines

Sélectionnez un catalogue de machines et sélectionnez le nombre de machines que vous souhaitez utiliser dans ce catalogue.

À savoir

- Au moins une machine doit rester non utilisée dans un catalogue de machines sélectionné.
- Un catalogue de machines peut être spécifié dans plus d'un groupe de mise à disposition ; cependant, une machine ne peut être utilisée que dans un seul groupe de mise à disposition.
- Un groupe de mise à disposition peut utiliser des machines de plus d'un catalogue, cependant ces catalogues doivent contenir les mêmes types de machines (OS de serveur, OS de bureau ou Remote PC Access). En d'autres termes, vous ne pouvez pas combiner des types de machines dans un groupe de mise à disposition. De même, si votre déploiement possède des catalogues

de machines Windows et des catalogues de machines Linux, un groupe de mise à disposition peut contenir des machines d'un des types de système d'exploitation, mais pas les deux.

- Citrix vous recommande d'installer ou de mettre à niveau les machines avec la dernière version de VDA, et de mettre à niveau les catalogues de machines et les groupes de mise à disposition en fonction de vos besoins. Lors de la création d'un groupe de mise à disposition, si vous sélectionnez des machines sur lesquelles sont installées différentes versions de VDA, le groupe de mise à disposition sera compatible avec la version de VDA la plus ancienne (Il s'agit du *niveau fonctionnel* du groupe.) Par exemple, si l'une des machines que vous sélectionnez dispose d'un VDA version 7.1 et que d'autres machines ont la version actuelle, toutes les machines du groupe peuvent uniquement utiliser les fonctionnalités qui étaient prises en charge dans le VDA 7.1. Cela signifie que certaines fonctionnalités qui nécessitent des versions de VDA ultérieures risquent de ne pas être disponibles dans ce groupe de mise à disposition. Par exemple, pour utiliser la fonctionnalité AppDisks, les VDA (et par conséquent le niveau fonctionnel du groupe) doivent être à la version 7.8 au minimum.
- Chaque machine dans un catalogue de machines Remote PC Access est automatiquement associée à un groupe de mise à disposition ; lorsque vous créez un site Remote PC Access, un catalogue nommé **Machines Remote PC Access** et un groupe de mise à disposition appelé **Bureaux Remote PC Access** sont créés automatiquement.

Étape 2 – Type de mise à disposition

Cette page s'affiche uniquement si vous avez choisi un catalogue de machines contenant des machines avec OS de bureau statiques (attribuées). Choisissez **Applications** ou **Bureaux** sur la page Type de mise à disposition. Vous ne pouvez pas activer les deux.

Si vous avez sélectionné des machines à partir d'un catalogue d'OS de serveur ou OS de bureau aléatoires (regroupés), le type de mise à disposition est applications et bureaux par défaut : vous pouvez mettre à disposition des applications, des bureaux, ou les deux.

Étape 3 – AppDisks

Pour ajouter un AppDisk, cliquez sur **Ajouter**. La boîte de dialogue Sélectionner des AppDisks dresse la liste des AppDisks disponibles dans la colonne de gauche. La colonne de droite dresse la liste des applications sur le AppDisk (la sélection de l'onglet **Applications** au-dessus de la colonne de droite dresse la liste des applications dans un format similaire à un menu Démarrer ; la sélection de l'onglet **Packages installés** dresse la liste des applications dans un format similaire à la liste Programmes et fonctionnalités.). Sélectionnez une ou plusieurs cases.

Les AppDisks sont obsolètes.

Étape 4 – Utilisateurs

Spécifiez les utilisateurs et les groupes d'utilisateurs qui peuvent utiliser les applications et les bureaux dans le groupe de mise à disposition.

Où les listes d'utilisateurs sont spécifiées

Les listes d'utilisateurs Active Directory sont spécifiées lorsque vous créez ou modifiez les informations suivantes :

- La liste d'accès utilisateur d'un site, qui n'est pas configurée dans Studio. Par défaut, la règle de stratégie d'admissibilité d'application inclut tout le monde ; consultez les applets de commande du kit de développement PowerShell BrokerAppEntitlementPolicyRule pour plus de détails.
- Les groupes d'applications (s'ils ont été configurés).
- Les groupes de mise à disposition.
- Les applications.

La liste des utilisateurs qui peuvent accéder à une application via StoreFront est constituée à partir de l'intersection des listes utilisateur ci-dessus. Par exemple, pour configurer l'utilisation d'une application A pour un département particulier, sans pour autant limiter l'accès à d'autres groupes :

- utiliser la règle de stratégie d'admissibilité d'application par défaut qui inclut tout le monde ;
- Configurez la liste des utilisateurs du groupe de mise à disposition pour autoriser les utilisateurs du siège social à utiliser toutes les applications spécifiées dans le groupe de mise à disposition.
- (Si des groupes d'applications sont configurés) Configurez la liste des utilisateurs du groupe d'applications pour permettre aux membres du département Administration et Finances d'accéder aux applications A à L.
- Configurez les propriétés de l'application A pour limiter sa visibilité uniquement au personnel des comptes clients du département Administration et Finances.

Utilisateurs authentifiés et non authentifiés

Il existe deux types d'utilisateurs : authentifiées et non authentifiés (les utilisateurs non authentifiés sont également appelés anonymes). Vous pouvez configurer un ou deux types dans un groupe de mise à disposition.

Authentifié

Pour accéder aux applications et aux bureaux, les utilisateurs et les membres du groupe que vous spécifiez par nom doivent présenter des informations d'identification comme une carte à puce ou un

nom d'utilisateur et mot de passe à StoreFront ou Citrix Receiver. Pour les groupes de mise à disposition contenant des machines avec OS de bureau, vous pouvez importer les données utilisateur (une liste des utilisateurs) plus tard en modifiant le groupe de mise à disposition.

Non authentifié (anonyme)

Pour les groupes de mise à disposition contenant les machines avec OS de serveur, vous pouvez autoriser les utilisateurs à accéder à des applications et des bureaux sans présenter d'informations d'identification à StoreFront ou à Citrix Receiver. Par exemple, l'application peut nécessiter des informations d'identification, mais ce n'est pas le cas pour le portail et les outils d'accès Citrix. Un groupe d'utilisateurs anonymes est créé lorsque vous installez le premier Delivery Controller.

Pour accorder l'accès à des utilisateurs non authentifiés, chaque machine du groupe de mise à disposition doit posséder un VDA pour OS Windows Server (version minimum 7.6) installé. Lorsque des utilisateurs non authentifiés sont activés, vous devez disposer d'un magasin StoreFront non authentifié.

Des comptes d'utilisateurs non authentifiés sont créés sur demande lorsqu'une session est lancée et nommée AnonXYZ, dans lequel XYZ est une valeur unique à trois chiffres.

Les sessions utilisateur non authentifiées possèdent un délai d'inactivité par défaut de 10 minutes, et leurs sessions sont automatiquement fermées lorsque le client se déconnecte. La reconnexion, l'itinérance entre les clients et le contrôle de l'espace de travail ne sont pas pris en charge.

Le tableau suivant décrit les choix disponibles sur la page Utilisateurs :

Activer l'accès pour	Ajouter/affecter des utilisateurs et des groupes d'utilisateurs ?	Activer la case à cocher « Autoriser les utilisateurs non authentifiés » ?
Seuls les utilisateurs authentifiés	Oui	Non
Seuls les utilisateurs non authentifiés	Non	Oui
À la fois les utilisateurs authentifiées et non authentifiés	Oui	Oui

Étape 5 – Applications

À savoir

- vous ne pouvez pas ajouter d'applications aux groupes de mise à disposition Remote PC Access.
- Par défaut, les applications que vous ajoutez sont placées dans un dossier nommé Applications. Vous pouvez spécifier un dossier différent. Pour de plus amples informations, veuillez consulter l'article Gérer les applications.
- Vous pouvez modifier les propriétés d'une application lorsque vous l'ajoutez à un groupe de mise à disposition ou ultérieurement. Pour de plus amples informations, veuillez consulter l'article Gérer les applications.
- Si vous essayez d'ajouter une application et qu'une application avec le même nom existe déjà dans ce dossier, vous êtes invité à renommer l'application que vous ajoutez. Si vous refusez, l'application est ajoutée avec un suffixe qui la rend unique dans ce dossier d'application.
- Lorsque vous ajoutez une application à plusieurs groupes de mise à disposition, vous risquez de rencontrer un problème de visibilité si vous ne disposez pas d'autorisations suffisantes pour afficher l'application dans tous les groupes de mise à disposition. Dans ce cas, consultez un administrateur disposant des autorisations appropriées ou demandez une extension de vos autorisations à tous les groupes de mise à disposition auxquels l'application a été ajoutée.
- Si vous publiez deux applications du même nom vers les mêmes utilisateurs, modifiez la propriété Nom de l'application (pour l'utilisateur) dans Studio ; sinon, les utilisateurs verront des noms en double s'afficher dans Receiver.

Cliquez sur la liste déroulante **Ajouter** pour afficher les sources des applications.

- **À partir du menu Démarrer :** applications qui sont découvertes sur une machine créée à partir de l'image principale du catalogue sélectionné. Lorsque vous sélectionnez cette source, une nouvelle page s'ouvre avec une liste d'applications découvertes ; sélectionnez les applications que vous souhaitez ajouter, puis cliquez sur **OK**.
- **Manuellement définies :** applications qui se trouvent dans le site ou ailleurs dans votre réseau. Lorsque vous sélectionnez cette source, une nouvelle page s'affiche dans laquelle vous pouvez taper le chemin d'accès de l'exécutable, le répertoire de travail, les arguments de la ligne de commande (facultatifs), et les noms affichés des administrateurs et des utilisateurs. Après avoir entré ces informations, cliquez sur **OK**.
- **Existantes :** applications déjà ajoutées au site, peut-être dans un autre groupe de mise à disposition. Lorsque vous sélectionnez cette source, une nouvelle page s'ouvre avec une liste d'applications découvertes ; sélectionnez les applications que vous souhaitez ajouter, puis cliquez sur **OK**.
- **App-V :** applications dans des packages App-V. Lorsque vous sélectionnez cette source, une nouvelle page s'affiche dans laquelle vous pouvez sélectionner le serveur App-V ou la bibliothèque d'applications. Sélectionnez les applications que vous souhaitez ajouter à partir de l'écran des résultats et cliquez sur **OK**. Pour plus d'informations, veuillez consulter l'article App-V.

Si une source d'applications ou une application n'est pas disponible ou valide, elle n'est pas visible ou ne peut pas être sélectionnée. Par exemple, la source **existante** n'est pas disponible si aucune application n'a été ajoutée au site. Ou une application peut ne pas être compatible avec les types de

session pris en charge sur des machines du catalogue sélectionné.

Étape 6 – Bureaux (ou règles d'attribution de bureau)

Le titre de cette page dépend du catalogue de machines que vous avez choisi dans l'assistant :

- Si vous avez choisi un catalogue de machines contenant des machines regroupées, cette page est appelée Bureaux.
- Si vous avez choisi un catalogue de machines contenant des machines attribuées et spécifié « Bureaux » sur la page Type de mise à disposition, cette page est appelée Desktop User Assignments (Attributions utilisateur bureau).
- Si vous avez choisi un catalogue de machines contenant des machines attribuées et spécifié « Applications » sur la page Type de mise à disposition, cette page est appelée Application Machine User Assignments (Attributions utilisateur machine application).

Cliquez sur **Ajouter**. Effectuez les opérations suivantes dans cette boîte de dialogue :

- Dans les champs Nom d'affichage et Description, tapez les informations à afficher dans Receiver.
- Pour ajouter une restriction de balise à un bureau, sélectionnez **Restreindre les lancements aux machines dotées de balises** puis sélectionnez la balise dans la liste déroulante. (consultez l'article Balises pour de plus amples informations).
- À l'aide des boutons radio, indiquez qui peut démarrer un bureau (pour les groupes avec machines regroupées) ou qui sera attribué à une machine lorsqu'ils démarrent le bureau (pour les groupes avec machines attribuées). Les utilisateurs peuvent être tout utilisateur pouvant accéder à ce groupe de mise à disposition, ou des utilisateurs et groupes d'utilisateurs spécifiques.
- Si le groupe contient des machines attribuées, spécifiez le nombre maximal de bureaux par utilisateur. Cette valeur doit être de 1 au minimum.
- Activez ou désactivez le bureau (pour les machines regroupées) ou la règle d'attribution de bureau (pour les machines attribuées). La désactivation d'un bureau arrête la mise à disposition de bureaux ; la désactivation d'une règle d'attribution de bureau arrête l'attribution automatique de bureaux aux utilisateurs.
- Lorsque vous avez terminé avec la boîte de dialogue, cliquez sur **OK**.

Étape 7 – Synthèse

Entrez un nom pour le groupe de mise à disposition. Vous pouvez également entrer une description (facultatif), qui s'affichera dans Receiver et dans Studio.

Consultez les informations récapitulatives, puis cliquez sur **Terminer**. Si vous n'avez pas sélectionné d'applications ou spécifié de bureaux à mettre à disposition, vous êtes invité à indiquer si vous voulez continuer.

Gérer les groupes de mise à disposition

February 28, 2019

Introduction

Cet article décrit les procédures permettant de gérer des groupes de mise à disposition. En plus de la modification des paramètres spécifiés lors de la création du groupe, vous pouvez configurer d'autres paramètres qui ne sont pas disponibles lorsque vous créez un groupe de mise à disposition.

Consultez l'article Applications pour de plus amples informations sur la gestion des applications dans les groupes de mise à disposition, notamment comment ajouter et supprimer des applications dans un groupe de mise à disposition, et modifier les propriétés d'application.

La gestion des groupes de mise à disposition nécessite les autorisations d'administration déléguée du rôle intégré d'administrateur de groupe de mise à disposition. Consultez Administration déléguée pour plus de détails.

Modifier les paramètres utilisateur dans un groupe de mise à disposition

Le nom de cette page peut apparaître sous **Paramètres utilisateur** ou **Paramètres de base**.

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe, puis sélectionnez **Modifier le groupe de mise à disposition** dans le volet Actions.
3. Sur la page **Paramètres utilisateur** (ou **Paramètres de base**), modifiez les paramètres dans le tableau suivant.
4. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Paramètre	Description
Description	Le texte que StoreFront utilise et que les utilisateurs voient.
Activer le groupe de mise à disposition	Indique si le groupe de mise à disposition est activé ou non.
Fuseau horaire	

Paramètre	Description
Activer Secure ICA	Sécurise toutes les communications en provenance et à destination de machines dans le groupe de mise à disposition à l'aide de SecureICA, qui crypte le protocole ICA. Le niveau par défaut est 128 bits. Le niveau peut être modifié en utilisant le SDK. Citrix vous recommande d'utiliser des méthodes de cryptage supplémentaires telles que le cryptage TLS lorsque d'un passage au travers de réseaux publics. SecureICA n'effectue pas non plus de contrôle d'intégrité des données.

Ajouter ou supprimer des utilisateurs dans un groupe de mise à disposition

Pour de plus amples informations sur les utilisateurs, consultez la section Utilisateurs dans l'article Créer un groupe de mise à disposition.

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe, puis sélectionnez **Modifier le groupe de mise à disposition** dans le volet Actions.
3. Sur la page **Utilisateurs**, pour ajouter des utilisateurs, cliquez sur **Ajouter**, puis spécifiez les utilisateurs que vous souhaitez ajouter. Pour supprimer des utilisateurs, sélectionnez un ou plusieurs utilisateurs, puis cliquez sur **Supprimer**. Vous pouvez également sélectionner/désactiver la case à cocher qui permet d'activer ou de désactiver l'accès par des utilisateurs non authentifiés.
4. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Importer ou exporter des listes d'utilisateurs

Pour les groupes de mise à disposition contenant des machines avec OS de bureau physique, vous pouvez importer les informations de l'utilisateur à partir d'un fichier .csv après la création du groupe de mise à disposition. Vous pouvez également exporter des informations utilisateur vers un fichier .csv. Le fichier .csv peut contenir des données provenant d'une version antérieure du produit.

La première ligne du fichier .csv doit contenir les en-têtes de colonnes séparés par des virgules (dans n'importe quel ordre), ce qui peut inclure: ADComputerAccount, AssignedUser, VirtualMachine et

HostId. Les lignes suivantes dans le fichier contiennent des données de valeurs séparées par des virgules. Les entrées ADComputerAccount peuvent être des noms communs, des adresses IP ou des noms uniques, le domaine et les paires de nom d'ordinateur.

Pour importer ou exporter des informations sur l'utilisateur :

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe de mise à disposition, puis sélectionnez **Modifier le groupe de mise à disposition** dans le volet Actions
3. Sur la page **Allocation de machine**, sélectionnez **Importer** la liste ou **Exporter** la liste, puis accédez à l'emplacement du fichier.
4. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Modifier le type de mise à disposition d'un groupe de mise à disposition

Le type indique ce que le groupe de mise à disposition peut mettre à disposition : des applications, des bureaux, ou les deux.

Avant de changer un type **application uniquement** ou **bureaux et applications** en type **bureaux uniquement**, supprimez toutes les applications du groupe de mise à disposition.

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe, puis sélectionnez **Modifier le groupe de mise à disposition** dans le volet Actions.
3. Sur la page **Type de mise à disposition**, sélectionnez le type de mise à disposition que vous voulez.
4. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Modifier les adresses de StoreFront

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe, puis sélectionnez **Modifier le groupe de mise à disposition** dans le volet Actions.
3. Sur la page **StoreFront**, sélectionnez ou ajoutez des adresses URL StoreFront qui seront utilisées par Citrix Receiver qui est installé sur chaque machine dans le groupe de mise à disposition.
4. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Vous pouvez également spécifier l'adresse de serveur StoreFront en sélectionnant l'option **Configuration > StoreFront** dans le volet de navigation Studio.

Ajouter, modifier ou retirer une restriction de balise pour un bureau

L'ajout, la modification et la suppression de restrictions de balise peut avoir des effets inattendus sur les bureaux qui sont pris en compte pour le démarrage. Consultez les informations et précautions dans l'article Balises.

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe, puis sélectionnez **Modifier le groupe de mise à disposition** dans le volet Actions.
3. Sur la page **Bureaux**, sélectionnez le bureau, puis cliquez sur **Modifier**.
4. Pour ajouter une restriction de balise, sélectionnez **Restreindre les lancements aux machines dotées de balises** puis sélectionnez la balise.
5. Pour modifier ou supprimer une restriction de balise, sélectionnez une autre balise ou supprimez la restriction de balise complètement en désactivant le paramètre **Restreindre les lancements aux machines dotées de balises**.
6. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Mettre à niveau un groupe de mise à disposition ou rétablir une mise à niveau

Mettez à niveau un groupe de mise à disposition après avoir mis à niveau les VDA sur les machines et les catalogues de machines contenant les machines utilisées dans le groupe de mise à disposition.

Avant de commencer la mise à niveau du groupe de mise à disposition :

- Si vous utilisez Provisioning Services, vous devez mettre à niveau la version du VDA dans la console Provisioning Services.
- Démarrez les machines contenant le VDA mis à niveau afin qu'elles puissent s'enregistrer avec le Delivery Controller. Ce processus informe Studio de la nature des éléments nécessitant une mise à niveau dans le groupe de mise à disposition.
- Si vous devez continuer à utiliser des versions antérieures du VDA, il se peut que des fonctionnalités plus récentes ne soient pas disponibles. Pour de plus amples informations, consultez les articles sur la mise à niveau.

Pour mettre à niveau un groupe de mise à disposition :

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe de mise à disposition, puis sélectionnez **Mettre à niveau le groupe de mise à disposition** dans le volet Actions. L'action **Mettre à niveau le groupe de mise à disposition** apparaît uniquement si Studio détecte les VDA mis à niveau.

Avant de démarrer le processus de mise à niveau, Studio vous indique quelles machines, le cas échéant, ne peuvent pas être mises à niveau et pourquoi. Vous pouvez alors annuler la mise à niveau, résoudre les problèmes de la machine, puis démarrer la mise à niveau.

Une fois la mise à niveau terminée, vous pouvez rétablir les machines à leur état précédent en sélectionnant le groupe de mise à disposition, puis en sélectionnant **Annuler** dans le volet Actions.

Gérer les groupes de mise à disposition Remote PC Access

Si une machine dans un catalogue de machines Remote PC Access n'est pas affectée à un utilisateur, Studio attribue temporairement la machine à un groupe de mise à disposition associé à ce catalogue de machine. Cette affectation temporaire permet à la machine d'être affectée à un utilisateur ultérieurement.

L'association du groupe de mise à disposition avec le catalogue de machines a une valeur de priorité. La priorité détermine à quel groupe de mise à disposition cette machine est attribuée lorsque celui-ci s'enregistre auprès du système ou lorsqu'un utilisateur a besoin d'une machine : plus la valeur est basse, plus la priorité est élevée. Si un catalogue de machine Remote PC Access possède plusieurs affectations de groupe de mise à disposition, le logiciel sélectionne la correspondance avec la priorité la plus élevée. Vous pouvez définir cette valeur de priorité à l'aide du SDK du PowerShell.

Lors de leur création, les catalogues de machines Remote PC Access sont associés à un groupe de mise à disposition. Cela signifie que les comptes de machines ou unités d'organisation ajoutés au catalogue ultérieurement peuvent être ajoutés au groupe de mise à disposition. Cette association peut être désactivée ou activée.

Pour ajouter ou supprimer une association de catalogue de machines Remote PC Access avec un groupe de mise à disposition :

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe Remote PC Access.
3. Dans la section Détails, sélectionnez l'onglet **Catalogues de machines**, puis sélectionnez un catalogue Remote PC Access.
4. Pour ajouter ou restaurer une association, sélectionnez **Ajouter des bureaux**. Pour supprimer une association, sélectionnez **Supprimer l'association**.

Arrêter et redémarrer les machines d'un groupe de mise à disposition

Cette procédure n'est pas prise en charge par les machines Remote PC Access.

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe, puis sélectionnez **Afficher les machines** dans le volet Actions.
3. Sélectionnez la machine et sélectionnez l'une des options suivantes dans le volet Actions (il se peut que certaines options ne soient pas disponibles, en fonction de l'état des machines) :
    - **Forcer l'arrêt.** Place la machine hors tension de manière forcée et actualise la liste des machines.

- **Redémarrer.** Requiert la fermeture du système d'exploitation de la machine, puis redémarrage de la machine. Si le système d'exploitation ne peut pas s'y conformer, la machine reste dans son état actuel.
- **Forcer le redémarrage.** Force l'arrêt du système d'exploitation, puis redémarre la machine.
- **Suspendre.** Met en pause la machine sans la fermer et actualise la liste de machines.
- **Arrêtez la machine.** Requiert la fermeture du système d'exploitation.

Pour les actions qui ne sont pas forcées, si la machine ne se ferme pas dans les 10 minutes, elle est mise hors tension. Si Windows tente d'installer des mises à jour durant la fermeture, il y a un risque que la machine soit mise hors tension avant la fin des mises à jour.

Citrix vous recommande d'empêcher les utilisateurs des machines avec OS de bureau de sélectionner **Arrêter** dans une session. Consultez la documentation des stratégies Microsoft pour plus de détails.

Vous pouvez également arrêter et redémarrer des machines sur une connexion ; consultez l'article Connexions et ressources.

Gérer l'alimentation des machines d'un groupe de mise à disposition

Vous pouvez gérer l'alimentation des machines avec OS de bureau virtuelles uniquement, pas celle des machines physiques (y compris les machines Remote PC Access). Les machines d'OS de bureau avec capacités GPU ne peuvent pas être suspendues, par conséquent les opérations de mise hors tension échouent. Pour les machines avec OS de serveur, vous pouvez créer un programme de redémarrage, qui est également décrit dans cet article.

Dans des groupes de mise à disposition contenant des machines regroupées, les machines avec OS de bureau virtuelles peuvent être dans l'un des états suivants :

- Allouées de manière aléatoire et en cours d'utilisation.
- Non allouées et non connectées

Dans des groupes de mise à disposition contenant des machines statiques, les machines avec OS de bureau virtuelles peuvent être :

- allouées à titre permanent et en cours d'utilisation ;
- Allouées à titre permanent et non connectées (mais prêtes)
- Non allouées et non connectées

Lors d'une utilisation normale, les groupes de mise à disposition statiques contiennent toujours des machines allouées et non allouées à titre permanent. Initialement, aucune machine n'est allouée (sauf celles manuellement allouées lors de la création du groupe de mise à disposition). Lorsque les utilisateurs se connectent, les machines sont allouées à titre permanent. Vous pouvez gérer l'alimentation des machines non allouées complètement dans les groupes de mise à disposition, mais uniquement partiellement gérer les machines allouées à titre permanent.

Regroupements et tampons : pour les groupes de mise à disposition regroupés et les groupes de mise à disposition statiques avec des machines non allouées, un regroupement (dans ce cas) est un ensemble de machines non allouées ou allouées temporairement qui sont conservées à l'état sous tension, prêtes pour la connexion des utilisateurs ; un utilisateur reçoit une machine immédiatement après l'ouverture de session. La taille du regroupement (le nombre de machines conservées sous tension) est configurable par heure de la journée. Pour les groupes de mise à disposition statiques, utilisez le kit de développement pour configurer le regroupement.

Un tampon en veille est un ensemble de machines non allouées qui sont activées lorsque le nombre de machines du regroupement tombe en dessous d'un seuil qui est un pourcentage de la taille du groupe de mise à disposition. Pour les grands groupes de mise à disposition, un certain nombre de machines peut être activé lors du dépassement du seuil. Aussi, planifiez attentivement les tailles de groupes de mise à disposition ou utiliser le kit de développement pour ajuster la taille de tampon par défaut.

Horloges d'état d'alimentation : vous pouvez utiliser les horloges d'état d'alimentation pour suspendre des machines une fois que les utilisateurs se sont déconnectés depuis un laps de temps spécifié. Par exemple, les machines seront suspendues automatiquement en dehors des heures ouvrables si les utilisateurs se sont déconnectés depuis au moins 10 minutes. Les machines aléatoires ou les machines avec Personal vDisks sont automatiquement arrêtées lorsque les utilisateurs ferment leur session, à moins que vous n'ayez configuré la propriété de groupe de mise à disposition ShutdownDesktopsAfterUse dans le kit de développement.

Vous pouvez configurer des horloges pour les jours de la semaine et les week-ends et, pour les heures de pointe et les intervalles calmes.

Gestion partielle de l'alimentation des machines allouées à titre permanent : pour des machines allouées à titre permanent, vous pouvez définir des horloges d'état d'alimentation, mais pas des regroupements ou des mémoires tampons. Les machines sont activées au début de chaque période de pointe et désactivées au début de chaque période creuse. Vous n'avez pas de contrôle précis comme avec les machines non allouées sur le nombre de machines qui deviennent disponibles pour compenser les machines qui sont utilisées.

Pour gérer la consommation des machines virtuelles avec OS de bureau :

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe, puis sélectionnez **Modifier le groupe de mise à disposition** dans le volet Actions.
3. Sur la page **Gestion de l'alimentation**, sélectionnez **Jours ouvrés** dans la liste déroulante Gestion de l'alimentation des machines. Par défaut, les jours de la semaine vont du lundi au vendredi.
4. Pour les groupes de mise à disposition aléatoires, dans **Machines à allumer**, cliquez sur **Modifier** et spécifiez la taille du regroupement durant les jours ouvrés. Ensuite, sélectionnez le nombre de machines à mettre sous tension.

5. Dans **Heures de pointe**, définissez les heures de pointe et les heures creuses de chaque jour.
6. Définissez les horloges d'état d'alimentation pour les heures de pointe et les heures creuses des jours de la semaine : Dans **Durant les heures de pointe > Après déconnexion**, indiquez le délai (en minutes) avant la suspension des machines déconnectées dans le groupe de mise à disposition, puis sélectionnez Suspendre. Dans **Durant les heures creuses > Après déconnexion**, indiquez le délai avant la suspension des machines déconnectées dans le groupe de mise à disposition, puis sélectionnez **Arrêter**. Cette horloge n'est pas disponible pour les groupes de mise à disposition avec des machines aléatoires.
7. Sélectionnez **Week-end** dans la liste déroulante Gérer l'alimentation des machines, puis configurez les heures de pointe et les horloges d'état d'alimentation pour les week-ends.
8. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Utilisez le SDK pour :

- Arrêter, plutôt que suspendre, les machines en réponse aux horloges d'état d'alimentation ou si vous voulez que les horloges soient basées sur les fermetures de session et non sur les déconnexions.
- Modifier les définitions par défaut des jours de la semaine et du week-end.
- Désactiver la gestion de l'alimentation ; consultez l'article CTX217289.

Créer un programme de redémarrage pour les machines d'un groupe de mise à disposition

Cette section décrit comment configurer un seul programme de redémarrage dans Studio. Vous pouvez aussi utiliser PowerShell pour configurer plusieurs programmes de redémarrage pour différents sous-ensembles de machines dans un groupe de mise à disposition. Consultez la section suivante pour plus de détails.

Un programme de redémarrage spécifie quand redémarrer périodiquement toutes les machines d'un groupe de mise à disposition.

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe, puis sélectionnez **Modifier le groupe de mise à disposition** dans le volet Actions.
3. Sur la page **Programme de redémarrage**, si vous ne souhaitez pas redémarrer automatiquement les machines du groupe de mise à disposition, sélectionnez le bouton radio **Non** et passez à la dernière étape de cette procédure. Aucun programme de redémarrage ni aucune stratégie de déploiement ne sera configuré(e). Si un programme a été configuré précédemment, cette sélection l'annule.
4. Si vous souhaitez redémarrer automatiquement les machines du groupe de mise à disposition, sélectionnez le bouton radio **Oui**.

5. Pour la fréquence de **redémarrage**, choisissez **Quotidien** ou le jour de la semaine pour le redémarrage.
6. Pour **Commencer le redémarrage à**, à l'aide d'une horloge 24 heures, spécifiez l'heure de la journée à laquelle le redémarrage commence.
7. Pour **Durée du redémarrage**, indiquez si toutes les machines doivent démarrer en même temps, ou le temps total que devra prendre le lancement du redémarrage de toutes les machines dans le groupe de mise à disposition. Un algorithme interne détermine le moment où chaque machine est redémarrée pendant cet intervalle.
8. Dans la liste déroulante **Notification** de gauche, indiquez si un message de notification doit s'afficher sur les machines concernées avant qu'un redémarrage commence. Par défaut, aucun message ne s'affiche. Si vous choisissez d'afficher un message 15 minutes avant que le redémarrage commence, vous pouvez choisir (dans la liste déroulante **Répéter la notification**) de répéter le message toutes les cinq minutes après le premier message. Par défaut, le message n'est pas répété.
9. Entrez le texte de notification dans la zone **Message de notification** ; il n'existe pas de texte par défaut. Si vous souhaitez que le message contienne le nombre de minutes avant le redémarrage, incluez la variable **%m%** (par exemple : *Avertissement : votre ordinateur sera automatiquement redémarré dans % m% minutes.*) Si vous sélectionnez un intervalle de notification répété et que votre message inclut l'espace réservé %m%, la valeur diminue de cinq minutes dans chaque message répété. Si vous avez choisi de redémarrer toutes les machines en même temps, le message de notification s'affiche sur chaque machine du groupe de mise à disposition à l'heure appropriée avant que le redémarrage ne commence, calculée par l'algorithme interne.
10. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Vous ne pouvez pas réaliser de mise sous tension ou arrêt automatisé(e) dans Studio, un redémarrage uniquement.

Créer plusieurs programmes de redémarrage pour les machines d'un groupe de mise à disposition

Vous pouvez utiliser des applets de commande PowerShell pour créer plusieurs programmes de redémarrage pour des machines d'un groupe de mise à disposition. Chaque programme peut être configuré pour affecter uniquement les machines du groupe qui ont une balise spécifique. Cette fonctionnalité de restriction de balise vous permet de créer facilement différents programmes de redémarrage pour différents sous-ensembles de machines dans un groupe de mise à disposition.

Par exemple, supposons que vous utilisez un seul groupe de mise à disposition pour toutes les machines de l'entreprise. Vous voulez redémarrer chaque machine au moins une fois par semaine (le dimanche soir), mais les machines utilisées par l'équipe de comptabilité doivent être redémarrées

quotidiennement. Vous pouvez configurer un programme hebdomadaire pour toutes les machines, et un programme quotidien uniquement pour les machines utilisées par l'équipe de comptabilité.

Chevauchement de programmes :

Plusieurs programmes peuvent se chevaucher. Dans l'exemple ci-dessus, les machines utilisées par l'équipe de comptabilité sont affectées par les deux programmes, et peuvent être redémarrées deux fois le dimanche.

Le code de programmation est conçu pour éviter le redémarrage d'une même machine plus souvent que nécessaire, mais cela ne peut pas être garanti. Si l'heure de début et la durée des deux programmes coïncident précisément, il est plus probable que les machines seront redémarrées une seule fois. Toutefois, plus l'heure de début et/ou la durée diffèrent, plus il est probable que deux redémarrages seront effectués. En outre, le nombre de machines affectées par les programmes peut aussi influencer les risques de chevauchement. Dans cet exemple, le programme hebdomadaire qui redémarre toutes les machines peut initier des redémarrages beaucoup plus rapidement que le programme quotidien (en fonction de la durée configurée pour chacun d'eux).

Exigences :

La prise en charge de la création de plusieurs programmes de redémarrage et l'utilisation de restrictions de balises dans un programme de redémarrage est actuellement uniquement disponible depuis la ligne de commande PowerShell à l'aide des applets de commande PowerShell RebootScheduleV2, qui ont été introduites dans XenApp et XenDesktop 7.12. (elles sont appelées applets de commande « V2 » dans cet article).

L'utilisation des applets de commande V2 requiert :

- Version 7.12 de Delivery Controller (minimum).
  - Si vous utilisez la version la plus récente du Plug-in SDK avec un Controller antérieur à 7.12, les nouveaux programmes que vous créez ne fonctionneront pas comme prévu.
  - Dans un site mixte (où certains Controller, mais pas tous, ont été mis à niveau), les applets de commande V2 ne fonctionnent pas jusqu'à ce que la base de données ait été mise à niveau et qu'au moins un Controller ait été mis à niveau et soit utilisé (en spécifiant le paramètre –adminaddress <Controller> avec les applets de commande V2).
  - Recommandation : ne pas créer de nouveaux programmes jusqu'à ce que tous les Controller du site soient mis à niveau.
- Le composant logiciel enfichable du kit de développement PowerShell fourni avec XenApp et XenDesktop 7.12 (minimum). Lorsque vous installez ou mettez à niveau vos composants et votre site, exécutez asnp Citrix.* pour charger les applets de commande de la dernière version.

Studio utilise actuellement une version antérieure des applets de commande PowerShell V1 RebootSchedule et n'affichera pas les programmes qui sont créés avec les applets de commande V2.

Une fois que vous avez créé un programme de redémarrage qui utilise une restriction de balise, si vous utilisez Studio pour supprimer la balise d'une machine affectée pendant un intervalle de redémarrage (cycle) ou ajoutez la balise à des machines supplémentaires pendant un cycle de redémarrage, ces modifications ne prennent pas effet jusqu'au prochain cycle de redémarrage. (Les modifications n'affectent pas le cycle de redémarrage en cours).

Applets de commande PowerShell :

Utilisez les applets de commande RebootScheduleV2 suivantes à partir de la ligne de commande pour créer plusieurs programmes et utiliser des restrictions de balises dans les programmes.

- New-BrokerRebootScheduleV2 (remplace New-BrokerRebootSchedule)
- Get-BrokerRebootScheduleV2 (remplace Get-BrokerRebootSchedule)
- Set-BrokerRebootScheduleV2 (remplace Set-BrokerRebootSchedule)
- Remove-BrokerRebootScheduleV2 (remplace Remove-BrokerRebootSchedule)
- Rename-BrokerRebootScheduleV2 (nouveau, pas un remplacement)

Pour obtenir la syntaxe complète et des descriptions des paramètres de l'applet de commande, entrez **Get-Help –full** <*nom-applet*>.

Rappel de terminologie : dans le kit de développement PowerShell, le paramètre DesktopGroup identifie le groupe de mise à disposition.

Si vous avez l'habitude d'utiliser l'interface de Studio pour créer un programme de redémarrage, tous ces paramètres sont disponibles lorsque vous utilisez l'applet de commande V2 pour créer ou mettre à jour un programme. En outre, vous pouvez :

- limiter la programmation aux machines qui ont une balise spécifique ;
- spécifier un intervalle avant d'envoyer le premier message d'avertissement, pendant lequel aucune nouvelle session ne sera établie sur les machines affectées.

Configuration :

Si vous configurez un programme de redémarrage qui utilise une restriction de balise, vous devez également ajouter (appliquer) cette balise aux machines auxquelles vous souhaitez affecter le programme. (Pour plus d'informations, veuillez consulter la section Balises.)

1. Dans Studio, sélectionnez **Groupes de mise à disposition** dans le volet de navigation.
2. Sélectionnez le groupe de mise à disposition contenant les machines qui seront affectées par le programme.
3. Sélectionnez Afficher les machines, puis sélectionnez les machines auxquelles vous ajouterez une balise.
4. Sélectionnez **Gérer les balises** dans le volet Actions.
5. Si la balise existe déjà, activez la case à cocher en regard du nom de la balise. Si la balise n'existe pas, cliquez sur **Créer**, puis spécifiez le nom de la balise. Une fois que la balise est créée, activez la case à cocher en regard du nom de la balise créée.

6. Cliquez sur **Enregistrer** dans la boîte de dialogue Gérer les balises.

Après la création et l'ajout (l'application) des balises, utilisez le paramètre –RestrictToTag pour spécifier le nom de la balise lors de la création ou de la modification du programme avec l'applet de commande V2.

Si vous avez créé un programme de redémarrage avec une version antérieure de XenApp ou XenDesktop :

Studio utilise actuellement les applets de commande V1 RebootSchedule. Si un programme de redémarrage a été créé avant que vous mettiez à niveau vers 7.12 (minimum), vous pouvez continuer à le gérer dans Studio avec les applets de commande V1, mais vous ne pouvez pas utiliser Studio pour ajouter une restriction de balise à ce programme, ou pour créer d'autres programmes (car Studio ne prend pas en charge les applets de commande V2). Tant que vous utilisez les applets de commande V1 pour votre programme, Studio affiche les informations correctes sur le programme de redémarrage.

Vous pouvez aussi modifier votre programme à partir de la ligne de commande, à l'aide des nouvelles applets de commande V2 RebootSchedule. Lors de l'utilisation des nouvelles applets de commande V2, vous pouvez utiliser les paramètres de restriction de balise dans ce programme, et créer des programmes de redémarrage supplémentaires. Cependant, une fois que vous avez utilisé des applets de commande V2 pour modifier votre programme, Studio ne peut pas afficher d'informations complètes sur le programme (car il reconnaît uniquement les informations V1). Vous ne pouvez pas vérifier si une restriction de balise est utilisée ou le nom et la description du programme.

```
New-BrokerRebootScheduleV2 (remplace New-BrokerRebootSchedule)
Get-BrokerRebootScheduleV2 (remplace Get-BrokerRebootSchedule)
Set-BrokerRebootScheduleV2 (remplace Set-BrokerRebootSchedule)
Remove-BrokerRebootScheduleV2 (remplace Remove-BrokerRebootSchedule)
Rename-BrokerRebootScheduleV2 (nouveau, pas un remplacement)
New-BrokerRebootScheduleV2 (remplace New-BrokerRebootSchedule)
Get-BrokerRebootScheduleV2 (remplace Get-BrokerRebootSchedule)
Set-BrokerRebootScheduleV2 (remplace Set-BrokerRebootSchedule)
Remove-BrokerRebootScheduleV2 (remplace Remove-BrokerRebootSchedule)
Rename-BrokerRebootScheduleV2 (nouveau, pas un remplacement)
New-BrokerRebootScheduleV2 (remplace New-BrokerRebootSchedule)
Get-BrokerRebootScheduleV2 (remplace Get-BrokerRebootSchedule)
Set-BrokerRebootScheduleV2 (remplace Set-BrokerRebootSchedule)
Remove-BrokerRebootScheduleV2 (remplace Remove-BrokerRebootSchedule)
Rename-BrokerRebootScheduleV2 (nouveau, pas un remplacement)
```


Empêcher les utilisateurs de se connecter à une machine (mode de maintenance) dans un groupe de mise à disposition

Lorsque vous devez arrêter temporairement les nouvelles connexions aux machines, vous pouvez activer le mode de maintenance pour une ou toutes les machines dans un groupe de mise à disposition. Vous pouvez effectuer cette opération avant d'appliquer des correctifs ou à l'aide d'outils de gestion.

- Lorsqu'une machine avec OS de serveur se trouve en mode de maintenance, les utilisateurs peuvent se connecter à des sessions existantes mais ne peuvent pas démarrer de nouvelles sessions.
- Lorsqu'une machine avec OS de bureau (ou un ordinateur utilisant Remote PC Access) est en mode de maintenance, les utilisateurs ne peuvent pas se connecter ou se reconnecter. Les connexions courantes restent connectées jusqu'à ce qu'elles se déconnectent ou ferment leur session.

Pour activer ou désactiver le mode de maintenance :

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe.
3. Pour activer le mode de maintenance pour toutes les machines dans le groupe de mise à disposition, sélectionnez **Activer le mode de maintenance** dans le volet Actions. Pour activer le mode de maintenance pour une machine, sélectionnez **Afficher les machines** dans le volet Actions. Sélectionnez une machine, puis sélectionnez **Activer le mode de maintenance** dans le volet Actions.
4. Pour désactiver le mode de maintenance pour une ou toutes les machines dans un groupe de mise à disposition, suivez les instructions précédentes, sélectionnez **Désactiver le mode de maintenance** dans le volet Actions.

Les paramètres Windows RDC (Remote Desktop Connection) affectent également le fait qu'une machine avec OS de serveur est en mode de maintenance. Le mode de maintenance est activé dans l'un des cas suivants :

- Le mode de maintenance est défini sur Activé, comme décrit ci-dessus.
- RDC est défini sur **Ne pas autoriser les connexions à cet ordinateur**.
- RDC n'est pas défini sur **Ne pas autoriser les connexions à cet ordinateur** et le paramètre de mode d'ouverture de session utilisateur de la configuration à distance d'hôte est **Autoriser les reconnexions mais refuser les nouvelles ouvertures de session** ou **Autoriser les reconnexions mais refuser les nouvelles ouvertures de session jusqu'au redémarrage du serveur**.

Vous pouvez également activer ou désactiver le mode de maintenance pour une connexion (ce qui affecte les machines qui utilisent cette connexion), ou pour un catalogue de machines (ce qui affecte les machines de ce catalogue).

Modifier les attributions de machines des utilisateurs d'un groupe de mise à disposition

Vous pouvez modifier les attributions des machines avec OS de bureau, des machines avec OS de serveur ou des machines créées au travers de Provisioning Services.

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe.
3. Sélectionnez **Modifier le groupe de mise à disposition** dans le volet Actions. Sur la page **Bureaux** ou **Règles d'attribution de bureau** (une seule de ces pages sera disponible, en fonction du type de catalogue de machines que le groupe de mise à disposition utilise), spécifiez les nouveaux utilisateurs.
4. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Modifier le nombre maximal de machines par utilisateur

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe, puis sélectionnez **Modifier le groupe de mise à disposition** dans le volet Actions.
3. Sur la page **Règles d'attribution de bureau**, définissez le nombre maximal de bureaux par utilisateur.
4. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Gérer la charge des machines dans les groupes de mise à disposition

Vous pouvez gérer la charge des machines avec OS de serveur uniquement.

La gestion de la charge mesure la charge du serveur et détermine le serveur à sélectionner dans les conditions actuelles d'environnement. Cette sélection est basée sur :

État du mode de maintenance du serveur : une machine avec OS de serveur est considérée pour l'équilibrage de charge uniquement lorsque le mode de maintenance est désactivé.

Indice de charge du serveur : détermine la probabilité qu'un serveur qui met à disposition des machines avec OS de serveur a de recevoir des connexions. L'index est une combinaison de calculateurs de charge : le nombre de sessions et les paramètres des mesures de performances tels que l'UC, le disque et l'utilisation de la mémoire. Vous devez spécifier des calculateurs de charge dans les paramètres de la stratégie de gestion de la charge.

Vous pouvez surveiller l'index de charge dans Director, la recherche Studio et le kit de développement.

Dans Studio, la colonne Indice de charge du serveur est masquée par défaut. Pour l'afficher, sélectionnez une machine, cliquez avec le bouton droit de la souris sur un en-tête de colonne, puis choisissez Sélectionner les colonnes. Dans la catégorie Machine, sélectionnez Indice de charge.

Dans le kit de développement, utilisez l'applet de commande Get-BrokerMachine. Pour de plus amples informations, consultez l'article CTX202150.

Un serveur d'index de charge de 10 000 indique que le serveur est complètement chargé. Si aucun des autres serveurs n'est disponible, il se peut que les utilisateurs reçoivent un message indiquant que le bureau ou l'application est actuellement indisponible lorsqu'ils lancent une session.

Paramètre de stratégie de tolérance d'ouvertures de session simultanées : le nombre maximal de demandes simultanées pour ouvrir une session sur le serveur. (Ce paramètre est équivalent à l'optimisation de la charge dans les versions antérieures à la version 7.5 de XenApp.)

Si le nombre de demandes d'ouvertures de session que tous les serveurs reçoivent est égal ou supérieur au paramètre Tolérance d'ouvertures de session simultanées, la prochaine demande d'ouverture de session est attribuée au serveur avec le nombre d'ouvertures de session en attente le plus faible. Si plusieurs serveurs répondent à ces critères, le serveur ayant l'index de charge le plus faible est sélectionné.

Supprimer une machine d'un groupe de mise à disposition

La suppression d'une machine la supprime d'un groupe de mise à disposition, mais ne la supprime pas dans le catalogue de machines que le groupe de mise à disposition utilise. Par conséquent, cette machine est disponible pour l'affectation à un autre groupe de mise à disposition.

Les machines doivent être arrêtées avant de pouvoir être supprimées. Pour empêcher temporairement les utilisateurs de se connecter à une machine pendant que vous la supprimez, placez-la en mode maintenance avant de l'arrêter.

Gardez à l'esprit que les machines peuvent contenir des données personnelles, soyez donc prudent avant d'allouer la machine à un autre utilisateur. Il se peut que vous souhaitiez créer une nouvelle image de la machine.

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe, puis sélectionnez **Afficher les machines** dans le volet Actions.
3. Vérifiez que la machine est arrêtée.
4. Sélectionnez **Supprimer du groupe de mise à disposition** dans le volet Actions.

Vous pouvez également supprimer une machine d'un groupe de mise à disposition au travers de la connexion utilisée par la machine. Pour de plus amples informations, veuillez consulter la section Connexions et ressources.

Restreindre l'accès aux machines dans un groupe de mise à disposition

Toute modification que vous apportez pour restreindre l'accès aux machines dans un groupe de mise à disposition remplace les paramètres précédents, quelle que soit la méthode que vous utilisez. Vous pouvez :

Limiter l'accès des administrateurs à l'aide des étendues d'administration déléguée. Vous pouvez créer et allouer une étendue qui permet aux administrateurs d'accéder à toutes les applications, et une autre qui ne leur donne accès qu'à certaines applications. Consultez l'article Administration déléguée pour plus de détails.

Limiter l'accès des utilisateurs via des expressions de stratégie SmartAccess qui filtrent les connexions utilisateur effectuées via NetScaler Gateway.

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe, puis sélectionnez **Modifier le groupe de mise à disposition** dans le volet Actions.
3. Dans la page **Stratégie d'accès**, sélectionnez **Connexions transitant par NetScaler Gateway**.
4. Pour choisir un sous-ensemble de ces connexions, sélectionnez **Connexions remplissant l'un des critères de filtre suivants**. Ensuite, définissez le site NetScaler Gateway, et ajoutez, modifiez ou supprimez les expressions de la stratégie SmartAccess pour les scénarios d'accès des utilisateurs autorisés. Pour plus d'informations, consultez la documentation relative à NetScaler Gateway.
5. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Limiter l'accès des utilisateurs via des filtres d'exclusion sur les stratégies d'accès que vous définissez dans le kit de développement. Des stratégies d'accès sont appliquées aux groupes de mise à disposition pour affiner les connexions. Par exemple, vous pouvez restreindre l'accès aux machines à un sous-ensemble d'utilisateurs, vous pouvez spécifier les machines utilisateur autorisées. Les filtres d'exclusion affinent davantage les stratégies d'accès. Vous pouvez, par exemple, refuser l'accès à un sous-ensemble d'utilisateurs ou de machines pour des raisons de sécurité. Par défaut, les filtres d'exclusion sont désactivés.

Par exemple, un laboratoire d'enseignement sur un sous-réseau du réseau d'entreprise, pour empêcher l'accès à ce laboratoire à un certain groupe de mise à disposition, quelle que soit la personne qui utilise les machines dans le laboratoire, utilisez la commande suivante : **Set-BrokerAccessPolicy -Name VPDesktops_Direct -ExcludedClientIPFilterEnabled $True**.

Vous pouvez également utiliser un astérisque (*) en tant que caractère générique afin de faire correspondre toutes les balises qui commencent par la même expression de stratégie. À titre d'exemple, si vous avez ajouté la balise VPDesktops_Direct à une machine et VPDesktops_Test à une autre machine, la définition de la balise dans le script Set-BrokerAccessPolicy sur VPDesktops_* applique le filtre aux deux machines.

Si vous êtes connecté à l'aide d'un navigateur Web ou avec la fonctionnalité d'expérience Citrix Receiver unifiée activée dans le magasin, vous ne pouvez pas utiliser un filtre d'exclusion du nom de client.

Mettre à jour une machine dans un groupe de mise à disposition

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe, puis sélectionnez **Afficher les machines** dans le volet Actions.
3. Sélectionnez une machine, puis sélectionnez **Mettre à jour les machines** dans le volet Actions.

Pour sélectionner une autre image principale, sélectionnez **Image principale**, puis sélectionnez un instantané.

Pour appliquer les modifications et notifier les utilisateurs de la machine, sélectionnez **Envoyer une notification aux utilisateurs**. Ensuite, spécifiez : quand effectuer la mise à jour de l'image principale (maintenant ou lors du prochain redémarrage), l'horaire de distribution du redémarrage (le délai total imparti pour commencer la mise à jour de toutes les machines du groupe), et si les utilisateurs seront notifiés du redémarrage, ainsi que le message qu'ils recevront.

Fermer ou déconnecter une session, ou envoyer un message aux utilisateurs d'un groupe de mise à disposition

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe, puis sélectionnez **Afficher les machines** dans le volet Actions.
3. Pour fermer la session d'un utilisateur, sélectionnez la session ou le bureau, puis sélectionnez **Fermer la session** dans le volet Actions. La session se ferme et la machine devient disponible auprès des autres utilisateurs, à moins qu'elle ne soit attribuée à un utilisateur spécifique.
4. Pour déconnecter une session, sélectionnez la session ou le bureau, puis sélectionnez **Déconnecter** dans le volet Actions. Les applications continuent à être exécutées et la machine reste attribuée à cet utilisateur. L'utilisateur peut se reconnecter à la même machine.
5. Pour envoyer un message aux utilisateurs, sélectionnez la session, la machine ou l'utilisateur, puis sélectionnez **Envoyer un message** dans le volet Actions. Entrez le message.

Vous pouvez configurer les horloges d'état d'alimentation pour les machines avec OS de bureau pour gérer automatiquement les sessions non utilisées. Consultez la section Gérer l'alimentation des machines pour plus de détails.

Configurer le pré-lancement de session et la persistance de session dans un groupe de mise à disposition

Ces fonctionnalités sont prises en charge sur les machines avec OS de serveur uniquement.

Les fonctionnalités de pré-lancement de session et de persistance de session aident les utilisateurs spécifiés à accéder aux applications rapidement, en démarrant des sessions avant qu'elles ne sont demandées (pré-lancement de session) et conserver les sessions d'applications actives après qu'un utilisateur ferme toutes les applications (persistance de session).

Par défaut, le pré-lancement de session et la persistance de session ne sont pas utilisées : une session démarre (se lance) lorsqu'un utilisateur démarre une application et reste active jusqu'à ce que la dernière application ouverte dans la session se ferme.

Notions importantes :

- Le groupe de mise à disposition doit prendre en charge les applications, et les machines doivent être exécutées sur un VDA pour OS de serveur Windows, version minimale 7.6.
- Ces fonctionnalités sont uniquement prises en charge lors de l'utilisation de Citrix Receiver pour Windows, et requièrent également une configuration de Citrix Receiver supplémentaire. Pour obtenir des instructions, recherchez pré-lancement de session dans la documentation produit pour votre version de Citrix Receiver pour Windows.
- Veuillez noter que Citrix Receiver pour HTML5 n'est pas pris en charge.
- Lorsque vous utilisez le pré-lancement de session, si une machine utilisateur est placée en mode « suspendue » ou « veille prolongée », le pré-lancement ne fonctionne pas (quels que soient les paramètres de pré-lancement de session). Les utilisateurs peuvent verrouiller leurs machines/sessions, mais si un utilisateur ferme sa session sur Citrix Receiver, la session est fermée et le pré-lancement ne s'applique plus.
- Lorsque vous utilisez le pré-lancement de session, les machines clientes physiques ne peuvent pas utiliser les fonctions de gestion de l'alimentation en veille ou veille prolongée. Les utilisateurs de la machine cliente peuvent verrouiller leurs sessions, mais ne doivent pas les fermer.
- Les sessions pré-lancées et persistantes utilisent une licence, mais uniquement lorsque vous êtes connecté. Toute session pré-lancée et persistante non utilisée se déconnecte après 15 minutes par défaut. Cette valeur peut être configurée dans PowerShell (applet de commande New/Set-BrokerSessionPreLaunch).
- Une planification et un contrôle attentif des modèles d'activité de vos utilisateurs sont essentiels pour personnaliser ces fonctionnalités afin qu'elles se complètent l'une avec l'autre. Une configuration optimale équilibre les avantages d'une disponibilité d'application antérieure pour les utilisateurs par rapport au coût de licences en cours d'utilisation et de ressources allouées.
- Vous pouvez également configurer le pré-lancement de session pour une heure de la journée planifiée dans Citrix Receiver.

Durée pendant laquelle les sessions pré-lancées et persistantes restent actives

Il existe plusieurs façons de spécifier la durée pendant laquelle une session non utilisée reste active si l'utilisateur ne démarre pas une application : un délai configuré et des seuils de charge du serveur. Vous pouvez tous les configurer ; l'événement qui se produit en premier provoque la fin de la session non utilisée.

- **Expiration du délai :** une expiration de délai configurée spécifie le nombre de minutes, heures ou jours pendant lesquels une session pré-lancée inutilisée ou une session de persistance restent actives. Si vous configurez un délai d'expiration trop court, les sessions pré-lancées se termineront avant de permettre aux utilisateurs de bénéficier d'un accès aux applications plus rapide. Si vous configurez un délai d'expiration trop long, les connexions utilisateur entrantes peuvent être refusées car le serveur ne dispose pas de suffisamment de ressources.

  Vous ne pouvez pas désactiver cette expiration du délai depuis Studio, mais vous pouvez dans le kit de développement (applet de commandes New/Set-BrokerSessionPreLaunch). Si vous désactivez l'expiration du délai, elle n'apparaît pas dans l'affichage de Studio pour ce groupe de mise à disposition ou dans l'Assistant Modifier le groupe de mise à disposition.

- **Seuils :** les sessions pré-lancées se terminant automatiquement et les sessions de persistance basées sur la charge d'un serveur assurent que les sessions restent ouvertes le plus longtemps possible, en supposant que les ressources serveur sont disponibles. Les sessions pré-lancées et les sessions de persistance inutilisées ne provoqueront pas de refus de connexions, car elles seront arrêtées automatiquement lorsque les ressources sont nécessaires pour de nouvelles sessions utilisateur.

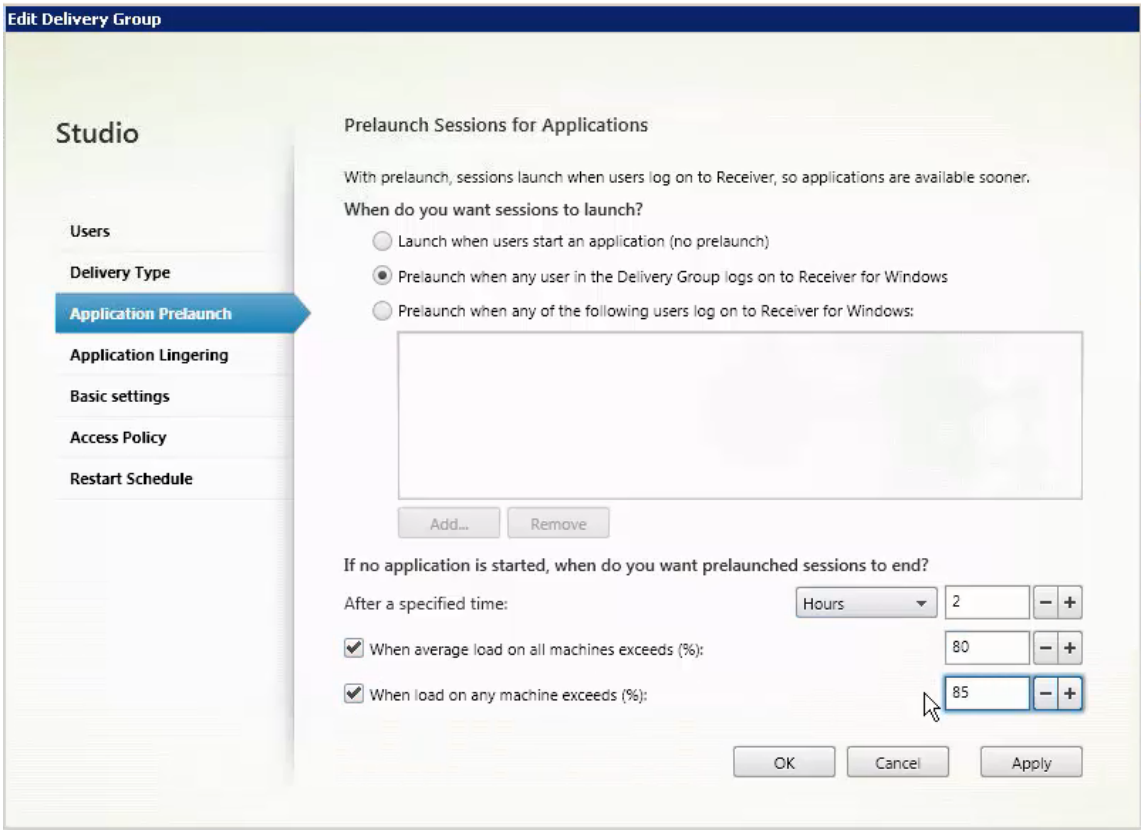
  Vous pouvez configurer deux seuils : la charge de pourcentage moyenne de tous les serveurs dans le groupe de mise à disposition et le pourcentage maximal de charge d'un serveur dans le groupe de mise à disposition. Lorsqu'un seuil est dépassé, les sessions qui se sont trouvées dans un état de pré-lancement ou de persistance pour la période la plus longue est terminée, les sessions sont arrêtés une à une à toutes les minutes jusqu'à ce que la charge tombe en dessous du seuil. (Lorsque la valeur de seuil est dépassée, aucune nouvelle session de pré-lancement n'est démarrée

Les serveurs avec des VDA qui n'ont pas été inscrits avec le Controller et les serveurs en mode de maintenance sont considérés comme entièrement chargés. Un problème inattendu provoque la fermeture automatique des sessions de pré-lancement et des sessions de persistance pour libérer de la capacité.

Pour activer le pré-lancement de session

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe de mise à disposition, puis cliquez sur **Modifier le groupe de mise à disposition** dans le volet Actions.

3. Sur la page **Pré-démarrage d'application**, activez le pré-lancement de session, en choisissant le moment de démarrage des sessions :
    - Lorsqu'un utilisateur démarre une application. Il s'agit du paramètre par défaut ; le pré-lancement de session est désactivé.
    - Lorsqu'un utilisateur du groupe de mise à disposition ouvre une session sur Citrix Receiver pour Windows.
    - Lorsque tout le monde dans une liste d'utilisateurs et de groupes d'utilisateurs ouvre une session sur Citrix Receiver pour Windows. Veuillez également spécifier les utilisateurs ou les groupes d'utilisateurs si vous choisissez cette option.



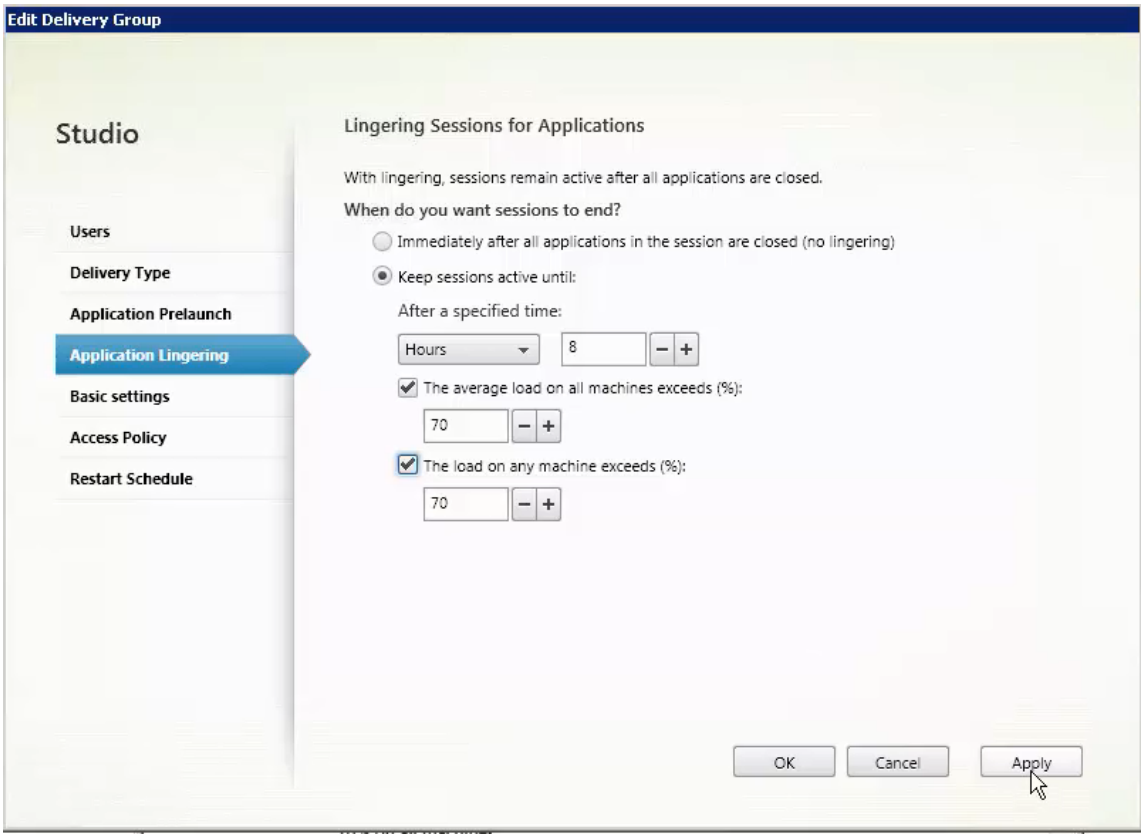
4. Une session pré-lancée est remplacée par une session régulière lorsque l'utilisateur démarre une application. Si l'utilisateur ne démarre pas une application (la session pré-lancée n'est pas utilisée), les paramètres suivants affectent la durée pour laquelle la session reste active.
    - Lorsqu'un intervalle de temps spécifié expire. Vous pouvez modifier l'intervalle de temps (1-99 jours, 1-2 376 heures, heures ou 1-142 560 minutes).
    - Lorsqu'une charge moyenne sur toutes les machines du groupe de mise à disposition dépasse un pourcentage spécifié (1-99%).
    - Lorsque la charge de toute machine du groupe de mise à disposition dépasse un pourcentage spécifié (1-99%).

    Récapitulatif : une session pré-lancée reste active jusqu'à ce que l'un des événements suivants

se produise : un utilisateur lance une application, la durée spécifiée est écoulée, ou un seuil de charge spécifié est dépassé.

Pour activer la persistance de session

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe de mise à disposition, puis cliquez sur **Modifier le groupe de mise à disposition** dans le volet Actions.
3. Sur la page **Attente d'application**, activez la persistance de session en sélectionnant le bouton radio **Maintenir les sessions dans l'état actif jusqu'à**.



4. Plusieurs paramètres affectent la durée pendant laquelle une session persistante reste active si l'utilisateur ne démarre pas d'autre application.
   - Lorsqu'un intervalle de temps spécifié expire. Vous pouvez modifier l'intervalle de temps (1-99 jours, 1-2 376 heures, heures ou 1-142 560 minutes).
   - Lorsqu'une charge moyenne sur toutes les machines du groupe de mise à disposition dépasse un pourcentage spécifié (1-99%).
   - Lorsque la charge de toute machine du groupe de mise à disposition dépasse un pourcentage spécifié (1-99%).

Récapitulatif : une session de persistance reste active jusqu'à ce que l'un des événements suivants se produise : un utilisateur démarre une application, la durée spécifiée est écoulée, ou un seuil de charge spécifié est dépassé.

Dépannage

- Les VDA qui ne sont pas enregistrés auprès d'un Delivery Controller ne sont pas pris en compte lors du lancement de sessions non négociées, ce qui entraîne une sous-utilisation des ressources disponibles par ailleurs. Il existe un certain nombre de raisons pour lesquelles un VDA peut ne pas être enregistré, un grand nombre d'entre elles pouvant être résolues par un administrateur. Studio offre des informations de dépannage dans l'Assistant de création de catalogue de machines, et après l'ajout d'un catalogue de machines à un groupe de mise à disposition.

  Une fois que vous avez créé un groupe de mise à disposition, Studio affiche davantage de détails sur les machines associées à ce groupe. Le panneau de détails pour un groupe de mise à disposition indique le nombre de machines qui devraient être enregistrées, mais ne le sont pas. En d'autres termes, une ou plusieurs machines peuvent être sous tension et pas en mode de maintenance, mais pas enregistrées auprès d'un Controller. Lors de l'affichage d'une machine « non enregistrée », mais qui devrait l'être, consultez l'onglet Dépannage dans le panneau Détails pour connaître les causes possibles et les actions correctives recommandées.

  Pour les messages sur le niveau fonctionnel, consultez la section Versions VDA et niveaux fonctionnels. Pour plus d'informations sur le dépannage de l'enregistrement de VDA, voir l'article CTX136668.

- dans l'affichage Studio d'un groupe de mise à disposition, la « version de VDA installée » dans le panneau Détails peut différer de la version installée sur les machines. Les programmes et fonctionnalités Windows de la machine affichent la version actuelle du VDA.

- Pour les machines affichant un « état d'alimentation inconnu », consultez l'article CTX131267 pour plus d'informations.

Créer des groupes d'applications

February 28, 2019

Introduction

Les groupes d'applications vous permettent de gérer des collections d'applications. Vous pouvez créer des groupes d'applications pour les applications partagées entre différents groupes de mise à

disposition ou utilisées par un sous-ensemble d'utilisateurs dans des groupes de mise à disposition. Les groupes d'applications sont facultatifs ; ils offrent une alternative à l'ajout des mêmes applications sur plusieurs groupes de mise à disposition. Les groupes de mise à disposition peuvent être associés à plus d'un groupe d'applications, et un groupe d'applications peut être associée à plus d'un groupe de mise à disposition.

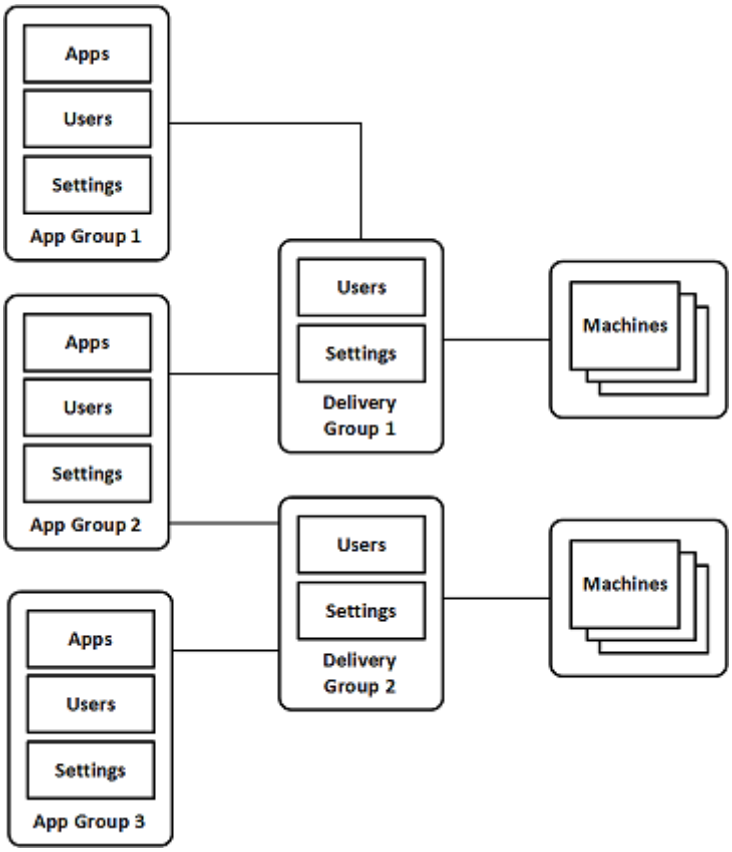
Comparativement à l'utilisation d'un plus grand nombre de groupes de mise à disposition, les groupes d'applications permettent de gérer les applications et de contrôler les ressources :

- Le regroupement logique d'applications et de leurs paramètres vous permet de gérer ces applications comme une unité unique. Par exemple, vous n'avez pas besoin d'ajouter (publier) la même application, une par une, à des groupes de mise à disposition individuels.
- Le partage de session entre des groupes d'applications peut économiser la consommation de ressources. Dans d'autres cas, la désactivation du partage de session entre les groupes d'applications peut s'avérer bénéfique.
- Vous pouvez utiliser la fonction de *restriction de balise* pour publier des applications à partir d'un groupe d'applications, prenant en compte un seul sous-ensemble de machines dans les groupes de mise à disposition sélectionnés. Avec les restrictions de balise, vous pouvez utiliser des machines existantes pour plusieurs tâches de publication, éliminant ainsi les coûts associés avec le déploiement et la gestion de machines supplémentaires. L'utilisation d'une restriction de balise équivaut à diviser (ou partitionner) des machines dans un groupe de mise à disposition. L'utilisation d'un groupe d'applications ou de bureaux avec une restriction de balise peut s'avérer utile pour isoler et dépanner un sous-ensemble de machines dans un groupe de mise à disposition.

Exemples de configuration

Exemple 1

Le graphique suivant illustre un déploiement XenApp ou XenDesktop qui comprend des groupes d'applications :



Dans cette configuration, les applications sont ajoutées à des groupes d'applications, et non à des groupes de mise à disposition. Les groupes de mise à disposition spécifient les machines qui seront utilisées. (Bien que cela ne soit pas affiché, les machines se trouvent dans des catalogues de machines).

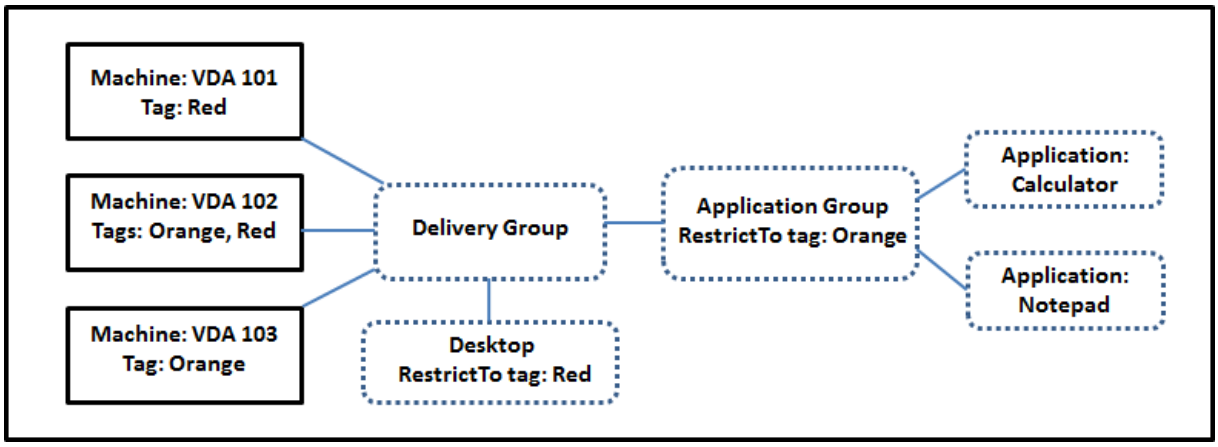
Le groupe d'applications 1 est associé au groupe de mise à disposition 1. Les applications du groupe d'applications 1 sont accessibles par les utilisateurs spécifiés dans le groupe d'applications 1, à condition qu'ils figurent également dans la liste des utilisateurs du groupe de mise à disposition 1. Cette approche suit les recommandations selon lesquelles la liste d'utilisateurs d'un groupe d'applications doit être un sous-ensemble (une restriction) des listes d'utilisateurs des groupes de mise à disposition associés. Les paramètres du groupe d'applications 1 (tels que le partage de session d'application entre groupes d'applications, groupes de mise à disposition associés) s'appliquent aux applications et utilisateurs de ce groupe. Les paramètres du groupe de mise à disposition de 1 (tels que la prise en charge des utilisateurs anonymes) s'appliquent aux utilisateurs des groupes d'applications 1 et 2, car ces groupes d'applications ont été associés à ce groupe de mise à disposition.

Le groupe d'applications 2 est associé à deux groupes de mise à disposition : 1 et 2. Chacun de ces groupes de mise à disposition peut se voir attribuer une priorité dans le groupe d'applications 2, ce qui indique l'ordre dans lequel les groupes de mise à disposition vont être vérifiés lorsqu'une application est lancée. La charge des groupes de disposition ayant le même niveau de priorité est équilibrée. Les applications du groupe d'applications 2 sont accessibles par les utilisateurs spécifiés dans le groupe

d'applications 2, à condition qu'ils figurent également dans les listes d'utilisateurs du groupe de mise à disposition 1 et du groupe de mise à disposition 2.

Exemple 2

Cette configuration simple utilise des restrictions de balise pour limiter les machines qui seront prises en compte pour certains lancements de bureau et d'application. Le site dispose d'un groupe de mise à disposition partagé, d'un bureau publié et d'un groupe d'applications configuré avec deux applications.



Des balises ont été ajoutées à chacune des trois machines (VDA 101-103).

Le groupe d'applications a été créé avec la restriction de balise « Orange », de sorte que chacune de ses applications (calculatrice et Bloc-notes) puisse être lancée uniquement sur les machines de ce groupe de mise à disposition qui ont la balise « Orange » : VDA 102 et 103.

Pour obtenir des exemples et des instructions sur l'utilisation des restrictions de balise dans des groupes d'applications (et pour des bureaux), veuillez consulter l'article Balises.

Conseils et considérations

Citrix vous recommande d'ajouter des applications à des groupes d'applications ou des groupes de mise à disposition, mais pas aux deux. Sinon, la complexité engendrée par le fait d'avoir des applications dans deux types de groupes peut rendre leur gestion plus difficile.

Par défaut, un groupe d'applications est activé. Lorsque vous créez un groupe d'applications, vous pouvez modifier le groupe pour modifier ce paramètre. Consultez l'article Gérer des groupes d'applications.

Par défaut, le partage de session d'application entre les groupes d'applications est activé. Consultez l'article Partage de session entre des groupes d'applications.

Citrix recommande de mettre à niveau vos groupes de mise à disposition vers la version actuelle. Cela requiert (1) de mettre à niveau les VDA sur les machines utilisées dans le groupe de mise à disposition, (2) de mettre à niveau les catalogues de machines contenant ces machines, puis (3) de mettre à niveau le groupe de mise à disposition. Pour de plus amples informations, consultez la section Gérer des groupes d'applications. Pour utiliser des groupes d'applications, vos composants principaux doivent être à la version minimale 7.9.

La création de groupes d'applications nécessite les autorisations d'administration déléguée du rôle intégré d'administrateur de groupe de mise à disposition. Voir Administration déléguée.

Cet article introduit la notion d'association d'une application avec plus d'un groupe d'applications pour opérer une distinction avec l'ajout d'une nouvelle instance de cette application à partir d'une source disponible. De même, les groupes de mise à disposition sont associés à des groupes d'applications (et vice versa), plutôt que des ajouts ou des composants de l'un ou l'autre.

Partage de session avec des groupes d'applications

Lorsque le partage de session d'application est activé, toutes les applications démarrent dans la même session d'application. Cette option permet d'économiser les coûts associés au lancement de sessions d'application supplémentaires et d'utiliser les fonctionnalités applicatives qui impliquent le Presse-papiers, telles que les opérations de copier-coller. Toutefois, dans certaines situations, vous souhaiterez peut-être désactiver le partage de session.

Lorsque vous utilisez des groupes d'applications, vous pouvez configurer le partage de session d'application de trois manières qui étendent le comportement du partage de session standard disponible lorsque vous utilisez uniquement des groupes de mise à disposition :

- Partage de session activé entre des groupes d'applications.
- Partage de session activé uniquement entre les applications d'un même groupe d'applications.
- Partage de session désactivé.

Partage de session entre des groupes d'applications

Vous pouvez activer le partage de session d'application entre groupes d'applications, ou vous pouvez le désactiver pour limiter le partage de session d'application aux applications d'un même groupe d'applications.

Exemple dans lequel l'activation du partage de session entre des groupes d'applications est utile :

- Le groupe d'applications 1 contient des applications Microsoft Office telles que Word et Excel. Le groupe d'applications 2 contient d'autres applications telles que le bloc-notes et la calculatrice, et les deux groupes d'applications sont associés au même groupe de mise à disposition. Un utilisateur qui a accès aux deux groupes d'applications démarre une session d'application

en lançant Word, puis ouvre le bloc-notes. Si le Controller détermine que la session existante de l'utilisateur exécutant Word peut exécuter le bloc-notes, le bloc-notes est démarré dans la session existante. Si le bloc-notes ne peut pas être exécuté à partir de la session existante (par exemple, si la restriction de balise exclut la machine sur laquelle la session est en cours d'exécution), une nouvelle session sur une machine appropriée est préférée au partage de session.

Exemple dans lequel la désactivation du partage de session entre des groupes d'applications est utile :

- Vous disposez d'applications qui ne fonctionnent pas correctement avec d'autres applications qui sont installées sur la même machine, telles que deux versions différentes de la même suite logicielle ou deux versions différentes du même navigateur Web. Vous ne souhaitez pas autoriser un utilisateur à lancer les deux versions dans la même session.

  Vous créez un groupe d'applications pour chaque version de la suite logicielle, et ajoutez les applications de chaque version de la suite logicielle au groupe d'applications correspondant. Si le partage de session entre les groupes est désactivé pour chacun de ces groupes d'application, un utilisateur spécifié dans ces groupes peuvent exécuter les applications de la même version dans la même session et peut toujours exécuter d'autres applications simultanément, mais pas dans la même session. Si l'utilisateur lance une des applications dont la version est différente (qui se trouvent dans un autre groupe d'applications), ou lance une application qui ne figure pas dans un groupe d'applications, cette application est lancée dans une nouvelle session.

Cette fonctionnalité de partage de session entre groupes d'applications n'est pas une fonctionnalité de sécurité faisant appel à un sandbox. Elle n'est pas infaillible et elle ne peut pas empêcher les utilisateurs de lancer des applications dans leurs sessions via d'autres moyens (par exemple, au travers de l'Explorateur Windows).

Si une machine fonctionne à pleine capacité, les nouvelles sessions ne sont pas démarrées sur cette dernière. Les nouvelles applications sont démarrées dans des sessions existantes sur la machine, si nécessaire, à l'aide du partage de session (à condition que ce comportement soit conforme aux restrictions décrites ici pour le partage de session).

Vous pouvez uniquement mettre des sessions pré-lancées à disposition des groupes d'applications pour lesquels le partage de session d'application est autorisé. (Les sessions qui utilisent la fonctionnalité de persistance de session sont à disposition de tous les groupes d'application.) Ces fonctionnalités doivent être activées et configurées dans chacun des groupes de mise à disposition associés au groupe d'applications ; vous ne pouvez pas les configurer dans les groupes d'applications.

Par défaut, le partage de session d'applications entre groupes d'applications est activé lorsque vous créez un groupe d'applications ; vous ne pouvez pas changer ce paramètre lors de la création du groupe. Lorsque vous créez un groupe d'applications, vous pouvez modifier le groupe pour modifier ce paramètre. Consultez l'article Gérer des groupes d'applications.

Désactiver le partage de session dans un groupe d'applications

Vous pouvez empêcher le partage de session d'application entre les applications qui appartiennent au même groupe d'applications.

Exemple dans lequel la désactivation du partage de session dans des groupes d'applications est utile :

- Vous voulez que vos utilisateurs accèdent à plusieurs sessions plein écran simultanées d'une application sur des écrans distincts.

  Vous créez un groupe d'applications et ajoutez les applications à ce groupe. Si le partage de session n'est pas autorisé entre les applications de ce groupe d'applications, un utilisateur spécifié dans le groupe démarre les applications les unes après les autres dans des sessions distinctes et il peut déplacer chaque application sur un autre écran.

Par défaut, le partage de session d'applications est activé lorsque vous créez un groupe d'applications ; vous ne pouvez pas changer ce paramètre lors de la création du groupe. Lorsque vous créez un groupe d'applications, vous pouvez modifier le groupe pour modifier ce paramètre. Consultez l'article Gérer des groupes d'applications.

Créer un groupe d'applications

Pour créer un groupe d'applications :

1. Sélectionnez **Applications** dans le panneau de navigation de Studio, puis sélectionnez **Créer groupe d'applications** dans le volet Actions.
2. L'assistant Créer groupe d'applications s'ouvre avec une page **Introduction**, que vous pouvez supprimer des lancements ultérieurs de cet assistant.
3. L'assistant vous guide ensuite au travers des pages décrites ci-dessous. Lorsque vous avez terminé chaque page, cliquez sur **Suivant** jusqu'à la page finale.

Groupes de mise à disposition

Tous les groupes de mise à disposition sont répertoriés, avec le nombre de machines qu'ils contiennent.

- La liste **Groupes de mise à disposition compatibles** contient les groupes de mise à disposition que vous pouvez sélectionner. Les groupes de mise à disposition compatibles contiennent des machines avec OS de bureau ou de serveur aléatoires (non attribuées de façon permanente ou statique).
- La liste **Groupes de mise à disposition incompatibles** contient les groupes de mise à disposition que vous ne pouvez pas sélectionner. Chaque entrée explique pourquoi un groupe n'est pas compatible, par exemple parce qu'il contient machines attribuées de manière statique.

Un groupe d'applications peut être associé à des groupes de mise à disposition contenant des machines partagées (non privées) qui peuvent mettre à disposition des applications.

Vous pouvez également sélectionner des groupes de mise à disposition contenant des machines partagées qui mettent uniquement à disposition des bureaux, si (1) le groupe de mise à disposition contient des machines partagées et a été créé avec une version antérieure de XenDesktop 7.x, et (2) vous disposez de l'autorisation Modifier le groupe de mise à disposition. Le type de groupe de mise à disposition est automatiquement converti en « bureaux et applications » lorsque l'assistant Créer groupe d'applications est validé.

Bien que vous puissiez créer un groupe d'applications qui n'est associé à aucun groupe de mise à disposition – par exemple pour organiser les applications ou pour servir de stockage aux applications non utilisées – le groupe d'applications ne peut pas être utilisé pour mettre à disposition des applications tant qu'il ne spécifie pas au moins un groupe de mise à disposition. En outre, vous ne pouvez pas ajouter d'applications au groupe d'applications à partir de la source Depuis le menu Démarrer si aucun groupe de mise à disposition n'est spécifié.

Les groupes de mise à disposition que vous sélectionnez spécifient les machines qui seront utilisées pour mettre à disposition des applications. Sélectionnez les cases à cocher en regard des groupes de mise à disposition que vous souhaitez associer au groupe d'applications.

Pour ajouter une restriction de balise, sélectionnez **Restreindre les lancements aux machines dotées de balises** puis sélectionnez la balise dans la liste déroulante. Consultez l'article Balises pour plus de détails.

Utilisateurs

Spécifiez quiconque peut utiliser les applications dans le groupe d'applications. Vous pouvez autoriser tous les utilisateurs et groupes d'utilisateurs dans les groupes de mise à disposition que vous avez sélectionnés sur la page précédente, ou sélectionner des utilisateurs et groupes d'utilisateurs spécifiques à partir de ces groupes de mise à disposition. Si vous limitez l'utilisation aux utilisateurs que vous spécifiez, seuls les utilisateurs spécifiés dans le groupe de mise à disposition et le groupe d'applications peuvent accéder aux applications dans ce groupe d'applications. Concrètement, la liste d'utilisateurs du groupe d'applications filtre les listes d'utilisateurs des groupes de mise à disposition.

La possibilité d'activer ou de désactiver l'utilisation d'applications par des utilisateurs non authentifiés est uniquement disponible dans les groupes de mise à disposition, et pas dans les groupes d'applications.

Où les listes d'utilisateurs sont spécifiées

Les listes d'utilisateurs Active Directory sont spécifiées lorsque vous créez ou modifiez les informations suivantes :

- La liste des droits d'utilisateur pour le groupe de mise à disposition, qui n'est pas configurée dans Studio. Par défaut, la règle de stratégie d'admissibilité d'application inclut tout le monde ; consultez les applets de commande du kit de développement PowerShell BrokerAppEntitlementPolicyRule pour plus de détails.
- La liste d'utilisateurs du groupe d'applications.
- La liste d'utilisateurs du groupe de mise à disposition.
- La propriété de visibilité de l'application.

La liste des utilisateurs qui peuvent accéder à une application via StoreFront est constituée à partir de l'intersection des listes utilisateur ci-dessus. Par exemple, pour configurer l'utilisation d'une application A pour un département particulier, sans pour autant limiter l'accès à d'autres groupes :

- utiliser la règle de stratégie d'admissibilité d'application par défaut qui inclut tout le monde ;
- Configurez la liste des utilisateurs du groupe de mise à disposition pour autoriser les utilisateurs du siège social à utiliser toutes les applications spécifiées dans le groupe de mise à disposition.
- Configurez la liste des utilisateurs du groupe d'applications pour permettre aux membres du département Administration et Finances d'accéder aux applications A à L.
- Configurez les propriétés de l'application A pour limiter sa visibilité uniquement au personnel des comptes clients du département Administration et Finances.

Applications

À savoir

- Par défaut, les applications que vous ajoutez sont placées dans un dossier nommé Applications. Vous pouvez spécifier un dossier différent. Si vous essayez d'ajouter une application et qu'une application avec le même nom existe déjà dans ce dossier, vous êtes invité à renommer l'application que vous ajoutez. Si vous acceptez le nom unique suggéré, l'application est ajoutée avec ce nouveau nom ; sinon, vous devez la renommer vous-même avant de pouvoir l'ajouter. Pour de plus amples informations, consultez la section Gérer les dossiers d'applications.
- Vous pouvez modifier les propriétés d'une application (paramètres) lorsque vous l'ajoutez ou ultérieurement. Voir la section Modifier les propriétés de l'application. Si vous publiez deux applications du même nom vers les mêmes utilisateurs, modifiez la propriété Nom de l'application (pour l'utilisateur) dans Studio ; sinon, les utilisateurs verront des noms en double s'afficher dans Citrix Receiver.
- Lorsque vous ajoutez une application à plusieurs groupes d'applications, vous risquez de rencontrer un problème de visibilité si vous ne disposez pas d'autorisations suffisantes pour afficher l'application dans tous ces groupes. Dans ce cas, consultez un administrateur disposant

des autorisations appropriées ou demandez une extension de vos autorisations à tous les groupes auxquels l'application a été ajoutée.

Cliquez sur la liste déroulante **Ajouter** pour afficher les sources des applications.

- **À partir du menu Démarrer :** applications qui sont découvertes sur une machine dans les groupes de mise à disposition sélectionnés. Lorsque vous sélectionnez cette source, une nouvelle page se lance avec une liste des applications découvertes. Sélectionnez les cases des applications à ajouter, puis cliquez sur **OK**. Cette source ne peut pas être sélectionnée si vous avez (1) sélectionné des groupes d'applications qui ne sont associés à aucun groupe de mise à disposition, (2) sélectionné des groupes d'applications avec des groupes de mise à disposition associés qui ne contiennent aucune machine, ou (3) sélectionné un groupe de mise à disposition ne contenant aucune machine.
- **Manuellement définies :** applications qui se trouvent dans le site ou ailleurs dans votre réseau. Lorsque vous sélectionnez cette source, une nouvelle page s'affiche dans laquelle vous pouvez taper le chemin d'accès de l'exécutable, le répertoire de travail, les arguments de la ligne de commande (facultatifs), et les noms affichés des administrateurs et des utilisateurs. Après avoir entré ces informations, cliquez sur **OK**.
- **Existantes :** applications déjà ajoutées au site. Lorsque vous sélectionnez cette source, une nouvelle page se lance avec une liste des applications découvertes. Sélectionnez les cases à cocher des applications à ajouter, puis cliquez sur **OK**. Cette source ne peut pas être sélectionnée si le site ne dispose d'aucune application.
- **App-V :** applications dans des packages App-V. Lorsque vous sélectionnez cette source, une nouvelle page s'affiche dans laquelle vous pouvez sélectionner le serveur App-V ou la bibliothèque d'applications. À partir de l'écran qui s'affiche, sélectionnez les cases à cocher des applications à ajouter, puis cliquez sur **OK**. Pour obtenir davantage d'informations, veuillez consulter la section App-V. Cette source ne peut pas être sélectionnée (ou peut ne pas s'afficher) lorsque App-V n'est pas configuré pour le site.

Comme indiqué, certaines sources dans la liste déroulante **Ajouter** ne peuvent pas être sélectionnées s'il n'existe source valide de ce type. Les sources qui ne sont pas compatibles ne sont pas répertoriées (par exemple, vous ne pouvez pas ajouter de groupe d'applications à des groupes d'applications), par conséquent la source n'est pas répertoriée lorsque vous créez un groupe d'applications.

Étendues

Cette page s'affiche uniquement si vous avez déjà créé une étendue. Par défaut, l'étendue Tous est sélectionnée. Pour plus d'informations, veuillez consulter la section Administration déléguée.

Synthèse

Entrez un nom pour le groupe d'applications. Vous pouvez également entrer une description (facultatif).

Consultez les informations récapitulatives, puis cliquez sur **Terminer**.

Gérer des groupes d'applications

January 23, 2019

Introduction

Cet article décrit comment gérer les groupes d'applications que vous avez créés.

Consultez Applications pour savoir comment gérer les applications de groupes d'applications ou de groupes de mise à disposition, notamment comment :

- Ajouter ou supprimer des applications d'un groupe d'applications.
- Modifier les associations de groupes d'applications.

La gestion des groupes d'applications nécessite les autorisations d'administration déléguée du rôle intégré d'administrateur de groupe de mise à disposition. Consultez Administration déléguée pour plus de détails.

Activer ou désactiver un groupe d'applications

Lorsqu'un groupe d'applications est activé, il peut mettre à disposition les applications qui lui ont été ajoutées. La désactivation d'un groupe d'applications désactive chaque application dans ce groupe. Cependant, si ces applications sont également associées à d'autres groupes d'applications activés, elles peuvent être mises à disposition à partir de ces groupes. De même, si l'application a été expressément ajoutée à des groupes de mise à disposition associés au groupe d'applications (en plus d'être ajoutée au groupe d'applications), la désactivation du groupe d'applications n'affecte pas les applications dans ces groupes de mise à disposition.

Un groupe d'applications est activé lorsque vous le créez ; vous ne pouvez pas changer ce paramètre lors de la création du groupe.

1. Sélectionnez **Applications** dans le volet de navigation de Studio.
2. Sélectionnez un groupe d'applications dans le volet central, puis sélectionnez **Modifier groupe d'applications** dans le volet Actions.

3. Sur la page **Paramètres**, sélectionnez ou désélectionnez la case à cocher **Activer groupe d'applications**.
4. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Activer ou désactiver le partage de session d'application entre des groupes d'applications

Le partage de session entre des groupes d'applications est activé lorsque vous créez un groupe d'applications ; vous ne pouvez pas changer ce paramètre lors de la création du groupe. Pour de plus amples informations sur le partage de session d'application, consultez la section Partage de session entre des groupes d'applications.

1. Sélectionnez **Applications** dans le volet de navigation de Studio.
2. Sélectionnez un groupe d'applications dans le volet central, puis sélectionnez **Modifier groupe d'applications** dans le volet Actions.
3. Sur la page **Paramètres**, sélectionnez ou désélectionnez la case à cocher **Activer le partage de session d'application entre les groupes d'applications**.
4. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Désactiver le partage de session d'application dans un groupe d'applications

Le partage de session entre applications dans le même groupe d'applications est activé par défaut lorsque vous créez un groupe d'applications. Si vous désactivez le partage de session d'application entre groupes d'applications, le partage de session entre applications dans le même groupe d'applications reste activé. Vous pouvez utiliser le SDK PowerShell Broker pour configurer des groupes d'applications avec le partage de session d'application désactivé entre les applications qu'ils contiennent. Dans certaines circonstances, cela peut être préférable : par exemple, vous pouvez souhaiter que les utilisateurs lancent des applications non transparentes dans des fenêtres d'application plein écran utilisent sur des écrans distincts. Pour de plus amples informations sur le partage de session d'application, consultez la section Partage de session avec des groupes d'applications.

Lorsque vous désactivez le partage de session d'application dans un groupe d'applications, chaque application dans ce groupe se lance dans une nouvelle session d'application. Si une session déconnectée appropriée exécutant la même application est disponible, elle est reconnectée. Par exemple, si vous démarrez Bloc-notes et qu'il existe une session déconnectée exécutant Bloc-notes, cette session est reconnectée au lieu d'en créer une nouvelle. Si plusieurs sessions déconnectées appropriées sont disponibles, l'une des sessions est sélectionnée de manière aléatoire pour la

reconnexion : si cette situation se reproduit dans les mêmes circonstances, la même session est choisie, mais la session n'est pas toujours prévisible.
Vous pouvez utiliser le KSDK PowerShell Broker pour désactiver le partage de session d'application pour toutes les applications d'un groupe d'applications existant, ou pour créer un groupe d'applications avec le partage de session d'application désactivé.

Exemples d'applets de commande PowerShell

Pour désactiver le partage de session, utilisez les applets de commande PowerShell du Broker **New-BrokerApplicationGroup** ou **Set-BrokerApplicationGroup** avec le paramètre **-SessionSharingEnabled** défini sur False et le paramètre **-SingleAppPerSession** défini sur True.

Par exemple pour créer un groupe d'applications avec le partage de session d'application désactivé pour toutes les applications dans le groupe :

```
New-BrokerApplicationGroup AppGr1 -SessionSharingEnabled $False -SingleAppPerSession
 $True
```

Par exemple pour désactiver le partage de session d'application entre toutes les applications d'un groupe d'applications existant :

```
Set-BrokerApplicationGroup AppGR1 -SessionSharingEnabled $False -SingleAppPerSession
 $True
```

> **Remarques :**
>
> - Pour activer la propriété SingleAppPerSession, vous devez définir la propriété SessionSharingEnabled sur False. Les deux propriétés ne doivent pas être activées en même temps. Le paramètre SessionSharingEnabled fait référence au partage de sessions entre groupes d'applications.
> - Le partage de session d'application ne fonctionne que pour les applications qui sont associées à des groupes d'applications, mais qui ne sont pas associées à des groupes de mise à disposition. (Toutes les applications associées directement à un groupe de mise à disposition partagent les sessions par défaut.)
> - Si une application est attribuée à plusieurs groupes d'applications, assurez-vous que les groupes ne présentent aucun paramètre conflictuel (par exemple, l'option définie sur True sur l'un et sur False sur l'autre), ce qui entraîne un comportement imprévisible.

Renommer un groupe d'applications

1. Sélectionnez **Applications** dans le volet de navigation de Studio.
2. Sélectionnez un groupe d'applications dans le volet central, puis sélectionnez **Renommer groupe d'applications** dans le volet Actions.

3. Spécifiez le nouveau nom unique puis cliquez sur **OK**.

Ajouter, supprimer ou modifier la priorité d'associations de groupe de mise à disposition avec un groupe d'applications

Un groupe d'applications peut être associé à des groupes de mise à disposition contenant des machines partagées (non privées) qui peuvent mettre à disposition des applications.

Vous pouvez également sélectionner des groupes de mise à disposition contenant des machines partagées qui mettent uniquement à disposition des bureaux, si (1) le groupe de mise à disposition contient des machines partagées et a été créé avec une version antérieure de XenDesktop 7.x, et (2) vous disposez de l'autorisation Modifier le groupe de mise à disposition. Le type de groupe de mise à disposition est automatiquement converti en « bureaux et applications » lorsque la boîte de dialogue Modifier groupe d'applications est validée.

1. Sélectionnez **Applications** dans le volet de navigation de Studio.
2. Sélectionnez un groupe d'applications dans le volet central, puis sélectionnez **Modifier groupe d'applications** dans le volet Actions.
3. Sélectionnez la page **Groupes de mise à disposition**.
4. Pour ajouter des groupes de mise à disposition, cliquez sur **Ajouter**. Sélectionnez les cases à cocher des groupes de mise à disposition disponibles. (Les groupes de mise à disposition non compatibles ne peuvent pas être sélectionnés). Lorsque vous avez terminé vos sélections, cliquez sur **OK**.
5. Pour supprimer des groupes de mise à disposition, cochez les cases des groupes que vous souhaitez supprimer, puis cliquez sur **Supprimer**. Confirmez la suppression lorsque vous y êtes invité.
6. Pour modifier la priorité des groupes de mise à disposition, cochez la case du groupe de mise à disposition, puis cliquez sur **Modifier la priorité**. Entrez la priorité (0 = priorité la plus élevée), puis cliquez sur **OK**.
7. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Ajouter, modifier ou supprimer une restriction de balise dans un groupe d'applications

Important : l'ajout, la modification et la suppression de restrictions de balise peut avoir des effets inattendus sur les machines qui sont prises en compte pour le démarrage de l'application. Consultez les informations et précautions dans l'article Balises.

1. Sélectionnez **Applications** dans le volet de navigation de Studio.
2. Sélectionnez un groupe d'applications dans le volet central, puis sélectionnez **Modifier groupe d'applications** dans le volet Actions.

3. Sélectionnez la page **Groupes de mise à disposition**.
4. Pour ajouter une restriction de balise, sélectionnez **Restreindre les lancements aux machines dotées de balises** puis sélectionnez la balise dans la liste déroulante.
5. Pour modifier ou supprimer une restriction de balise, sélectionnez une autre balise à partir de la liste déroulante ou supprimez la restriction de balise complètement en désactivant le paramètre **Restreindre les lancements aux machines dotées de balises**.
6. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Ajouter ou supprimer des utilisateurs d'un groupe d'applications

Pour de plus amples informations sur les utilisateurs, consultez la section *Utilisateurs* dans l'article Créer des groupes de mise à disposition.

1. Sélectionnez **Applications** dans le volet de navigation de Studio.
2. Sélectionnez un groupe d'applications dans le volet central, puis sélectionnez **Modifier groupe d'applications** dans le volet Actions.
3. Sélectionnez la page **Utilisateurs**. Indiquez si vous souhaitez autoriser tous les utilisateurs dans les groupes de mise à disposition associés à utiliser les applications du groupe d'applications, ou uniquement des utilisateurs et groupes spécifiques. Pour ajouter des utilisateurs, cliquez sur **Ajouter**, puis spécifiez les utilisateurs que vous souhaitez ajouter. Pour supprimer des utilisateurs, sélectionnez un ou plusieurs utilisateurs, puis cliquez sur **Supprimer**.
4. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Modifier les étendues dans un groupe d'applications

Vous pouvez modifier une étendue uniquement si vous avez créé une étendue (vous ne pouvez pas modifier l'étendue Tout). Pour plus d'informations, veuillez consulter l'article Administration déléguée.

1. Sélectionnez **Applications** dans le volet de navigation de Studio.
2. Sélectionnez un groupe d'applications dans le volet central, puis sélectionnez **Modifier groupe d'applications** dans le volet Actions.
3. Sélectionnez la page **Portées**. Cochez ou décochez la case à cocher en regard d'une étendue.
4. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Supprimer un groupe d'applications

Une application doit être associée à au moins un groupe de mise à disposition ou groupe d'applications. Si votre tentative de suppression d'un groupe d'applications a pour conséquence qu'une ou plusieurs applications n'appartiennent plus à un groupe, vous serez averti que la suppression de ce groupe supprimera également ces applications. Vous pouvez ensuite confirmer ou annuler la suppression.

La suppression d'une application ne la supprime pas de sa source d'origine, mais si vous souhaitez de nouveau la rendre disponible, vous devez l'ajouter à nouveau.

1. Sélectionnez **Applications** dans le volet de navigation de Studio.
2. Sélectionnez un groupe d'applications dans le volet central, puis sélectionnez **Supprimer le groupe** dans le volet Actions.
3. Confirmez la suppression lorsque vous y êtes invité.

Remote PC Access

January 23, 2019

Remote PC Access permet à un utilisateur final d'ouvrir une session à distance pratiquement depuis n'importe quel emplacement sur le PC Windows physique au bureau.

Virtual Delivery Agent (VDA) est installé sur le PC de bureau ; il s'enregistre auprès du Cloud Connector ou Delivery Controller et permet de gérer la connexion HDX entre le PC et les machines clientes de l'utilisateur final. Remote PC Access prend en charge un modèle en libre-service, après avoir configuré la liste blanche des machines auxquelles les utilisateurs sont autorisés à accéder, les utilisateurs peuvent joindre leurs PC de bureau d'eux-mêmes, sans l'intervention de l'administrateur. Le Citrix Receiver exécuté sur leur machine cliente permet d'accéder aux applications et données sur le PC de bureau à partir de la session de bureau Remote PC Access.

Il se peut qu'un utilisateur possède plusieurs bureaux, y compris plus d'un PC physique ou une combinaison de PC physiques et de bureaux virtuels.

Les modes Veille et Veille prolongée ne sont pas pris en charge pour Remote PC Access.

> **Remarque :**
>
> Pour les déploiements sur site : Remote PC Access est uniquement valide pour les licences XenDesktop. Les sessions consomment des licences de la même manière que les autres sessions XenDesktop.

Considérations relatives à Active Directory

Avant de configurer le site de déploiement de Remote PC Access, configurez vos unités d'organisation (OU) et groupes de sécurité puis créez des comptes d'utilisateur.

Si vous modifiez Active Directory après l'ajout d'une machine à un catalogue de machines, Remote PC Access ne réévalue pas cette affectation. Vous pouvez réaffecter manuellement une machine à un autre catalogue, si nécessaire.

Si vous déplacez ou supprimez des unités d'organisation, celles utilisées pour Remote PC Access peuvent devenir obsolètes. VDA risque de ne plus être associé avec le catalogue de machines ou le groupe de mise à disposition le plus approprié (le cas échéant).

Considérations de catalogue de machines et groupes de mise à disposition

- Une machine peut uniquement être attribuée à un catalogue de machines et un groupe de mise à disposition à la fois.
- Vous pouvez placer les machines dans un ou plusieurs des catalogues de machines Remote PC Access.
- Lors du choix des comptes de machines pour un catalogue, sélectionnez la plus basse unité d'organisation (OU) applicable afin d'éviter des conflits potentiels avec des machines d'un autre catalogue de machines. Par exemple, dans le cas d'employés de banque, sélectionnez Guichets.
- Vous pouvez affecter toutes les machines d'un catalogue de machines Remote PC Access via un ou plusieurs groupes de mise à disposition. Si vous disposez d'un groupe d'utilisateurs qui nécessite certains paramètres de stratégie et d'un autre groupe d'utilisateurs qui requiert des paramètres différents, l'attribution d'utilisateurs à différents groupes de mise à disposition vous permet de filtrer les stratégies HDX en fonction de chaque groupe de mise à disposition.
- Si votre infrastructure informatique attribue une responsabilité pour traiter les utilisateurs en fonction de leur emplacement géographique, département, ou une autre catégorie, vous pouvez grouper les machines et les utilisateurs en conséquence afin de permettre l'administration déléguée. Assurez-vous que chaque administrateur dispose des permissions nécessaires pour les catalogues et les groupes de mise à disposition correspondants.

Considérations de déploiement

- Vous pouvez créer un déploiement Remote PC Access, puis ajouter des bureaux ou applications VDI (Virtual Desktop Infrastructure) traditionnelles ultérieurement. Vous pouvez également ajouter des bureaux Remote PC Access à un déploiement VDI existant.
- Considérez l'activation de la fonction Assistance à distance de Windows lorsque vous installez le VDA sur le PC de bureau. Cette option permet aux équipes d'assistance utilisant Director d'afficher une session utilisateur et d'interagir avec elle via l'Assistance à distance Windows.

- Déterminez la manière dont vous souhaitez déployer le VDA sur chaque PC de bureau. Citrix vous recommande d'utiliser la distribution électronique de logiciels telle que des scripts Active Directory et Microsoft System Center Configuration Manager. Le support d'installation contient des exemples de scripts Active Directory.
- Consultez les considérations de sécurité pour les déploiements Remote PC Access.
- Le démarrage sécurisé pour Remote PC Access est pris en charge sur Windows 10.
- Chaque PC de bureau doit être membre d'un domaine avec une connexion réseau câblée.
- Windows 7 Aero est pris en charge sur le PC de bureau, mais n'est pas obligatoire.
- Connectez le clavier et la souris directement sur l'ordinateur ou sur un ordinateur portable, mais pas sur le moniteur ou autres composants qui peuvent être éteints. Si vous devez connecter des périphériques d'entrée pour les composants tels que les moniteurs, ils ne doivent pas être éteints.
- Si vous utilisez des cartes à puce, consultez la section Cartes à puce.
- Remote PC Access peut être utilisé sur la plupart des ordinateurs portables. Pour améliorer l'accessibilité et offrir la meilleure expérience de connexion possible, configurez les options d'économie d'énergie de l'ordinateur portable sur celles d'un PC de bureau. Par exemple :
  - Désactivez la fonctionnalité Veille prolongée. Le mode Veille prolongée n'est pas pris en charge pour Remote PC Access.
  - Désactivez la fonctionnalité Veille. Le mode Veille n'est pas pris en charge pour Remote PC Access.
  - Définissez l'action de fermeture de l'écran sur Ne rien faire.
  - Définissez l'action d'appuyer sur le bouton d'alimentation sur Arrêter.
  - Désactivez les fonctionnalités d'économie d'énergie de la carte vidéo.
  - Désactivez les fonctionnalités d'économie d'énergie de la carte d'interface réseau.
  - Désactivez les technologies d'économie de la batterie.
- Les éléments suivants ne sont pas pris en charge pour les machines Remote PC Access :
  - Ancrage et retrait de l'ordinateur portable.
  - Commutateurs KVM ou autres composants qui peuvent déconnecter une session.
  - PC hybride, y compris PC et ordinateurs portables tout en un et NVIDIA Optimus.
- Citrix prend en charge Remote PC Access sur les Surface Pro avec Windows 10. Pour améliorer l'accessibilité et offrir la meilleure expérience de connexion possible, configurez la machine Surface de manière similaire à un ordinateur portable ou de bureau. Par exemple :
  - Désactiver la fonctionnalité de mise en veille ou veille prolongée
  - Utiliser une connexion réseau filaire
  - Toujours garder le clavier attaché lors de l'initiation ou de la reconnexion à une session
  - Désactiver les technologies d'économie de la batterie
- Installez Citrix Receiver sur chaque machine cliente qui accède au PC de bureau à distance.
- Plusieurs utilisateurs avec l'accès distant au même PC de bureau voient la même icône dans Citrix Receiver. Lorsqu'un utilisateur ouvre une session à distance sur le PC, cette ressource est

marquée comme non disponible pour d'autres utilisateurs.

Par défaut, une session d'utilisateur distant est automatiquement déconnectée lorsqu'un utilisateur local initie une session sur cette machine (en appuyant sur CTRL+ALT+Suppr). Pour éviter cette action automatique, ajoutez l'entrée de registre suivante sur le PC de bureau, puis redémarrez la machine.

Avertissement : toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

HKLM\SOFTWARE\Citrix\PortICA\RemotePC "SasNotification"=dword:00000001

Pour personnaliser le comportement de cette fonctionnalité sous HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortIC
PC

RpcaMode (dword) :

- 1 = L'utilisateur distant aura toujours priorité s'il ne répond pas à l'interface utilisateur de messagerie dans le délai imparti.
- 2 = L'utilisateur local aura toujours priorité. Si ce paramètre n'est pas spécifié, l'utilisateur distant aura toujours priorité par défaut.

RpcaTimeout (dword) :

- Nombre de secondes accordées à l'utilisateur avant que le type de mode à appliquer soit déterminé. Si ce paramètre n'est pas spécifié, la valeur par défaut est 30 secondes. La valeur minimale doit être 30 secondes. L'utilisateur doit redémarrer la machine pour que ces modifications soient appliquées.

Lorsque l'utilisateur souhaite forcer l'accès à la console : l'utilisateur local peut appuyer sur Ctr+Alt+Suppr à deux reprises à intervalle de 10 secondes pour obtenir le contrôle local d'une session distante et forcer une déconnexion.

Une fois le Registre modifié et la machine redémarrée, si un utilisateur local appuie sur CTRL+ALT+Suppr pour ouvrir une session sur ce PC lorsqu'il est en cours d'utilisation par un utilisateur distant, cet utilisateur reçoit une invite lui demandant s'il souhaite ou non autoriser ou refuser la connexion de l'utilisateur local. L'action d'autorisation de la connexion déconnectera la session de l'utilisateur distant.

Remote PC Access et mode HDX 3D Pro

Pour Remote PC Access, le VDA est généralement configuré à l'aide de l'option VDA standard. Lorsque Remote PC Access est configuré avec HDX 3D Pro, l'occultation de moniteur est prise en charge avec

Intel Iris Pro Graphics et Intel HD Graphics 5300 et supérieur (Processeurs Intel Core 5ème Génération et Processeurs Intel Core i5 6ème Génération), et NVIDIA Quadro et NVIDIA GRID

Pour de plus amples informations, consultez la section Accélération GPU pour OS de bureau Windows.

Wake on LAN

Wake on LAN n'est pas pris en charge avec Remote PC Access dans Citrix Cloud.

Remote PC Access prend en charge Wake on LAN, qui donne aux utilisateurs la possibilité d'activer des ordinateurs physiques à distance. Cette fonctionnalité permet aux utilisateurs de garder leur PC de bureau éteint lorsqu'il n'est pas en cours d'utilisation, et d'économiser de l'énergie. Il offre également un accès distant quand une machine a été éteinte par inadvertance, tel que lors d'événements météo.

La fonctionnalité Remote PC Access Wake on LAN est prise en charge sur :

- PC sur lesquels l'option Wake on LAN est activée dans le BIOS. Cette prise en charge inclut le proxy de mise en éveil et les paquets magiques bruts, lors de l'utilisation de Microsoft System Center Configuration Manager (ConfigMgr) 2012, ConfigMgr 2012 R2 et ConfigMgr 2016.
- PC qui prennent en charge la technologie AMT (Intel Active Management). Sur les machines compatibles AMT, la fonctionnalité Wake on LAN prend également en charge les actions Forcer l'arrêt et Forcer le redémarrage dans Studio et Director. En outre, une action de redémarrage est disponible dans StoreFront et Citrix Receiver. **IMPORTANT :** la prise en charge AMT est disponible uniquement lors de l'utilisation de ConfigMgr 2012 ou de 2012 R2, mais pas de ConfigMgr 2016.

Configurez ConfigMgr pour utiliser la fonctionnalité Wake on LAN. Ensuite, lorsque vous utilisez Studio pour créer un déploiement Remote PC Access (ou lorsque vous ajoutez une autre connexion de gestion de l'alimentation à utiliser pour Remote PC Access), vous activez la fonction de gestion de l'alimentation et spécifiez des informations d'accès ConfigMgr.

Pour plus de détails sur la configuration, consultez la section Configuration Manager et Remote PC Access Wake on LAN.

Configuration Manager et Remote PC Access Wake on LAN

Pour configurer la fonctionnalité Remote PC Access Wake on LAN, procédez comme suit avant d'installer un VDA sur le PC de bureau.

- Configurez ConfigMgr 2012, 2012 R2 ou 2016 au sein de l'organisation. Déployez ensuite le client ConfigMgr sur toutes les machines Remote PC Access, tout en allouant un délai suffisant pour l'exécution du cycle d'inventaire SCCM programmé (ou en forcer un manuellement, si nécessaire). Les informations d'identification d'accès que vous avez spécifiées dans Studio

pour configurer la connexion à ConfigMgr doivent inclure des collections dans l'étendue et le rôle d'opérateur des outils à distance.

- Pour activer la prise en charge d'Intel Active Management Technology (AMT) :
  - La version minimale prise en charge sur le PC doit être AMT 3.2.1.
  - Configurez le PC pour l'utilisation d'AMT avec des certificats et des processus de provisioning associés.
  - Seuls ConfigMgr 2012 et 2012 R2 peuvent être utilisés, et non ConfigMgr 2016.
- Pour ConfigMgr Wake Proxy et/ou la prise en charge de paquet magique :
  - Configurez Wake on LAN dans chacun des paramètres BIOS du PC.
  - Pour la prise en charge de Wake Proxy, activez l'option dans ConfigMgr. Pour chaque sous-réseau de l'organisation contenant les PC qui utiliseront la fonctionnalité Remote PC Access Wake on LAN, vérifiez que trois machines ou plus peuvent servir de machines sentinelles.
  - Pour une prise en charge de paquet magique, configurez des routeurs réseau et des pare-feu pour autoriser l'envoi des paquets magiques, en utilisant soit une diffusion dirigée vers un sous-réseau, soit une monodiffusion.

Une fois que vous avez installé le VDA sur les PC de bureau, activez ou désactivez la gestion de l'alimentation lorsque vous créez la connexion et le catalogue de machines.

- Si vous activez la gestion de l'alimentation dans le catalogue, spécifiez les détails de connexion : l'adresse ConfigMgr et les informations d'identification d'accès et un nom.
- Si vous n'activez pas la gestion de l'alimentation, vous pouvez ajouter une connexion de gestion de l'alimentation (Configuration Manager) ultérieurement, puis modifier un catalogue de machines Remote PC Access pour activer la gestion de l'alimentation et spécifier la nouvelle connexion de gestion de l'alimentation.

Vous pouvez modifier une connexion de gestion de l'alimentation pour configurer les paramètres avancés. Vous pouvez activer :

- le proxy de mise en éveil mis à disposition par ConfigMgr ;
- les paquets Wake on LAN (magiques). Si vous activez les paquets Wake on LAN, vous pouvez sélectionner une méthode de transmission Wake on LAN : émissions ou monodiffusions dirigées par des sous-réseaux.

Le PC utilise des commandes de mise sous tension AMT (si prises en charge), ainsi que tout paramètre avancé activé. Si le PC n'utilise pas de commandes de mise sous tension AMT, il utilise les paramètres avancés.

Déploiements Citrix Cloud : séquence de configuration et considérations

Consultez la section CTX220737 : Comment activer XenDesktop Remote PC Access dans Citrix Cloud.

Déploiements sur site : séquence de configuration et considérations

Avant de créer le site Remote PC Access

Si vous prévoyez d'utiliser la fonctionnalité de gestion de l'alimentation Remote PC Access (également appelée Remote PC Access Wake on LAN), effectuez les tâches de configuration sur les PC et sur Microsoft System Center Configuration Manager (ConfigMgr) 2012 avant de créer le déploiement Remote PC Access dans Studio. Consultez la section Configuration Manager et Remote PC Access Wake on LAN.

Dans l'Assistant de création de site

- Sélectionnez le type de site Remote PC Access.
- Sur la page **Gestion de l'alimentation**, vous pouvez activer ou désactiver la gestion de l'alimentation pour les machines dans le catalogue de machines Remote PC Access par défaut. Si vous activez la gestion de l'alimentation, spécifiez les informations de connexion ConfigMgr.
- Sur les pages **Utilisateurs et Comptes de machines**, spécifiez les utilisateurs et les comptes de machines.

La création d'un site Remote PC Access crée un catalogue de machines appelé Machines Remote PC Access et un groupe de mise à disposition par défaut appelé Bureaux Remote PC Access.

Si vous créez un autre catalogue de machines pour une utilisation avec Remote PC Access

- Sur la page **Système d'exploitation**, sélectionnez Remote PC Access, puis choisissez une connexion de gestion de l'alimentation. Vous pouvez également choisir de ne pas utiliser la gestion de l'alimentation. S'il n'existe aucune connexion de gestion de l'alimentation configurée, vous pouvez en ajouter une à la fin de l'Assistant de création de catalogue de machines (type de connexion = Microsoft Configuration Manager Wake on LAN), puis modifiez le catalogue de machines, en spécifiant cette nouvelle connexion.
- Sur la page **Comptes de machines**, vous pouvez sélectionner les comptes de machines ou les unités d'organisation (UO) affichés, ou ajouter des comptes de machines et des unités d'organisation.

Installez le VDA sur les PC de bureau utilisés pour un accès local et distant. En général, vous pouvez déployer le VDA automatiquement à l'aide de votre logiciel de gestion de pack ; cependant, pour les déploiements d'évaluation ou de petite taille, vous pouvez installer le VDA manuellement sur chaque PC de bureau. Il existe plusieurs méthodes permettant d'installer un VDA de bureau pour un déploiement Remote PC Access.

Utiliser le programme d'installation du produit entier ou VDAWorkstationSetup.exe :

- Interface graphique : sélectionnez **Remote PC Access** sur la page **Environnement** de l'assistant. Les composants de la page **Composants supplémentaires** ne sont pas sélectionnés par défaut. Ils ne sont pas requis pour Remote PC Access.
- Interface de ligne de commande : spécifiez l'option /remotepc. Cette option empêche l'installation des composants suivants (qui sont les mêmes que les éléments sur la page **Composants supplémentaires** de l'assistant) : Éventuellement, vous pouvez utiliser l'option /exclude pour exclure chacun de ces composants.
  - App-V
  - Citrix User Profile Manager
  - Citrix User Profile Manager WMI Plugin
  - Machine Identity Service
  - Personal vDisk

Utiliser le programme d'installation VDAWorkstationCoreSetup.exe : ni Citrix Receiver ni composants supplémentaires ne peuvent être installés avec ce programme d'installation.

Une fois le VDA installé, le prochain utilisateur de domaine qui ouvre une session de console (localement ou via RDP) sur le PC de bureau est automatiquement affecté au bureau Remote PC Access. Si des utilisateurs de domaine supplémentaires se connectent à une session de console, ils sont également ajoutés à la liste des utilisateurs de bureau, en fonction des restrictions que vous avez configurés.

Pour utiliser des connexions RDP en dehors de votre environnement XenApp ou XenDesktop, vous devez ajouter des utilisateurs ou des groupes au groupe d'utilisateurs de l'accès direct.

Demandez aux utilisateurs de télécharger et d'installer Citrix Receiver sur chaque machine cliente qu'ils utiliseront pour accéder au PC de bureau à distance. Citrix Receiver est disponible depuis https://www.citrix.com ou depuis le système de distribution d'application pour appareils mobiles.

Résolution des problèmes

Les informations de diagnostic sur Remote PC Access sont écrites dans le Journal d'événements d'application Windows. Les messages d'informations ne sont pas optimisés. Les messages d'erreur sont optimisés en éliminant les messages en double.

- 3300 (informations) : machine ajoutée au catalogue
- 3301 (informations) : machine ajoutée au groupe de mise à disposition
- 3302 (informations) : machine attribuée à l'utilisateur
- 3303 (erreur) : exception

Pour les déploiements sur site uniquement : lorsque la gestion de l'alimentation est activée pour Remote PC Access, il se peut que des diffusions dirigées par des sous-réseaux ne parviennent pas

à démarrer des machines qui sont situées sur un sous-réseau différent du Controller. Si vous avez besoin de la gestion de l'alimentation sur les sous-réseaux utilisant des diffusions dirigées par des sous-réseaux et AMT n'est pas disponible, essayez la méthode du proxy de mise en éveil ou de monodiffusion (assurez-vous que ces paramètres sont activés dans les propriétés avancées de la connexion de gestion de l'alimentation).

App-V

February 28, 2019

Utilisation de App-V avec XenApp et XenDesktop

La Virtualisation d'application Microsoft (App-V) vous permet de déployer, mettre à jour et prendre en charge des applications en tant que services. Les utilisateurs accèdent aux applications sans les installer sur leur propre machine. App-V et Microsoft User State Virtualization (USV) fournissent l'accès aux applications et aux données, quel que soit l'emplacement et la connexion à Internet.

Le tableau suivant répertorie les versions prises en charge.

App-V	Versions XenDesktop et XenApp	
	Delivery Controller	**VDA**
5.0 et 5.0 SP1	XenDesktop 7 jusqu'à la version actuelle, XenApp 7.5 jusqu'à la version actuelle	7.0 jusqu'à la version actuelle
5.0 SP2	XenDesktop 7 jusqu'à la version actuelle, XenApp 7.5 jusqu'à la version actuelle	7.1 jusqu'à la version actuelle
5.0 SP3 et 5.1	XenDesktop 7.6 jusqu'à la version actuelle, XenApp 7.6 jusqu'à la version actuelle	7.6 300 jusqu'à la version actuelle
App-V dans Windows Server 2016	XenDesktop 7.12 jusqu'à la version actuelle, XenApp 7.12 jusqu'à la version actuelle	7.12 jusqu'à la version actuelle

Le client App-V ne prend pas en charge l'accès en mode déconnecté aux applications. La prise en charge de l'intégration App-V comprend l'utilisation de partages SMB pour les applications. Le proto-

cole HTTP n'est pas pris en charge.

Si vous n'êtes pas un utilisateur expérimenté de App-V, veuillez consulter la documentation Microsoft. Voici un récapitulatif des composants App-V mentionnés dans cet article :

- **Serveur de gestion**. Fournit une console centralisée de gestion de l'infrastructure App-V et met à disposition des applications virtuelles pour le client de bureau App-V ainsi qu'un client aux services Bureau à distance. Le serveur d'administration App-V authentifie, requiert et fournit la sécurité, les mesures, la surveillance et la collecte des données requis par l'administrateur. Le serveur utilise Active Directory et ses outils de soutien pour gérer les utilisateurs et les applications.
- **Serveur de publication**. Fournit des clients App-V avec des applications pour certains utilisateurs, et héberge le pack d'application virtuelle en vue du streaming. Il récupère les packs depuis le serveur d'administration.
- **Client**. Récupère des applications virtuelles, publie les applications sur le client et configure et gère automatiquement les environnements virtuels au moment de l'exécution sur les machines Windows. Vous installez le client App-V sur le VDA où il stocke les paramètres d'application virtuelle spécifiques à l'utilisateur, tels que le registre et les modifications apportées aux fichiers dans chaque profil utilisateur.

Les applications sont disponibles en toute transparence sans pré-configuration ou modifications apportées aux paramètres du système d'exploitation. Vous pouvez lancer les applications App-V à partir de machines avec OS de serveur et les groupes de mise à disposition avec OS de bureau :

- Via Citrix Receiver
- Depuis le menu Démarrer
- Via le client App-V et Citrix Receiver
- Simultanément par de multiples utilisateurs sur plusieurs machines
- Via Citrix StoreFront

Les propriétés de l'application App-V modifiées sont implémentées lorsque l'application est démarrée. Par exemple, pour les applications avec un nom d'affichage ou une icône personnalisée modifié(e), la modification s'affiche lorsque les utilisateurs démarrent l'application.

Méthodes de gestion

Vous pouvez utiliser des packages App-V créés avec App-V Sequencer puis placés sur des serveurs App-V ou des partages réseau.

- **Serveurs App-V :** l'utilisation d'applications depuis des packages situés sur des serveurs App-V requiert une communication constante entre Studio et les serveurs App-V pour la découverte, la configuration et le téléchargement vers les VDA. Cela entraîne des frais de matériel,

d'infrastructure et d'administration. Studio et les serveurs App-V doivent rester synchronisés, particulièrement pour les permissions utilisateur.

C'est ce que l'on appelle la méthode de gestion à *administrateur double*, car l'accès au package et à l'application App-V nécessite les consoles Studio et de serveur App-V. Cette méthode fonctionne mieux dans des déploiements App-V et Citrix étroitement liés.

- **Partage réseau :** avec les packages placés sur un partage réseau, Studio ne dépend plus de l'infrastructure serveur App-V et base de données, ce qui diminue les frais (vous devez quand même installer le client Microsoft App-V sur chaque VDA).

  C'est ce que l'on appelle la méthode de gestion à *un seul administrateur*, car l'utilisation du package et de l'application App-V nécessite uniquement la console Studio. Vous accédez au partage réseau et vous ajoutez un ou plusieurs packages App-V à partir de cet emplacement de la bibliothèque d'applications au niveau du site.

  La bibliothèque d'applications est un terme Citrix désignant un référentiel de mise en cache qui stocke des informations sur les packages App-V. La bibliothèque d'applications stocke également des informations sur les autres technologies de mise à disposition d'applications Citrix.

Vous pouvez utiliser une ou les deux méthodes de gestion simultanément. En d'autres termes, lorsque vous ajoutez des applications aux groupes de mise à disposition, les applications peuvent provenir de packages App-V situés sur des serveurs App-V et/ou sur un partage réseau.

Lorsque vous sélectionnez **Configuration > App-V Publishing** dans le panneau de navigation de Studio, l'écran affiche les noms et les sources des packages App-V. La colonne Source indique si les packages sont situés sur le serveur App-V ou mis en cache dans la bibliothèque d'applications. Lorsque vous sélectionnez un package, le panneau Détails répertorie les applications contenues dans le package.

Répartition de la charge des serveurs App-V

La répartition de la charge des serveurs de gestion et de publication à l'aide du DNS round-robin sont pris en charge si vous utilisez la méthode de gestion d'administration double. Lorsque la charge du serveur de gestion est répartie derrière Netscaler, l'adresse IP virtuelle de F5 (ou similaire) n'est pas prise en charge en raison de la manière dont Studio a besoin de communiquer avec le serveur de gestion via PowerShell à distance. Pour plus d'informations, consultez cet article sur le blog Citrix.

Groupes d'isolement

Lorsque vous utilisez la méthode administration unique App-V, la création de groupes d'isolement vous permet de spécifier des groupes d'applications interdépendants qui doivent être exécutés dans le sandbox. Cette fonctionnalité est similaire, mais pas identique, aux groupes de connexion App-V.

Au lieu des termes « facultatif » et « obligatoire » utilisés par le serveur de gestion App-V, Citrix utilise les termes « automatique » et « explicite » pour les options de déploiement des packages.

- Lorsqu'un utilisateur lance une application App-V (l'application principale), une recherche est effectuée dans les groupes d'isolement pour trouver d'autres packages d'applications qui sont marqués pour inclusion automatique. Ces packages sont téléchargés et inclus automatiquement dans le groupe d'isolement. Vous n'avez pas besoin de les ajouter au groupe de mise à disposition qui contient l'application principale.
- Un package d'applications présent dans le groupe d'isolement qui est marqué pour inclusion explicite est téléchargé uniquement si vous avez ajouté explicitement cette application au groupe de mise à disposition qui contient l'application principale.

Cela vous permet de créer des groupes d'isolement contenant un mélange d'applications incluses automatiquement et mises à disposition de tous les utilisateurs. De plus, le groupe peut contenir des plug-ins et autres applications (qui peuvent avoir des contraintes de licence spécifiques) que vous pouvez limiter à un ensemble d'utilisateurs (identifiés par les groupes de mise à disposition), sans avoir à créer des groupes d'isolement supplémentaires.

Par exemple, l'application « app-a » requiert JRE 1.7 pour s'exécuter. Vous pouvez créer un groupe d'isolement contenant app-a (avec un type de déploiement explicite) et JRE 1.7 (avec un type de déploiement automatique). Ensuite, ajoutez ces packages App-V à un ou plusieurs groupes de mise à disposition. Lorsqu'un utilisateur démarre l'application app-a, JRE 1.7 est automatiquement déployé.

Vous pouvez ajouter une application à plusieurs groupes d'isolement App-V. Cependant, lorsqu'un utilisateur lance l'application, le premier groupe d'isolement pour lequel cette application a été ajoutée est toujours utilisé. Vous ne pouvez pas définir d'ordre ou de priorité pour les autres groupes d'isolement contenant cette application.

Installation

Le tableau suivant décrit la séquence de tâches de configuration permettant d'utiliser App-V dans XenApp et XenDesktop.

Administration unique	Administration double	Tâche
X	X	Déployer App-V
X	X	Création de packages et placement
	X	Configurer des adresses de serveurs App-V dans Studio
X	X	Installer le logiciel sur des machines VDA

Administration unique	Administration double	Tâche
X		Ajouter des packages App-V à la bibliothèque d'applications
X		Ajouter des groupes d'isolement App-V (facultatif)
X	X	Ajouter des applications App-V à des groupes de mise à disposition

Déployer Microsoft App-V

Pour les instructions de déploiement App-V, voir https://technet.microsoft.com/en-us/windows/hh826068.

Si vous le souhaitez, vous pouvez modifier les paramètres de serveur de publication App-V. Citrix vous recommande d'utiliser les applets de commande du SDK sur le Controller. Pour de plus amples informations, consultez la documentation du SDK.

- Pour afficher les paramètres du serveur de publication, entrez **Get-CtxAppvServerSetting -AppVPublishingServer <*ServeurPub*>**.
- Pour vous assurer que les applications App-V se lancent correctement, entrez **Set-CtxAppvServerSetting -UserRefreshonLogon 0**.

Si vous avez préalablement utilisé des paramètres d'objet de stratégie de groupe pour gérer les paramètres du serveur de publication, ces paramètres remplacent les paramètres d'intégration App-V, y compris les paramètres de l'applet de commande. Cela peut entraîner l'échec de lancement de l'application App-V. Citrix vous recommande de supprimer tous les paramètres de stratégie d'objet de stratégie de groupe, puis d'utiliser le kit de développement pour configurer ces paramètres.

Création de packages et placement

Quelle que soit la méthode de gestion, créez les packages d'applications à l'aide de App-V Sequencer. Reportez-vous à la documentation Microsoft pour plus d'informations.

- Dans le cas d'une administration unique, assurez-vous que les packages sont disponibles sur un emplacement réseau partagé UNC ou SMB. Assurez-vous que l'administrateur Studio qui ajoute des applications aux groupes de mise à disposition possède au moins un accès en lecture à cet emplacement.
- En cas de double administration, publiez les packages sur le serveur de gestion App-V depuis un chemin d'accès UNC. (La publication à partir d'URL HTTP n'est pas prise en charge.)

Que les packages se trouvent sur le serveur App-V ou sur un partage réseau, assurez-vous qu'ils possèdent les autorisations de sécurité appropriées pour permettre à l'administrateur Studio d'y accéder. Les partages réseau doivent être partagés avec « Utilisateurs authentifiés » pour garantir que le VDA et Studio ont accès en lecture par défaut.

Configurer des adresses de serveurs App-V dans Studio

> **Important :**
>
> Citrix recommande d'utiliser des applets de commande PowerShell sur le Controller pour spécifier les adresses de serveur App-V si ces serveurs utilisent des valeurs de propriété autres que celles par défaut. Pour de plus amples informations, consultez la documentation du SDK. Si vous modifiez des adresses de serveur App-V dans Studio, certaines propriétés des connexions de serveur que vous spécifiez peuvent revenir à leurs valeurs par défaut. Ces propriétés sont utilisées sur les VDA pour se connecter aux serveurs de publication App-V. Dans ce cas, vous devez reconfigurer les valeurs autres que celles par défaut pour toutes les propriétés réinitialisées sur les serveurs.

Cette procédure est valide uniquement pour la méthode de gestion « double administration ».

Spécifiez les adresses des serveurs de gestion et de publication App-V pour la double administration pendant ou après la création du site. Vous pouvez effectuer cette opération pendant ou après la création du site.

Lors de la création du site :

- Sur la page **App-V** de l'assistant, entrez l'URL du serveur de gestion Microsoft App-V ainsi que l'URL et le numéro de port du serveur de publication App-V. Testez la connexion avant de continuer avec l'assistant. Si le test échoue, veuillez consulter la section Dépannage ci-dessous.

Après la création du site :

1. Sélectionnez **Configuration > App-V Publishing** dans le panneau de navigation de Studio.
2. Si vous n'avez pas spécifié d'adresses de serveur App-V, sélectionnez **Ajouter Microsoft Server** dans le volet Actions.
3. Pour modifier des adresses de serveur App-V, sélectionnez **Modifier Microsoft Server** dans le volet Actions.
4. Entrez l'URL du serveur de gestion Microsoft App-V ainsi que l'URL et le numéro de port du serveur de publication App-V.
5. Testez la connexion à ces serveurs avant de fermer la boîte de dialogue. Si le test échoue, veuillez consulter la section Dépannage ci-dessous.

Par la suite, si vous souhaitez supprimer tous les liens vers les serveurs de gestion et de publication App-V et empêcher Studio de découvrir les packages App-V de ces serveurs, sélectionnez **Supprimer**

Microsoft Server dans le volet Actions. Cette action est autorisée uniquement si aucune des applications des packages situés sur ces serveurs n'est actuellement publiée dans des groupes de mise à disposition. Si c'est le cas, vous devez supprimer ces applications des groupes de mise à disposition avant de pouvoir supprimer les serveurs App-V.

Installer le logiciel sur des machines VDA

Les machines contenant des VDA doivent disposer de deux ensembles de logiciels pour prendre en charge App-V : un ensemble fourni par Microsoft et l'autre par Citrix.

Client Microsoft App-V

Ce logiciel récupère des applications virtuelles, publie les applications sur le client et configure et gère automatiquement les environnements virtuels au moment de l'exécution sur les machines Windows. Le client App-V stocke les paramètres d'application virtuelle spécifiques à l'utilisateur, tels que le registre et les modifications apportées aux fichiers dans chaque profil utilisateur.

Le client App-V est disponible auprès de Microsoft. Installez un client sur chaque machine contenant un VDA, ou sur l'image principale qui est utilisée dans un catalogue de machines pour créer des VM. **Remarque :** Windows 10 (1607 ou version supérieure) et Windows Server 2016 comprennent déjà le client App-V. Sur ces systèmes d'exploitation uniquement, activez le client App-V en exécutant l'applet de commande PowerShell **Enable-AppV** (sans paramètres). L'applet de commande **Get-AppVStatus** récupère l'état actuel d'activation.

Conseil : après avoir installé le client App-V, avec des autorisations d'administrateur, exécutez l'applet de commande PowerShell **Get-AppvClientConfiguration** et assurez-vous que EnablePackageScripts est défini sur 1. S'il n'est pas défini sur 1, exécutez **Set-AppvClientConfiguration -EnablePackageScripts $true**.

Composants Citrix App-V

Le composant logiciel Citrix App-V est installé et activé par défaut lorsque vous installez un VDA.

Vous pouvez définir cette action par défaut lors de l'installation du VDA. Dans l'interface graphique, désactivez la case à cocher **Citrix Personalization pour App-V** : VDA sur la page **Composants supplémentaires**. Dans l'interface de ligne de commande, incluez l'option **/exclude "Citrix Personalization for App-V - VDA"**.

Si vous désactivez l'installation des composants Citrix App-V lors de l'installation de VDA, mais souhaitez utiliser les applications App-V ultérieurement : dans la liste Programmes et fonctionnalités de la machine Windows, cliquez avec le bouton droit sur l'entrée **Citrix Virtual Delivery Agent**, puis sélectionnez **Modifier**. Un assistant démarre. Dans l'assistant, activez l'option qui installe et active les composants de publication App-V.

Ajouter ou supprimer des packages App-V dans la bibliothèque d'applications

Ces procédures sont valides uniquement pour la méthode de gestion « administration unique ».

Vous devez disposer d'au moins un accès en lecture pour le partage réseau contenant les packages App-V.

Ajouter un package App-V à la bibliothèque d'applications

1. Sélectionnez **Configuration > App-V Publishing** dans le panneau de navigation de Studio.
2. Sélectionnez **Ajouter des packages** dans le volet Actions.
3. Recherchez le partage contenant les packages App-V et sélectionnez un ou plusieurs packages.
4. Cliquez sur **Ajouter**.

Supprimer un package App-V de la bibliothèque d'applications

La suppression d'un package App-V de la bibliothèque d'applications le supprime de l'affichage du nœud Studio App-V Publishing. Toutefois, cela ne supprime pas ses applications des groupes de mise à disposition et ces applications peuvent toujours être lancées. Le package reste dans son emplacement réseau physique (cette opération diffère de la suppression d'une application App-V d'un groupe de mise à disposition).

1. Sélectionnez **Configuration > App-V Publishing** dans le panneau de navigation de Studio.
2. Sélectionnez un ou plusieurs packages à supprimer.
3. Cliquez sur **Supprimer le package** dans le volet Actions.

Ajouter, modifier ou supprimer des groupes d'isolement App-V

Ajouter un groupe d'isolement App-V

1. Sélectionnez **App-V Publishing** dans le panneau de navigation de Studio.
2. Sélectionnez **Ajouter un groupe d'isolement** dans le panneau Actions.
3. Dans la boîte de dialogue **Ajouter les paramètres du groupe d'isolement**, saisissez un nom et une description pour le groupe d'isolement.
4. Dans la liste Packages disponibles, sélectionnez les applications que vous souhaitez ajouter au groupe d'isolement, puis cliquez sur la flèche de droite. Les applications sélectionnées doivent maintenant s'afficher dans la liste Packages en groupe d'isolement. Dans la liste déroulante **Déploiement** en regard de chaque application, sélectionnez **Explicite** ou **Automatique**. Vous pouvez également utiliser les flèches haut et bas pour modifier l'ordre des applications dans la liste.
5. Lorsque vous avez terminé, cliquez sur **OK**.

Modifier un groupe d'isolement App-V

1. Sélectionnez **App-V Publishing** dans le panneau de navigation de Studio.
2. Sélectionnez l'onglet **Groupes d'isolement** dans le panneau central, puis sélectionnez le groupe d'isolement à modifier.
3. Sélectionnez **Modifier un groupe d'isolement** dans le panneau Actions.
4. Dans la boîte de dialogue **Modifier les paramètres du groupe d'isolement**, modifiez le nom ou la description du groupe d'isolement, ajoutez ou supprimez des applications, modifiez leur type de déploiement ou modifiez l'ordre des applications.
5. Lorsque vous avez terminé, cliquez sur **OK**.

Supprimer un groupe d'isolement App-V

La suppression d'un groupe d'isolement ne supprime pas les packages d'application. Elle supprime uniquement le regroupement.

1. Sélectionnez **App-V Publishing** dans le panneau de navigation de Studio.
2. Sélectionnez l'onglet **Groupes d'isolement** dans le panneau central, puis sélectionnez le groupe d'isolement à supprimer.
3. Sélectionnez **Supprimer groupe d'isolement** dans le panneau Actions.
4. Confirmez la suppression.

Ajouter des applications App-V à des groupes de mise à disposition

La procédure suivante se concentre sur l'ajout d'applications App-V à des groupes de mise à disposition. Pour des informations complètes sur la création d'un groupe de mise à disposition, consultez la section Créer des groupes de mise à disposition.

Étape 1 : choisissez si vous souhaitez créer un nouveau groupe de mise à disposition ou ajouter des applications App-V à un groupe de mise à disposition existant :

Pour créer un groupe de mise à disposition contenant des applications App-V :

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez **Créer un groupe de mise à disposition**dans le volet Actions.
3. Sur les pages successives de l'assistant, spécifiez un catalogue de machines et des utilisateurs.

Pour ajouter des applications App-V à des groupes de mise à disposition existants :

1. Sélectionnez **Applications** dans le volet de navigation de Studio.
2. Sélectionnez **Ajouter des applications** dans le volet Actions.
3. Sélectionnez un ou plusieurs groupes de mise à disposition dans lesquels les applications App-V seront ajoutées.

Étape 2 : sur la page **Applications** de l'assistant, cliquez sur la liste déroulante **Ajouter** pour afficher les sources d'applications. Sélectionnez **App-V**.

Étape 3 : sur la page **Ajouter des applications App-V**, choisissez la source App-V : le serveur App-V ou la bibliothèque d'applications. L'écran suivant inclut les noms des applications ainsi que le nom de leur package et les versions de package. Activez les cases à cocher en regard des applications que vous souhaitez ajouter. Cliquez ensuite sur **OK**.

Étape 4 : terminez l'assistant.

À savoir

- Si vous modifiez les propriétés d'une application App-V lorsque vous l'ajoutez à un groupe de mise à disposition, les modifications sont apportées lorsque l'application est démarrée. Par exemple, si vous modifiez le nom d'affichage ou l'icône d'une application lorsque vous l'ajoutez au groupe, la modification est visible lorsque l'utilisateur démarre l'application.
- Si vous modifiez ultérieurement un groupe de mise à disposition contenant des applications App-V, les performances des applications App-V ne changent pas si vous modifiez le type de groupe de mise à disposition de « bureaux et applications » vers « applications uniquement ».

Dépannage

Les problèmes qui peuvent se produire uniquement lors de l'utilisation du mode ?« double administration » sont indiqués par la mention (DOUBLE).

(DOUBLE) Il existe une erreur de connexion PowerShell lorsque vous sélectionnez **Configuration > App-V Publishing** dans le volet de navigation Studio.

- L'administrateur Studio est-il également un administrateur de serveur App-V ? L'administrateur de Studio doit appartenir au groupe « Administrateurs » sur App-V Management Server afin qu'ils puissent communiquer avec lui.

(DOUBLE) L'opération de test de la connexion a renvoyé une erreur lorsque vous spécifiez des adresses de serveur App-V dans Studio.

- Le serveur App-V est-il sous tension ? Envoyez une commande Ping ou vérifiez le Gestionnaire des services IIS ; chaque serveur App-V doit être dans un état démarré et en cours d'exécution.
- PowerShell à distance est-elle activée sur le serveur App-V ? Sinon, voir https://technet.microsoft.com/en-us/magazine/ff700227.aspx.
- L'administrateur Studio est-il également un administrateur de serveur App-V ? L'administrateur de Studio doit appartenir au groupe « Administrateurs » sur App-V Management Server afin qu'ils puissent communiquer avec lui.
- Le partage de fichiers est-il activé sur le serveur App-V ? Entrez le ***<nom complet du serveur App-V>*** dans l'Explorateur Windows ou avec la commande Exécuter.

- Le serveur App-V possède-t-il les mêmes autorisations de partage de fichiers que l'administrateur App-V ? Sur le serveur App-V, ajoutez une entrée pour le \\<*nom complet du serveur App-V Server FQDN*> dans Noms et mots de passe utilisateur enregistrés, en spécifiant les informations d'identification de l'utilisateur qui dispose de privilèges d'administrateur sur le serveur App-V. Pour des conseils, voir https://support.microsoft.com/kb/306541.
- Le serveur App-V est-il dans Active Directory ?

  Si les machines Studio et le serveur App-V se trouvent dans différents domaines Active Directory qui ne disposent pas d'une relation d'approbation, à partir de la console PowerShell sur les machines Studio, exécutez **winrm s winrm/Config/client '@(TrustedHosts="<*Nom complet du serveur App-V*>")'**.

  Si TrustedHosts est géré par l'objet de stratégie de groupe, le message d'erreur suivant s'affiche : « Le paramètre de configuration TrustedHosts ne peut pas être modifié car il est contrôlé par des stratégies. La stratégie doit être définie sur Non configuré pour changer le paramètre de configuration. » Dans ce cas, ajoutez une entrée pour le nom de serveur App-V à la stratégie TrustedHosts dans l'objet de stratégie de groupe (**Modèles d'administration > Composants Windows > Gestion à distance de Windows (WinRM) > Client WinRM**).

(DOUBLE) La découverte échoue lors de l'ajout d'une application App-V à un groupe de mise à disposition.

- L'administrateur Studio est-il également un administrateur du serveur d'administration App-V ? L'administrateur de Studio doit appartenir au groupe « Administrateurs » sur App-V Management Server afin qu'ils puissent communiquer avec lui.
- Le serveur d'administration App-V est-il en cours d'exécution ? Envoyez une commande Ping ou vérifiez le Gestionnaire des services IIS ; chaque serveur App-V doit être dans un état démarré et en cours d'exécution.
- PowerShell à distance est-elle activée sur les deux serveurs App-V ? Sinon, voir https://technet.microsoft.com/en-us/magazine/ff700227.aspx.
- Les packages possèdent-ils des autorisations de sécurité appropriées pour que l'administrateur Studio ait accès ?

Les applications App-V ne démarrent pas.

- (DOUBLE) Le serveur de publication est-il en cours d'exécution ?
- (DOUBLE) Les packages App-V possèdent-ils les autorisations de sécurité nécessaires pour que les utilisateurs aient accès ?
- (DOUBLE) Sur le VDA, assurez-vous que Temp pointe vers l'emplacement correct et qu'il existe suffisamment d'espace disponible dans le répertoire Temp.
- (DOUBLE) Sur le serveur de publication App-V, exécutez **Get-AppvPublishingServer *** pour afficher la liste des serveurs de publication.
- (DOUBLE) Sur le serveur de publication App-V, assurez-vous que UserRefreshonLogon est défini

sur False.
- (DOUBLE) Sur le serveur de publication App-V, en tant qu'administrateur, exécutez **Set-AppvPublishingServer** et définissez UserRefreshonLogon sur False.
- Une version prise en charge du client App-V est-elle installée sur le VDA ? Le paramètre « enable package scripts » est-il activé pour le VDA ?
- Sur la machine contenant le client App-V et le VDA, à l'aide de l'Éditeur du Registre (regedit), accédez à la clé HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\AppV. Vérifiez que la clé AppVServers possède la valeur suivante format : AppVManagementServer+metadata;PublishingServer (par exemple : `http://xmas-demo-appv.blrstrm.com+0+0+0+1+1+1+0+1;http://xmas-demo-appv.blrstrm.com:8082`).
- Sur la machine ou l'image principale contenant le client App-V et le VDA, vérifiez que le paramètre ExecutionPolicy du PowerShell est défini sur RemoteSigned. Le client App-V fourni par Microsoft n'est pas signé et ce paramètre permet au PowerShell d'exécuter des scripts et applets de commande locaux non signés. Utilisez l'une des méthodes suivantes pour définir ExecutionPolicy : (1) En tant qu'administrateur, entrez l'applet de commande : **Set-ExecutionPolicy RemoteSigned** ou (2) Dans les paramètres de stratégie de groupe, accédez à **Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Windows PowerShell > Activer l'exécution des scripts**.

Si ces étapes ne résolvent pas les problèmes, l'administrateur doit activer et examiner les journaux.

Journaux

Les journaux liés à la configuration App-V se trouvent à l'emplacement suivant : C:\CtxAppvLogs. Les journaux de lancement de l'application se trouvent à l'emplacement suivant : %LOCALAPPDATA%\Citrix\CtxAppvLogs. LOCALAPPDATA résout le dossier local pour l'utilisateur connecté. Vérifiez dans le dossier local de l'utilisateur pour lequel le lancement de l'application a échoué.

Pour activer les journaux Studio et VDA utilisés pour App-V, vous devez disposer des privilèges d'administrateur. Vous aurez également besoin d'un éditeur de texte tel que le Bloc-notes.

Pour activer les journaux Studio :

1. Créez le dossier C:\CtxAppvLogs.
2. Accédez à C:\Program Files\Citrix\StudioAppVIntegration\SnapIn\Citrix.Appv.Admin.V1. Ouvrez CtxAppvCommon.dll.config dans un éditeur de texte et retirez les marques de commentaire de la ligne suivante : <add key =”LogFileName” value=”C:\CtxAppvLogs\log.txt”/>
3. Redémarrez le service Broker pour démarrer la journalisation.

Pour activer les journaux VDA :

1. Créez le dossier C:\CtxAppvLogs.

2. Accédez à C:\ProgramFiles\Citrix\Virtual Desktop Agent. Ouvrez CtxAppvCommon.dll.config dans un éditeur de texte et retirez les marques de commentaire de la ligne suivante : <add key =”LogFileName” value=”C:\CtxAppvLogs\log.txt”/>
3. Supprimez les marques de commentaire de la ligne suivante et définissez la valeur de champ sur 1 : <add key =”EnableLauncherLogs” value=”1”/>
4. Redémarrez la machine pour démarrer la journalisation.

AppDisks

February 28, 2019

Généralités

La gestion des applications et des images sur lesquelles elles sont installées peut être une tâche difficile. La fonctionnalité Citrix AppDisks apporte une solution. La fonctionnalité AppDisks sépare les applications et les groupes d’applications du système d’exploitation, ce qui vous permet de les gérer indépendamment.

Vous pouvez créer différents AppDisks contenant des applications conçues pour des groupes d’utilisateurs, puis assembler les AppDisks sur une image principale de votre choix. Regrouper et gérer les applications de cette manière vous offre un meilleur contrôle des applications et réduit le nombre d’images principales à gérer. Cela simplifie les tâches administratives et vous permet de répondre plus rapidement aux besoins de l’utilisateur. Vous pouvez mettre les applications à disposition dans des AppDisks par le biais de groupes de mise à disposition.

Si votre déploiement comprend également Citrix AppDNA, vous pouvez y intégrer la fonctionnalité AppDisks ; AppDNA permet à XenApp et à XenDesktop d’effectuer une analyse automatique des applications par AppDisk. L’utilisation d’AppDNA permet de profiter pleinement de la fonctionnalité AppDisks. Sans AppDNA, la compatibilité applicative n’est pas testée ou communiquée.

La fonctionnalité AppDisks diffère des autres technologies de provisioning d’applications par deux aspects : l’isolation et la gestion des modifications.

- Microsoft App-V permet aux applications incompatibles de co-exister en les isolant. La fonctionnalité AppDisks n’isole pas les applications. Elle sépare les applications (ainsi que les fichiers et les clés de registre associés) du système d’exploitation. Pour le système d’exploitation et l’utilisateur, l’aspect et le fonctionnement des AppDisks sont les mêmes que s’ils étaient installés directement sur une image principale.
- La gestion des modifications (la mise à jour des images principales et le test de compatibilité des mises à jour avec les applications installées) peut représenter une dépense importante. Les rapports AppDNA vous aident à identifier les problèmes et suggèrent des solutions. Par exemple,

AppDNA peut identifier les applications qui ont des dépendances communes telles que .NET, ce qui vous permet de les installer sur une seule image de base commune. AppDNA peut également identifier les applications qui se chargent tôt dans la séquence de démarrage du système d'exploitation, vous permettant de vous assurer qu'elles se comportent comme prévu.

À savoir

- Après la mise à jour d'une image, certaines applications peuvent ne pas fonctionner correctement car les licences installées précédemment ne peuvent pas être vérifiées. Par exemple, après une mise à niveau d'image, le lancement de Microsoft Office peut afficher un message d'erreur similaire à :

  « Microsoft Office Professionnel Plus 2010 ne peut pas vérifier la licence pour cette application. Une tentative de réparation a échoué ou a été annulée par l'utilisateur. L'application va s'arrêter. »

Pour résoudre ce problème, désinstallez Microsoft Office et installez la nouvelle version sur l'image de base.

- Dans certains cas, le téléchargement d'applications Metro à partir du Windows Store vers une machine virtuelle du catalogue publiée échoue après un long délai.
- Citrix recommande de toujours placer tous les composants de Microsoft Office dans le même AppDisk. Par exemple, un AppDisk avec Microsoft Office Project et un autre AppDisk avec Microsoft Office Project et Visio.
- Sur certains systèmes, SCCM se bloque lors de la mise à jour d'une image. Ce scénario se produit lorsque des mises à jour sont effectuées sur l'image de base, puis appliquées, ce qui entraîne l'échec du client SCCM. Pour résoudre ce problème, installez d'abord l'instance du client SCCM dans l'image de base.
- Dans certains cas, une application installée sur le AppDisk peut ne pas s'afficher dans le menu Démarrer de Windows après qu'elle a été attribuée à un groupe de mise à disposition et attribuée à la machine virtuelle d'un utilisateur. Consultez la section Affichage des applications dans le menu Démarrer pour plus d'informations.
- La séparation des applications et du système d'exploitation, ou tout autre aspect de la fonctionnalité AppDisks, n'est pas visible pour l'utilisateur. Les applications se comportent comme si elles étaient installées sur l'image. Les AppDisks contenant des applications complexes peuvent entraîner un léger délai de démarrage du bureau.
- Vous pouvez uniquement utiliser les AppDisks avec des bureaux regroupés et partagés hébergés.
- Vous pouvez utiliser les AppDisks avec des bureaux partagés hébergés.
- Vous pouvez partager les AppDisks sur différentes images principales et plates-formes de système d'exploitation (par application) ; toutefois, cela ne fonctionnera pas pour toutes les applications. Si vous disposez d'applications avec un script d'installation pour OS de bureau qui les empêche de fonctionner sur un OS de serveur, Citrix vous recommande de créer un package

distinct des applications pour les deux systèmes d'exploitation.

- Dans de nombreux cas, les AppDisks fonctionnent sur différents systèmes d'exploitation. Par exemple, vous pouvez ajouter un AppDisk qui a été créé sur une VM Windows 7 à un groupe de mise à disposition contenant des machines Windows 2008 R2, tant que les deux systèmes d'exploitation ont le même nombre de bits (32 bits ou 64 bits) et prennent en charge l'application. Cependant, Citrix vous recommande de ne pas ajouter un AppDisk créé sur une version ultérieure du système d'exploitation (telle que Windows 10) à un groupe de mise à disposition contenant des machines exécutant une version antérieure du système d'exploitation (telle que Windows 7), car il risque de ne pas fonctionner correctement.
- Si vous avez besoin de limiter l'accès à des applications d'un AppDisk à un sous-ensemble d'utilisateurs d'un groupe de mise à disposition, Citrix vous recommande d'utiliser la stratégie de groupe pour masquer les applications d'un AppDisk pour certains utilisateurs. Le fichier exécutable de cette application reste disponible, mais ne sera pas exécuté pour ces utilisateurs.
- Dans les environnements russes et chinois exécutant le système d'exploitation Windows 7, la boîte de dialogue de redémarrage ne disparaît pas automatiquement ; dans ce cas, après la connexion à un ordinateur de bureau mis à disposition, la boîte de dialogue de redémarrage apparaît et devrait disparaître rapidement.
- Lorsque vous utilisez l'outil de script **Upload-PvDDiags**, les informations de journal relatives à la couche utilisateur PVD sont manquantes lorsque la désignation du disque de l'utilisateur n'est pas définie sur « P ».
- Dans les environnements définis pour afficher la langue basque, un système d'exploitation Windows 7 peut ne pas afficher correctement la langue appropriée sur l'écran d'invite de redémarrage. Lorsque vous définissez la langue sur le basque, assurez-vous que vous avez déjà installé l'espagnol ou le français comme langue parente, puis installez le basque et définissez cette langue comme langue en cours.
- Lorsque vous arrêtez un ordinateur, le rappel de mise à jour PVD s'affiche même si le disque PVD est défini en mode lecture seule.
- Au cours d'une mise à niveau sur place, un fichier de Registre (DaFsFilter) peut être supprimé, ce qui entraîne l'échec de la mise à niveau.

> **Conseil :**
>
> Lorsque vous créez un AppDisk, utilisez une VM vierge de toute application ; seul le système d'exploitation doit être installé ; le système d'exploitation doit contenir toutes les mises à jour avant la création de l'AppDisk.

Vue d'ensemble du déploiement

La liste suivante résume les étapes de déploiement des AppDisks. Vous trouverez plus de détails dans cet article.

1. À partir de la console de gestion de l'hyperviseur, installez un Virtual Delivery Agent (VDA) sur une VM.
2. Créez un AppDisk, ce qui inclut des étapes dans la console de gestion de l'hyperviseur et dans Studio.
3. À partir de la console de gestion de l'hyperviseur, installez les applications sur le AppDisk.
4. Scellez le AppDisk (à partir de la console de gestion de l'hyperviseur ou dans Studio). La possibilité de sceller permet à XenApp et à XenDesktop d'enregistrer les applications du AppDisk et les fichiers associés dans une bibliothèque d'applications (AppLibrary).
5. Dans Studio, créez ou modifiez un groupe de mise à disposition et sélectionnez les AppDisks à inclure ; cela s'appelle *attribuer les AppDisks* (même si vous utilisez l'action **Gérer les AppDisks** dans Studio). Lorsque des machines virtuelles dans le groupe de mise à disposition démarrent, XenApp et XenDesktop se coordonnent avec l'AppLibrary, puis interagissent avec Creation Services (MCS) ou Provisioning Services (PVS) et le Delivery Controller pour livrer en streaming les périphériques de démarrage après que les AppDisks ont été configurés sur ces derniers.

Exigences

L'utilisation de AppDisks présente des exigences en plus de celles répertoriées dans l'article Configuration système requise.

La fonctionnalité AppDisks est uniquement prise en charge dans les déploiements contenant (au minimum) les versions du Delivery Controller et de Studio fournies dans le téléchargement de XenApp et XenDesktop 7.8, y compris les composants requis que le programme d'installation déploie automatiquement (tels que .NET 4.5.2).

Les AppDisks peuvent être créés sur les versions de système d'exploitation Windows prises en charge pour les VDA. Les machines sélectionnées pour les groupes de mise à disposition qui utiliseront AppDisks doivent disposer de VDA version 7.8 au minimum.

Citrix vous recommande d'installer ou de mettre à niveau les machines avec la dernière version de VDA (et de mettre à niveau les catalogues de machines et les groupes de mise à disposition en fonction de vos besoins). Lors de la création d'un groupe de mise à disposition, si vous sélectionnez des machines sur lesquelles sont installées différentes versions de VDA, le groupe de mise à disposition sera compatible avec la version de VDA la plus ancienne (Il s'agit du *niveau fonctionnel* du groupe). Pour plus d'informations sur le niveau fonctionnel, consultez l'article Créer des groupes de mise à disposition.

Pour provisionner des machines virtuelles qui seront utilisées pour créer des AppDisks, vous pouvez utiliser les éléments suivants :

- MCS fourni avec le Controller 7.8 (minimum).
- Version PVS fournie sur la page de téléchargement avec votre version XenApp et XenDesktop.
- Hyperviseurs pris en charge :

  - XenServer
  - VMware (version minimum 5.1)
  - Microsoft System Center Virtual Machine Manager

Les AppDisks ne peuvent pas être utilisés avec d'autres types d'hyperviseur et de service de cloud hôte pris en charge par XenApp et XenDesktop.

La création d'AppDisks n'est pas prise en charge avec les machines de catalogues MCS qui utilisent la mise en cache des données temporaires.

> **Remarque :**
>
> Vous pouvez attacher des AppDisks à des machines provisionnées avec MCS à l'aide du cache en écriture, mais elles ne peuvent pas être utilisées pour créer des AppDisks.

Les catalogues Remote PC Access ne prennent pas en charge les AppDisks.

Le service de cliché instantané des volumes Windows doit être activé sur la machine virtuelle sur laquelle vous créez un AppDisk. Ce service est activé par défaut.

Les groupes de mise à disposition utilisés avec les AppDisks peuvent contenir des machines regroupées au hasard dans des catalogues de machines avec OS de serveur ou OS de bureau. Vous ne pouvez pas utiliser les AppDisks avec des machines d'autres types de catalogue, tels que les catalogues de machines statiques regroupées ou dédiées (attribuées).

Les machines sur lesquelles Studio est installé doivent disposer de .NET Framework 3.5 (en plus d'autres versions .NET).

Les AppDisks peuvent affecter le stockage. Pour de plus amples informations, veuillez consulter la section Considérations sur le stockage et les performances.

Si vous utilisez AppDNA :

- Consultez la documentation AppDNA et la FAQ AppDisk.
- Le logiciel AppDNA doit être installé sur un autre serveur depuis un Controller. Utilisez la version AppDNA fournie avec cette version de XenApp et de XenDesktop. Pour les autres exigences de AppDNA, consultez sa documentation.
- Sur le serveur AppDNA, assurez-vous qu'il existe une exception de pare-feu pour le port par défaut 8199.
- Ne désactivez pas de connexion AppDNA lors de la création d'un AppDisk.
- Lorsque vous créez le site XenApp ou XenDesktop, vous pouvez activer l'analyse de compatibilité avec AppDNA sur la page **Fonctionnalités supplémentaires** de l'assistant de création de site. Vous pouvez également activer/désactiver cette fonctionnalité en sélectionnant l'option **Configuration > AppDNA** dans le volet de navigation Studio.
- Le lien Afficher rapport des problèmes dans Studio affiche le rapport AppDNA, toutefois les combinaisons de système d'exploitation qu'AppDNA utilise par défaut sont Windows 7 64 bits pour les groupes de mise à disposition de bureaux et Windows Server 2012 R2 pour les groupes de

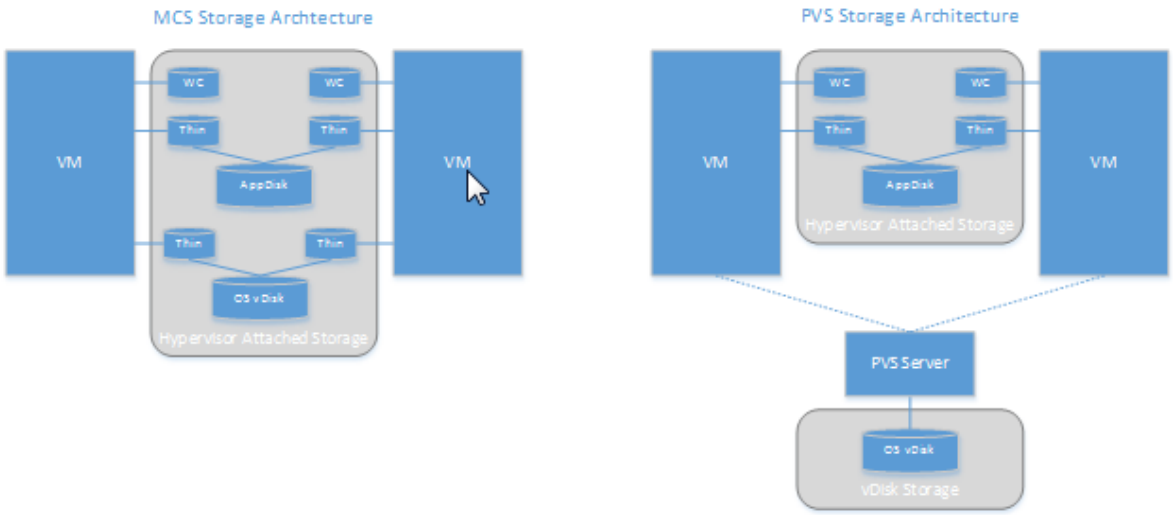
mise à disposition de serveurs. Si vos groupes de mise à disposition contiennent différentes versions de Windows, les combinaisons d'images par défaut seront incorrectes dans les rapports Studio. Pour contourner ce problème, modifiez manuellement la solution dans AppDNA après qu'elle ait été créée par Studio.

- Il existe une dépendance entre les versions du serveur AppDNA et de Studio.
  - À partir de la version 7.12, la version de Studio doit être la même ou une version plus élevée que celle du serveur AppDNA.
  - Pour les versions 7.9 et 7.11, les versions du serveur AppDNA et de Studio doivent correspondre.
  - Le tableau suivant indique les versions qui fonctionnent ensemble (Oui = les versions fonctionnent ensemble, – = les versions ne fonctionnent pas ensemble) :

Version du produit	Studio 7.9	Studio 7.11	Studio 7.12	Studio 7.13	Studio 7.14	Studio 7.15
AppDNA 7.9	Oui	–	–	–	–	–
AppDNA 7.11	–	Oui	–	–	–	–
AppDNA 7.12	–	–	Oui	Oui	Oui	Oui
AppDNA 7.13	–	–	Oui	Oui	Oui	Oui
AppDNA 7.14	–	–	–	–	Oui	Oui
AppDNA 7.15	–	–	–	–	–	Oui

Considérations sur le stockage et les performances

La séparation des applications et du système d'exploitation à l'aide de deux disques, et le stockage de ces disques dans différentes zones peuvent affecter votre stratégie de stockage. Le graphique suivant illustre les architectures de stockage MCS et PVS. « WC » indique le cache en écriture et « Thin » indique le disque léger utilisé pour stocker les différences entre le AppDisk d'une VM et les disques virtuels du système d'exploitation.



Dans les environnements MCS :

- Vous pouvez continuer à équilibrer la taille des AppDisks et des disques virtuels (vDisks) du système d'exploitation en suivant les recommandations de votre entreprise en termes de taille. Si les AppDisks sont partagés par plusieurs groupes de mise à disposition, la capacité de stockage générale peut être réduite.
- Les vDisks du système d'exploitation et les AppDisks sont situés dans les mêmes zones de stockage, vous devez donc planifier attentivement vos besoins en termes de capacité de stockage pour éviter tout effet négatif sur la capacité lorsque vous déployez les AppDisks. Les AppDisks entraînent une surcharge, donc assurez-vous que votre stockage prend en charge cette surcharge et les applications.
- Il n'y a aucun effet net sur IOPS car les vDisks du système d'exploitation et les AppDisks sont situés dans la même zone de stockage. Il n'existe pas de considérations à prendre en compte pour le cache en écriture lorsque vous utilisez MCS.

Dans les environnements PVS :

- Vous devez prévoir une capacité et des IOPS plus importantes car les applications se déplacent du stockage sur AppDisk vers le stockage lié à l'hyperviseur.
- Avec PVS, les vDisks du système d'exploitation et les AppDisks utilisent des zones de stockage différentes. La capacité de stockage des vDisks du système d'exploitation est réduite, mais le stockage lié à l'hyperviseur augmente. Par conséquent, vous devez configurer la taille de vos environnements PVS pour la prise en charge de ces modifications.
- Les AppDisks dans le stockage lié à l'hyperviseur requièrent plus d'IOPS alors que les vDisks du système d'exploitation en requièrent moins.
- Cache en écriture : PVS utilise un fichier VHDX dynamique sur un lecteur au format NTFS ; lorsque les blocs sont consignés dans le cache en écriture, le fichier VHDX est étendu de

manière dynamique. Lorsque les AppDisks sont connectés à leur machine virtuelle associée, ils sont fusionnés avec les vDisks du système d'exploitation pour fournir une vue unifiée du système de fichiers. Cette fusion entraîne généralement l'écriture de données supplémentaires sur les caches en écriture, ce qui augmente la taille du fichier du cache en écriture. Vous devez prendre en compte cet aspect lors de la planification de la capacité.

Dans les environnements MCS et PVS, pensez à réduire la taille des vDisks du système d'exploitation pour tirer parti des AppDisks que vous créez. Sinon, planifiez un stockage plus important.

Lorsque plusieurs utilisateurs d'un site allument leurs ordinateurs simultanément (par exemple, en début de journée), les multiples requêtes de démarrage exercent une pression sur l'hyperviseur, ce qui peut affecter les performances. Pour PVS, les applications ne se trouvent pas sur le vDisk du système d'exploitation, donc le serveur PVS reçoit moins de requêtes. La charge étant plus légère sur chaque machine cible, le serveur PVS peut transmettre vers un plus grand nombre de cibles. Cependant, une plus grande densité cible-serveur peut avoir un effet négatif sur les performances « boot storm ».

Créer un AppDisk

Il existe deux façons de créer un AppDisk, d'installer les applications et de le sceller. Les deux méthodes comprennent des étapes dans la console de gestion de l'hyperviseur et dans Studio. Les méthodes se distinguent par l'emplacement où se déroulent la plupart des étapes.

Quelle que soit la méthode que vous utilisez :

- Prévoyez 30 minutes pour la création du AppDisk.
- Si vous utilisez AppDNA, suivez les instructions de la section Configuration requise ci-dessus. Ne désactivez pas de connexion AppDNA lors de la création d'un AppDisk.
- Lorsque vous ajoutez des applications à un AppDisk, pensez à installer les applications pour tous les utilisateurs. Réarmez les applications qui utilisent l'activation de Key Management Server (KMS). Pour de plus amples informations, consultez la documentation de l'application.
- Les fichiers, dossiers ou entrées de registre créés dans des emplacements spécifiques à l'utilisateur lors de la création du AppDisk ne sont pas conservés. Par ailleurs, certaines applications exécutent un assistant de première utilisation pour créer les données de l'utilisateur au cours de l'installation. Utilisez une solution de gestion de profils pour conserver ces données et empêcher l'affichage de l'assistant chaque fois que le AppDisk démarre.
- Si vous utilisez AppDNA, l'analyse démarre automatiquement après la fin du processus de création. Pendant cet intervalle, l'état du AppDisk dans Studio est « Analyse ».

Considérations sur PVS

Les AppDisks sur des machines de catalogues de machines créés par Provisioning Services nécessitent une configuration supplémentaire durant la création du AppDisk. À partir de la console Provisioning

Services :

1. Créez une nouvelle version du vDisk associé à la collection de machines qui contient la VM.
2. Placez la VM en mode de maintenance.
3. Lors de la création du AppDisk, sélectionnez la version de maintenance sur l'écran de démarrage chaque fois que la VM redémarre.
4. Après avoir scellé le AppDisk, placez la VM en production et supprimez la version vDisk que vous avez créée.

Créer un AppDisk principalement dans Studio

Cette procédure comporte trois tâches : créer le AppDisk, créer des applications sur le AppDisk, puis sceller le AppDisk.

Créer un AppDisk

1. Sélectionnez **AppDisks** dans le panneau de navigation de Studio, puis sélectionnez **Créer un AppDisk** dans le volet Actions.
2. Passez en revue les informations sur la page **Introduction** de l'assistant, puis cliquez sur **Suivant**.
3. Sur la page **Créer un AppDisk**, sélectionnez le bouton radio **Créer un nouveau AppDisk**. Sélectionnez l'une des tailles de disque prédéfinies (petite, moyenne, grande) ou spécifiez une taille de disque en Go ; la taille minimale est de 3 Go. La taille du disque doit être suffisante pour contenir les applications que vous ajoutez. Cliquez sur **Suivant**.
4. Sur la page **Machine de préparation**, sélectionnez un catalogue regroupé aléatoire à utiliser comme image principale sur laquelle l'AppDisk sera construit. Remarque : l'écran dresse la liste de tous les catalogues de machines du site, séparés par type ; seuls les catalogues contenant au moins une machine disponible peuvent être sélectionnés. Si vous choisissez un catalogue qui ne contient pas de VM regroupées au hasard, la création de AppDisk échoue. Après avoir sélectionné une machine virtuelle dans un catalogue groupé aléatoire, cliquez sur **Suivant**.
5. Sur la page **Résumé**, tapez un nom et une description pour l'AppDisk. Vérifiez les informations que vous avez spécifiées sur les pages précédentes de l'assistant. Cliquez sur **Terminer**.

Rappel : si vous utilisez PVS, suivez les instructions dans la section Considérations sur PVS ci-dessus.

Lorsque l'assistant se ferme, l'écran Studio pour le nouveau AppDisk indique « Création ». Une fois que le AppDisk est créé, l'affichage change en « Prêt à installer les applications ».

Installer des applications sur AppDisk

À partir de la console de gestion de l'hyperviseur, installez les applications sur le AppDisk. (**Conseil :** si vous avez oublié le nom de la VM, sélectionnez **AppDisks** dans le panneau de navigation de Studio,

puis sélectionnez **Installer des applications** dans le panneau Actions pour afficher son nom). Consultez la documentation de l'hyperviseur pour obtenir des informations sur l'installation des applications. (**Rappel :** vous devez installer des applications sur le AppDisk à partir de la console de gestion de l'hyperviseur. N'utilisez pas la tâche Installer des applications dans le volet Actions de Studio.)

Sceller le AppDisk

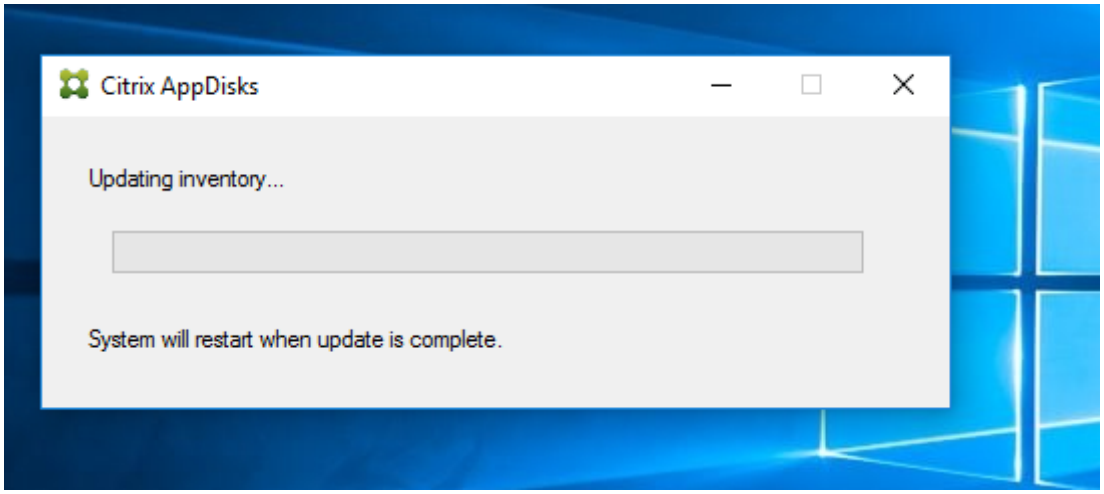
1. Sélectionnez **AppDisks** dans le volet de navigation de Studio.
2. Sélectionnez l'AppDisk que vous avez créé, puis sélectionnez **Sceller AppDisk** dans le panneau Actions.

Après avoir créé le AppDisk, installez-y des applications, puis scellez-le et attribuez-le à un groupe de mise à disposition.

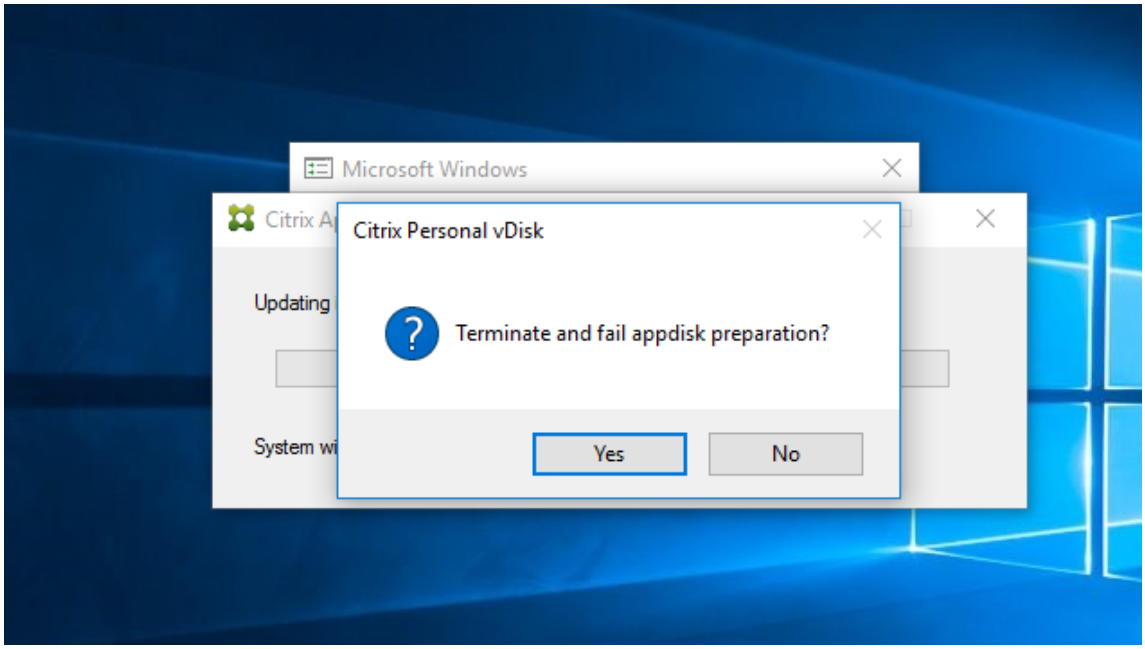
Annulation de la préparation et du scellement du AppDisk

Dans certains cas, il se peut qu'un administrateur soit amené à annuler la création ou le scellement d'un AppDisk :

1. Accédez à la VM.
2. Fermez la boîte de dialogue :



3. Une fois que la boîte de dialogue est fermée, un message apparaît demandant une vérification pour annuler l'opération sélectionnée ; cliquez sur **Oui**.



> **Remarque :**
>
> Si vous annulez la préparation d'un AppDisk, le redémarrage de la machine restaure son état initial, sinon, vous devez créer une nouvelle VM.

Créer un AppDisk sur l'hyperviseur et l'importer dans Studio

Dans cette procédure, vous effectuez la création du AppDisk et la préparation des tâches à partir de la console de gestion de l'hyperviseur, puis vous importez le AppDisk dans Studio.

Préparer, installer les applications et sceller un AppDisk sur l'hyperviseur

1. À partir de la console de gestion de l'hyperviseur, créez une VM et installez un VDA.
2. Arrêtez la machine et prenez un instantané.
3. Créez une nouvelle machine à partir de l'instantané, puis ajoutez-lui un nouveau disque. Ce disque (qui deviendra le AppDisk) doit être de taille suffisante pour stocker toutes les applications que vous installerez dessus.
4. Démarrez la machine et sélectionnez **Démarrer > Préparer AppDisk**. Si le raccourci du menu Démarrer n'est pas disponible sur l'hyperviseur, ouvrez une invite de commandes à C:\Program Files\Citrix Personal vDisk\bin et tapez : **CtxPvD.Exe –s LayerCreationBegin**. La machine redémarre et prépare le disque. Un second redémarrage se produit après quelques minutes lorsque la préparation est terminée.
5. Installez les applications que vous souhaitez mettre à la disposition des utilisateurs.
6. Double-cliquez sur le raccourci **Packager AppDisk** sur le bureau de la machine. La machine redémarre et le processus commence. Lorsque la boîte de dialogue se ferme, arrêtez la VM.

Utiliser Studio pour importer le AppDisk vous avez créé sur l'hyperviseur

1. Sélectionnez **AppDisks** dans le panneau de navigation de Studio, puis sélectionnez **Créer un AppDisk** dans le volet Actions.
2. Sur la page **Introduction** de l'assistant, passez en revue les informations, puis cliquez sur **Suivant**.
3. Sur la page **Créer un AppDisk**, sélectionnez le bouton radio **Importer un AppDisk existant**. Sélectionnez la ressource (réseau et stockage) dans laquelle le AppDisk que vous avez créé réside sur l'hyperviseur. Cliquez sur **Suivant**.
4. Sur la page **Machine de préparation**, accédez à la machine, sélectionnez le disque, puis cliquez sur **Suivant**.
5. Sur la page **Résumé**, tapez un nom et une description pour l'AppDisk. Vérifiez les informations que vous avez spécifiées sur les pages précédentes de l'assistant. Cliquez sur **Terminer**. Studio importe le AppDisk.

Une fois que vous avez importé le AppDisk dans Studio, attribuez-le à un groupe de mise à disposition.

Attribuer un AppDisk à un groupe de mise à disposition

Vous pouvez attribuer un ou plusieurs AppDisks à un groupe de mise à disposition lorsque vous créez le groupe de mise à disposition ou ultérieurement. Les informations AppDisks que vous fournissez sont quasiment les mêmes.

Si vous ajoutez des AppDisks à un groupe de mise à disposition que vous créez, utilisez les instructions suivantes pour la page **AppDisks** dans l'assistant de création de groupe de mise à disposition. (Pour de plus amples informations sur les autres pages de cet assistant, consultez l'article Créer des groupes de mise à disposition.)

Pour ajouter (ou supprimer) des AppDisks dans un groupe de mise à disposition existant :

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe de mise à disposition, puis sélectionnez **Gérer les AppDisks** dans le volet Actions. Veuillez consulter les instructions suivantes pour la page **AppDisks**.
3. Lorsque vous modifiez la configuration du AppDisk dans un groupe de mise à disposition, un redémarrage des machines du groupe est requis. Sur la page **Stratégie de déploiement**, suivez les instructions de la section Créer un programme de redémarrage.

Page AppDisks

La page **AppDisks** (dans l'assistant Créer un groupe de mise à disposition ou dans le flux Gérer les AppDisks) répertorie les AppDisks déjà déployés pour le groupe de mise à disposition et leur priorité. (si vous créez le groupe de mise à disposition, la liste est vide.) Pour de plus amples informations, consultez la section Priorité AppDisk.

1. Cliquez sur **Ajouter**. La boîte de dialogue Sélectionner des AppDisks dresse la liste de tous les AppDisks dans la colonne de gauche. Les cases des AppDisks qui sont déjà attribués à ce groupe de mise à disposition sont activées et ils ne peuvent pas être sélectionnés.
2. Sélectionnez les cases à cocher des AppDisks disponibles dans la colonne de gauche. La colonne de droite dresse la liste des applications sur le AppDisk (la sélection de l'onglet **Applications** au-dessus de la colonne de droite dresse la liste des applications dans un format similaire à un menu Démarrer ; la sélection de l'onglet **Packages installés** dresse la liste des applications dans un format similaire à la liste Programmes et fonctionnalités.)
3. Après avoir sélectionné un ou plusieurs AppDisks disponibles, cliquez sur **OK**.
4. Cliquez sur **Suivant** dans la page AppDisks.

Priorité AppDisk dans un groupe de mise à disposition

Lorsqu'un groupe de mise à disposition a plusieurs AppDisk assignés, la page **AppDisks** (dans les écrans Créer un groupe de mise à disposition, Modifier le groupe de mise à disposition et Gérer les AppDisks) répertorie les AppDisks en priorité décroissante. Les entrées en haut de la liste ont la priorité plus élevée. La priorité indique l'ordre dans lequel les AppDisks sont traités.

Vous pouvez utiliser les flèches haut et bas en regard de la liste pour modifier la priorité AppDisk. Si AppDNA est intégré avec votre déploiement AppDisk, il analyse automatiquement les applications et définit la priorité lorsque les AppDisks sont attribués au groupe de mise à disposition. Plus tard, si vous ajoutez ou supprimez des AppDisks du groupe, vous pouvez cliquer sur **Ordre automatique** pour demander à AppDNA d'analyser la liste actuelle des AppDisks et de déterminer les priorités. L'analyse (et le changement de priorité, si nécessaire) peut prendre plusieurs minutes.

Gestion de AppDisks

Une fois que vous avez créé et attribué des AppDisks à des groupes de mise à disposition, vous pouvez modifier les propriétés des AppDisks via le nœud AppDisks dans le panneau de navigation de Studio. Les modifications apportées aux applications dans un AppDisk doivent être effectuées à partir de la console de gestion de l'hyperviseur.

> **Important :**
>
> Vous pouvez utiliser le service Windows Update pour mettre à jour les applications (telles que la suite Microsoft Office) sur un AppDisk. Toutefois, n'utilisez pas le service Windows Update pour appliquer les mises à jour du système d'exploitation à un AppDisk. Appliquez les mises à jour du système d'exploitation à l'image principale, et non pas au AppDisk ; sinon, le AppDisk ne s'initialise pas correctement.
>
> - Lors de l'application de correctifs et d'autres mises à jour à des applications dans un Ap-

> pDisk, appliquez uniquement ceux dont a besoin l'application. N'appliquez pas les mises à jour pour d'autres applications.
> - Lors de l'installation des mises à jour Windows, vous devez d'abord désélectionner toutes les entrées, puis sélectionner le sous-ensemble requis par les applications sur les AppDisks que vous mettez à jour.

Considérations liées aux antivirus lors de la création d'un AppDisk

Dans certains cas, vous pouvez rencontrer des problèmes lors de la tentative de création d'un AppDisk si un agent antivirus est installé sur la VM de base. Dans de tels cas, la création du AppDisk peut échouer lorsque certains processus sont signalés par l'agent antivirus. Ces processus, **CtxPvD.exe** et **CtxPvDSrv.exe**, doivent être ajoutés à la liste des exceptions pour l'agent A/V utilisé par la machine virtuelle de base.

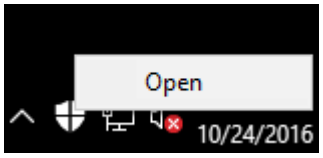
Cette section fournit des informations sur l'ajout d'exceptions pour les logiciels antivirus suivants :

- Windows Defender (pour Windows 10)
- OfficeScan (version 11.0)
- Symantec (version 12.1.16)
- McAfee (version 4.8)

Windows Defender

Si votre VM de base utilise Windows Defender (version 10) :

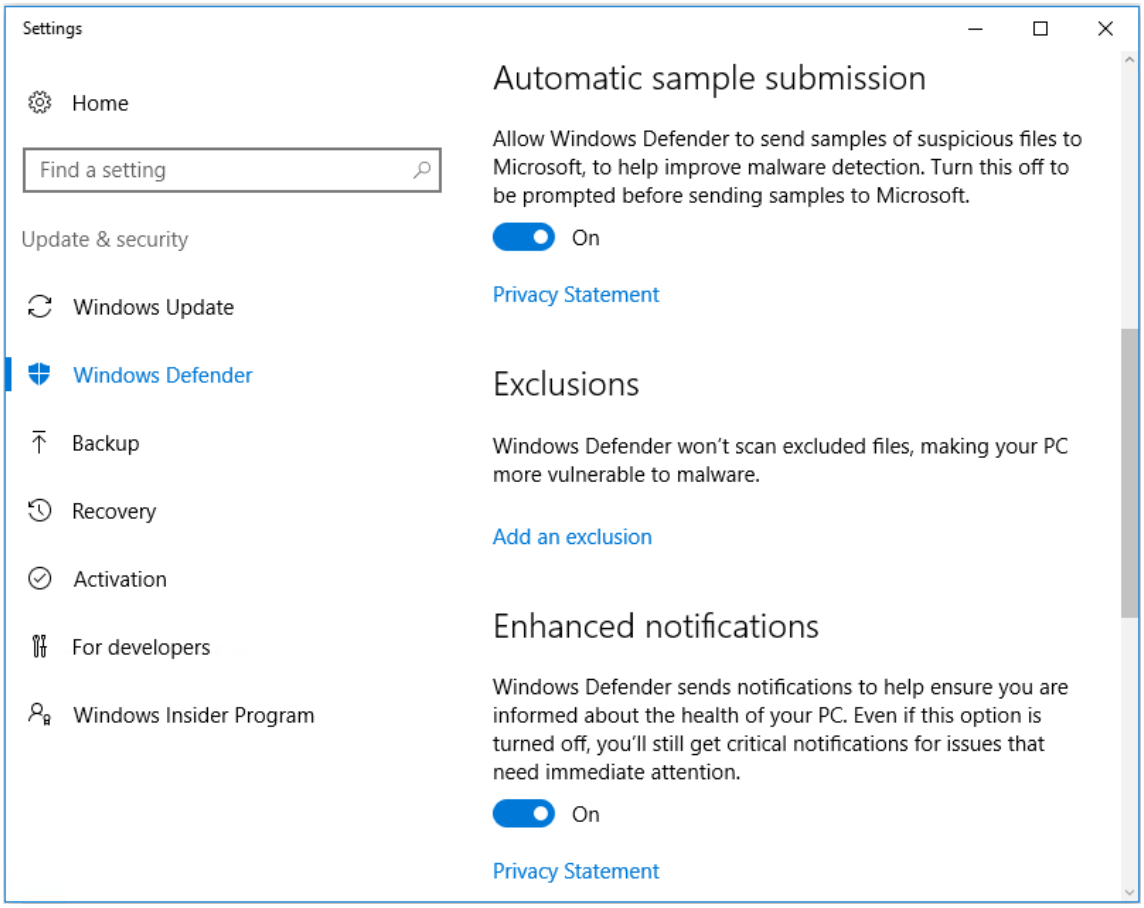
1. Ouvrez une session sur votre ordinateur avec des privilèges d'administrateur local.
2. Sélectionnez l'icône Windows Defender et cliquez avec le bouton droit pour afficher le bouton **Ouvrir** :



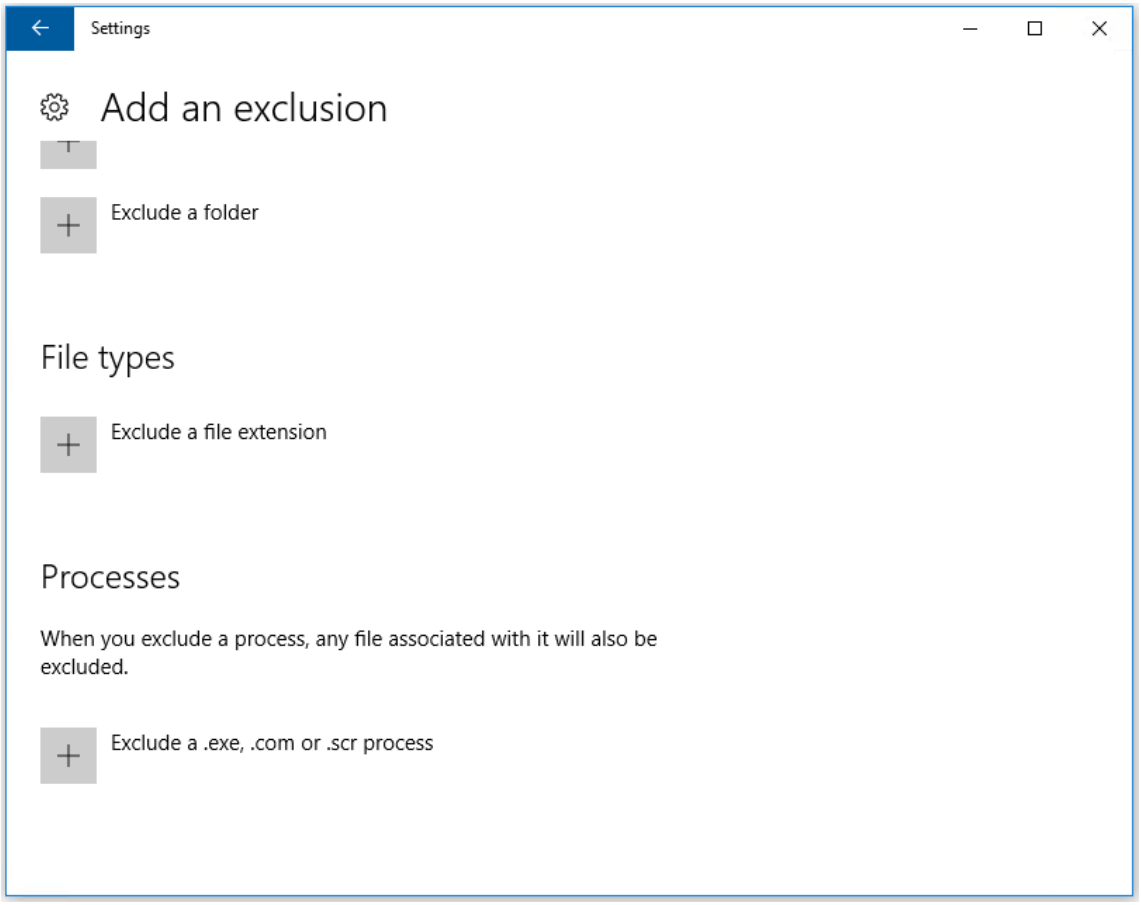
3. Dans la console Windows Defender, sélectionnez **Paramètres** dans la partie supérieure droite de l'interface :

   image localisée](/en-us/xenapp-and-xendesktop/7-15-ltsr/media/wd-main-page.png)

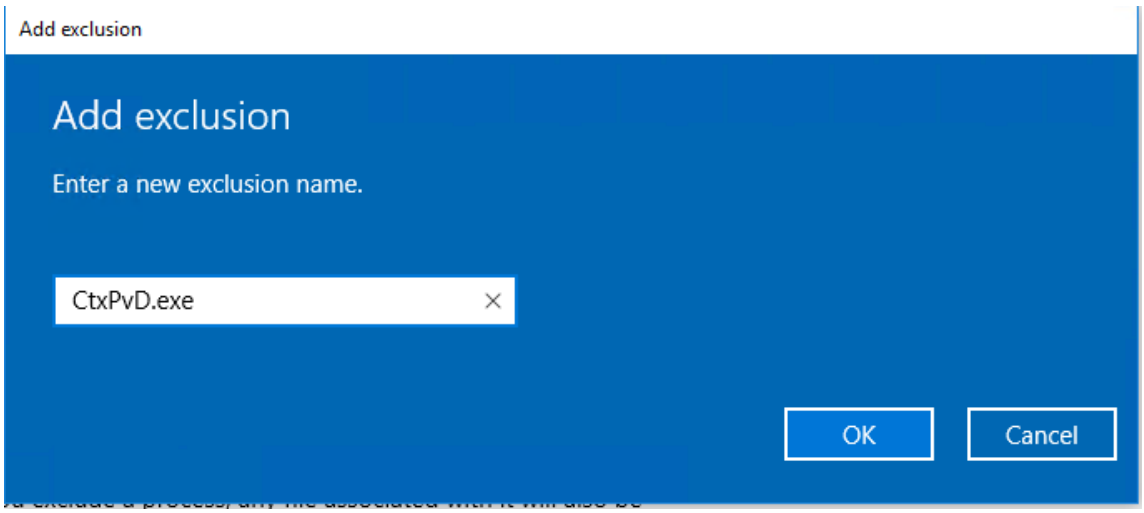
4. Dans la section **Exclusions** de l'écran Paramètres, cliquez sur **Ajouter une exclusion** :



5. Dans l'écran **Ajouter une exclusion**, sélectionnez **Exclure un processus .exe, .com ou .scr.** :



6. Dans l'écran **Ajouter une exclusion**, entrez le nom de l'exclusion ; **CtxPvD.exe** et **CtxPvDSvc.exe** doivent être ajoutés afin d'éviter les conflits lors de la création d'un AppDisk. Après avoir entré le nom de l'exclusion, cliquez sur **OK** :



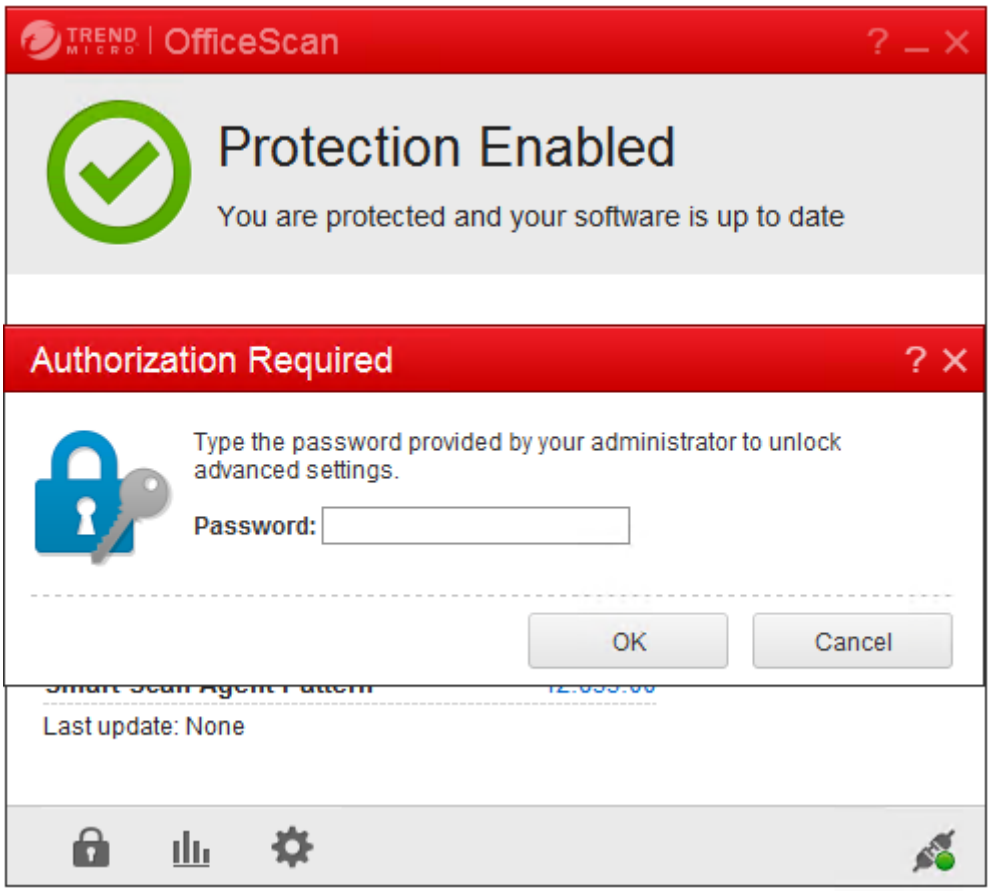
Lorsque vous ajoutez des exclusions, elles apparaissent dans la liste des processus exclus sur l'écran **Paramètres** :


```
1 ![image localiséé](/en-us/xenapp-and-xendesktop/7-15-ltsr/media/wd-
    process-added.png)
```

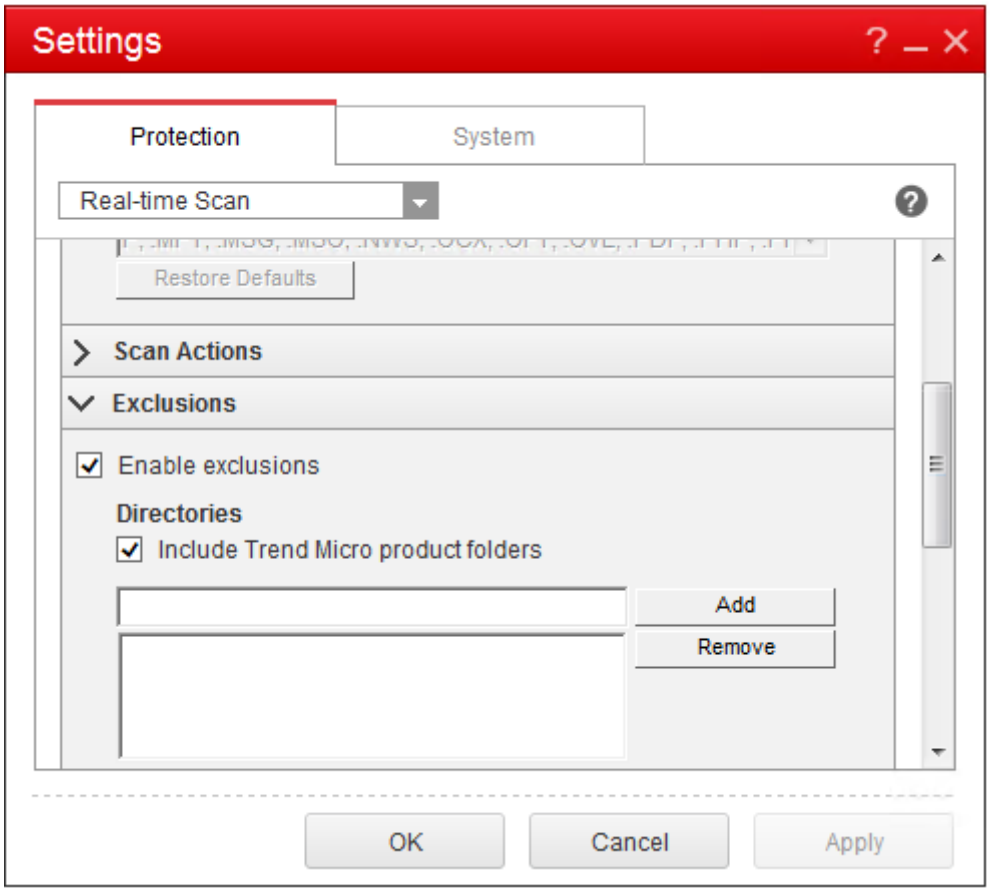
OfficeScan

Si votre VM de base utilise OfficeScan (version 11) :

1. Démarrez la console OfficeScan.
2. Cliquez sur l'icône de verrouillage dans la partie inférieure gauche de l'interface, et entrez votre mot de passe :

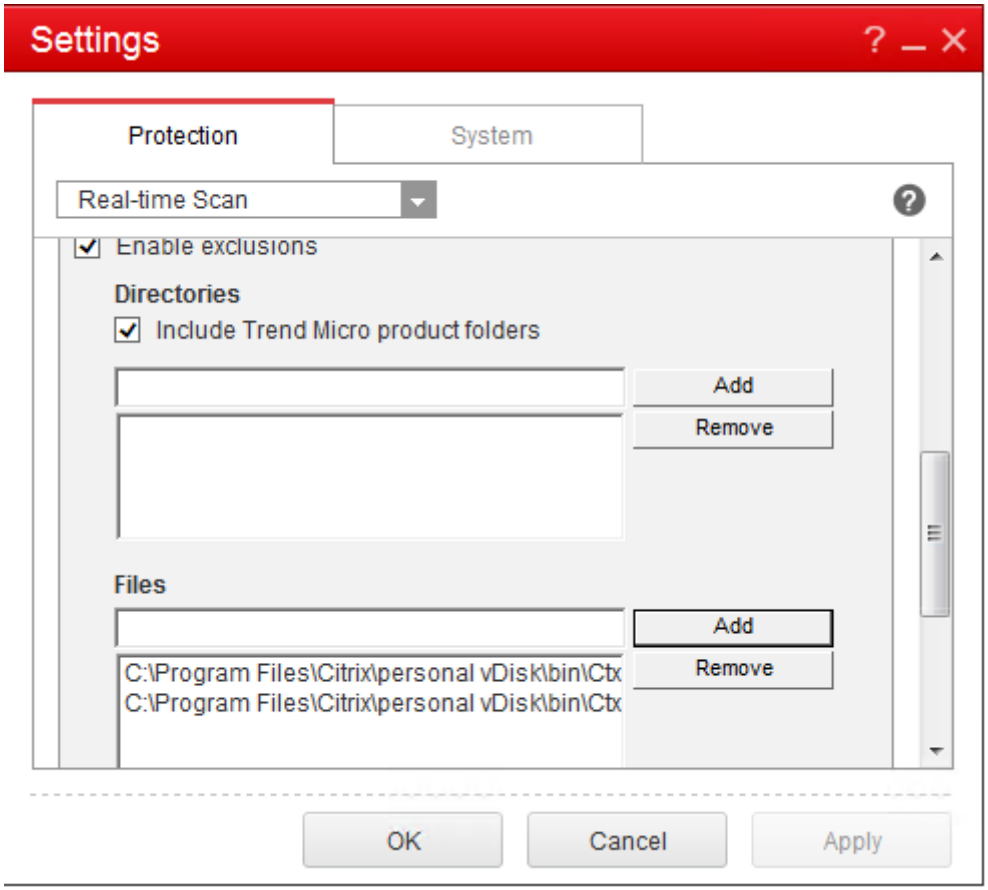


3. Cliquez sur l'icône **Paramètres** pour afficher les options de configuration :
4. Dans l'écran Paramètres, sélectionnez l'onglet **Protection**.
5. Dans l'onglet Protection, faites défiler jusqu'à la section **Exclusions**.



6. Dans la section **Fichiers**, cliquez sur **Ajouter** et entrez les processus AppDisk suivants à la liste des exceptions :

```
C:\Program Files\Citrix\personal vDisk\bin\CtxPvD.exe
C:\Program Files\Citrix\personal vDisk\bin\CtxPvDSvc.exe
```

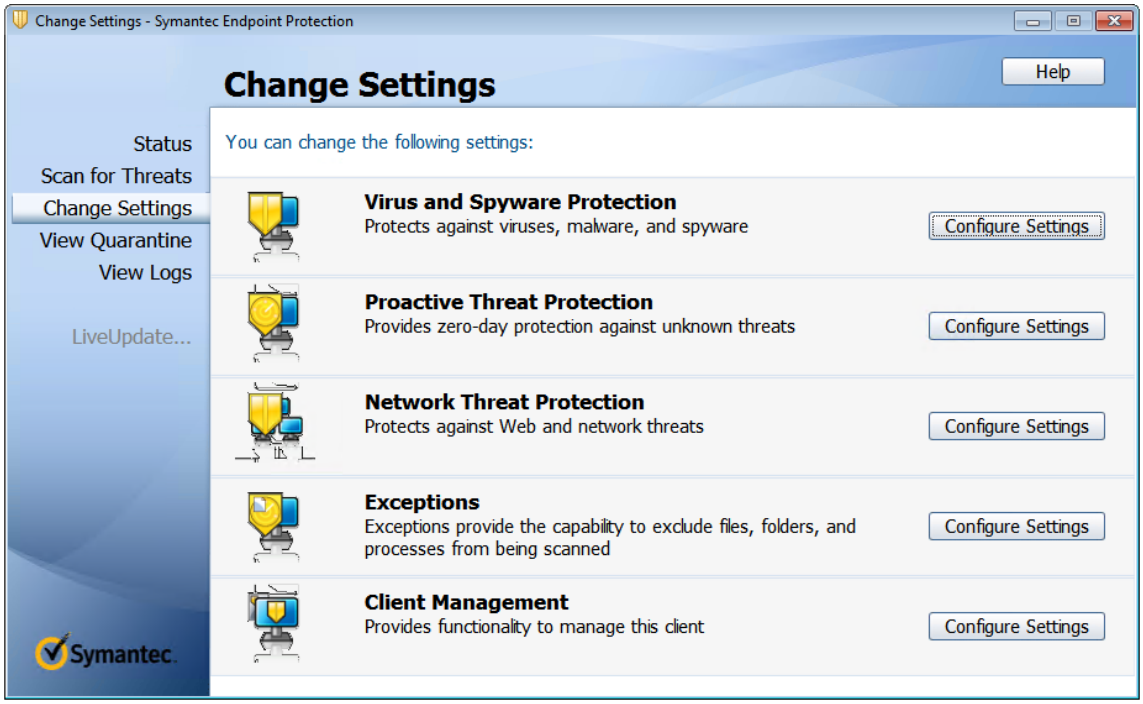



Cliquez sur **Appliquer**, puis sur **OK** pour ajouter les exclusions.

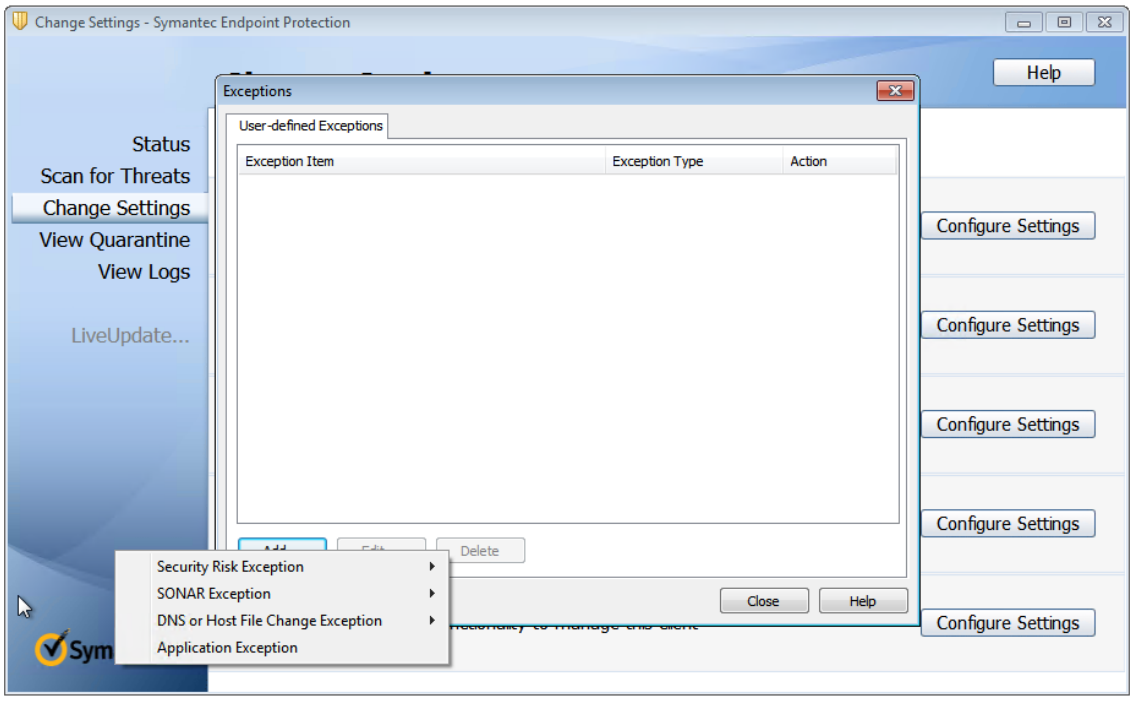
Symantec

Si votre VM de base utilise Symantec (version 12.1.16) :

1. Démarrez la console Symantec.
2. Cliquez sur **Modifier les paramètres**.
3. Dans la section **Exceptions**, cliquez sur **Configurer les paramètres** :

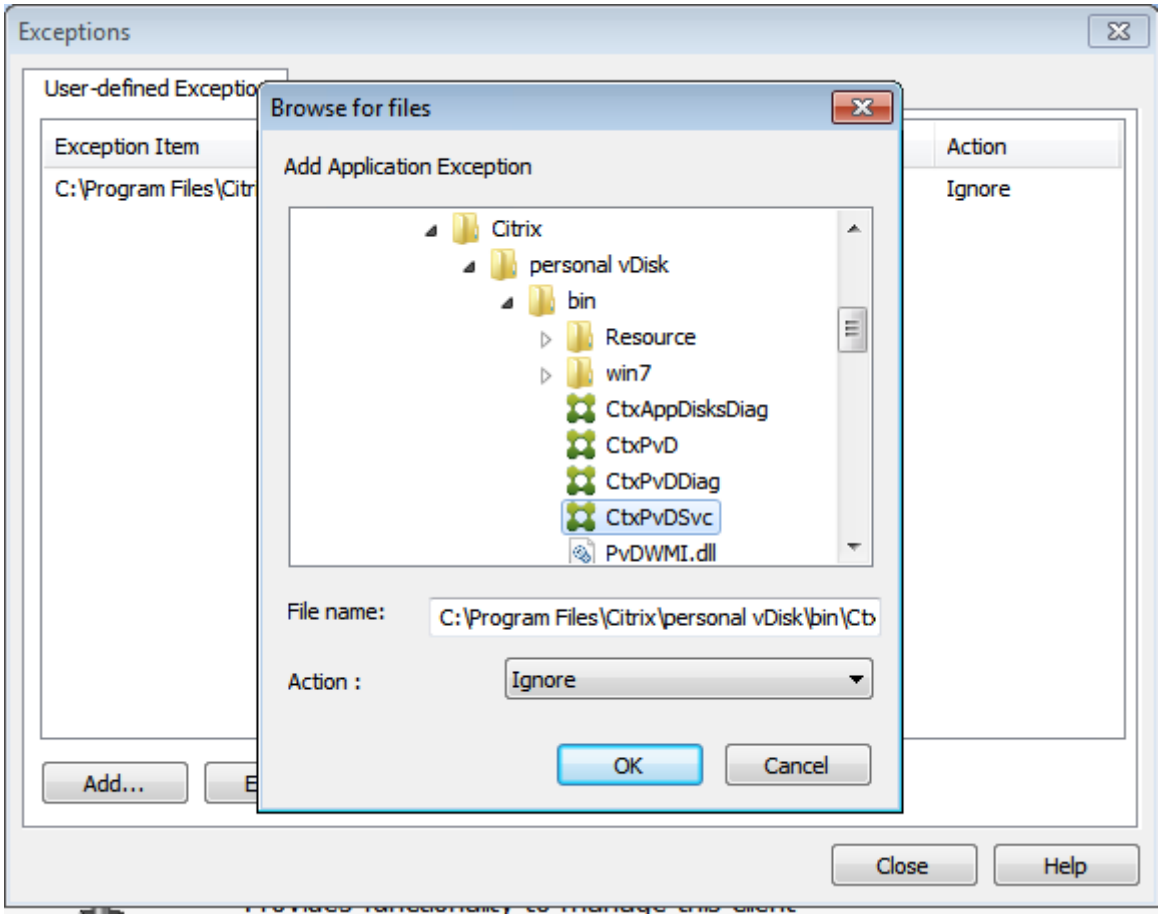


4. Dans l'écran Configurer les paramètres, cliquez sur **Ajouter**.
5. Lorsque vous cliquez sur Ajouter, un menu contextuel s'affiche pour vous permettre de spécifier le type d'application. Sélectionnez **Exception d'application** :

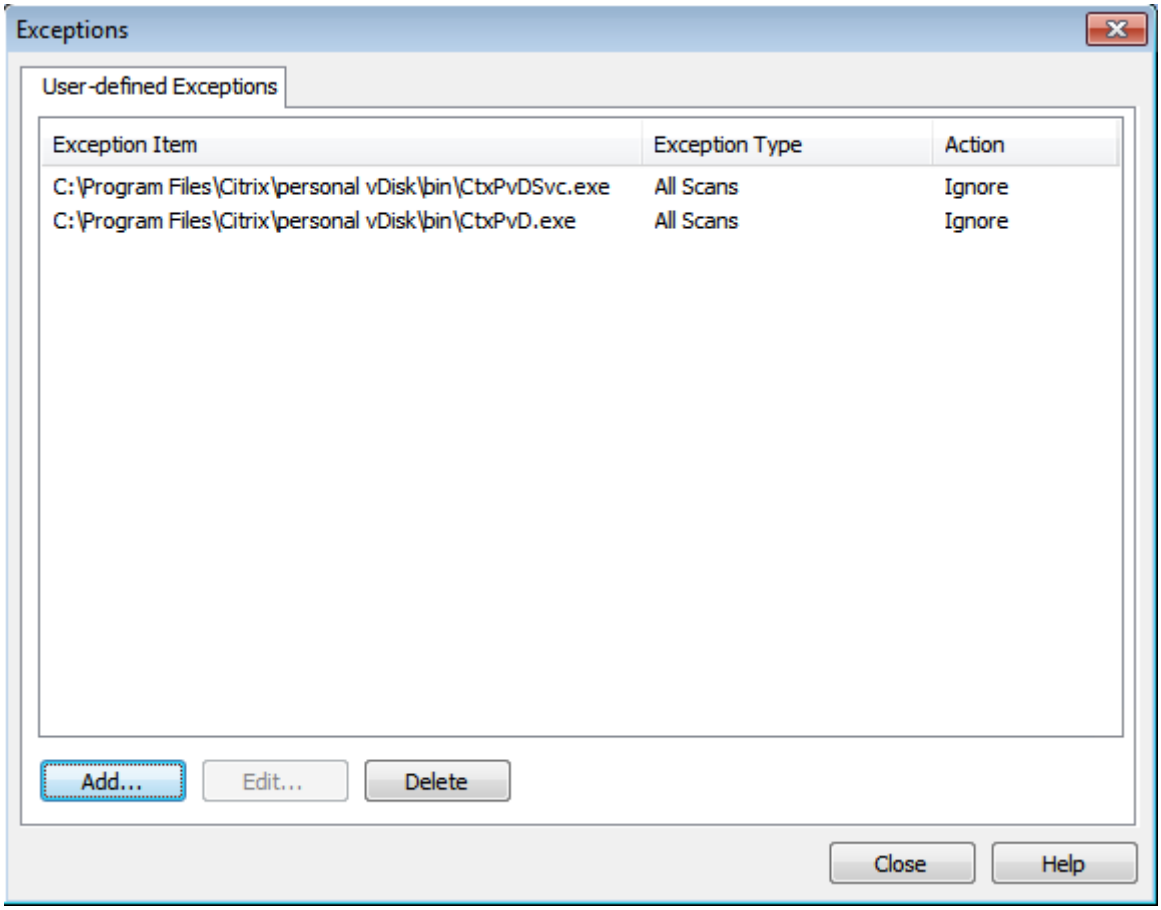


6. Dans l'écran Exceptions, entrez les chemins d'accès AppDisk suivants et définissez l'action sur **Ignorer** :


```
C:\Program Files\Citrix\personal vDisk\bin\CtxPvD.exe
C:\Program Files\Citrix\personal vDisk\bin\CtxPvDSvc.exe
```



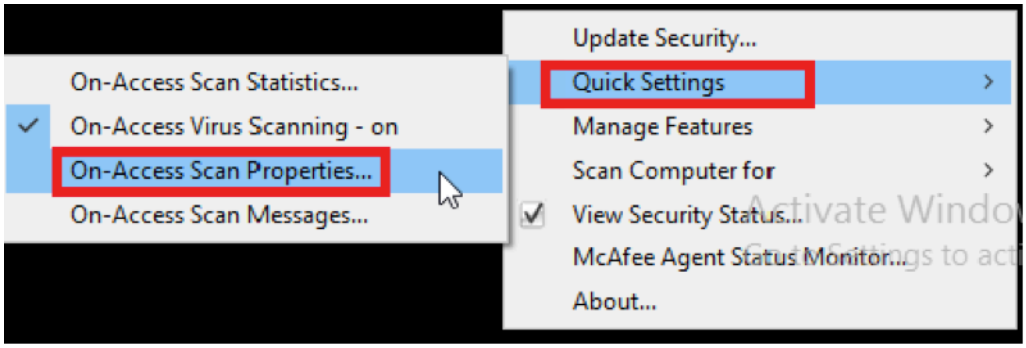
Les exceptions indiquées sont ajoutées à la liste. Fermez la fenêtre pour appliquer vos modifications :



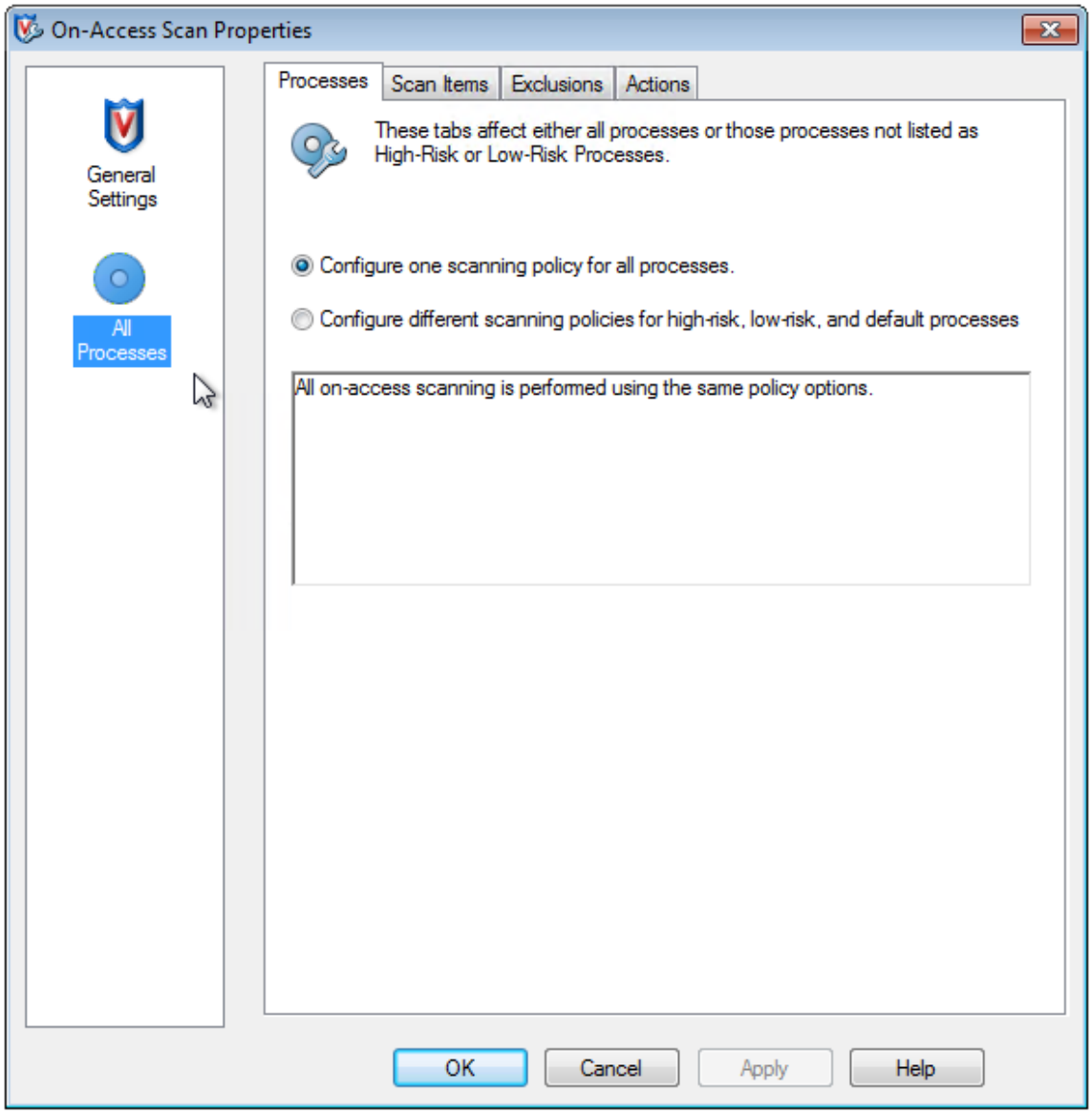
McAfee

Si votre VM de base utilise McAfee (version 4.8) :

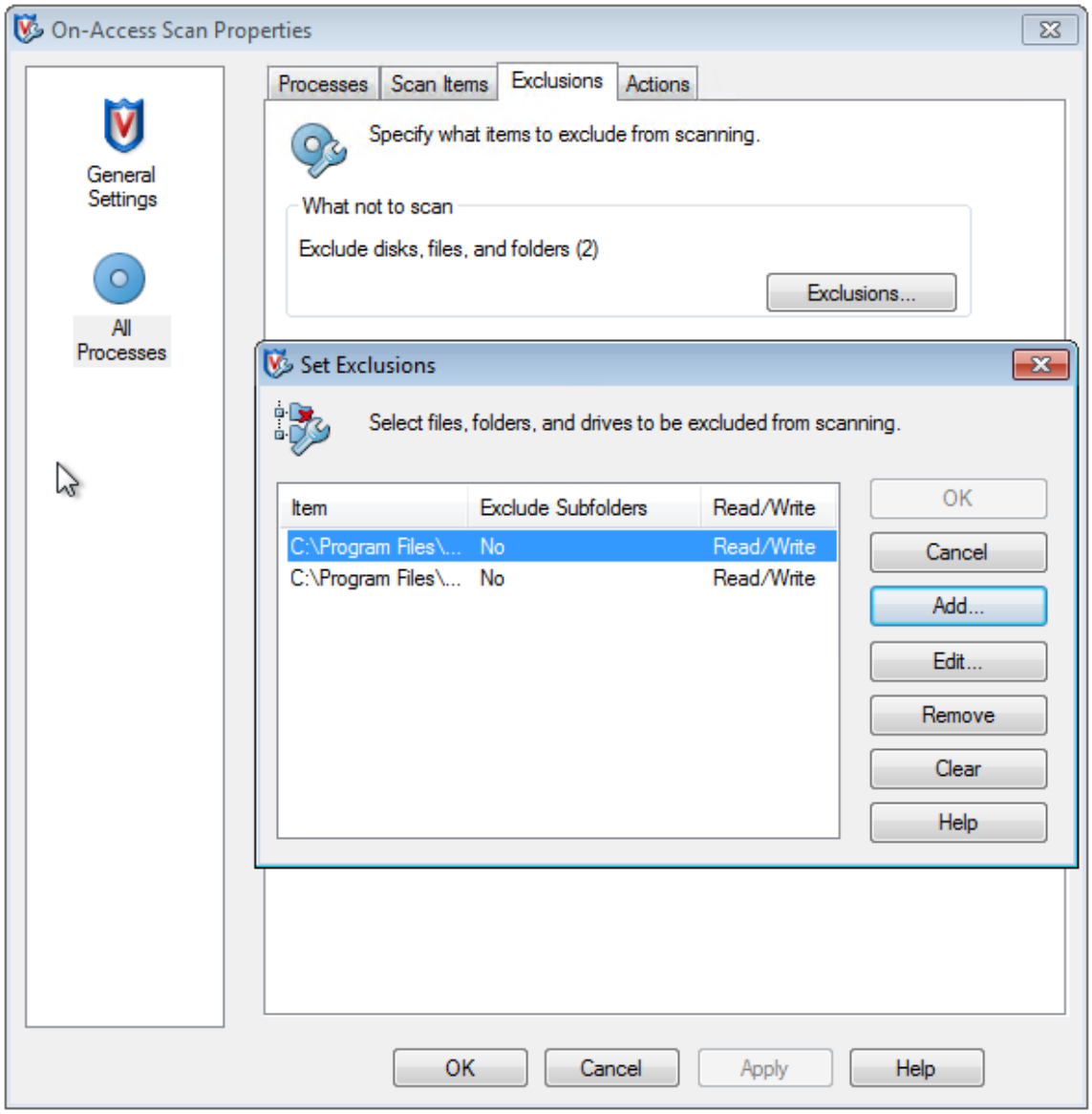
1. Cliquez avec le bouton droit sur l'icône McAfee et développez l'option **Paramètres rapides**.
2. Dans le menu développé, sélectionnez **On-Access Scan Properties** (Propriétés d'analyse lors de l'accès) :



3. Dans l'écran **On-Access Scan Properties** (Propriétés d'analyse lors de l'accès), cliquez sur **All Processes** (Tous les processus) :



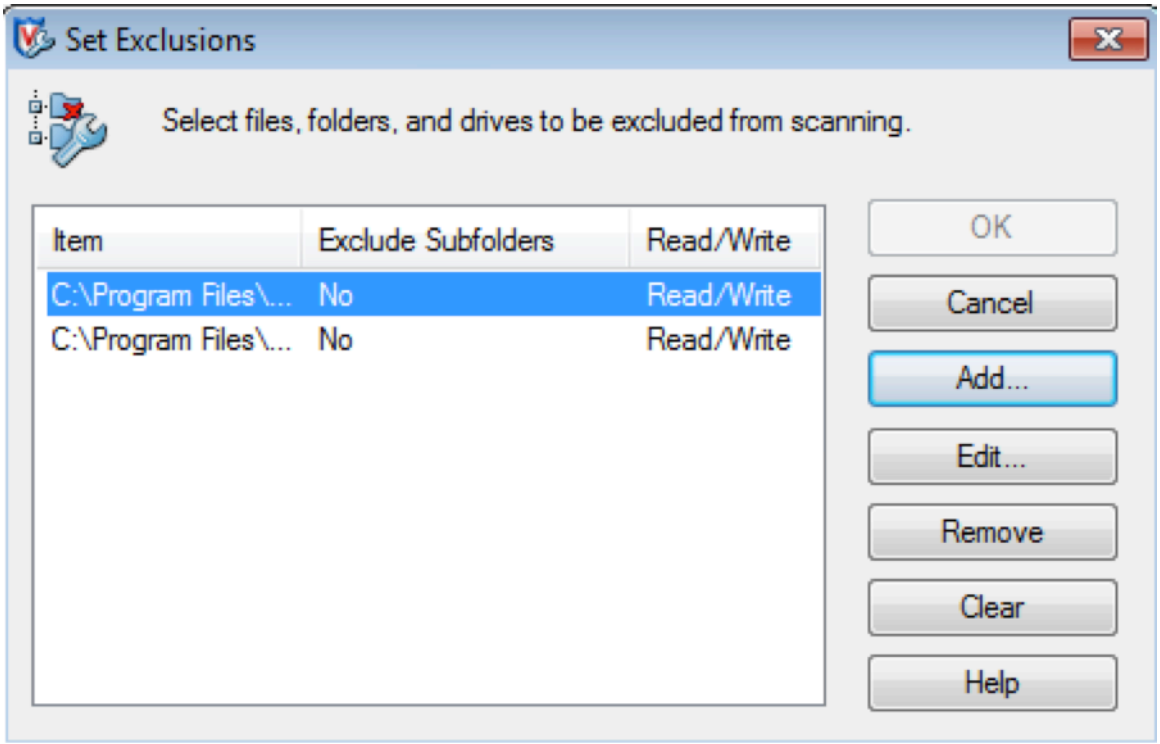
4. Sélectionnez l'onglet **Exclusions**.
5. Cliquez sur le bouton **Exclusions**.
6. Dans l'écran **Set Exclusions** (Définir des exclusions), cliquez sur **Add** (Ajouter) :



7. Dans l'écran **Add Exclusion Item** (Ajouter un élément d'exclusion), sélectionnez **By name/location (can include wildcards * or ?)** (Par nom/emplacement (peut inclure les caractères génériques * ou ?)). Cliquez sur **Parcourir** pour accéder aux fichiers exécutables d'exclusion :

```
C:\Program Files\Citrix\personal vDisk\bin\CtxPvD.exe
C:\Program Files\Citrix\personal vDisk\bin\CtxPvDSvc.exe
```

Cliquez sur **OK**. L'écran **Set Exclusions** affiche maintenant les exclusions ajoutées. Cliquez sur **OK** pour appliquer les modifications :



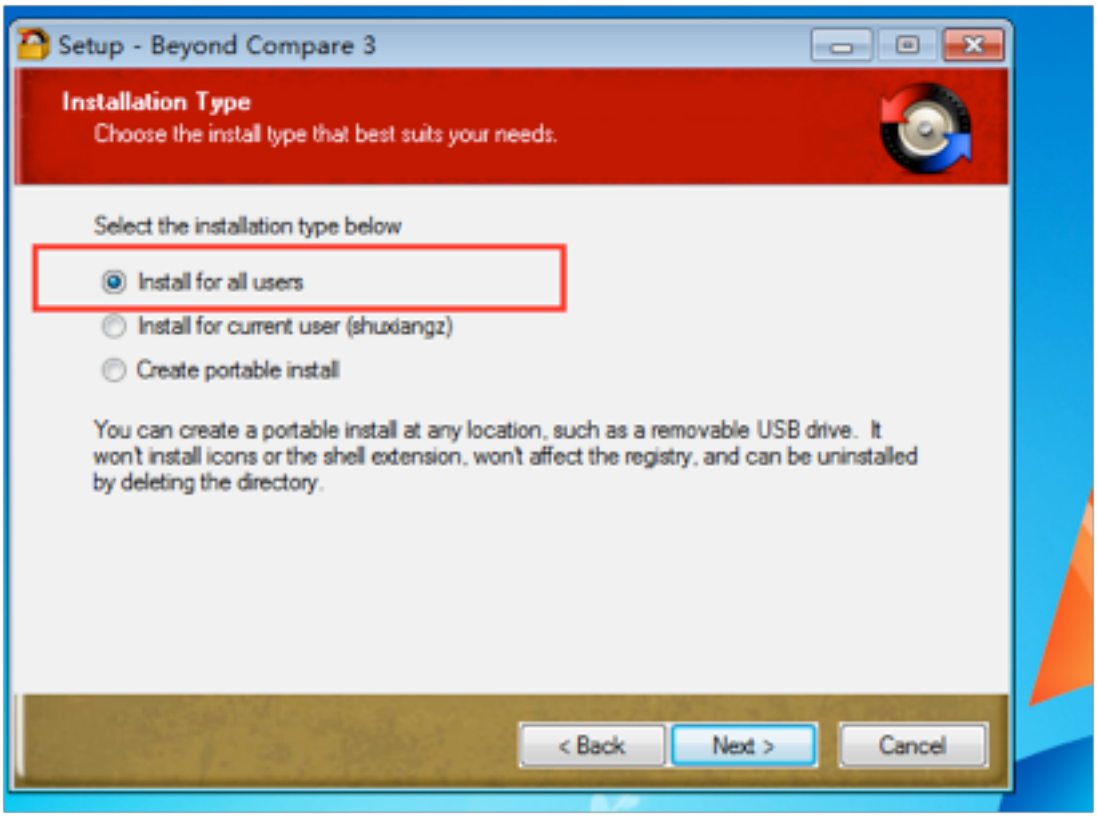
> **Remarque :**
>
> Après avoir configuré ces exclusions, créez le AppDisk.

Affichage des applications dans le menu Démarrer

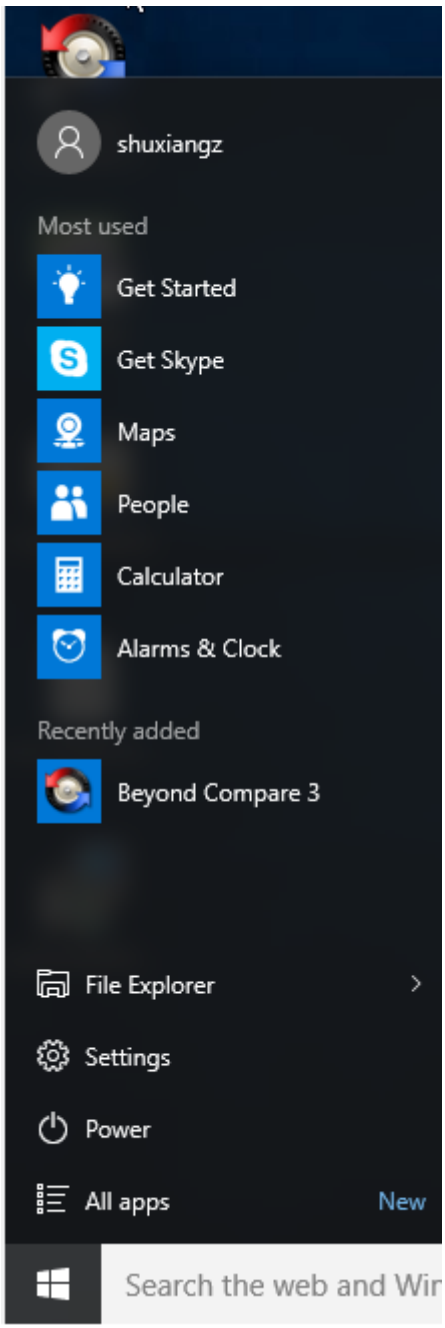
Si un nouveau AppDisk est créé et qu'une application est disponible pour tous les utilisateurs, le disque est connecté au bureau et un raccourci s'affiche pour l'application dans le menu Démarrer. Lorsqu'un AppDisk est créé et installé pour l'utilisateur actuel uniquement et que le disque est connecté au bureau, le raccourci de l'application ne parvient pas à s'afficher dans le menu Démarrer.

Pour créer une nouvelle application et la mettre à disposition de tous les utilisateurs

1. Installez une application sur le AppDisk (par exemple, *Beyond Compare* est l'application sélectionnée) :

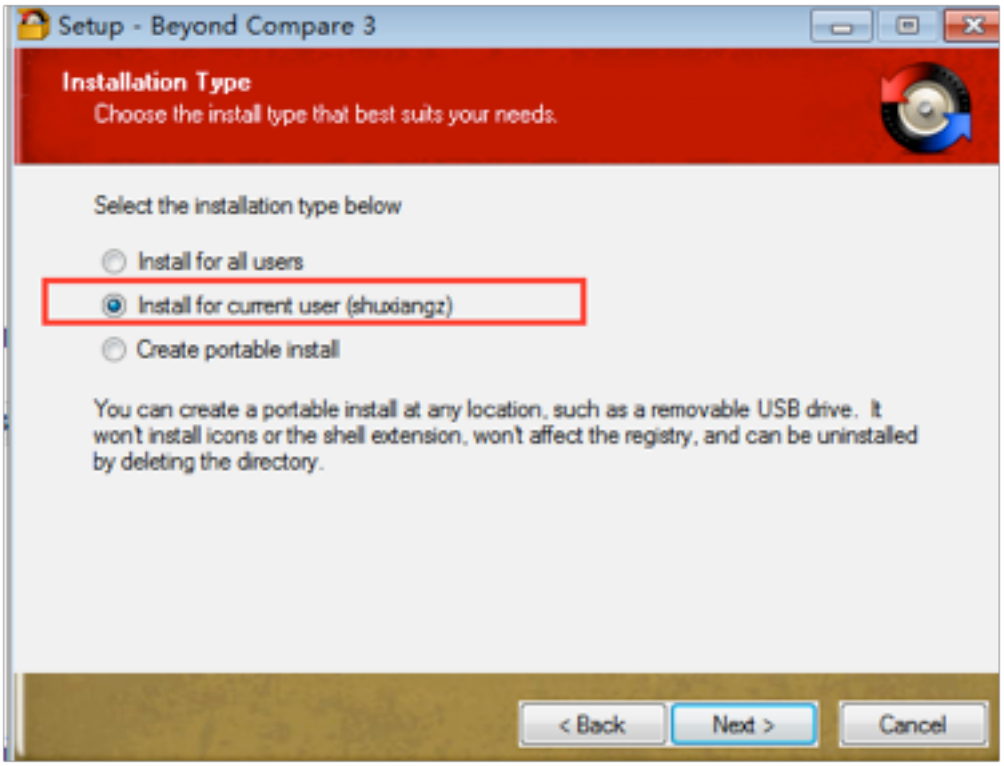


2. Connectez le disque au bureau ; le raccourci de l'application nouvellement installée (*Beyond Compare*) s'affiche dans le menu Démarrer :

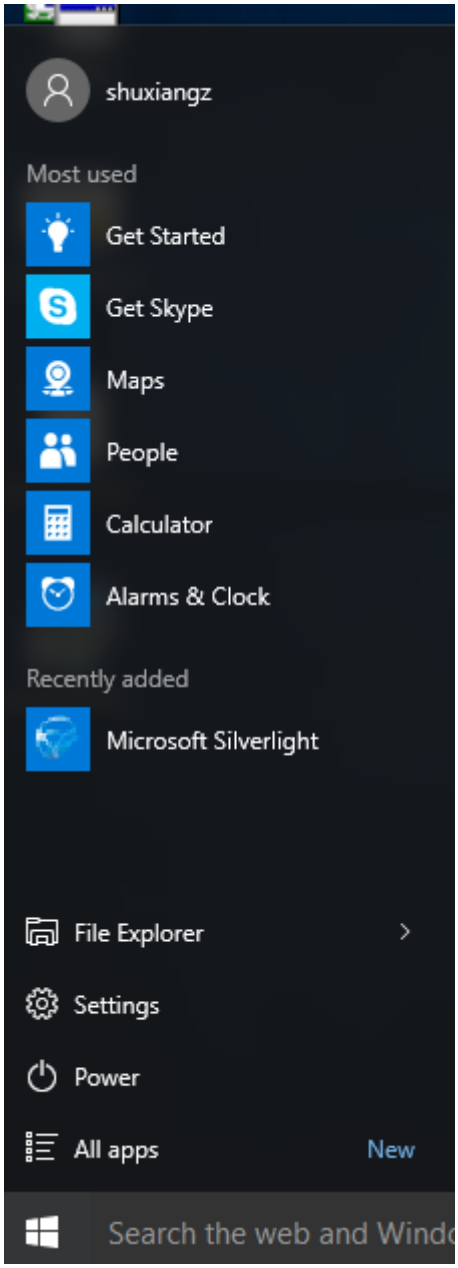


Pour installer une application pour l'utilisateur actuel uniquement

1. Installez une application sur le AppDisk et mettez-la à disposition de l'utilisateur actuel :



2. Connectez le disque au bureau ; notez que le raccourci ne s'affiche pas dans le menu Démarrer :



Mises à jour de la journalisation des AppDisk

Cette version améliore la prise en charge et la journalisation des AppDisk. Avec cette mise à jour, les utilisateurs de AppDisk peuvent maintenant obtenir des informations de diagnostic et éventuellement les charger sur le site Web de Citrix Insight Services (CIS).

Fonctionnement

Cette nouvelle fonctionnalité utilise un nouvel outil PowerShell basé sur des scripts qui identifie tous les fichiers journaux créés par AppDisk/PVD, collecte les résultats des commandes PowerShell contenant des informations sur le système (et les processus), compresse toutes ces informations dans un seul fichier et enfin offre la possibilité d'enregistrer le dossier compressé localement, ou de le charger sur CIS (Citrix Insight Services).

> **Remarque :**
>
> CIS collecte des informations de diagnostic anonymes qu'il utilise pour améliorer les fonctionnalités de AppDisk/PVD. Accédez au site Web Citrix Insight Services (CIS) pour charger manuellement le pack de diagnostic. Vous devez ouvrir une session avec vos informations d'identification Citrix pour accéder à ce site.

Utilisation de scripts PowerShell pour collecter les fichiers journaux de AppDisk/PVD

Le programme d'installation de AppDisk/PVD ajoute deux nouveaux scripts pour la collecte de données de diagnostic :

- **Upload-AppDDiags.ps1** – collecte les données de diagnostic AppDisk
- **Upload-PvDDiags.ps1** – collecte les données de diagnostic PvD

> **Remarque :**
>
> Ces scripts se trouvent dans C:\Program Files\Citrix\personal vDisk\bin\scripts. Vous devez exécuter ces scripts PowerShell en tant qu'administrateur.

Utilisez le script **Upload-AppDDiags.ps1** pour lancer la collecte des données de diagnostic AppDisk. Vous pouvez éventuellement charger les données manuellement sur le site Web CIS.

```
SYNTAXE
     Upload-AppDDiags [[-OutputFile] <string>] [-help] [<
        CommonParameters>]
         -OutputFile
             Chemin local pour le fichier zip au lieu de charger vers
                CIS
 EXEMPLES
     Upload-AppDDiags
         Charge les données de diagnostic sur le site Web Citrix CIS à
            l'aide des informations d'identification saisies par l'
            utilisateur interactif.
     Upload-AppDDiags -OutputFile C:\MyDiags.zip
         Enregistre les données de diagnostic AppDisk dans le fichier
            zip spécifié. Vous pouvez accéder à https://cis.citrix.com/
             pour le charger plus tard.
```


> **Conseil :**
>
> Lorsque l'argument **–OutputFile** n'est pas présent, le chargement se produit. Si **–OutputFile** est spécifié, le script crée un fichier zip que vous pouvez charger manuellement ultérieurement.

Utilisez le script **Upload-PvDDiags.ps1** pour lancer la collecte des données de diagnostic PvD. Vous pouvez éventuellement charger les données manuellement sur le site Web CIS.

```
SYNTAXE
 Upload-PvDDiags [[-OutputFile] <string>] [-help] [<CommonParameters>]
     -OutputFile
         Chemin local pour le fichier zip au lieu de charger vers CIS
 EXEMPLES
     Upload-PvDDiags
         Charge les données de diagnostic PvD sur le site Web Citrix
            CIS à l'aide des informations d'identification saisies par
            l'utilisateur interactif.
     Upload-PvDDiags -OutputFile C:\MyDiags.zip
         Enregistre les données de diagnostic PvD dans le fichier zip
            spécifié. Vous pouvez accéder à https://cis.citrix.com/
            pour le charger plus tard.
```

> **Conseil :**
>
> Lorsque l'argument **–OutputFile** n'est pas présent, le chargement se produit. Si **–OutputFile** est spécifié, le script crée un fichier zip que vous pouvez charger manuellement ultérieurement.

XenApp Secure Browser

January 23, 2019

Étant donné que les applications sont portées vers le Web, les utilisateurs doivent avoir recours à plusieurs fournisseurs et versions de navigateur pour assurer la compatibilité avec les applications Web. Si l'application est une application hébergée en interne, les organisations sont souvent obligées d'installer et de configurer des solutions VPN complexes pour fournir un accès aux utilisateurs distants. Les solutions VPN standard requièrent un agent côté client qui doit être maintenu sur de nombreux systèmes d'exploitation.

With the XenApp Secure Browser, users can have a seamless web-based application experience where a hosted web-based application simply appears within the user's preferred local browser. Par exemple, le navigateur par défaut d'un utilisateur est Mozilla Firefox, mais l'application est uniquement compatible avec Microsoft Internet Explorer. XenApp Secure Browser affiche l'application compatible avec Internet Explorer en tant qu'onglet du navigateur Firefox.

Déploiement de XenApp Secure Browser

Citrix vous recommande de tirer parti du modèle Citrix Smart Tools pour XenApp Secure Browser pour en faciliter le déploiement.

XenApp Secure Browser comprend des scripts permettant d'automatiser les tâches suivantes :

- Installer XenApp, y compris le serveur de licences Citrix et StoreFront
- Créer un site de mise à disposition XenApp
- Joindre les machines provisionnées à votre domaine

Utilisation de Citrix Smart Tools

Pour utiliser Citrix Smart Tools :

1. Dans la page d'accueil Citrix Cloud, accédez à Services ; cliquez sur Request Trial for Citrix Smart Tools. Lorsque vous effectuez une demande de version d'évaluation, vous recevez un e-mail vous informant que le service d'évaluation est disponible. Cet e-mail est généralement envoyé au bout de 5-10 minutes.
2. Cliquez sur Manage dans l'e-mail que vous avez reçu après avoir demandé l'affichage de la page d'accueil de Citrix Smart Tools.
3. Téléchargez l'ISO Citrix XenApp Secure Browser Edition depuis le site de téléchargement Citrix.

Prenez en compte les points suivants après le téléchargement de l'ISO Secure Browser Edition :

- Commencez à utiliser XenApp Secure Browser en suivant les instructions fournies dans XenApp Secure Installation with a Citrix Smart Tools Blueprint.
- Après avoir effectué l'installation, optimisez votre environnement pour la mise à disposition d'applications Web à l'aide de la procédure de configuration spécifiée dans le Guide de déploiement de XenApp Secure Browser.

Installation manuelle de XenApp Secure Browser

Pour installer manuellement XenApp Secure Browser :

1. Téléchargez l'ISO Citrix XenApp Secure Browser Edition depuis le site de téléchargement Citrix.
2. Suivez les instructions d'installation des composants de XenApp.
3. Configurez le mode de licence et l'édition de Secure Browser après l'installation, en effectuant les étapes supplémentaires suivantes :
    a) Sur le Delivery Controller, démarrez une session PowerShell en cliquant sur l'icône bleue sur la barre des tâches, ou en accédant au menu Démarrer > Tous les programmes > Accessoires > Windows PowerShell > Windows PowerShell.

Remarque : sur les systèmes 64 bits, cela démarre la version 64 bits. Les versions 32 bits et 64 bits sont prises en charge toutes les deux.

b) Tapez Asnp Citrix* et appuyez sur Entrée pour charger les modules PowerShell spécifiques à Citrix.

Remarque : « Asnp » représente Add-PSSnapin.

c) Vérifiez les paramètres de site et le mode de licence en exécutant l'applet de commande Get-ConfigSite.

d) Définissez le mode de licence sur l'édition XenApp Secure Browser en exécutant Set-ConfigSite -ProductCode XDT -ProductEdition BAS.

e) Vérifiez que le mode de licence et l'édition de XenApp Secure Browser sont correctement définis en exécutant l'applet de commande Get-BrokerSite.

> **Remarque :**
>
> Après avoir effectué l'installation, optimisez votre environnement pour la mise à disposition d'applications Web à l'aide de la procédure de configuration spécifiée dans le Guide de déploiement de XenApp Secure Browser.

Publier du contenu

February 28, 2019

Vous pouvez publier une application qui est simplement une URL ou un chemin UNC vers une ressource, par exemple un document Microsoft Word ou un lien web. Cette fonctionnalité est appelée contenu publié. La possibilité de publier du contenu offre davantage de souplesse pour livrer le contenu aux utilisateurs. Vous bénéficiez du contrôle d'accès et de la gestion des applications existants. De plus, vous pouvez spécifier les applications à utiliser pour ouvrir le contenu : locales ou publiées.

Le contenu publié apparaît comme d'autres applications dans StoreFront et Citrix Receiver. Les utilisateurs y accèdent de la même façon qu'ils accèdent aux applications. Sur le client, la ressource s'ouvre comme d'habitude.

- Si une application installée localement est appropriée, elle est lancée pour ouvrir la ressource.
- Si une association de type de fichier a été définie, une application publiée est lancée pour ouvrir la ressource.

Vous publiez contenu à l'aide du SDK PowerShell. (Vous ne pouvez pas utiliser Studio pour publier le contenu. Cependant, vous pouvez utiliser Studio pour modifier les propriétés d'application plus tard, après leur publication.)

Présentation et préparation de la configuration

La publication de contenu utilise l'applet de commande New-BrokerApplication avec les principales propriétés suivantes. (Reportez-vous à l'aide de l'applet de commande pour obtenir une description de toutes les propriétés de l'applet de commande).

```
New-BrokerApplication -ApplicationType PublishedContent
\-CommandLineExecutable \<*emplacement*> -Name \<*nom-appli*>
\-DesktopGroup \<*nom-groupe-miseàdisposition*>
```

La propriété ApplicationType doit être PublishedContent.

La propriété CommandLineExecutable spécifie l'emplacement du contenu publié. Les formats suivants sont pris en charge, avec une limite de 255 caractères.

- adresse de site Web HTML (`https://www.citrix.com`, par exemple) ;
- fichier de document sur un serveur Web (`https://www.citrix.com/press/pressrelease.doc`, par exemple) ;
- répertoire sur un serveur FTP (`ftp://ftp.citrix.com/code`, par exemple) ;
- fichier de document sur un serveur FTP (`ftp://ftp.citrix.com/code/Readme.txt`, par exemple) ;
- chemin de répertoire UNC (`file://myServer/myShare` ou `\\myServer\myShare`, par exemple) ;
- chemin de fichier UNC (`file://myServer/myShare/myFile.asf` ou `\\myServer\myShare\myFile.asf`, par exemple).

Assurez-vous que vous disposez du kit de développement logiciel correct.

- Pour les déploiements des services XenApp et XenDesktop, téléchargez et installez le SDK PowerShell à distance de XenApp et XenDesktop.
- Pour les déploiements sur site XenApp et XenDesktop, utilisez le SDK PowerShell qui est installé avec le Delivery Controller. L'ajout d'une application avec contenu publié requiert une version minimale de 7.11 pour le Delivery Controller.

Les procédures suivantes utilisent des exemples. Dans les exemples :

- Un catalogue de machines a été créé.
- Un groupe de mise à disposition nommé PublishedContentApps a été créé. Le groupe utilise une machine avec OS de serveur du catalogue. L'application WordPad a été ajoutée au groupe.
- Les affectations sont effectuées pour le nom du groupe de mise à disposition, l'emplacement de CommandLineExecutable et le nom de l'application.

Mise en route

Sur la machine contenant le SDK PowerShell, ouvrez PowerShell.

L'applet de commande suivante ajoute le composant logiciel enfichable SDK PowerShell approprié et attribue l'enregistrement de groupe de mise à disposition renvoyé.

```
Add-PsSnapin Citrix*
$dg = Get-BrokerDesktopGroup -Name PublishedContentApps
```

Si vous utilisez le service XenApp et XenDesktop, authentifiez-vous en saisissant vos informations d'identification Citrix Cloud. S'il y a plusieurs clients, choisissez-en un.

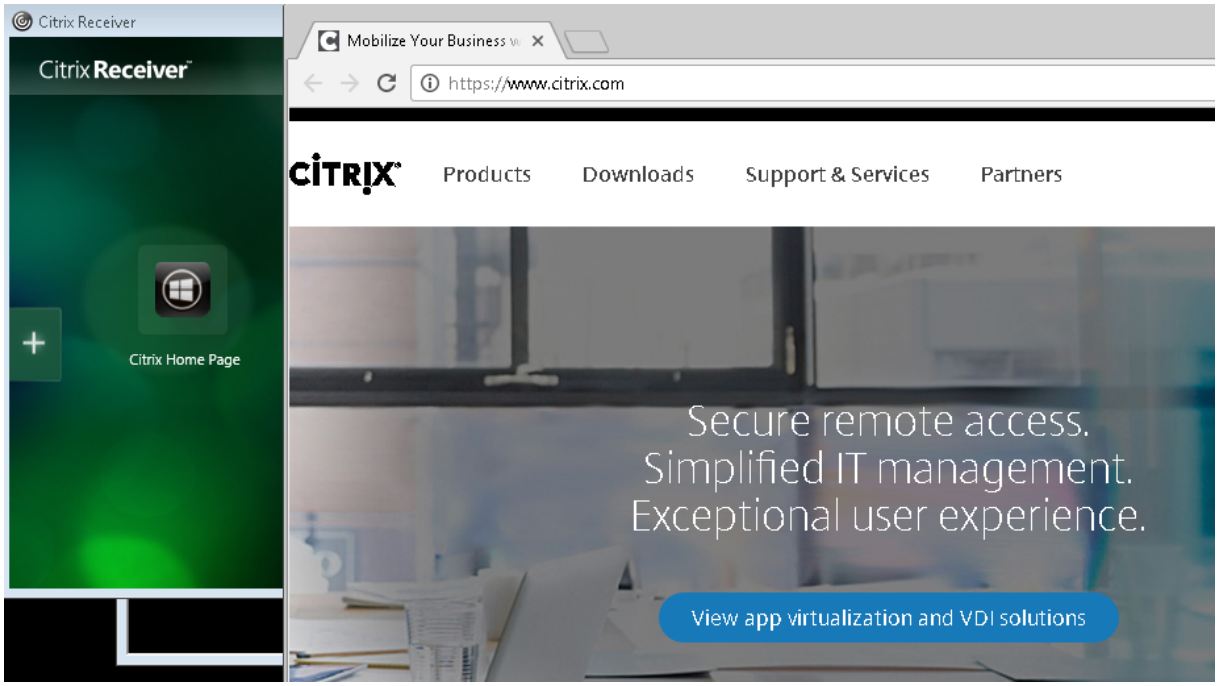
Publier une URL

Après avoir affecté l'emplacement et le nom de l'application, l'applet de commande suivante publie la page d'accueil Citrix comme application.

```
$citrixUrl = "https://www.citrix.com/"
$appName = "Citrix Home Page"

New-BrokerApplication -ApplicationType PublishedContent
 -CommandLineExecutable $citrixURL -Name $appName
 -DesktopGroup $dg.Uid
```

Vérifier si la commande a réussi

- Ouvrez StoreFront et connectez-vous en tant qu'utilisateur qui peut accéder à des applications dans le groupe de mise à disposition PublishedContentApps. L'affichage inclut l'application nouvellement créée avec l'icône par défaut. Pour en savoir plus sur la personnalisation de l'icône, voir https://www.citrix.com/blogs/2013/08/21/xd-tipster-changing-delivery-group-icons-revisited-xd7/.
- Cliquez sur l'application Citrix Home Page. L'URL s'ouvre dans un nouvel onglet dans une instance locale de votre navigateur par défaut.



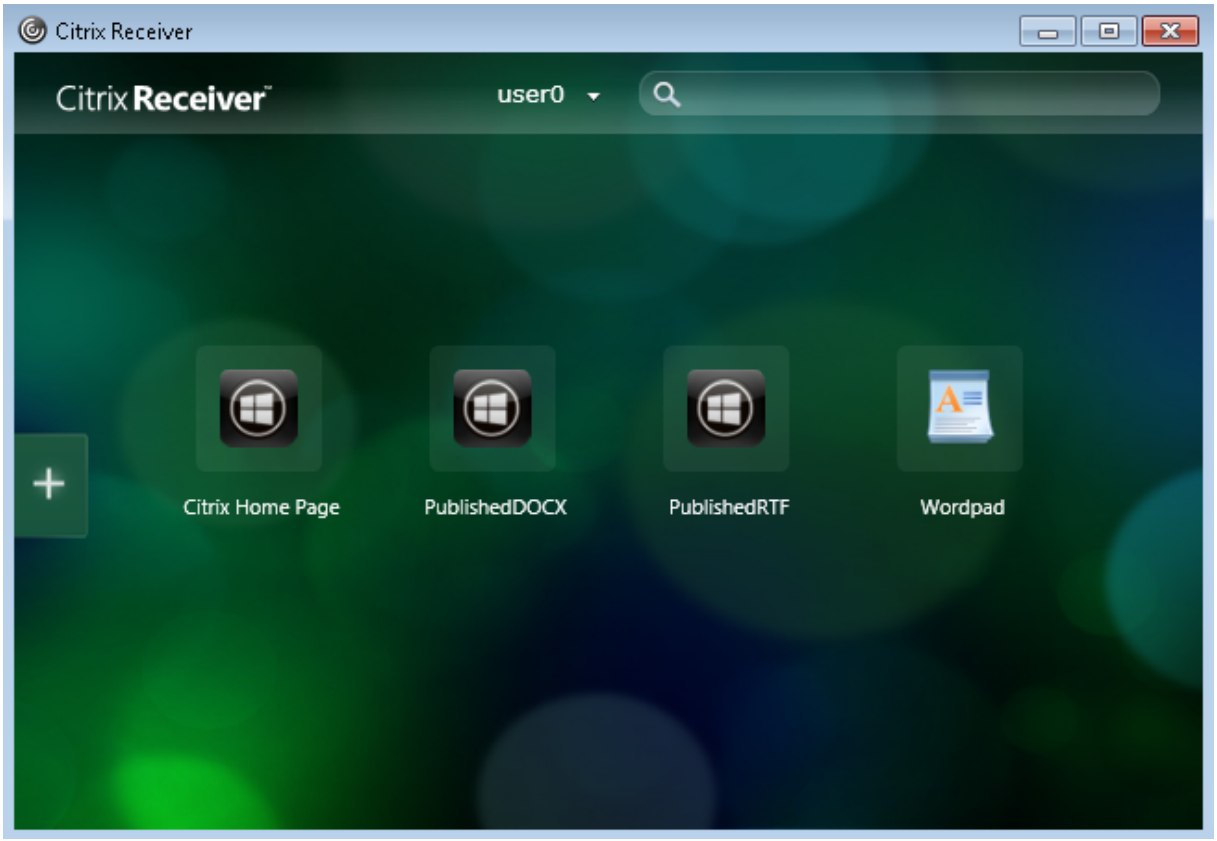
Publier des ressources situées sur des chemins UNC

Dans cet exemple, l'administrateur a déjà créé un partage nommé PublishedResources. Après avoir affecté les emplacements et les noms d'application, les applets de commande suivantes publient un fichier RTF et un fichier DOCX dans ce partage en tant que ressource.

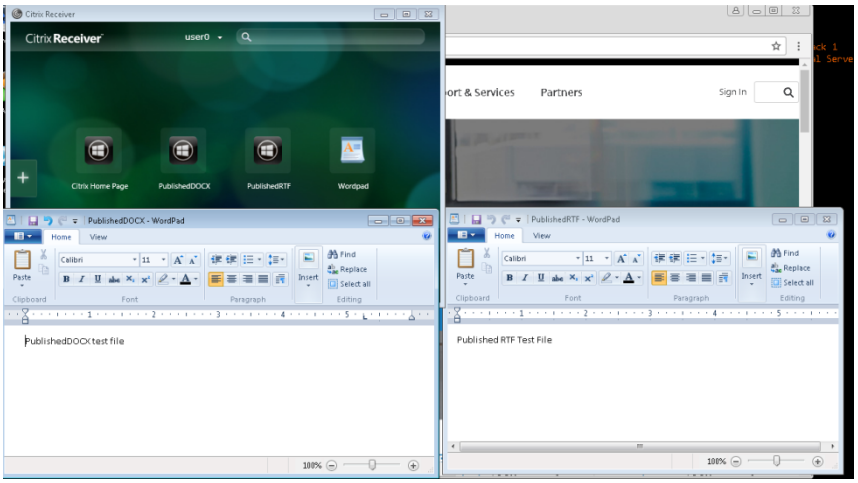
```
$rtfUNC = "\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedRTF.rtf"
$rtfAppName = "PublishedRTF"

New-BrokerApplication -ApplicationType PublishedContent
 -CommandLineExecutable $rtfUNC -Name $rtfAppName
-DesktopGroup $dg.Uid

$docxUNC = "\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedDOCX.docx
    "
$docxAppName = "PublishedDOCX"

New-BrokerApplication -ApplicationType PublishedContent
 -CommandLineExecutable $docxUNC -Name $docxAppName
-DesktopGroup $dg.Uid
```

Vérifier si la commande a réussi

- Actualisez votre fenêtre StoreFront pour voir les documents publiés récemment.

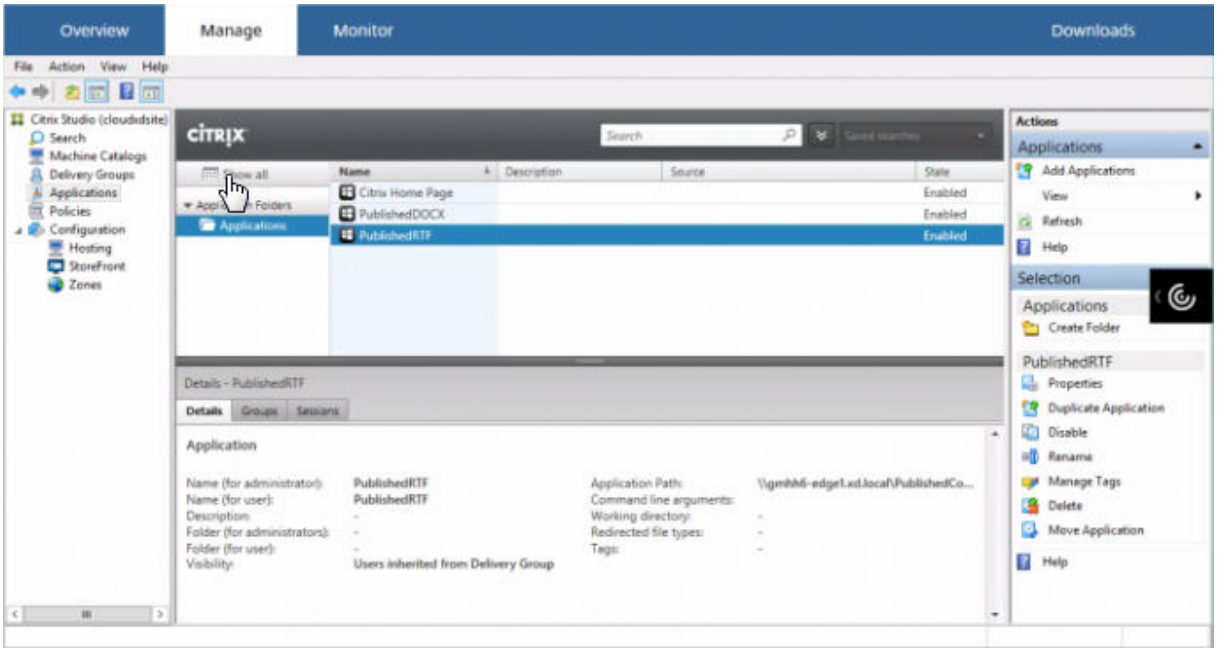


- Cliquez sur les applications PublishedRTF et PublishedDocx. Chaque document s'ouvre dans un WordPad en cours d'exécution au niveau local.

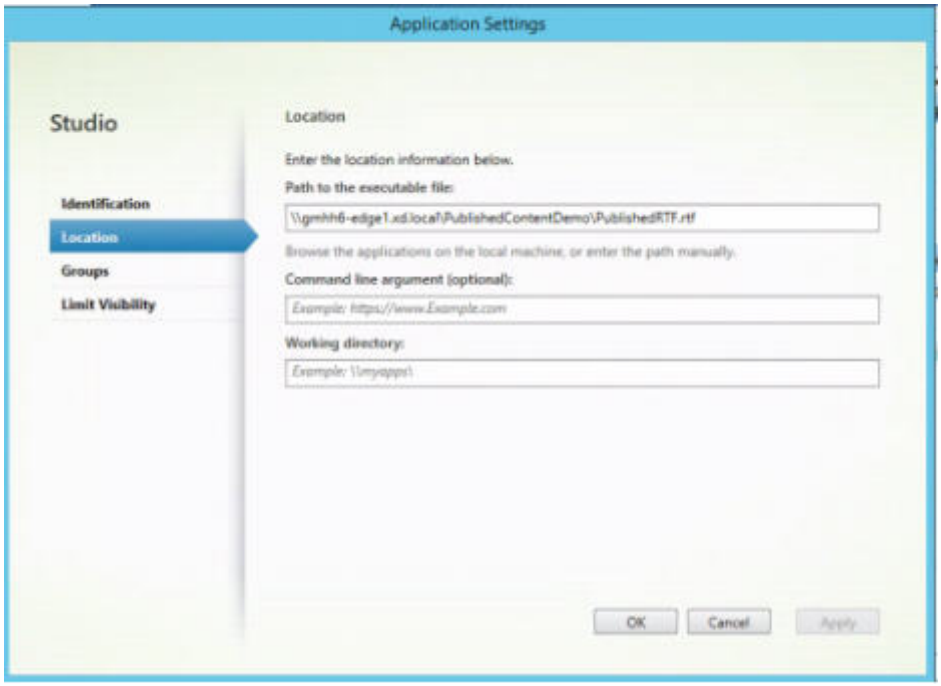


Afficher et modifier les applications PublishedContent

Vous gérez le contenu publié à l'aide des méthodes que vous utilisez pour les autres types d'applications. Les éléments du contenu publié s'affichent dans la liste Applications de Studio et peuvent être modifiés dans Studio.

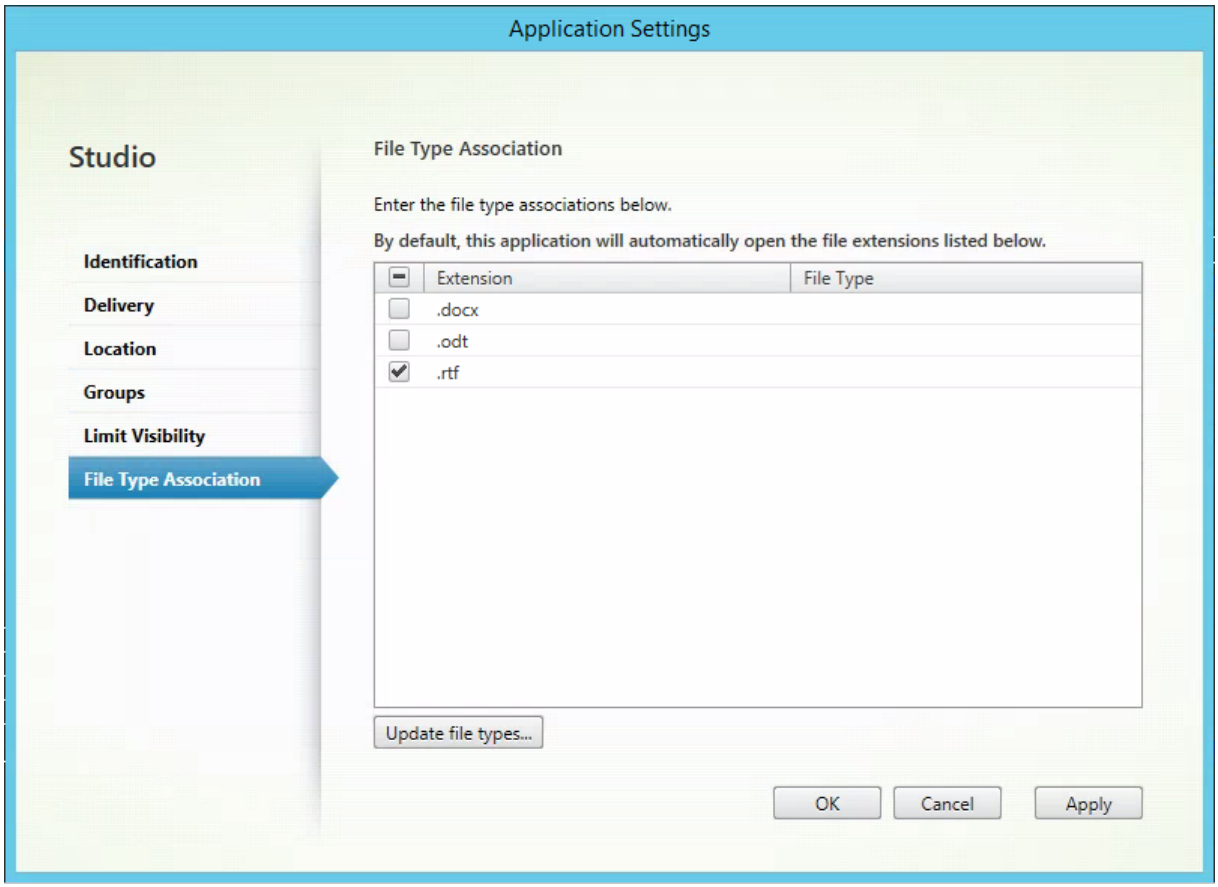


Les propriétés de l'application (par exemple, la visibilité de l'utilisateur, l'association de groupe et le raccourci) s'appliquent au contenu publié. Cependant, vous ne pouvez pas modifier les propriétés d'argument de ligne de commande ou de répertoire de travail sur la page **Emplacement**. Pour modifier la ressource, modifiez le champ « Chemin d'accès au fichier exécutable » sur cette page.

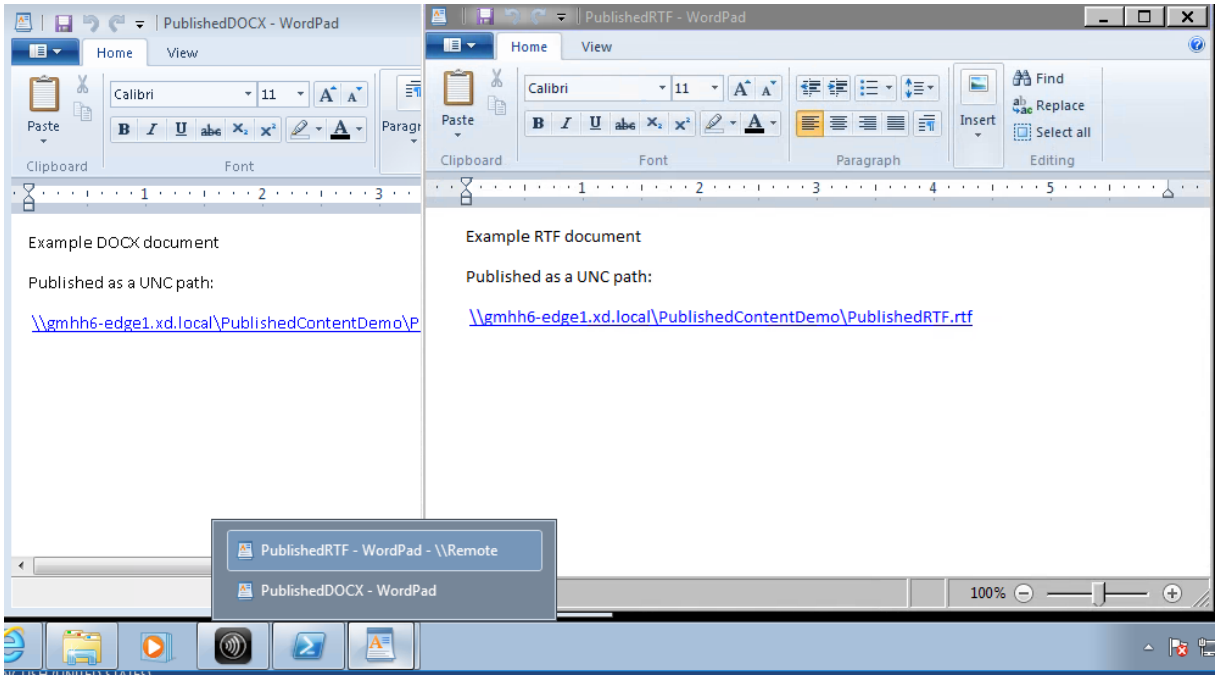


Pour utiliser une application publiée pour ouvrir une application PublishedContent (plutôt qu'une application locale), modifiez la propriété Association de type de fichier de l'application publiée. Dans cet exemple, l'application WordPad publiée a été modifiée pour créer une Association de type de fichier pour les fichiers .rtf.

> **Important :**
>
> Activez le mode de maintenance pour le groupe de mise à disposition avant de modifier l'association de type de fichier. N'oubliez pas de désactiver le mode de maintenance lorsque vous avez terminé.



Actualisez StoreFront pour charger les modifications apportées à l'association de type de fichier, puis cliquez sur les applications PublishedRTF et PublishedDOCX. Notez la différence. PublishedDOCX s'ouvre encore dans le WordPad local. Cependant, PublishedRTF s'ouvre maintenant dans le WordPad publié en raison de l'association de type de fichier.



Informations supplémentaires

- Créer des catalogues de machines
- Créer des groupes de mise à disposition
- Modifier les propriétés de l'application

Server VDI

February 28, 2019

Utilisez la fonctionnalité Server VDI (Virtual Desktop Infrastructure) pour mettre à disposition un bureau depuis un système d'exploitation serveur vers un utilisateur unique.

- Les administrateurs d'entreprise peuvent mettre à disposition des systèmes d'exploitation serveur en tant que bureaux VDI, ce qui peut être utile pour les utilisateurs tels que les ingénieurs et les concepteurs.
- Les fournisseurs de service peuvent offrir des bureaux depuis le cloud ; ces bureaux sont conformes avec Microsoft Services Provider License Agreement (SPLA).

Vous pouvez utiliser le paramètre de stratégie Expérience de bureau améliorée Citrix pour faire prendre au système d'exploitation serveur l'apparence d'un système d'exploitation de bureau.

Les fonctionnalités suivantes ne peuvent pas être utilisées avec Server VDI :

- Personal vDisk

- Applications hébergées
- Local App Access
- Connexions de bureau directes (sans broker)
- Remote PC Access

Pour que Server VDI fonctionne avec des périphériques TWAIN tels que des scanners, la fonctionnalité Expérience utilisateur de Windows Server doit être installée. Dans Windows Server 2012, il s'agit d'une option facultative que vous pouvez installer à partir de Outils d'administration > Gestionnaire de serveur > Fonctionnalités > Ajouter des fonctionnalités > Expérience utilisateur.

Server VDI est pris en charge par les systèmes d'exploitation sur le même serveur que le VDA pour système d'exploitation Windows Server.

Pour installer Server VDI :

Étape 1 – Préparez le serveur Windows en vue de l'installation.

- Utilisez le Gestionnaire de serveur Windows pour vous assurer que les services de rôle des services Bureau à distance ne sont pas installés. Supprimez-les si précédemment installés. (L'installation de VDA échoue si ces services de rôle sont installés.)
- Assurez-vous que la propriété « Restreindre chaque utilisateur à une seule session » est activée.

  Sur Windows Server 2008 R2, accédez à cette propriété via Outils d'administration > Services Bureau à distance > Configuration d'hôte de session Bureau à distance. Dans la section Modifier les paramètres > Général, le paramètre Restreindre chaque utilisateur à une seule session devrait indiquer Oui.

  Sur Windows Server 2012R2 ou Windows Server 2016, modifiez le Registre et définissez le paramètre de Terminal Server. Dans la clé de registre `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer`, définissez DWORD `fSingleSessionPerUser` sur 1.

Étape 2 – Pour Windows Server 2008 R2, installez Microsoft .NET Framework 3.5 SP1 sur le serveur avant d'installer le VDA.

Étape 3 – Utilisez l'interface de ligne de commande du programme d'installation pour installer un VDA sur un serveur pris en charge ou sur une image principale de serveur, en spécifiant les options /quiet et /servervdi : (Par défaut, l'interface graphique du programme d'installation bloque le VDA avec OS de bureau Windows sur un système d'exploitation de serveur. La ligne de commande ignore ce comportement.)

- Déploiements XenApp et XenDesktop sur site : `XenDesktopVdaSetup.exe /quiet /servervdi`
- Déploiements XenApp et XenDesktop ou XenDesktop Service sur site : `VDAWorkstationSetup.exe /quiet /servervdi`

Vous pouvez spécifier le Delivery Controller ou le Cloud Connector avec l'option **/controllers**.

Utilisez l'option **/enable_hdx_ports** pour ouvrir des ports dans le pare-feu, sauf si le pare-feu doit être configuré manuellement.

Ajoutez l'option **/masterimage** si vous installez le VDA sur une image, et que vous allez utiliser MCS pour créer des VM de serveur depuis cette image.

> **Remarque :**
>
> N'incluez pas les options des fonctionnalités qui ne sont pas prises en charge avec Server VDI, telles que **/baseimage**.

Étape 4 – Créez un catalogue de machines pour Server VDI.

- Sur la page **Système d'exploitation**, sélectionnez OS de bureau.
- Sur la page **Résumé**, spécifiez un nom de catalogue de machines et une description pour les administrateurs qui l'identifient clairement en tant que Server VDI ; ce sera le seul indicateur dans Studio que le catalogue prend Server VDI en charge.
- Lors de l'utilisation de la fonction de recherche dans Studio, le catalogue Server VDI que vous avez créé s'affichera sur la page de l'onglet Machines avec OS de bureau, même si le VDA a été installé sur un serveur.

Étape 5 – Créez un groupe de mise à disposition et attribuez le catalogue Server VDI que vous avez créé à l'étape précédente.

Si vous n'avez pas spécifié les Delivery Controller ou le Cloud Connector lors de l'installation du VDA, spécifiez-les après à l'aide du paramètre de stratégie Citrix, Active Directory, ou en modifiant les valeurs de registre de la machine VDA. Consultez la section Enregistrement de VDA.

Personal vDisk

January 23, 2019

La fonctionnalité Personal vDisk permet de gérer une image unique de bureaux regroupés et streamés tout en autorisant les utilisateurs à installer des applications et à modifier leurs paramètres de bureau. Contrairement aux déploiements VDI (infrastructure de bureau virtuel) traditionnels impliquant des bureaux regroupés, dans lesquels les utilisateurs perdent les personnalisations qu'ils ont apportées et leurs applications personnelles lorsque l'administrateur modifie l'image principale, les déploiements utilisant des Personal vDisk conservent ces changements. Cela signifie que les administrateurs peuvent facilement gérer de manière centralisée leurs images principales tout en offrant aux utilisateurs une expérience de bureau personnalisée.

Personal vDisk offre cette séparation en redirigeant toutes les modifications apportées à la VM de l'utilisateur vers un disque distinct (le personal vDisk) connecté à la VM de l'utilisateur. Le contenu

du Personal vDisk est fusionné au moment de l'exécution avec le contenu de l'image principale afin d'offrir une expérience unifiée. Ainsi, les utilisateurs peuvent toujours accéder aux applications approvisionnées par leur administrateur dans l'image principale.

Les Personal vDisk possèdent deux parties, qui utilisent différentes lettres de lecteur et sont de même taille par défaut :

- Profil utilisateur : contient les données utilisateur, les documents, et le profil de l'utilisateur. Par défaut, cette partie utilise le lecteur P: mais vous pouvez choisir une lettre de lecteur différente lorsque vous créez un catalogue de machines avec des machines qui utilisent des Personal vDisks. Le lecteur utilisé dépend également du paramètre EnableUserProfileRedirection.
- Fichier du disque dur virtuel (.vhd) : ce fichier contient tous les autres éléments, par exemple les applications installées dans C:\Program Files. Cette dernière n'est pas affichée dans Windows Explorer et ne nécessite pas de lettre de lecteur depuis la version 5.6.7.

Les Personal vDisk prennent en charge le provisioning d'applications au niveau du département, ainsi que les applications téléchargées et installées par les utilisateurs, y compris celles nécessitant des pilotes (mis à part les pilotes de phase 1), les bases de données et le logiciel de gestion de machine. Si une modification effectuée par un utilisateur entre en conflit avec une modification effectuée par un administrateur, un Personal vDisk offre une manière simple et automatique de concilier les modifications.

De plus, les applications administrées localement (telles que celles approvisionnées et gérées par les départements informatiques locaux) peuvent également être approvisionnées dans l'environnement de l'utilisateur. L'utilisateur n'observe aucune différence en termes de facilité d'utilisation ; Personal vDisk s'assure que toutes les modifications apportées et toutes les applications installées sont stockées sur le disque virtuel. Lorsqu'une application figurant sur un disque virtuel personnel est identique à une application figurant sur une image principale, la copie figurant sur le Personal vDisk est supprimée pour gagner de l'espace sans pour autant que l'utilisateur perde l'accès à l'application.

Les Personal vDisks sont stockés sur l'hyperviseur mais ils n'ont pas besoin d'être dans le même emplacement que d'autres disques attachés à ce bureau virtuel. Cela permet de réduire les coûts de stockage du Personal vDisk.

Au cours de la création d'un site, lorsque vous créez une connexion, vous définissez des emplacements de stockage pour les disques utilisés par les machines virtuelles. Vous pouvez séparer les Personal vDisks des disques utilisés par le système d'exploitation. Chaque machine virtuelle doit avoir accès à un emplacement de stockage pour les deux disques. Si le stockage local est utilisé pour les deux disques, ils doivent être accessibles à partir du même hyperviseur. Pour vous assurer que la configuration requise est présente, Studio offre uniquement des emplacements de stockage compatibles. Plus tard, vous pouvez également ajouter des Personal vDisks et du stockage sur les hôtes existants (mais pas les catalogues de machines) dans **Configuration > Hébergement** dans Studio.

Sauvegardez régulièrement les Personal vDisks à l'aide de la méthode de votre choix. Les vDisks sont

des volumes standards dans un niveau de stockage hyperviseur, vous pouvez donc les sauvegarder comme tout autre volume.

> **Remarque :**
>
> Reportez-vous à l'article Dépannage pour plus d'informations sur les rapports, les messages et les problèmes connus de PvD.

Installation et mise à niveau

January 23, 2019

Personal vDisk 7.x est pris en charge pour XenDesktop 5.6 jusqu'à la version actuelle. La documentation « Configuration requise » pour chaque version de XenDesktop dresse la liste des systèmes d'exploitation pris en charge par Virtual Delivery Agents (VDA), et les versions prises en charge des hôtes (ressources de virtualisation) et Provisioning Services. Pour de plus amples informations sur les tâches Provisioning Services, consultez la documentation Provisioning Services.

Installez et activez le PvD

Vous pouvez installer et activer des composants PvD lorsque vous installez ou mettez à niveau un VDA pour OS de bureau sur une machine. Ces actions sont sélectionnées sur les pages **Composants supplémentaires** et **Fonctionnalités** de l'assistant d'installation. Pour plus d'informations, consultez la section Installer des VDA.

Si vous mettez à jour le logiciel PvD après l'installation du VDA, utilisez le fichier MSI PvD fourni sur le support d'installation de XenApp ou XenDesktop.

Activation du PvD :

- Si vous utilisez Machine Creation Services (MCS), PvD est automatiquement activé lorsque vous créez un catalogue de machines avec des machines avec OS de bureau qui utiliseront un Personal vDisk.
- Si vous utilisez Provisioning Services (PVS), PvD est automatiquement activé lorsque vous exécutez l'inventaire pendant le processus de création d'image (de base) principale, ou lors de la mise à jour automatique de l'inventaire pour vous.

Par conséquent, si vous installez des composants PvD mais que vous ne les activez pas lors de l'installation du VDA, vous pouvez utiliser la même image pour créer des bureaux PvD et des bureaux non-PvD, car PvD est activé lors du processus de création du catalogue.

Ajouter des Personal vDisks

Vous ajoutez des Personal vDisks à des hôtes lorsque vous configurez un site. Vous pouvez choisir d'utiliser le même stockage sur l'hôte pour les VM et Personal vDisks, ou vous pouvez utiliser un stockage différent pour les Personal vDisks.

Plus tard, vous pouvez également ajouter des Personal vDisks et leur stockage à des hôtes existants (connexions), mais pas des catalogues de machines.

1. Sélectionnez Configuration > Hébergement dans le volet de navigation de Studio.
2. Sélectionnez Ajouter un stockage Personal vDisk dans le volet Actions et spécifiez l'emplacement de stockage.

Mettre à niveau PvD

La manière la plus facile de mettre à niveau Personal vDisk à partir d'une version antérieure à la version 7.x est simplement de mettre à niveau les VDA de votre système d'exploitation de bureau vers la version fournie avec la dernière version de XenDesktop. Exécutez ensuite l'inventaire PvD.

Désinstaller PvD

Vous pouvez utiliser l'une des deux manières suivantes pour supprimer le logiciel PvD :

- Désinstaller le VDA ; cette option supprime également le logiciel PvD.
- Si vous avez mis PvD à jour à l'aide du fichier MSI PvD, vous pouvez effectuer la désinstallation à partir de la liste des programmes.

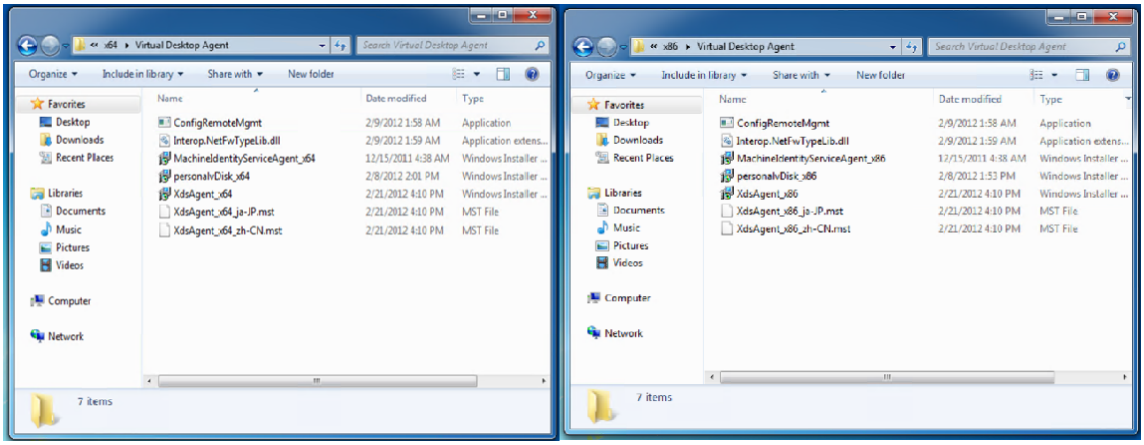
Si vous désinstallez PvD et que vous réinstallez la même version ou une version plus récente, sauvegardez la clé de registre HKLM\Software\Citrix\personal vDisk\config, qui contient les paramètres de configuration d'environnement susceptibles d'avoir été modifiés. Ensuite, après l'installation de PvD, réinitialisez les valeurs de registre qui peuvent avoir été modifiés en les comparant avec la version sauvegardée.

Remarques importantes pour la désinstallation de PvD

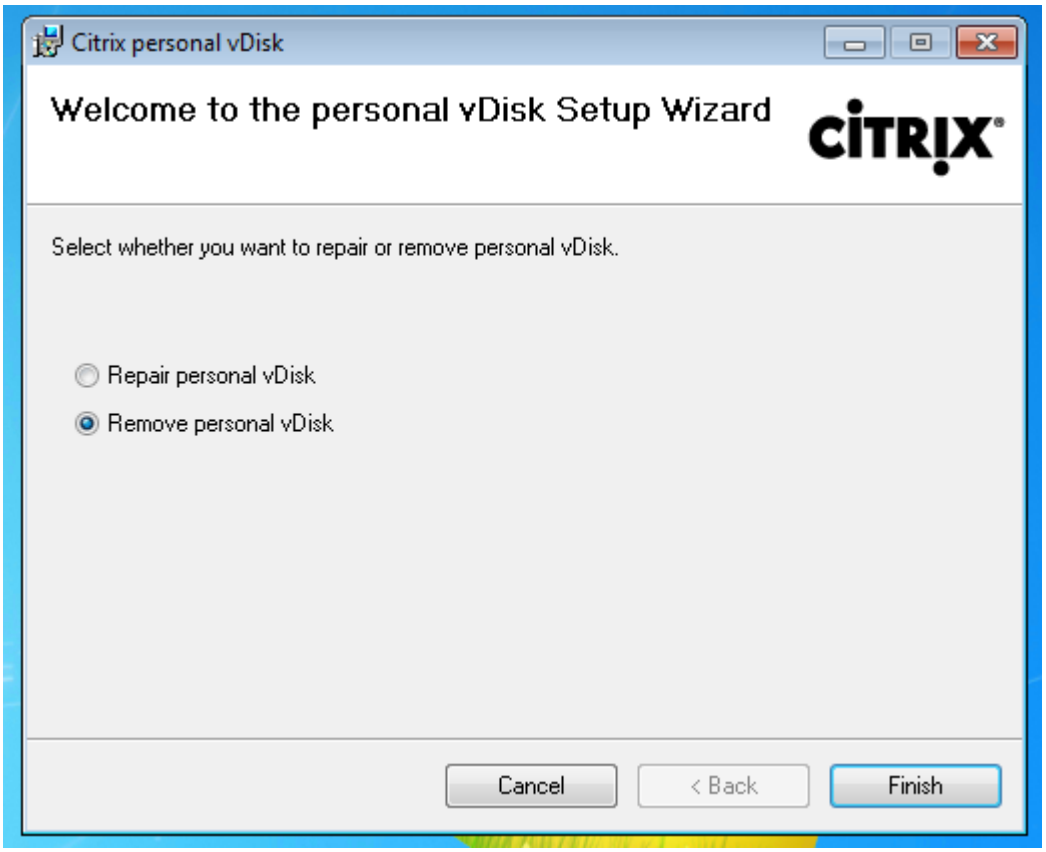
La désinstallation peut échouer lorsqu'un Personal vDisk avec Windows 7 (64 bits) est installé dans l'image de base. Pour résoudre ce problème, Citrix vous recommande de supprimer le Personal vDisk avant la mise à niveau :

1. Sélectionnez la copie appropriée du programme d'installation de vDisk à partir du support de XenApp/XenDesktop. Recherchez le dernier programme d'installation MSI du Personal vDisk sur l'image ISO de XenApp/XenDesktop dans l'un des répertoires suivants (dépend si la VM mise à niveau est 32 ou 64 bits) :

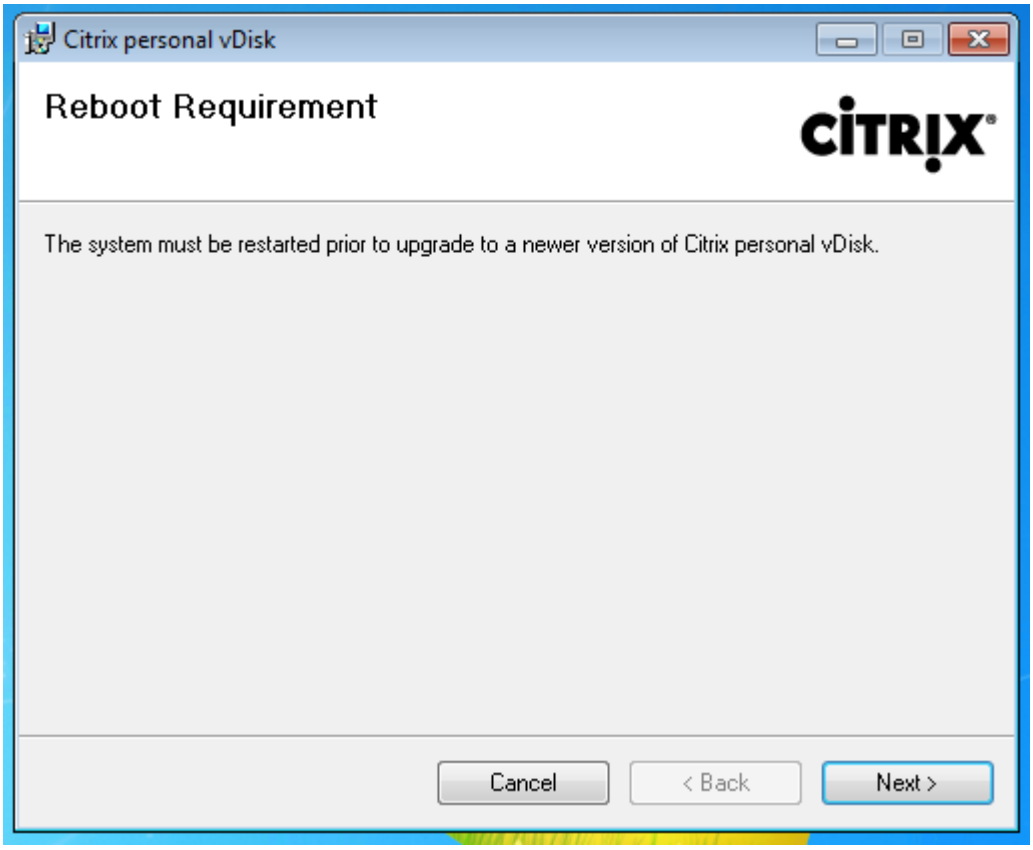
- 32 bits : XA and XD\x86\Virtual Desktop Components\personalvDisk_x86.msi
- 64 bits : XA and XD\x64\Virtual Desktop Components\personalvDisk_x64.msi



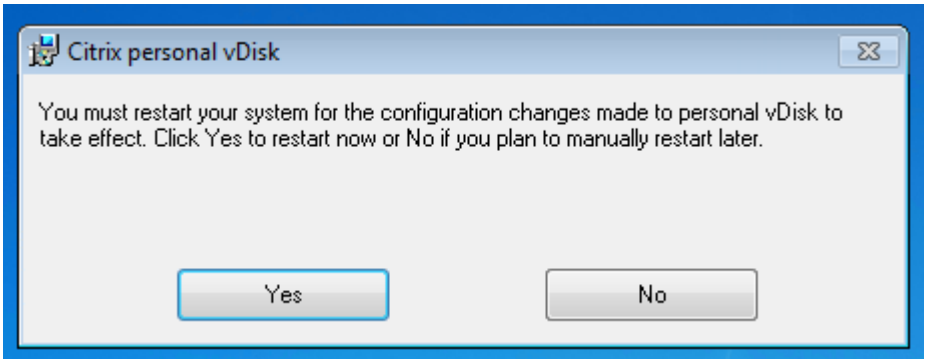
2. Supprimez l'installation du Personal vDisk. Sélectionnez le Pack d'installation MSI du Personal vDisk trouvé à l'étape 1. L'écran d'installation du Personal vDisk s'affiche.
3. Sélectionnez Remove personal vDisk.
4. Cliquez sur **Terminer**.



5. La page Demande de redémarrage s'affiche. Cliquez sur **Suivant** :



6. Cliquez sur **Oui** pour redémarrer le système et pour appliquer vos modifications de configuration :



Configurer et gérer

November 6, 2018

Cette rubrique décrit les éléments à prendre en compte lors de la configuration et de la gestion d'un environnement de Personal vDisk (PvD). Il couvre également des instructions et des descriptions de tâche conseillées.

Pour les procédures qui incluent l'utilisation du registre Windows :

> **Avertissement :**
>
> toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Considérations : taille du Personal vDisk

Les facteurs suivants affectent la taille du volume Personal vDisk principal :

- **Taille des applications que les utilisateurs installeront sur leurs PvD.**

  À chaque redémarrage, PvD détermine l'espace disponible restant dans la zone applicative (UserData.v2.vhd). Si cet espace tombe en dessous de 10 %, la zone applicative est étendue de façon à utiliser tout espace non utilisé dans la zone dédiée aux profils (par défaut, l'espace disponible sur le lecteur P:). L'espace ajouté à la zone applicative équivaut à 50 % de l'espace disponible combiné restant dans la zone applicative et la zone des profils.

  À titre d'exemple, si la zone applicative sur un PvD de 10 Go, qui est par défaut de 5 Go, atteint 4,7 Go et que la zone des profils dispose de 3 Go disponibles, l'espace ajouté à la zone applicative est calculé comme suit :

  Espace accru = (5.0 - 4.7)/2 + 3.0/2 = 1.65 Go

  L'espace ajouté à la zone applicative est approximatif car une provision est constituée pour le stockage des journaux et les surcharges potentielles. Le calcul et le dimensionnement possible sont effectués à chaque redémarrage.

- **Taille des profils utilisateur (si aucune solution de gestion des profils distincte n'est utilisée).**

  En plus de l'espace requis pour les applications, assurez-vous qu'il y ait suffisamment d'espace disponible sur les Personal vDisks pour stocker les profils utilisateur. Incluez tous les dossiers spéciaux non redirigés (tels que Mes documents et Ma musique) lors du calcul de l'espace requis. La taille des profils existants est disponible dans le Panneau de configuration (sysdm.cpl).

  Certaines solutions de redirection de profil stockent les fichiers stub (fichiers sentinel) à la place des données de profil réelles. Ces solutions de gestion des profils peuvent sembler ne stocker aucune donnée initialement, mais elles consomment en fait une entrée du répertoire du fichier dans le système de fichiers par fichier stub (environ 4 Ko par fichier). Si vous utilisez une telle solution, évaluez la taille en fonction des données de profil réelles et non des fichiers stub.

Les applications de partage des fichiers d'entreprise (telles que ShareFile et Dropbox) peuvent synchroniser ou télécharger des données sur les zones de profil des utilisateurs sur les Personal vDisks. Si vous utilisez de telles applications, incluez suffisamment d'espace dans votre estimation de taille pour ces données.

- **Quantité de mémoire consommée par le VHD modèle contenant l'inventaire PvD.**

  Le VHD modèle contient les données d'inventaire PvD (fichiers sentinelles correspondant au contenu de l'image principale). La zone applicative PvD est créée depuis ce VHD. Étant donné que chaque fichier ou dossier sentinel contient une entrée de répertoire de fichier dans le système de fichiers, le contenu du VHD modèle consomme l'espace applicatif PvD avant même que des applications ne soient installées par les utilisateurs. Vous pouvez déterminer la taille du VHD modèle en consultant l'image principale après la réalisation d'un inventaire. Vous pouvez également utiliser l'équation suivante pour effectuer un calcul approximatif :

  Taille du modèle VHD = (nombre de fichiers sur l'image de base) x 4 Ko

  Déterminez le nombre de fichiers et de dossiers en cliquant avec le bouton droit de la souris sur le lecteur C: sur l'image de VM de base et en sélectionnant Properties. À titre d'exemple, une image contenant 250 000 fichiers équivaut à un VHD modèle d'environ 1 024 000 000 octets (un peu moins d'1 Go). Cet espace ne pourra pas être utilisé pour l'installation d'applications dans la zone applicative PvD.

- **Quantité de mémoire utilisée par les opérations de mise à jour de l'image PvD**

  Durant les opérations de mise à jour de l'image PvD, un espace suffisant doit être disponible à la racine du PvD (par défaut, P:) afin de fusionner les modifications apportées aux deux versions de l'image et les modifications apportées par l'utilisateur à son PvD. En général, PvD se réserve quelques centaines de Mo à cette fin, mais les données supplémentaires écrites sur le lecteur P: peuvent consommer cet espace réservé et laisser un espace insuffisant pour mener à bien la mise à jour de l'image. Le script de statistiques du pool PvD (situé sur le support d'installation XenDesktop dans le dossier Support/Tools/Scripts) ou de la mise à jour de l'image PvD dans l'outil d'analyse (dans le dossier Support/Tools/Scripts/PvdTool) peut vous aider à identifier les disques PvD d'un catalogue en cours de mise à jour et qui sont presque plein.

  La présence de produits anti-virus peut affecter la durée nécessaire pour exécuter l'inventaire ou effectuer une mise à jour. Les performances peuvent s'améliorer si vous ajoutez CtxPvD.exe et CtxPvDSvc.exe à la liste d'exclusion de votre produit anti-virus. Ces fichiers sont situés dans C:\Program Files\Citrix\personal vDisk\bin. L'exclusion de ces exécutables de l'analyse du logiciel antivirus peut décupler les performances liées à l'inventaire et à la mise à jour d'image jusqu'à un facteur de 10.

- **La quantité de mémoire utilisée pour la croissance non anticipée (installation d'applications imprévue, etc).**

Surestimez la taille totale (une quantité fixe ou un pourcentage de la taille du vDisk) afin de tenir compte de l'installation d'applications imprévues effectuées par l'utilisateur lors du déploiement.

Procédures : configurer la taille du Personal vDisk et la répartition

Vous pouvez régler manuellement l'algorithme de redimensionnement automatique qui détermine la taille du VHD relative au lecteur P:, en définissant la taille initiale du VHD. Ceci peut être utile si, par exemple, vous savez que vos utilisateurs vont installer un certain nombre d'applications qui sont trop importantes pour contenir sur le VHD même après son redimensionnement par l'algorithme. Dans ce cas, vous pouvez augmenter la taille initiale de l'espace des applications pour accommoder les applications installées par l'utilisateur.

Il est préférable de régler la taille initiale du VHD sur une image principale. Éventuellement, vous pouvez régler la taille du VHD sur un bureau virtuel lorsqu'un utilisateur ne dispose pas de suffisamment d'espace pour installer une application. Cependant, vous devez répéter cette opération sur chaque bureau virtuel affecté ; vous ne pouvez pas régler la taille initiale du VHD dans un catalogue déjà créé.

assurez-vous que le VHD est assez important pour stocker des fichiers de définition antivirus, qui sont généralement importants.

Recherchez et définissez les clés de registre suivantes dans HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\personal vDisk\Config. (Ne modifiez pas d'autres paramètres de cette clé de Registre). Tous les paramètres doivent être spécifiés sur l'image principale (sauf pour MinimumVHDSizeInMB, qui peut être modifié sur un ordinateur individuel) ; les paramètres spécifiés sur l'image principale sont appliqués lors de la mise à jour d'image suivante.

- **MinimumVHDSizeMB**

  Spécifie la taille minimale (en mégaoctets) de la partie applicative (C:) du Personal vDisk. La nouvelle taille doit être supérieure à la taille existante mais inférieure à la taille du disque moins PvDReservedSpaceMB.

  L'augmentation de cette valeur alloue l'espace disponible de la partie réservée aux profils sur le vDisk à C:. Ce paramètre est ignoré si une valeur inférieure à la taille actuelle du lecteur C: est utilisée, ou si EnableDynamicResizeOfAppContainer est défini sur 0.

  Valeur par défaut = 2048

- **EnableDynamicResizeOfAppContainer**

  Active ou désactive l'algorithme de redimensionnement dynamique.

  – Lorsque cette option est définie sur 1, l'espace de l'application (C:) est redimensionné automatiquement lorsque l'espace libre sur C: est inférieur à 10%. Les valeurs autorisées sont 1 et 0. Un redémarrage est requis pour que le redimensionnement soit pris en compte.

- Lorsque cette option est définie sur 0, la taille du VHD est déterminée en fonction de la méthode utilisée dans les versions antérieures à la version 7.x de XenDesktop

Valeur par défaut = 1

- **EnableUserProfileRedirection**

  Active ou désactive la redirection du profil de l'utilisateur vers le vDisk.

  - Lorsque cette option est définie sur 1, PvD redirige les profils des utilisateurs sur le lecteur Personal vDisk (P: par défaut). Les profils sont généralement redirigés vers P:\Utilisateurs, ce qui correspond à un profil Windows standard. Cette redirection préserve les profils dans le cas où le bureau PvD doit être réinitialisé.
  - Lorsqu'elle est définie sur 0, tout l'espace disponible sur le vDisk moins PvDReservedSpaceMB est alloué à C:, la partie applicative du vDisk, et le lecteur du vDisk (P:) est masqué dans l'Explorateur Windows. Citrix vous recommande de désactiver la redirection en définissant la valeur sur 0, lorsque vous utilisez Citrix Profile Management ou une autre solution de gestion des profils itinérants.

    Ce paramètre permet de conserver les profils dans C:\Users plutôt que les rediriger vers le vDisk, et permet à la solution de profils itinérants de gérer les profils.

    Cette valeur assure que tout l'espace présent sur P: est attribué aux applications.

    Ceci suppose que cette valeur est définie sur 0, et qu'une solution de gestion des profils est en place. Si vous ne disposez pas d'une solution de gestion des profils itinérants, la désactivation de la redirection des profils n'est pas recommandée car les opérations de réinitialisation de PvD ultérieures entrainent la suppression des profils.

  Ne modifiez pas ce paramètre lorsque l'image est mise à jour car il ne modifie pas l'emplacement des profils existants mais il allouera tout l'espace disponible sur le Personal vDisk à C: et masquera le PvD.

  Configurez cette valeur avant de déployer un catalogue. Vous ne pouvez pas le modifier une fois que le catalogue est déployé.

  Important : à compter de XenDesktop 7.1, les modifications apportées à cette valeur ne sont pas appliquées lorsque vous effectuez une mise à jour d'image. Définissez la valeur de la clé lorsque vous créez tout d'abord le catalogue depuis lequel les profils proviennent. Vous ne pouvez pas modifier le comportement de redirection ultérieurement.

  Valeur par défaut = 1

- **PercentOfPvDForApps**

  Définit la répartition entre la partie applicative (C:) et la partie réservée aux profils du vDisk. Cette valeur est utilisée lors de la création de nouvelles VM et durant les mises à jour d'images si EnableDynamicResizeOfAppContainer est défini sur 0.

La modification de PercentOfPvDForApps fait la différence uniquement lorsque le paramètre EnableDynamicResizeOfAppContainer est défini sur 0. Par défaut, le paramètre EnableDynamicResizeOfAppContainer est défini sur 1 (activé), ce qui signifie que AppContainer (que vous voyez en tant que lecteur C) est développé uniquement lorsqu'il est presque plein (c'est-à-dire, dynamique) lorsque moins de 10% d'espace libre est restant.

L'augmentation de PercentOfPvDForApps augmente uniquement l'espace maximum pour lequel la partie Apps est autorisée à augmenter. Cet espace n'est pas provisionné pour vous immédiatement. Vous devez également configurer l'allocation fractionnée dans l'image principale, où elle sera appliquée lors de la prochaine mise à jour d'image.

Si vous avez déjà généré un catalogue de machines avec EnableDynamicResizeOfAppContainer défini sur 1, changez alors ce paramètre sur 0 dans l'image principale pour la mise à jour suivante, puis configurez une division d'allocation appropriée. La taille de division requise sera honorée tant qu'elle est plus importante que la taille allouée actuelle pour le lecteur C.

Si vous souhaitez conserver un contrôle total sur la division de l'espace, cette valeur devrait être définie sur 0. Ceci permet un contrôle total sur la taille du lecteur C, et ne compte pas sur la consommation de l'espace disque par l'utilisateur en dessous du seuil pour augmenter le lecteur.

Valeur par défaut = 50% (alloue une quantité d'espace égale pour les deux parties)

- **PvDReservedSpaceMB**

  Définit la taille de l'espace réservé (en méga-octets) sur le vDisk pour le stockage de journaux Personal vDisk et d'autres données.

  Si votre déploiement comprend XenApp 6.5 (ou une version antérieure) et utilise la fonctionnalité de streaming d'application, augmentant cette valeur par la taille du cache Rade.

  Valeur par défaut = 512

- **PvDResetUserGroup**

  Valide uniquement pour XenDesktop 5.6 : autorise le groupe d'utilisateurs spécifié à réinitialiser un Personal vDisk. Les versions ultérieures de XenDesktop utilisent l'administration déléguée pour cette opération.

Autres paramètres :

- **Service Windows Update :** assurez-vous que les mises à jour Windows sont définies sur Ne jamais rechercher des mises à jour et que le service Windows Update est désactivé (défini sur Disabled) dans l'image principale. Dans l'éventualité où le service Windows Update doit être exécuté sur le PvD, la définition de celui-ci sur Ne jamais rechercher des mises à jour vous aide à empêcher l'installation des mises à jour sur les machines associées.

Windows 8 Store a besoin de ce service en cours d'exécution pour installer toute application moderne.

- **Mises à jour Windows :** elles comprennent les mises à jour d'Internet Explorer et doivent être appliquées à l'image principale.
- **Mises à jour nécessitant un redémarrage :** les mises à jour Windows appliquées à l'image principale peuvent nécessiter plusieurs redémarrages pour être entièrement installées ; cela dépend du type de correctifs délivrés dans ces mises à jour. Veillez à redémarrer correctement l'image principale afin de terminer l'installation des mises à jour Windows appliquées à cette dernière avant de dresser l'inventaire PvD.
- **Mises à jour applicatives :** mettez à jour les applications installées sur l'image principale pour économiser l'espace sur les vDisk des utilisateurs. Cela permet aussi d'éviter d'avoir à mettre à jour les applications sur chaque vDisk de l'utilisateur.

Considérations : les applications sur l'image principale

Certains logiciels peuvent entrer en conflit avec la façon dont le PvD établit l'environnement de l'utilisateur, vous devez l'installer sur l'image principale (plutôt que sur la machine utilisateur) pour éviter ces conflits. En outre, bien que certains d'autres logiciels puissent ne pas entrer en conflit avec le bon fonctionnement du PvD, Citrix vous recommande d'installer le logiciel sur l'image principale.

Applications qui doivent être installées sur l'image principale :

- Agents et clients (par exemple, l'agent System Center Configuration Manager, le client App-V, Citrix Receiver)
- applications qui installent ou modifient des pilotes de démarrage précoce ;
- applications qui installent des logiciels d'impression ou de scanner ou des pilotes ;
- applications qui modifient la pile réseau Windows ;
- outils de VM tels que VMware Tools et XenServer Tools.

Applications qui devraient être installées sur l'image principale :

- Applications qui sont distribuées à un grand nombre d'utilisateurs. Dans les deux cas, désactivez la mise à jour des applications avant le déploiement :
  - Applications d'entreprise qui utilisent des licences en volume, par exemple Microsoft Office, Microsoft SQL Server
  - Applications communes, par exemple Adobe Reader, Firefox et Chrome
- Applications volumineuses telles que SQL Server, Visual Studio et infrastructures applicatives telles que .NET

Les recommandations et restrictions suivantes s'appliquent aux applications installées par les utilisateurs sur les machines disposant de Personal vDisks. Certaines ne peuvent pas être appliquées si les utilisateurs disposent de privilèges administratifs :

- Les utilisateurs ne devraient pas désinstaller une application à partir de l'image principale et réinstaller la même application sur leur Personal vDisk.
- Soyez prudent lors de la mise à jour ou de la désinstallation d'applications sur l'image principale. Après avoir installé la version d'une application sur l'image, un utilisateur peut installer un module d'extension (un plug-in par exemple) qui requiert cette version. Si une telle dépendance existe, la mise à jour ou la désinstallation de l'application sur l'image pourrait entraîner un dysfonctionnement de ce module complémentaire. Par exemple, avec Microsoft Office 2010 installé sur une image principale, un utilisateur installe Visio 2010 sur son Personal vDisk. Une mise à niveau ultérieure d'Office sur l'image principale peut rendre le logiciel Visio installé localement inutilisable.
- Les logiciels dotés de licences liées au matériel (via un dongle ou matériel basé sur signature) ne sont pas pris en charge.

Considérations : Provisioning Services

Lors de l'utilisation de Provisioning Services avec PvD :

- Le compte Soap Service doit être ajouté au nœud Administrateur de Studio et doit disposer du rôle d'administrateur de la machine ou d'un rôle supérieur. Cela garantit que les bureaux PvD sont placés en mode de préparation lorsque le vDisk Provisioning Services (PVS) passe en mode de production.
- La fonctionnalité de gestion des versions de Provisioning Services doit être utilisée pour mettre à jour Personal vDisk. Lorsque la version est promue au rôle de production, le Soap Service place les bureaux PvD en mode de préparation.
- La taille du Personal vDisk doit toujours être supérieure au disque de cache en écriture de Provisioning Services (dans le cas contraire, Provisioning Services peut, par erreur, sélectionner Personal vDisk pour utilisation en tant que cache en écriture).
- Une fois que vous avez créé un groupe de mise à disposition, vous pouvez contrôler le Personal vDisk à l'aide de l'outil PvD Image Update Monitoring Tool ou des Scripts resize et poolstats (personal-vdisk-poolstats.ps1).

Taille du disque de cache en écriture créée correctement. En mode de fonctionnement normal, PvD capture la plupart des écritures des utilisateurs (modifications) et les redirige vers le Personal vDisk. Cela implique que vous pouvez réduire la taille du disque de cache en écriture Provisioning Services. Toutefois, lorsque PvD n'est pas actif (comme lors des opérations de mise à jour de l'image), un disque de cache en écriture Provisioning Services de petite taille peut se remplir rapidement, ce qui entraîne des blocages de la machine.

Citrix vous recommande de créer la taille des disques de cache en écriture Provisioning Services, conformément aux meilleures pratiques de Provisioning Services et ajouter une quantité d'espace égale à deux fois la taille du modèle VHD sur l'image principale (afin de répondre aux exigences de fusion).

Il est très improbable qu'une opération de fusion utilise tout cet espace, mais cela est possible.

Lors de l'utilisation de Provisioning Services pour déployer un catalogue de machines PvD :

- Suivez les instructions de la documentation Provisioning Services.
- Vous pouvez modifier les paramètres de limitation de l'action d'alimentation en modifiant la connexion dans Studio, voir ci-dessous.
- Si vous mettez à jour le vDisk Provisioning Services, après l'installation ou la mise à jour des applications et d'autres logiciels et le redémarrage du vDisk, exécutez l'inventaire PvD, puis arrêtez la VM. Ensuite, effectuez la promotion de la nouvelle version en Production. Les bureaux PvD dans le catalogue devraient automatiquement entrer en mode de préparation. Si ce n'est pas le cas, vérifiez que le compte Soap Service possède des privilèges d'administrateur de machines ou plus élevés sur le Controller.

La fonctionnalité du mode de test de Provisioning Services vous permet de créer un catalogue de machines de test à l'aide d'une image principale mise à jour. Si des tests confirment la viabilité du catalogue de test, vous pouvez le promouvoir en production.

Considérations : Machine Creation Services

Lors de l'utilisation de Machine Creation Services (MCS) pour déployer un catalogue de machines PvD :

- Suivez les instructions de la documentation XenDesktop.
- Exécutez un inventaire PvD après la création de l'image principale et arrêter la VM (PvD ne fonctionnera pas correctement si vous n'éteignez pas la VM). Prenez ensuite un instantané de l'image principale.
- Dans l'assistant Créer un catalogue de machines, spécifiez la taille du Personal vDisk et la lettre de lecteur.
- Une fois que vous avez créé un groupe de mise à disposition, vous pouvez contrôler le Personal vDisk à l'aide de l'outil PvD Image Update Monitoring Tool ou des Scripts resize et poolstats (personal-vdisk-poolstats.ps1).
- Vous pouvez modifier les paramètres de limitation de l'action d'alimentation en modifiant la connexion dans Studio, voir ci-dessous.
- Si vous mettez à jour l'image principale, exécutez l'inventaire PvD après la mise à jour des applications et d'autres logiciels sur l'image, puis arrêter la VM. Prenez ensuite un instantané de l'image principale.
- Utilisez l'outil de contrôle de mise à jour de l'image PvD (PvD Image Update Monitoring Tool) ou le script personal-vdisk-poolstats.ps1 afin de valider qu'il y a suffisamment d'espace sur chaque VM PvD qui utilisera l'image principale mise à jour.
- Lorsque vous mettez à jour le catalogue de machines, les bureaux PvD entrent en mode de préparation lorsqu'ils traitent individuellement les modifications apportées à la nouvelle image

principale. Les bureaux sont mis à jour en fonction de la stratégie de déploiement spécifiée lors de la mise à jour de machine.

- Utilisez l'outil de contrôle de mise à jour de l'image PvD ou le script personal-vdisk-poolstats.ps1 afin de contrôler le PvD en mode de préparation.

Procédures : exclure les fichiers et les dossiers des vDisks

Utilisez les fichiers de règles pour exclure des fichiers et dossiers des vDisks. Vous pouvez les utiliser lorsque les Personal vDisks sont en déploiement. Les fichiers de règles sont appelés custom_*_rules.template.txt et sont situés dans le dossier \config. Les commentaires dans chaque fichier fournissent une documentation supplémentaire.

Procédures : exécuter l'inventaire lors de la mise à jour d'une image principale

Lorsque vous activez le PvD et après toute mise à jour de l'image principale après l'installation, il est important d'actualiser l'inventaire du disque (appelé « exécuter l'inventaire ») et de créer une nouvelle capture instantanée.

Étant donné que ce sont les administrateurs qui gèrent les images principales et non les utilisateurs, si vous installez une application qui place des fichiers binaires dans le profil utilisateur de l'administrateur, les utilisateurs de bureaux virtuels partagés ne peuvent pas accéder à l'application (y compris les bureaux basés sur des catalogues de machines regroupés et regroupés avec des catalogues de machines PvD). Les utilisateurs doivent installer eux-mêmes de telles applications.

Il est recommandé de prendre un instantané de l'image après chaque étape de cette procédure.

1. Mettez à jour l'image principale en installant des applications ou des mises à jour du système d'exploitation et en procédant à la configuration du système sur la machine.

   Pour ce qui est des images principales basées sur Windows XP que vous prévoyez de déployer avec des disques virtuels personnels, vérifiez qu'aucune boîte de dialogue n'est ouverte (par exemple, des messages confirmant l'installation de logiciels ou vous invitant à utiliser des pilotes non signés). L'ouverture de boîtes de dialogue sur les images principales dans cet environnement empêche le VDA de s'enregistrer auprès de Delivery Controller. Vous pouvez désactiver les invites de pilotes non signés à l'aide du Panneau de configuration. Par exemple, accédez à Système > Matériel > Signature des pilotes et sélectionnez l'option permettant d'ignorer les avertissements.

2. Arrêtez la machine. Sur les machines Windows 7, cliquez sur Annuler lorsque Citrix Personal vDisk bloque la fermeture.

3. Dans la boîte de dialogue Citrix Personal vDisk, cliquez sur Mettre l'inventaire à jour. Cette opération peut prendre plusieurs minutes.

Important : si vous interrompez la fermeture (ne serait-ce que pour apporter une mise à jour mineure à l'image), l'inventaire de Personal vDisk ne correspond plus à l'image principale. Cela provoque l'arrêt de la fonctionnalité Personal vDisk. Si vous interrompez la fermeture, vous devez redémarrer la machine, l'arrêter, et lorsque vous y êtes invité, cliquer de nouveau sur Mettre l'inventaire à jour.

4. Lorsque l'opération d'inventaire arrête la machine, prenez un instantané de l'image principale.

Vous pouvez exporter un inventaire vers un partage réseau, puis importer cet inventaire vers une image principale. Pour de plus amples informations, consultez la section Exporter et importer un inventaire PvD.

Procédures : configurer les paramètres de limitation de la connexion

Citrix Broker Service contrôle l'état de l'alimentation des machines qui fournissent des bureaux et des applications. Le Broker Service peut contrôler plusieurs hyperviseurs via un Delivery Controller. La négociation des actions d'alimentation contrôlent l'interaction entre un Controller et l'hyperviseur. Pour éviter de surcharger l'hyperviseur, les actions de modification de l'état de l'alimentation d'une machine se voient attribuer une priorité et sont envoyées à l'hyperviseur à l'aide d'un mécanisme de limitation. Les paramètres suivants affectent la limitation. Vous pouvez spécifier ces valeurs en modifiant une connexion (onglet Avancé) dans Studio.

Pour configurer les valeurs de limitation de la connexion :

1. Sélectionnez Configuration > Hébergement dans le volet de navigation de Studio.
2. Sélectionnez la connexion, puis sélectionnez Modifier la connexion dans le volet Actions.
3. Vous pouvez changer les valeurs suivantes :
   - **Actions simultanées (tous types) :** nombre maximal d'actions d'alimentation en cours simultanées autorisées. Ce paramètre est spécifié en tant que valeur absolue et en tant que pourcentage de la connexion à l'hyperviseur. La plus faible de ces deux valeurs est utilisée.
     Valeur par défaut = 100 absolue, 20%
   - **Mises à jour de l'inventaire de Personal vDisk simultanées :** nombre maximal d'actions d'alimentation Personal vDisk simultanées autorisées. Ce paramètre est spécifié en tant que valeur absolue et en tant que pourcentage de la connexion. La plus faible de ces deux valeurs est utilisée.
     Valeur par défaut = 50 absolue, 25%
     Pour calculer la valeur absolue : déterminez les valeurs totales IOPS (TIOPS) prises en charge par le stockage de l'utilisateur final (ceci doit être spécifié par le fabricant ou calculé). L'utilisation de 350 IOPS par machine virtuelle (IOPS/VM), détermine le nombre de machines virtuelles qui devraient être actives à tout moment donné sur le stockage. Calculez cette valeur en divisant le total des IOPS par IOPS/VM.

Par exemple, si le stockage utilisateur est de 14000 IPS, le nombre de machines virtuelles actives est de 14000 IOPS / 350 IOPS/VM = 40.

- **Nouvelles actions maximales par minute :** le nombre maximal de nouvelles actions d'alimentation qui peuvent être envoyées à l'hyperviseur par minute. Spécifié en tant que valeur absolue.
  Valeur par défaut = 10

Pour vous aider à identifier les valeurs optimales pour les paramètres suivants dans votre déploiement :

1. À l'aide des valeurs par défaut, mesurez le temps de réponse total pour une mise à jour d'image d'un catalogue de test. Il s'agit de la différence entre le début de la mise à jour d'une image (T1) et le moment où le VDA de la dernière machine du catalogue s'enregistre auprès du Controller (T2). Temps de réponse total = T2 - T1.
2. Mesurez les opérations E/S par seconde (IOPS) du stockage de l'hyperviseur lors de la mise à jour d'image. Ces données peuvent servir de référentiel pour l'optimisation. (Les valeurs par défaut peuvent être le meilleur paramètre ; il se peut également que le système comporte trop d'IOPS, ce qui nécessite de diminuer les valeurs des paramètres).
3. Modifiez la valeur « Opérations de mises à jour de l'inventaire de Personal vDisk » comme décrit ci-dessous (conserver tous les autres paramètres inchangés).
   a) Augmentez la valeur de 10 et mesurez le temps de réponse total après chaque modification. Continuez à augmenter la valeur de 10 et testez le résultat, jusqu'à détérioration ou aucun changement du temps de réponse total.
   b) Si l'étape précédente n'a entraîné aucune amélioration en augmentant la valeur, réduisez la valeur par incréments de 10 et mesurez le temps de réponse total après chaque diminution. Répétez ce processus jusqu'à ce que le temps de réponse total reste inchangé ou ne s'améliore pas davantage. Il est probable que cela soit la valeur de l'action d'alimentation PvD optimale.
4. Après l'obtention de la valeur du paramètre de l'action d'alimentation PvD, modifiez les actions simultanées (tous types) et les valeurs des nouvelles actions maximales par minute, une à la fois. Suivez la procédure décrite ci-dessus (en augmentant ou diminuant par incréments) pour tester des valeurs différentes.

Procédures : System Center Configuration Manager 2007 avec PvD

System Center Configuration Manager (Configuration Manager) 2012 ne requiert aucune configuration spéciale et peut être installé de la même façon que toute autre image principale de l'application. Les informations suivantes s'appliquent uniquement à System Center Configuration Manager 2007. Les versions de Configuration Manager antérieures à Configuration Manager 2007 ne sont pas prises en charge.

Effectuez les opérations suivantes pour utiliser le logiciel agent de Configuration Manager 2007 dans un environnement PvD.

1. Installez l'agent du client sur l'image principale.
    a) Installez le client Configuration Manager sur l'image principale.
    b) Arrêtez le service ccmexec (Agent SMS) et désactivez-le.
    c) Supprimez les certificats SMS ou les certificats clients du magasin de certificats de l'ordinateur local comme suit :
        - Mode mixte : Certificats (ordinateur local)\SMS\Certificats
        - Mode natif
            - Certificats (ordinateur local)\Personal\Certificates
            - Supprimez le certificat client émis par votre autorité de certification (généralement une infrastructure interne à clé publique)
    d) Supprimez ou renommez C:\Windows\smscfg.ini.
2. Supprimez les informations qui identifient de façon unique le client.
    a) (Facultatif) Supprimez ou déplacez les fichiers journaux de C:\Windows\System32\CCM\Logs.
    b) Installez Virtual Delivery Agent (s'il n'est pas déjà installé) et exécutez l'inventaire PvD.
    c) Arrêtez l'image principale, prenez un instantané et créez un catalogue de VM à l'aide de cet instantané.
3. Validez Personal vDisk et démarrez les services. Effectuez ces étapes une seule fois, sur chaque bureau PvD, après qu'ils aient été démarrés pour la première fois. Pour ce faire, vous pouvez utiliser un objet de stratégie de groupe du domaine, par exemple.
    - Confirmez que PvD est actif en vérifiant la présence de la clé de registre HKLM\Software\Citrix\personal vDisk\config\virtual.
    - Définissez le service ccmexec (Agent SMS) sur Automatique et démarrez le service. Le client de Configuration Manager contacte le serveur Configuration Manager et récupère les nouveaux certificats et GUID uniques.

Outils

November 6, 2018

Vous pouvez utiliser les outils et utilitaires suivants pour configurer, personnaliser et surveiller les opérations de PvD.

Fichiers de règles personnalisés

Les fichiers de règles personnalisés fournis avec PvD vous permettent de modifier le comportement par défaut des mises à jour de l'image PvD des manières suivantes :

- Visibilité des fichiers sur PvD
- Comment les modifications apportées aux fichiers sont fusionnées
- Fichiers accessibles en écriture

Pour obtenir des instructions détaillées sur les fichiers de règles personnalisés et la fonctionnalité CoW, reportez-vous aux commentaires figurant dans les fichiers qui se trouvent dans C:\ProgramData\Citrix\personal vDisk\Config sur la machine sur laquelle PvD est installé. Les fichiers appelés « custom_* » décrivent les règles et comment les activer.

Scripts resize et poolstats

Deux scripts sont fournis pour surveiller et gérer la taille des PvD ; ils se trouvent dans le dossier Support\Tools\Scripts sur le support d'installation XenDesktop. Vous pouvez également utiliser l'outil de contrôle de mise à jour de l'image PvD, qui se trouve dans le dossier Support\Tools\Scripts\PvdTool, consultez la section https://blogs.citrix.com/2014/06/02/introducing-the-pvd-image-update-monitoring-tool/ pour plus de détails.

Utilisez resize-personalvdisk-pool.ps1 pour augmenter la taille des PvD dans tous les bureaux d'un catalogue. Les composants logiciels enfichables ou modules suivants pour votre hyperviseur doivent être installés sur la machine exécutant Studio :

- XenServer requiert XenServerPSSnapin
- vCenter requiert vSphere PowerCli
- System Center Virtual Machine Manager requiert la console VMM

Utilisez personal-vdisk-poolstats.ps1 pour vérifier l'état des mises à jour de l'image et pour vérifier l'espace réservé aux applications et aux profils utilisateur dans un groupe de PvD. Exécutez ce script avant de mettre à jour une image pour détecter si des bureaux sont à court d'espace, ce qui évite les défaillances durant la mise à jour. Ce script requiert l'activation du pare-feu Windows Management Instrumentation (WMI-In) sur les bureaux PvD. Vous pouvez l'activer sur l'image principale ou via un objet de stratégie de groupe.

Si la mise à jour d'une image échoue, l'entrée dans la colonne Update indique la raison.

Réinitialiser la zone applicative

Si un bureau devient endommagé ou altéré (en installant une application défectueuse ou autre), vous pouvez restaurer la zone applicative du PvD à un état par défaut (vide). La réinitialisation laisse les données du profil utilisateur intactes.

Pour réinitialiser la zone applicative du PvD, utilisez l'une des méthodes suivantes :

- Ouvrez une session sur le bureau de l'utilisateur en tant qu'administrateur. Lancez une invite de commandes et exécutez la commande **C:\Program Files\Citrix\Personal vDisk\bin\CtxPvD.exe -s Reset**.
- Accédez au bureau de l'utilisateur dans Citrix Director. Cliquez sur **Réinitialiser Personal vDisk** puis cliquez sur **OK**.

Exporter et importer un inventaire PvD

Le processus de mise à jour de l'image fait partie intégrante de la distribution de nouvelles images vers des bureaux PvD ; il comprend l'ajustement du Personal vDisk existant pour fonctionner avec la nouvelle image de base. Pour les déploiements qui utilisent Machine Creation Services (MCS), vous pouvez exporter un inventaire à partir d'une VM active sur un partage réseau, puis l'importer dans une image principale. Un différentiel est calculé à l'aide de cet inventaire dans l'image principale. Bien que l'utilisation de la fonctionnalité d'exportation/importation de l'inventaire ne soit pas obligatoire, elle peut améliorer les performances du processus général de mise à jour de l'image.

Pour utiliser la fonctionnalité d'exportation/importation de l'inventaire, vous devez être un administrateur. Si nécessaire, authentifiez-vous auprès du partage de fichiers utilisé pour l'importation/l'exportation avec « net use ». Le contexte utilisateur doit être en mesure d'accéder aux partages de fichiers utilisés pour l'importation et l'exportation.

Exporter

- Pour exporter un inventaire, exécutez la commande d'exportation en tant qu'administrateur sur une machine qui contient un VDA avec PvD activé (version minimum 7.6) :

  ```
  Ctxpvdsvc.exe exportinventory "\<path-to-export-location>"
  ```

  Le logiciel détecte l'emplacement de l'inventaire actuel et exporte l'inventaire vers un dossier nommé « ExportedPvdInventory » à l'emplacement spécifié. Voici un extrait de la sortie de la commande :

  ```
  1 C:\Program Files\Citrix\personal vDisk\bin> .\CtxPvDSvc.exe
      exportinventory
  2 \share location\ExportedInventory
  3 Current inventory source location C:\CitrixPvD\Settings\Inventory
      \VER-LAS
  4 ...
  5 Exporting current inventory to location \ ... .
  6 ...
  7 Deleting any pre-existing inventory folder at \ ... .
  8 .Successfully exported current inventory to location \ ... .
      Error code = OPS
  ```


- Pour importer un inventaire exporté précédemment, exécutez la commande d'importation en tant qu'administrateur sur l'image principale :

Importer

Exécuter la commande d'importation en tant qu'administrateur sur l'image principale.

```
Ctxpvdsvc.exe importinventory "\<path-to-exported-inventory>"
```

Le chemin <path to exported inventory> doit être le chemin d'accès complet à l'inventaire des fichiers, qui est généralement <emplacement réseau\ExportedPvdInventory>.

L'inventaire est obtenu à partir de l'emplacement d'importation (où il a été préalablement exporté à l'aide de l'option exportinventory), puis importe l'inventaire vers le magasin d'inventaire sur l'image principale. Voici un extrait de la sortie de la commande :

```
1 C:\Program Files\Citrix\personal vDisk\bin> .\CtxPvDSvc.exe
     importinventory
2 \share location\ExportedInventory\ExportedPvdInventory
3 Importing inventory \share location\ExportedInventory\
     ExportedPvdInventory
4 ...
5 Successfully added inventory \share location\ExportedInventory\
     ExportedPvdInventory to the
6 store at c:\ProgramData\Citrix\personal vDisk\InventoryStore
```

Une fois l'exportation terminée, le partage réseau devrait inclure les noms de fichiers suivants. Après l'importation, l'inventaire magasin sur l'image principale doit inclure les mêmes noms de fichier.

- Components.DAT
- règles_fichiers
- règles_dossiers
- règles_clé_registre
- RINGTHREE.DAT
- S-1-5-18.DAT
- SAM.DAT
- SECURITY.DAT
- SNAPSHOT.DAT
- SOFTWARE.DAT
- SYSTEM.CurrentControlSet.DAT
- VDCATALOG.DAT
- vDiskJournalData

Affichages, messages et résolution des problèmes

January 23, 2019

Surveiller les PvD via des rapports

Vous pouvez utiliser un outil de diagnostic pour surveiller les modifications effectuées par les utilisateurs pour les deux parties de leurs Personal vDisks (les données de l'utilisateur et l'application). Ces modifications incluent les applications que les utilisateurs ont installé et les fichiers qu'ils ont modifié. Les modifications sont stockées dans un ensemble de rapports.

1. Sur la machine que vous voulez surveiller, exécutez **C:\Program Files\Citrix\personal vDisk\bin\CtxPvdDiag.exe**.
2. Recherchez un emplacement où vous souhaitez stocker les rapports et les journaux, sélectionnez les rapports à générer, et cliquez sur **OK**. Les rapports disponibles sont répertoriés ci-dessous.

Rapport de la ruche de logiciels : ce rapport génère deux fichiers :Software.Dat.Report.txt et Software.Dat.delta.txt.

Le fichier Software.Dat.Report.txt enregistre les modifications effectuées par l'utilisateur dans la ruche HKEY_LOCAL_MACHINE\Software. Il contient les sections suivantes :

- Liste des applications installées sur la base : les applications qui ont été installées dans Layer 0.
- Liste des logiciels installés par l'utilisateur : les applications installées par l'utilisateur sur la partie de l'application du vDisk personnel.
- Liste de logiciels désinstallés par l'utilisateur : les applications supprimées par l'utilisateur qui étaient présentes à l'origine dans Layer 0.

Voir le rapport delta de la ruche pour de plus amples informations sur Software.Dat.delta.txt.

Rapport de la ruche système : le fichier SYSTEM.CurrentControlSet.DAT.Report.txt généré enregistre les modifications apportées à la ruche HKEY_LOCAL_MACHINE\System par l'utilisateur. Il contient les sections suivantes :

- Liste des services installés par l'utilisateur : les services et les pilotes installés par l'utilisateur.
- Le démarrage des services suivants a été modifié : les services et les pilotes dont le type de démarrage a été modifié par l'utilisateur.

Rapport de la ruche de sécurité : le fichier SECURITY.DAT.Report.txt généré surveille toutes les modifications que l'utilisateur effectue dans la ruche HKEY_LOCAL_MACHINE\Security.

Rapport de ruche du gestionnaire de comptes de sécurité (SAM) : le fichier SAM.DAT.Report.txt généré surveille toutes les modifications que l'utilisateur effectue dans la ruche HKEY_LOCAL_MACHINE\SAM.

Rapport delta de la ruche : le fichier Software.Dat.delta.txt généré enregistre toutes les clés de Registre et les valeurs ajoutées ou supprimées, et toutes les valeurs modifiées par l'utilisateur dans la ruche HKEY_LOCAL_MACHINE\Software.

Journal Personal vDisk : les fichiers journaux Pud-IvmSupervisor.log, PvDActivation.log, PvDSvc.log, PvDWMI.log, SysVol-IvmSupervisor.log et vDeskService-[#].log sont générés par défaut dans *P:\Users\<compte utilisateur>\AppData\Local\Temp\PVDLOGS*, mais sont déplacés vers l'emplacement sélectionné.

Journaux du système d'exploitation Windows :

- EvtLog_App.xml et EvtLog_System.xml sont les journaux d'événements application et système au format XML du format Personal vDisk.
- Setupapi.app.log et setuperr.log contiennent des messages de journal de msiexec.exe qui était exécuté pendant l'installation de Personal vDisk.
- Setupapi.dev.log contient des messages de journal d'installation du périphérique.
- Msinfo.txt contient la sortie de msinfo32.exe. Pour de plus amples informations, veuillez consulter la documentation Microsoft.

Rapport du système de fichiers : le fichier FileSystemReport.txt généré enregistre les modifications effectuées par l'utilisateur pour le système de fichiers dans les sections suivantes :

- Fichiers déplacés : les fichiers dans Layer 0 qui ont été déplacés par l'utilisateur vers le vDisk. Les fichiers Layer 0 sont hérités de l'image principale par la machine à laquelle le Personal vDisk est connecté.
- Fichiers supprimés : les fichiers dans Layer 0 qui ont été masqués par une action de l'utilisateur (par exemple, la suppression d'une application).
- Fichiers ajoutés (MOF, INF, SYS) : les fichiers qui possèdent des extensions .mof, .inf ou .sys que l'utilisateur a ajouté au Personal vDisk (par exemple, lorsqu'ils installé une application telle que Visual Studio 2010 qui enregistre un fichier .mof pour la récupération automatique).
- Fichiers ajoutés (autres) : autres fichiers que l'utilisateur a ajouté au vDisk (par exemple, lors de l'installation d'une application).
- Fichiers de base modifiés mais pas déplacés : les fichiers dans Layer 0 que l'utilisateur a modifié mais que les pilotes Personal vDisk en mode Kernel n'ont pas capturé dans le vDisk.

Mises à jour d'image

Dans Studio, lorsque vous choisissez une machine PvD dans un catalogue de machines, l'onglet « PvD » offre un statut de surveillance lors des mises à jour de l'image, ainsi que l'heure de fin et de progression estimée. Les affichages possibles de l'état lors de la mise à jour d'une image sont : Prêt, Préparation, En attente, En échec et Demandée.

Une mise à jour d'image peut échouer pour d'autres raisons par manque d'espace ou un bureau ne

trouve pas le PvD suffisamment rapidement. Lorsque Studio indique qu'une mise à jour d'image a échoué, un code d'erreur est fourni avec un texte descriptif pour faciliter la résolution des problèmes. Utilisez l'outil de contrôle de mise à jour d'image Personal vDisk ou le script personal-vdisk-poolstats.ps1 afin de contrôler la progression de la mise à jour de l'image et obtenir les codes d'erreur associés à l'échec.

Si une mise à jour d'image échoue, les fichiers journaux suivants peuvent fournir davantage d'informations sur la résolution de ce problème :

- Journal du service PvD : C:\ProgramData\Citrix\personal vDisk\Logs\PvDSvc.log.txt
- Journal d'activation PvD : P:\PVDLOGS\PvDActivation.log.txt

Le contenu le plus récent se trouve à la fin du fichier journal.

Messages d'erreur : version 7.6 et ultérieure

Les erreurs suivantes sont valides pour la version 7.6 de PvD et version ultérieure :

- **Une erreur interne s'est produite. Vérifiez les journaux Personal vDisk pour plus de détails. Code d'erreur %d (%s)**

  Ceci est un passe-partout pour les erreurs n'appartenant à aucune catégorie, et il ne possède ainsi pas de valeur numérique. Toutes les erreurs inattendues qui se sont produites lors de la création de l'inventaire ou de la mise à jour de Personal vDisk sont indiquées par ce code d'erreur.

  - Collectez les journaux et contactez l'assistance Citrix.
  - Si cette erreur se produit lors de la mise à jour du catalogue, restaurez le catalogue vers la version précédente de l'image principale.

- **Il existe des erreurs de syntaxe dans les fichiers de règle. Consultez les journaux pour plus de détails.**

  Code d'erreur 2. Le fichier de règle contient des erreurs de syntaxe. Les fichiers journaux Personal vDisk contiennent le nom du fichier de règles et le numéro de ligne sur laquelle l'erreur de syntaxe a été détectée. Corrigez l'erreur de syntaxe dans le fichier de règle, puis recommencez l'opération.

- **L'inventaire stocké dans le Personal vDisk correspondant à la version précédente de l'image principale est endommagé ou illisible.**

  Code d'erreur 3. Le dernier inventaire est stocké dans *\ProgramData\CitrixPvD\Settings\Inventory\VER-LAST\UserData.V2.vhd*. Restaurez l'inventaire correspondant à la dernière version de l'image principale en important le dossier « VER-LAST » à partir d'une machine PvD en cours d'exécution connue associée à la version précédente de l'image principale.

- **L'inventaire stocké dans le Personal vDisk correspondant à la version précédente de l'image principale est une version supérieure.**

  Code d'erreur 4. Ceci est dû à une incompatibilité de version de Personal vDisk entre la dernière image principale et l'image principale courante. Réessayez d'effectuer la mise à jour du catalogue après l'installation de la dernière version de Personal vDisk dans l'image principale.

- **Un dépassement de capacité du journal des modifications de a été détecté.**

  Code d'erreur 5. Un dépassement de capacité du journal USN a été causé par un nombre important de modifications apportées à l'image principale lors de la création de l'inventaire. Si ce problème persiste après plusieurs tentatives, utilisez procmon pour déterminer si un logiciel tiers tente de créer ou de supprimer un grand nombre de fichiers pendant la création de l'inventaire.

- **Personal vDisk n'a pas pu détecter un disque connecté au système pour le stockage des données de l'utilisateur.**

  Code d'erreur 6. Vérifiez, tout d'abord, que le disque PvD est connecté à la VM au travers de la console de l'hyperviseur. Cette erreur se produit généralement à cause d'un logiciel de « prévention des fuites de données » empêchant l'accès au disque PvD. Si le disque PvD est connecté à la VM, essayez d'ajouter une exception pour « disque connecté » dans la configuration du logiciel de « prévention des fuites de données ».

- **Le système n'a pas été redémarré après l'installation. Effectuez le redémarrage pour appliquer les modifications.**

  Code d'erreur 7. Redémarrez le bureau et recommencez l'opération.

- **Installation altérée. Essayez de réinstaller Personal vDisk.**

  Code d'erreur 8. Installez Personal vDisk et réessayez.

- **L'inventaire Personal vDisk n'est pas à jour. Mettez à jour l'inventaire de l'image principale, puis réessayez.**

  Code d'erreur 9. L'inventaire Personal vDisk n'a pas été mis à jour dans l'image principale avant fermeture du bureau. Redémarrez l'image principale et arrêter le bureau au moyen de l'option « Mettre Personal vDisk à jour », puis créez un nouvel instantané ; utilisez cet instantané pour mettre le catalogue à jour.

- **Une erreur interne s'est produite lors du démarrage du Personal vDisk. Vérifiez les journaux Personal vDisk pour plus de détails.**

  Code d'erreur 10. Cela peut être causé par le pilote de PvD qui ne peut pas démarrer une session de virtualisation en raison d'une erreur interne ou d'une altération de Personal vDisk. Essayez de redémarrer le bureau via le Controller. Si le problème persiste, collectez les journaux et contactez l'assistance Citrix.

- **Le délai de Personal vDisk a expiré lors de la recherche d'un disque de stockage pour les paramètres de personnalisation des utilisateurs.**

  Code d'erreur 11. Cette erreur se produit lorsque le pilote PvD ne parvient pas à détecter le disque PvD dans les 30 secondes suivant le redémarrage. Ceci est généralement dû à un contrôleur SCSI non pris en charge ou une latence de stockage. Si ce problème se produit avec tous les bureaux du catalogue, modifiez le type de contrôleur SCSI associé à la « VM modèle »/« VM principale » pour un type pris en charge par la technologie Personal vDisk. Si ce problème se produit uniquement avec certains bureaux du catalogue, il peut être dû à des pics de latence de stockage dus à un nombre important de bureaux démarrant en même temps. Essayez de limiter le paramètre des actions d'alimentation actives maximales associées à la connexion hôte.

- **Le Personal vDisk a été désactivé car un arrêt du système non sécurisé a été détecté. Redémarrez la machine.**

  Code d'erreur 12. Cela peut être dû au fait que le bureau n'est pas parvenu à terminer le processus de redémarrage avec PvD activé. Essayez de redémarrer le bureau. Si le problème persiste, observez le démarrage du bureau via la console de l'hyperviseur et vérifiez si le bureau est bloqué. Si un bureau se bloque lors du démarrage, restaurez le PvD à partir d'une sauvegarde (si vous en possédez une) ou réinitialisez le PvD.

- **La lettre de lecteur spécifiée pour le montage du Personal vDisk n'est pas disponible.**

  Code d'erreur 13. Cela peut être dû au fait que le PvD n'est pas parvenu à monter le disque PvD lors du montage spécifié par l'administrateur. Le montage du disque PvD échouera si la lettre de lecteur est déjà utilisée par d'autres matériels. Sélectionnez une lettre différente comme point de montage pour le Personal vDisk.

- **Les pilotes en mode noyau de Personal vDisk n'ont pas réussi à s'installer.**

  Code d'erreur 14. Personal vDisk installe des pilotes lors de la première mise à jour de l'inventaire après l'installation. Certains produits anti-virus empêchent l'installation de ce pilote en dehors du contexte d'un programme d'installation. Désactivez temporairement l'analyse antivirus en temps réel ou ajoutez des exceptions dans l'antivirus pour les pilotes PvD lors de la première création d'inventaire.

- **Impossible de créer un instantané du volume système. Vérifiez que le service de cliché instantané des volumes est activé.**

  Code d'erreur 15. Cela peut se produire si le service de cliché instantané des volumes est désactivé. Activez le service de cliché instantané des volumes et réessayez d'effectuer un inventaire.

- **L'activation du journal des modifications a échoué. Réessayez après une attente de quelques minutes.**

  Code d'erreur 16. Personal vDisk utilise le journal des modifications pour le suivi des modifications apportées à l'image principale. Au cours de la mise à jour d'un inventaire, si le PvD détecte

que le journal des modifications est désactivé, il tente de l'activer, cette erreur se produit lorsque cette tentative échoue. Patientez quelques minutes, puis réessayez.

- **Il n'y a pas suffisamment d'espace disponible sur le volume système.**

  Code d'erreur 17. Il n'y a pas suffisamment d'espace disponible sur le lecteur C du bureau pour l'opération de mise à jour de l'image. Développez le volume système ou supprimez des fichiers non utilisés pour libérer de l'espace dans le volume système. La mise à jour d'image doit commencer après le redémarrage suivant.

- **Il n'y a pas suffisamment d'espace disponible dans le stockage Personal vDisk. Développez le stockage Personal vDisk pour fournir plus d'espace.**

  Code d'erreur 18. Il n'y a pas suffisamment d'espace disponible sur le lecteur Personal vDisk lors de la réalisation d'une opération de mise à jour de l'image. Développez le stockage Personal vDisk ou supprimez des fichiers non utilisés pour libérer de l'espace dans le stockage Personal vDisk. La mise à jour d'image devrait redémarrer après le redémarrage suivant.

- **Le stockage Personal vDisk est trop engagé. Développez le stockage Personal vDisk pour fournir plus d'espace.**

  Code d'erreur 19. Il n'y a pas suffisamment d'espace disponible sur le lecteur Personal vDisk pour accueillir complètement un « UserData.V2.vhd » provisionné. Développez le stockage Personal vDisk ou supprimez des fichiers non utilisés pour libérer de l'espace dans le stockage Personal vDisk.

- **Registre système endommagé.**

  Code d'erreur 20. Le Registre système est altéré, endommagé, manquant ou illisible. Réinitialisez le Personal vDisk ou effectuez sa restauration à partir d'une sauvegarde antérieure.

- **Une erreur interne s'est produite lors de la réinitialisation de Personal vDisk. Vérifiez les journaux Personal vDisk pour plus de détails.**

  Code d'erreur 21. Ceci est un passe-partout pour toutes les erreurs rencontrées lors de la réinitialisation d'un Personal vDisk. Collectez les journaux et contactez l'assistance Citrix.

- **Échec de réinitialisation de Personal vDisk, car il n'y a pas suffisamment d'espace disponible dans le stockage Personal vDisk.**

  Code d'erreur 22. Il n'y a pas suffisamment d'espace disponible sur le lecteur Personal vDisk lors de la réalisation d'une opération de réinitialisation. Développez le stockage Personal vDisk ou supprimez des fichiers non utilisés pour libérer de l'espace dans le stockage Personal vDisk.

Messages d'erreur : versions antérieures à 7.6

Les erreurs suivantes sont valides pour les versions PvD 7.x antérieures à 7.6 :

- **Échec de démarrage. Personal vDisk n'a pas pu détecter de disque de stockage pour les paramètres de personnalisation des utilisateurs.**

  Le logiciel PvD n'a pas réussi à trouver le Personal vDisk (par défaut le lecteur P:) ou n'a pas pu le monter en tant que point de montage sélectionné par l'administrateur lors de la création du catalogue.

  - Cherchez l'entrée suivante dans le journal du service PvD : « PvD 1 status –> 18:183 ».
  - Si vous utilisez une version de PvD antérieure à la version 5.6.12, la mise à niveau vers la dernière version résout ce problème.
  - Si vous utilisez la version 5.6.12 ou supérieure, utilisez l'outil de gestion du disque (diskmgmt.msc) pour déterminer si le lecteur P: est présent en tant que volume non monté. S'il est présent, exécutez chkdsk sur le volume pour déterminer s'il est endommagé, et essayez de le réparer à l'aide de chkdsk.

- **Échec de démarrage. Échec de démarrage de Citrix Personal vDisk. Pour obtenir de l'aide… Code d'état : 7, code d'erreur : 0x70**

  Le code d'état 7 implique qu'une erreur s'est produite lors de la tentative de mise à jour du PvD. Le code d'erreur peut être l'un des suivants :

Code d'erreur	Description
0x20000001	Impossible d'enregistrer le package de différentiel, probablement à cause d'un espace insuffisant dans le VHD.
0x20000004	Impossible d'obtenir les privilèges requis pour la mise à jour du PvD.
0x20000006	Impossible de charger la ruche depuis l'image PvD où l'inventaire PvD, probablement en raison d'une image ou d'un inventaire PvD endommagé.
0x20000007	Impossible de charger l'inventaire du système de fichiers, probablement en raison d'une image ou d'un inventaire PvD altéré.
0x20000009	Impossible d'ouvrir le fichier contenant l'inventaire du système de fichiers, probablement en raison d'une image ou d'un inventaire PvD altéré.
0x2000000B	Impossible d'enregistrer le package de différentiel, probablement à cause d'un espace insuffisant dans le VHD.

Code d'erreur	Description
0x20000010	Impossible de charger le package de différentiel.
0x20000011	Fichiers de règles manquants.
0x20000021	Inventaire PvD endommagé.
0x20000027	Le catalogue « MojoControl.dat » est altéré.
0x2000002B	Inventaire PvD endommagé ou manquant.
0x2000002F	Impossible d'enregistrer le fichier MOF installé par l'utilisateur sur la mise à jour de l'image, mettez à niveau vers 5.6.12 pour résoudre le problème.
0x20000032	Consultez le fichier PvDactivation.log.txt pour rechercher la dernière entrée de journal avec un code d'erreur Win32.
0x20	Impossible de monter le conteneur d'application pour une mise à jour d'image, mettez à niveau vers 5.6.12 pour résoudre le problème.
0x70	Espace insuffisant sur le disque.

- **Échec de démarrage. Citrix Personal vDisk n'est pas parvenu à démarrer [ou Personal vDisk a rencontré une erreur interne]. Pour obtenir de l'aide... Code d'état : 20, code d'erreur : 0x20000028**

  Les Personal vDisk ont été détecté mais aucune session PvD n'a pu être créée.

  Collectez les journaux et vérifiez SysVol-IvmSupervisor.log pour des échecs de création de session :

  1. Recherchez l'entrée suivante dans le journal : « IvmpNativeSessionCreate: failed to create native session, status XXXXX ».
  2. Si l'état est 0xc00002cf, vous pouvez résoudre le problème en ajoutant une nouvelle version de l'image principale au catalogue. Le code d'état implique une saturation du journal USN en raison d'un grand nombre de changements apportés après la mise à jour d'un inventaire.
  3. Redémarrez le bureau virtuel affecté. Si le problème persiste, contactez le support technique Citrix.

- **Échec de démarrage. Citrix Personal vDisk a été désactivé car un arrêt du système non sécurisé a été détecté. Pour réessayer, sélectionnez Réessayez. Si le problème persiste, contactez votre administrateur système.**

  La VM groupée ne peut pas terminer son démarrage avec le PvD activé. Déterminez tout d'abord la raison pour laquelle le démarrage ne peut pas être effectué. Les raisons possibles peuvent être l'apparition d'un écran bleu car :

  - Un produit anti-virus incompatible est présent sur l'image principale, par exemple des versions anciennes de Trend Micro.
  - L'utilisateur a installé un logiciel incompatible avec PvD. Cela est fort peu probable, mais vous pouvez le vérifier en ajoutant une nouvelle machine au catalogue et voir si elle redémarre correctement.
  - L'image PvD est endommagée. Cela a été rencontré dans la version 5.6.5.

  Pour vérifier que la VM affiche un écran bleu ou qu'elle redémarre prématurément :

  - Ouvrez une session sur la machine via la console de l'hyperviseur.
  - Cliquez sur Try Again et attendez que la machine s'arrête.
  - Démarrez la machine via Studio.
  - Utilisez la console de l'hyperviseur pour observer la console de machine lorsqu'elle démarre.

  Autres résolutions de problèmes :

  - Collectez l'image mémoire de la machine affichant l'écran bleu et envoyez-la à l'assistance technique de Citrix pour une analyse plus approfondie.
  - Vérifiez les erreurs dans les journaux d'événements associés au PvD :
    1. Montez UserData.V2.vhd à partir de la racine du lecteur P: à l'aide de DiskMgmt.msc en cliquant sur Action > Attach VHD.
    2. Lancez Eventvwr.msc.
    3. Ouvrez le journal d'événements système (Windows\System32\winevt\logs\system.evtx) depuis UserData.V2.vhd en cliquant sur Action > Open saved logs.
    4. Ouvrez le journal d'événements d'applications (Windows\System32\winevt\logs\application.evtx) depuis UserData.V2.vhd en cliquant sur Action > Open saved logs.

- **Le Personal vDisk ne peut pas démarrer. Le Personal vDisk n'a pas pu démarrer car l'inventaire n'a pas été mis à jour. Mettez l'inventaire à jour dans l'image principale, puis réessayez. Code d'état : 15, code d'erreur : 0x0**

  L'administrateur a sélectionné un instantané incorrect lors de la création ou de la mise à jour du catalogue PvD (en d'autres termes, l'image principale n'a pas été arrêtée à l'aide de l'option Update Personal vDisk lors de la création de l'instantané).

Événements consignés par Personal vDisk

Si Personal vDisk n'est pas activé, vous pouvez afficher les événements suivants dans l'Observateur d'événements de Windows. Sélectionnez le nœud Applications dans le panneau de gauche ; la Source des événements dans le panneau de droite est Citrix Personal vDisk. Si Personal vDisk est activé, aucun de ces événements n'est affiché.

Un ID d'événement de 1 signifie un message d'information et un ID de 2 signifie une erreur. Les événements ne peuvent pas tous être utilisés dans chaque version de Personal vDisk.

ID d'événement	Description
1	État de Personal vDisk : inventaire de mise à jour démarré.
1	État de Personal vDisk : inventaire de mise à jour terminé. GUID : %s.
1	État de Personal vDisk : mise à jour de l'image démarrée.
1	État de Personal vDisk : mise à jour de l'image terminée.
1	Réinitialisation en cours.
1	OK.
2.	État de Personal vDisk : échec de l'inventaire de mise à jour avec : %s.
2.	État de Personal vDisk : échec de mise à jour de l'image avec : %s.
2.	État de Personal vDisk : échec de mise à jour de l'image avec erreur interne.
2.	État de Personal vDisk : échec de l'inventaire de mise à jour avec : erreur interne.
2.	Personal vDisk a été désactivé suite à un arrêt incorrect.
2.	Échec de la mise à jour de l'image. Code d'erreur %d.
2.	Personal vDisk a rencontré une erreur interne. Code d'état[%d] Code d'erreur[0x%X].
2.	Échec de réinitialisation de Personal vDisk.

ID d'événement	Description
2.	Détection du disque utilisé pour stocker les paramètres de personnalisation utilisateur impossible.
2.	Espace disponible sur le disque de stockage insuffisant pour créer un conteneur Personal vDisk.

Problèmes connus indépendants des versions

Les problèmes de PvD suivants ont été identifiés :

- Lorsqu'une application installée sur un Personal vDisk (PvD) est liée à une autre application de la même version installée sur l'image principale, l'application sur le PvD peut s'arrêter de fonctionner après une mise à jour d'image. Ceci se produit si vous désinstallez l'application à partir de l'image principale ou si vous effectuez une mise à niveau vers une version plus récente, car cette action supprime les fichiers nécessaires à l'application sur le PvD à partir de l'image principale. Pour éviter ce problème, gardez l'application contenant les fichiers nécessaires à l'application sur le PvD sur l'image principale.

  Par exemple, l'image principale contient Office 2007 et un utilisateur installe Visio 2007 sur le PvD ; les applications Office et Visio fonctionnent correctement. Plus tard, l'administrateur remplace Office 2007 avec Office 2010 sur l'image principale, puis met à jour toutes les machines affectées par l'image mise à jour. Visio 2007 ne fonctionne plus. Pour éviter ce problème, gardez Office 2007 dans l'image principale. [320915]

- Lors du déploiement de McAfee Virus Scan Enterprise (VSE), utilisez la version 8.8 correctif 4 ou version ultérieure sur une image principale si vous utilisez Personal vDisk. [303472]
- Si un raccourci créé vers un fichier dans l'image principale cesse de fonctionner (car le raccourci cible est renommé au sein de PvD), recréez le raccourci. [367602]
- N'utilisez pas de liens absolus/directs dans une image principale. [368678]
- La fonctionnalité de sauvegarde et de restauration de Windows 7 n'est pas prise en charge sur le Personal vDisk. [360582]
- Après qu'une mise à jour de l'image principale ait été appliquée, l'utilisateur local et la console de groupe sont inaccessibles ou affichent des données incohérentes. Pour résoudre le problème, réinitialisez les comptes d'utilisateur sur la VM, ce qui nécessite la réinitialisation de la ruche de sécurité. Ce problème est résolu dans la version 7.1.2 (et fonctionne pour les machines

virtuelles créées dans les versions ultérieures), mais le correctif ne fonctionne pas pour les machines virtuelles qui ont été créées avec une version antérieure puis mises à niveau. [488044]

- Lors de l'utilisation d'une VM regroupée sur un environnement d'hyperviseur ESX, les utilisateurs voient une invite de redémarrage si le type de contrôleur SCSI sélectionné est de type « VMware Paravirtual ». Pour contourner ce problème, utilisez un type de contrôleur LSI SCSI. [394039]
- Après une réinitialisation de PvD sur un bureau créé à l'aide de Provisioning Services, il se peut que les utilisateurs reçoivent une invite de redémarrage après l'ouverture de session sur la VM. Pour contourner le problème, redémarrez le bureau. [340186]
- Les utilisateurs de bureaux Windows 8.1 peuvent ne pas être en mesure d'ouvrir une session sur leurs PvD. Un administrateur peut voir le message « PvD was disabled due to unsafe shutdown » et le journal PvDActivation peut contenir le message « Failed to load reg hive [\Device\IvmVhdDisk00000001\CitrixPvD\Settings\RingCube.dat]. ». Ceci se produit lorsque la VM de l'utilisateur s'arrête dangereusement. Pour contourner le problème, réinitialisez le Personal vDisk. [474071]

Supprimer des composants

January 23, 2019

Pour supprimer des composants, Citrix vous recommande d'utiliser la fonctionnalité Windows destinée à supprimer ou modifier des programmes. Vous pouvez également supprimer des composants à l'aide de la ligne de commande, ou d'un script sur le support d'installation.

Lorsque vous supprimez des composants, les composants pré-requis ne sont pas supprimés, et les paramètres du pare-feu ne sont pas modifiés. Lorsque vous supprimez un Controller, le logiciel SQL Server et les bases de données ne sont pas supprimés.

Avant de supprimer un Controller, supprimez-le du site. Avant de supprimer Studio ou Director, Citrix recommande de les fermer.

Si vous avez mis à niveau un Controller à partir d'un déploiement antérieur contenant l'Interface Web, vous devez supprimer le composant Interface Web séparément ; vous ne pouvez pas utiliser le programme d'installation pour supprimer l'Interface Web.

Lorsque vous supprimez un VDA, la machine redémarre automatiquement après la suppression, par défaut.

Supprimer des composants à l'aide de la fonctionnalité Windows pour la suppression ou la modification de programmes

À partir de la fonctionnalité Windows pour la suppression ou la modification de programmes :

- Pour supprimer un Controller, Studio, Director, le serveur de licences ou StoreFront, sélectionnez Citrix XenApp <*version*> ou Citrix XenDesktop <*version*>, puis cliquez avec le bouton droit de la souris et sélectionnez **Désinstaller**. Le programme d'installation démarre, et vous permet de sélectionner les composants à supprimer. Sinon, vous pouvez supprimer StoreFront en cliquant avec le bouton droit de la souris sur **Citrix StoreFront** et en sélectionnant **Désinstaller**.
- Pour supprimer un VDA, sélectionnez **Citrix Virtual Delivery Agent** <*version*>, puis cliquez avec le bouton droit de la souris et sélectionnez **Désinstaller**. Le programme d'installation démarre et vous permet de sélectionner les composants à supprimer.
- Pour supprimer le Serveur d'impression universelle, sélectionnez **Serveur d'impression universelle Citrix**, puis cliquez avec le bouton droit de la souris et sélectionnez **Désinstaller**.

Supprimer les composants principaux à l'aide de la ligne de commande

À partir du répertoire d'installation \x64\XenDesktop sur le support d'installation, exécutez la commande **XenDesktopServerSetup.exe**.

- Pour supprimer un ou plusieurs composants principaux, utilisez les options /remove et /components.
- Pour supprimer tous les composants, utilisez l'option /removeall.

Pour plus d'informations sur les commandes et les paramètres, consultez la section Installer à l'aide de la ligne de commande.

Par exemple, les commandes suivantes suppriment Studio.

```
1 \x64\XenDesktop Setup\XenDesktopServerSetup.exe /remove /components
     studio
```

Supprimer un VDA à l'aide de la ligne de commande

À partir du répertoire d'installation \x64\XenDesktop sur le support d'installation, exécutez la commande **XenDesktopVdaSetup.exe**.

- Pour supprimer un ou plusieurs composants principaux, utilisez les options /remove et /components.
- Pour supprimer tous les composants, utilisez l'option /removeall.

Pour plus d'informations sur les commandes et les paramètres, consultez la section Installer à l'aide de la ligne de commande.

Par exemple, la commande suivante supprime le VDA et Citrix Receiver.

```
1 \x64\XenDesktop Setup\XenDesktopVdaSetup.exe /removeall
```

Pour supprimer des VDA à l'aide d'un script dans Active Directory, consultez la section Installer ou supprimer des Virtual Delivery Agents à l'aide de scripts.

Mettre à niveau et migrer

November 6, 2018

Mise à niveau

Mise à niveau des déploiements de modifications vers les dernières versions des composants sans définir de nouvelles machines ou sites. Cela s'appelle une mise à niveau sur place. Vous pouvez mettre à niveau vers la version actuelle depuis :

- XenDesktop 5.6 *
- XenDesktop 7.0
- XenDesktop 7.1
- XenApp/XenDesktop 7.5
- XenApp/XenDesktop 7.6
- XenApp/XenDesktop 7.6 LTSR
- XenApp/XenDesktop 7.7
- XenApp/XenDesktop 7.8
- XenApp/XenDesktop 7.9
- XenApp/XenDesktop 7.11
- XenApp/XenDesktop 7.12
- XenApp/XenDesktop 7.13
- XenApp/XenDesktop 7.14
- XenApp/XenDesktop 7.15 LTSR

* Pour mettre à niveau depuis XenDesktop 5.6, vous devez d'abord mettre à niveau vers 7.6 LTSR (avec la dernière CU), puis mettre à niveau vers 7.15 LTSR (avec la dernière CU).

Vous pouvez également mettre à niveau un serveur de tâches XenApp 6.5 vers un VDA actuel pour système d'exploitation Windows Server. Ceci est une activité supplémentaire à la migration de XenApp 6.5. Voir la section Mettre à niveau une tâche XenApp 6.5 vers un VDA pour OS Windows Server

Pour effectuer la mise à niveau, procédez comme suit :

1. Exécutez le programme d'installation sur les machines sur lesquelles les composants principaux et les VDA sont installés. Le logiciel détermine si une mise à niveau est disponible et installe la nouvelle version.
2. Utilisez Studio nouvellement mis à niveau pour mettre à niveau la base de données et le site.

Pour de plus amples informations, consultez la section Mettre un déploiement à niveau.

Pour plus d'informations sur l'installation des corrections pour le Controller, consultez l'article CTX201988.

Migrer

La migration déplace les données depuis déploiement antérieur vers la version la plus récente. Vous pouvez migrer un déploiement XenApp 6. La migration comprend l'installation de composants actuels et la création d'un nouveau site, l'exportation de données à partir de l'ancienne batterie, puis l'importation des données vers le nouveau site.

Conseil : pour de plus amples informations sur les modifications apportées à l'architecture, aux composants et aux fonctionnalités pour les versions 7.x, consultez Modifications apportées dans la version 7.x.

Pour effectuer la migration de XenApp 6.5 :

1. Installez les composants de base et créez un nouveau site XenApp.
2. Dans le Controller XenApp 6.5, utilisez les applets de commande PowerShell pour l'exportation des données de stratégie et/ou de batterie vers les fichiers XML. Vous pouvez modifier le contenu de fichier XML pour personnaliser les informations que vous allez importer.
3. Dans le nouveau site, utilisez les applets de commande PowerShell et les fichiers XML pour importer les données de stratégie et/ou d'application vers le nouveau site.
4. Effectuez les tâches de post-migration dans le nouveau site.

Pour plus d'informations, voir Migrer XenApp 6.x.

Modifications apportées dans la version 7.x

January 23, 2019

L'architecture, la terminologie et les fonctionnalités de XenApp et XenDesktop ont changé à compter des versions 7.x. Si vous ne connaissez que les versions antérieures à 7.x, cet article peut vous aider à vous familiariser avec les modifications.

Une fois que vous avez migré vers la version 7.x, les modifications apportées aux versions ultérieures sont répertoriées dans Nouveautés.

Sauf mention contraire, *7.x* fait référence à XenApp 7.5 ou version ultérieure et XenDesktop version 7 ou ultérieure.

Cet article fournit une vue d'ensemble. Pour obtenir des informations détaillées sur la migration depuis une version antérieure à 7.x vers la version la plus récente, consultez la section Mettre à niveau vers XenApp 7.

Différences d'éléments entre XenApp 6 et la version XenApp actuelle

Bien qu'ils ne soient pas totalement équivalents, le tableau suivant permet de mapper des éléments de fonctionnalité de XenApp 6.5 et versions précédentes avec XenApp et XenDesktop 7.x. Les différences d'architecture sont décrites plus loin.

Concepts dans XenApp 6.x et versions antérieures	Concepts correspondants dans la version 7.x
Independent Management Architecture (IMA)	FlexCast Management Architecture (FMA)
Batterie	Site
Groupe de tâches	Catalogue de machines, groupe de mise à disposition
Tâche	Virtual Delivery Agent (VDA), machine avec OS de serveur, VDA avec OS de serveur, machine avec OS de bureau, VDA avec OS de bureau
Machine RDS (Remote Desktop Services) ou Terminal Server	Machine avec OS de serveur, VDA avec OS de serveur
Collecteur de zone et de données	Delivery Controller
Delivery Services Console	Citrix Studio et Citrix Director
Publication d'applications	Mise à disposition des applications
Magasin de données	Base de données
Calculateur de charge	Stratégie de gestion de charge
Administrateur	Administrateur délégué, rôle, étendue

Différences d'architecture

À compter des versions 7.x, XenApp et XenDesktop sont basés sur FlexCast Management Architecture (FMA). FMA est une architecture orientée services qui permet l'interopérabilité et la gestion de modularité sur les technologies Citrix. FMA fournit une plate-forme pour la mise à disposition

d'applications, la mobilité, les services, le provisioning flexible et le cloud.

FMA remplace le service IMA (Independent Management Architecture) utilisé dans XenApp 6.5 et versions antérieures.

Ces éléments représentent les éléments clé de FMA en termes de la façon dont ils sont liés aux éléments de XenApp 6.5 et versions précédentes :

- **Sites de mise à disposition :** les batteries sont des objets de niveau supérieur dans XenApp 6.5 et versions antérieures. Dans XenApp 7.x et XenDesktop 7.x, le site représente l'élément de plus haut niveau. Les sites offre des bureaux et des applications aux groupes d'utilisateurs. FMA requiert que vous vous trouviez dans un domaine pour déployer un site. Par exemple, pour installer les serveurs, votre compte doit disposer des privilèges d'administrateur local et être un utilisateur de domaine dans Active Directory.
- **Catalogues de machines et groupes de mise à disposition :** les machines hébergeant des applications dans XenApp 6.5 et versions précédentes appartenaient à des groupes de tâches pour une gestion efficace des applications et du logiciel serveur. Les administrateurs peuvent gérer toutes les machines d'un groupe de tâches comme une unité unique pour leurs besoins de gestion d'application et d'équilibrage de charge. Des dossiers étaient utilisés pour organiser les applications et les machines. Dans XenApp 7.x et XenDesktop 7.x, vous pouvez utiliser une combinaison de catalogues de machines, de groupes de mise à disposition et de groupes d'applications pour gérer les machines, l'équilibrage de charge et les applications ou les bureaux hébergés. Vous pouvez également utiliser des dossiers d'applications.
- **VDA :** dans XenApp 6.5 et versions précédentes, les machines de travail des groupes de tâches exécutaient les applications pour l'utilisateur et communiquaient avec les collecteurs de données. Dans XenApp 7.x et XenDesktop 7.x, le VDA communique avec les Delivery Controller qui gèrent les connexions utilisateur.
- **Delivery Controller :** dans XenApp 6.5 et versions précédentes, il existait une zone principale responsable des requêtes de connexion utilisateur et des communications avec les hyperviseurs. Dans XenApp 7.x et XenDesktop 7.x, les Controller du site distribuent et gèrent les demandes de connexion. Dans XenApp 6.5 et versions précédentes, les zones fournies de manière à agréger les serveurs et répliquer des données entre des connexions de réseau étendu. Bien que les zones n'aient pas d'équivalent exact dans XenApp 7.x et XenDesktop 7.x, la fonctionnalité des zones et préférences de zone 7.x aide les utilisateurs situés dans des régions éloignées à se connecter à des ressources sans que leurs connexions soient obligées de traverser des segments important de réseau étendu.
- **Studio et Director :** utilisez la console Studio pour configurer vos environnements et fournir aux utilisateurs un accès aux applications et aux bureaux. Studio remplace la console Delivery Services Console dans XenApp 6.5 et versions antérieures. Les administrateurs peuvent utiliser Director pour contrôler l'environnement, observer les machines des utilisateurs et résoudre les problèmes informatiques. Pour observer les utilisateurs, l'Assistance à distance Windows doit être activée ; elle est activée par défaut lorsque le VDA est installé.

- **Mise à disposition d'applications :** XenApp 6.5 et versions précédentes utilise l'assistant de publication d'application pour préparer les applications et les mettre à la disposition des utilisateurs. Dans XenApp 7.x et XenDesktop 7.x, vous utilisez Studio pour créer et ajouter des applications afin de les mettre à disposition auprès des utilisateurs qui sont inclus dans un groupe de mise à disposition et éventuellement des groupes d'applications. À l'aide de Studio, vous devez tout d'abord configurer un site, créer et spécifier des catalogues de machines, puis créer des groupes de mise à disposition qui utilisent les machines de ces catalogues. Les groupes de mise à disposition déterminent quels utilisateurs ont accès aux applications que vous mettez à disposition. Vous pouvez également choisir de créer des groupes d'applications comme une alternative à plusieurs groupes de mise à disposition.
- **Base de données :** XenApp 7.x et XenDesktop 7.x n'utilisent pas le magasin de données IMA pour obtenir des informations de configuration. Ils utilisent une base de données Microsoft SQL Server pour stocker les informations de configuration et de session.
- **Stratégie de gestion de charge :** dans XenApp 6.5 et versions précédentes, les calculateurs de charge utilisent des mesures prédéfinies pour déterminer la charge sur une machine. Les connexions utilisateur peuvent être associées aux machines possédant une charge moins importante. Dans XenApp 7.x et XenDesktop 7.x, utilisez les stratégies de gestion de la charge pour l'équilibrage de charge entre les machines.
- **Administration déléguée :** dans XenApp 6.5 et versions précédentes, vous pouvez créer des administrateurs personnalisés et leur attribuer des autorisations basées sur des dossiers et des objets. Dans XenApp 7.x et XenDesktop 7.x, les administrateurs personnalisés sont basés sur des rôles et des paires d'étendues. Un rôle représente une fonction de tâche et possède des permissions définies qui lui sont associées afin de permettre la délégation. Une étendue représente une collection d'objets. Les rôles d'administrateur intégré possèdent des ensembles de permissions spécifiques, tels que l'assistance technique, des applications, l'hébergement et les catalogues. Par exemple, les administrateurs de bureaux d'assistance ne peuvent fonctionner qu'avec des utilisateurs individuels sur ces sites spécifiques, alors que les administrateurs complets peuvent contrôler la totalité du déploiement et résoudre les problèmes du service informatique.

Comparaison des fonctionnalités

La transition vers FMA signifie également que certaines fonctionnalités disponibles dans XenApp 6.5 et versions précédentes sont implémentées différemment ou nécessitent que vous utilisiez d'autres fonctionnalités, composants, ou outils pour obtenir les mêmes objectifs.

Au lieu de cela, dans XenApp 6.5 et versions antérieures :	Utilisez ceci dans 7.x :
Pré-lancement de session et persistance de session configurés avec des paramètres de stratégie	Le pré-lancement de session et la persistance de session sont configurés en modifiant les paramètres du groupe de mise à disposition. Comme dans XenApp 6.5, ces fonctionnalités permettent aux utilisateurs de se connecter à des applications plus rapidement, en démarrant des sessions avant qu'elles ne soient requises (pré-lancement de session) et en gardant les sessions actives après qu'un utilisateur ferme toutes les applications (persistance de session). Dans XenApp 7.x et XenDesktop 7.x, vous activez ces fonctionnalités pour les utilisateurs spécifiés en configurant ces paramètres pour les groupes de mise à disposition existants. Consultez la section Configurer le pré-lancement de session et la persistance de session.
Prise en charge des utilisateurs non authentifiés (anonymes) fournie lors de l'octroi de droits à l'utilisateur anonyme lors de la définition des propriétés des applications publiées	Prise en charge des utilisateurs non authentifiés (anonymes) fournie par la configuration de cette option lors de la définition des propriétés de l'utilisateur d'un groupe de mise à disposition. Consultez la section Utilisateurs.
Le cache de l'hôte local permet aux serveurs de tâches de fonctionner même lorsqu'une connexion au magasin de données n'est pas disponible	Le cache d'hôte local permet aux opérations de négociation de connexion de se poursuivre lorsque la connexion entre un Controller et la base de données du site échoue. Cette implémentation est plus solide et requiert moins de maintenance. Consultez la section Cache d'hôte local.
Streaming d'application	Citrix App-V met à disposition des applications livrées en streaming, gérées à l'aide de Studio. Consultez la section App-V.
Interface Web	Citrix vous recommande d'effectuer la transition vers StoreFront.

Au lieu de cela, dans XenApp 6.5 et versions antérieures :	Utilisez ceci dans 7.x :
SmartAuditor pour enregistrer les activités à l'écran d'une session d'utilisateur	À compter de 7.6 Feature Pack 1, cette fonctionnalité est fournie par l'enregistrement de session. Vous pouvez également utiliser la journalisation de la configuration pour consigner toutes les activités de session d'un point de vue administratif.
La fonctionnalité de gestion de la capacité et de la consommation pour vous aider à réduire la consommation d'énergie et à gérer la capacité du serveur.	Utilisez Microsoft Configuration Manager.

Prise en charge et modifications des fonctionnalités

Les fonctionnalités suivantes ne sont actuellement pas fournies, ne sont plus prises en charge, ou ont beaucoup changé dans XenApp ou XenDesktop, à compter des versions 7.x.

Cryptage ICA Sécurisé en-dessous de 128 bits : dans les versions antérieures à 7.x, Secure ICA pouvait crypter les connexions clientes pour le cryptage de base, 40 bits, 56 bits et 128 bits. Dans les versions 7.x, le cryptage Secure ICA est uniquement disponible pour le cryptage 128 bits.

Impression d'ancienne génération : les fonctionnalités d'impression suivantes ne sont plus prises en charge dans les versions 7.x :

- Rétrocompatibilité pour les clients DOS et les imprimantes 16 bits.
- Prise en charge des imprimantes connectées aux systèmes d'exploitation Windows 95 et Windows NT, y compris les propriétés d'imprimante étendues et Win32FavorRetainedSetting.
- Possibilité d'activer ou désactiver les imprimantes conservées et restaurées automatiquement.
- DefaultPrnFlag, un paramètre de registre pour les serveurs qui est utilisé pour activer ou désactiver des imprimantes conservées et restaurées automatiquement, qui sont stockées dans les profils utilisateur sur le serveur.

Les noms d'imprimantes clientes d'ancienne génération sont pris en charge.

Secure Gateway : dans les versions antérieures à 7.x, Secure Gateway était une option pour sécuriser les connexions entre le serveur et les machines utilisateur. NetScaler Gateway est l'option de remplacement pour sécuriser les connexions externes.

Observation des utilisateurs : dans les versions antérieures à la version 7.x, les administrateurs définissaient des stratégies pour contrôler l'observation utilisateur-utilisateur. Dans les versions 7.x, l'observation des utilisateurs finaux est une fonctionnalité intégrée du composant Director, qui utilise

Microsoft Remote Assistance pour autoriser les administrateurs à observer et résoudre les problèmes de mise à disposition des applications transparentes et des bureaux virtuels.

Redirection Flash v1 : les clients qui ne prennent pas en charge la redirection Flash de deuxième génération (y compris les versions Citrix Receiver pour Windows antérieures à la version 3.0, Citrix Receiver pour Linux antérieures à la version 11.100 et Citrix Online Plug-in 12.1) retourneront à la restitution côté serveur pour les fonctionnalités de redirection Flash d'ancienne génération. Les VDA inclus avec les versions 7.x prennent en charge les fonctionnalités de redirection Flash de deuxième génération.

Écho local du texte : cette fonctionnalité était utilisée avec une version antérieure des technologies d'application Windows pour accélérer l'affichage du texte saisi sur les machines utilisateur sur des connexions à latence élevée. Elle n'est pas incluse dans les versions 7.x à cause des améliorations apportées au sous-système graphique et SuperCodec HDX.

Single Sign-On : cette fonctionnalité, qui fournit le mot de passe de sécurité, n'est pas prise en charge pour les environnements Windows 8, Windows Server 2012 et les versions des systèmes d'exploitation Windows plus récentes prises en charge. Elle est toujours prise en charge pour les environnements Windows 2008 R2 et Windows 7, mais n'est pas incluse dans les versions 7.x. Vous pouvez la rechercher sur le site Web de téléchargement Citrix : https://citrix.com/downloads.

Prise en charge de base de données Oracle : les versions 7.x nécessitent une base de données SQL Server.

Suivi et rétablissement de l'état (HMR) : dans les versions antérieures à la version 7.x, HMR peut effectuer des tests sur les serveurs d'une batterie de serveurs afin de contrôler leur état et détecter tout problème éventuel. Dans les versions 7.x, Director offre une vue centralisée de l'intégrité du système en présentant l'analyse et les alertes de l'ensemble de l'infrastructure à partir de la console Director.

Fichiers ICA personnalisés : les fichiers ICA personnalisés étaient utilisés pour activer les connexions directes à partir des machines utilisateur (avec le fichier ICA) pour une machine spécifique. Dans les versions 7.x, cette fonctionnalité est désactivée par défaut, mais peut être activée pour l'utilisation normale à l'aide d'un groupe local ou peut être utilisée en mode haute disponibilité si le Controller devient non disponible.

Pack d'administration de System Center Operations Manager (SCOM) 2007 : le pack d'administration, qui surveille l'activité des batteries de serveurs XenApp à l'aide de SCOM, ne prend pas en charge les versions 7.x. Pour plus d'informations, consultez le Citrix SCOM Management Pack pour XenApp et XenDesktop.

Fonction CNAME : la fonction CNAME était activée par défaut dans les versions antérieures à 7.x. Les déploiements qui dépendent des enregistrements CNAME pour le nouveau routage FQDN et l'utilisation de noms NETBIOS peut échouer. Dans les versions 7.x, la mise à jour automatique de Delivery Controller met à jour la liste de Controller dynamiquement et notifie automatiquement les VDA lorsque les Controller sont ajoutés et supprimés du site. La fonctionnalité de mise à jour

automatique du Controller est activée par défaut dans les stratégies Citrix, mais peut être désactivé. Sinon, vous pouvez activer à nouveau la fonction CNAME dans le Registre pour continuer avec votre déploiement existant et autoriser le nouveau routage FQDN et l'utilisation de noms NETBIOS. Pour obtenir davantage d'informations, veuillez consulter l'article CTX137960.

Assistant de déploiement rapide : dans les versions de XenDesktop antérieures à la version 7.x, cette option de Studio permettait le déploiement rapide d'un déploiement XenDesktop complètement installé. La nouvelle installation simplifiée et workflow de configuration dans les versions 7.x élimine la nécessité d'utiliser l'option de l'assistant de déploiement rapide.

Fichier de configuration et fichier de script PowerShell pour l'administration automatique du service Remote PC : Remote PC Access est désormais intégré dans Studio et le Controller.

Workflow Studio : dans les versions antérieures à la version 7.x, Workflow Studio était l'interface graphique pour la composition du flux de travail pour XenDesktop. La fonctionnalité n'est pas prise en charge dans les versions 7.x.

Lancement de programmes non publiés lors de la connexion du client : dans les versions antérieures à 7.x, ce paramètre de stratégie Citrix spécifiait si les applications initiales ou les applications publiées devaient être lancées via ICA ou RDP sur le serveur. Dans les versions 7.x, ce paramètre spécifie uniquement si les applications initiales ou publiées doivent être lancées via RDP sur le serveur.

Démarrages de bureaux : dans les versions antérieures à la version 7.x, ce paramètre de stratégie Citrix spécifiait si les utilisateurs non administrateurs pouvaient se connecter à une session de bureau. Dans les versions 7.x, les utilisateurs qui ne sont pas des administrateurs doivent appartenir au groupe d'utilisateurs DirectAccess d'une machine VDA pour se connecter à des sessions sur ce VDA. Le paramètre Démarrages de bureaux permet aux utilisateurs qui ne sont pas des administrateurs d'un groupe d'utilisateurs DirectAccess dans un VDA de se connecter au VDA à l'aide d'une connexion ICA. Le paramètre Démarrages de bureaux n'a aucun effet sur les connexions RDP ; les utilisateurs d'un groupe d'utilisateurs Direct Access dans un VDA peuvent se connecter au VDA à l'aide d'une connexion Bureau à distance que ce paramètre soit activé ou non.

Nombre de couleurs : dans les versions de Studio antérieures à 7.6, vous spécifiez le nombre de couleurs dans les paramètres utilisateur d'un groupe de mise à disposition. À compter de la version 7.6, le nombre de couleurs pour le groupe de mise à disposition peut être défini à l'aide de l'applet de commande PowerShell New-BrokerDesktopGroup ou Set-BrokerDesktopGroup.

Démarrer un bureau tactile : ce paramètre est désactivé et n'est pas disponible pour les machines Windows 10 et Windows Server 2016. Pour plus d'informations, veuillez consulter la section Paramètres de stratégie Expérience mobile.

Fonctionnalités absentes de Citrix Receiver ou qui ont des valeurs par défaut différentes

- **Mappage des ports COM :** le mappage de port COM permet ou empêche l'accès aux ports COM sur la machine utilisateur. Le mappage de port COM était précédemment activé par défaut. Dans les versions 7.x de XenDesktop et XenApp, le mappage des ports COM est désactivé par défaut. Pour de plus amples informations, consultez la section Configurer les paramètres de redirection du port COM et LPT à l'aide du Registre.
- **Mappage de port LPT :** le mappage de port LPT contrôle l'accès aux applications d'ancienne génération sur des ports LPT. Le mappage de port LPT était précédemment activé par défaut. Dans les versions 7.x, le mappage des ports LPT est désactivé par défaut.
- **Codec audio PCM :** seuls les clients HTML5 prennent en charge le codec audio PCM dans les versions 7.x.
- **Prise en charge de Microsoft ActiveSync**.
- **Prise en charge de proxy pour les versions plus anciennes :** cela inclut :
  - Microsoft Internet Security et Acceleration (ISA) 2006 (Windows Server 2003)
  - Oracle iPlanet Proxy Server 4.0.14 (Windows Server 2003)
  - Serveur proxy Squid 3.1.14 (serveur Linux Ubuntu 11.10)

Pour de plus amples informations, consultez la documentation relative à Citrix Receiver sur votre version.

Mettre un déploiement à niveau

February 28, 2019

Introduction

Vous pouvez mettre à niveau certains déploiements vers des versions plus récentes sans devoir d'abord configurer les nouvelles machines ou sites. Ce processus est appelé une mise à niveau sur place. Consultez la section Mettre à niveau pour obtenir une liste des versions que vous pouvez mettre à niveau.

Vous pouvez également utiliser le programme d'installation de la version XenApp actuelle pour mettre à niveau un serveur de tâches XenApp 6.5 vers une version actuelle de VDA pour système d'exploitation Windows Server. Ceci est une activité supplémentaire à la migration de XenApp 6.5. Consultez la section Mettre à niveau une tâche XenApp 6.5 vers un VDA pour OS Windows Server.

Pour démarrer une mise à niveau, vous devez exécuter le programme d'installation à partir de la nouvelle version pour mettre à niveau la version précédemment installée des composants principaux (De-

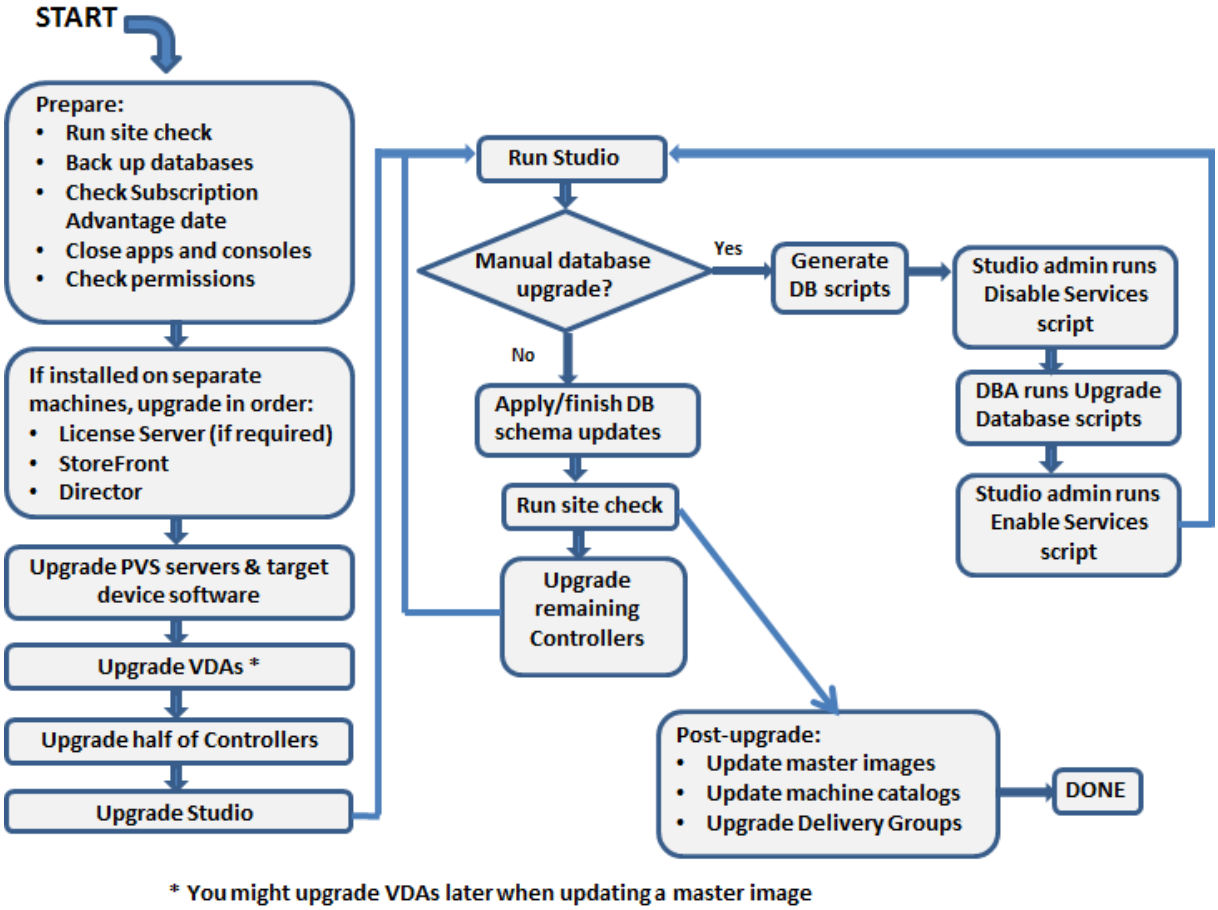
livery Controller, Citrix Studio, Citrix Director, le serveur de licences Citrix) et les VDA. Mettez ensuite à niveau les bases de données et le site.

Veillez à consulter toutes les informations dans cet article avant de procéder à la mise à niveau.

(Si vous effectuez une mise à niveau vers la version 7.16 ou une version ultérieure, consultez les instructions de la section Mise à niveau d'un déploiement.)

Séquence de mise à niveau

Le diagramme suivant résume la séquence de mise à niveau. Des détails sont fournis dans la section Procédure de mise à niveau ci-dessous. Par exemple, si plusieurs composants de base sont installés sur un serveur, l'exécution du programme d'installation sur cette machine met à niveau tous les composants qui ont de nouvelles versions. Vous pouvez mettre à niveau le VDA utilisé dans une image principale et ensuite mettre à jour l'image. Ensuite, mettez à jour le catalogue qui utilise cette image et le groupe de mise à disposition qui utilise ce catalogue. Les détails expliquent aussi comment mettre à niveau les bases de données du site et le site automatiquement ou manuellement.



Quelles versions des composants du produit peuvent être mises à niveau

Le programme d'installation du produit vous permet de mettre à niveau :

- Serveur de licences Citrix, Studio et StoreFront
- Delivery Controller 5.6 ou versions supérieures
- VDA 5.6 ou version ultérieure
  - Contrairement aux versions antérieures de VDA, vous devez utiliser le programme d'installation du produit pour mettre à niveau les VDA ; vous ne pouvez pas utiliser de MSI.
  - Si le programme d'installation détecte Receiver pour Windows (Receiver.exe) sur la machine, il est mis à niveau vers la version de Receiver incluse sur le support d'installation du produit.
  - VDA 5.6 à VDA 7.8 : si le programme d'installation détecte Receiver pour Windows Enterprise (CitrixReceiverEnterprise.exe) sur la machine, il est mis à niveau vers Receiver pour Windows Enterprise 3.4.
- Director 1 ou version ultérieure
- Base de données : cette action de Studio permet de mettre à niveau le schéma et migre les données pour la base de données du site (ainsi que les bases de données de journalisation de la configuration et de surveillance, si vous effectuez une mise à niveau à partir d'une version antérieure à la version 7.x)
- Personal vDisk

Remarque : pour mettre à niveau depuis XenDesktop 5.6, vous devez d'abord mettre à niveau vers 7.6 LTSR (avec la dernière CU), puis mettre à niveau vers cette version.

Utilisation de l'aide de la fonctionnalité/documentation du produit, mettez à niveau les éléments suivants si nécessaire :

- Provisioning Services (pour XenApp 7.x et XenDesktop 7.x, Citrix vous recommande d'utiliser la dernière version ; la version minimale prise en charge est Provisioning Services 7.0).
  - Mettez à niveau le serveur Provisioning Services à l'aide de la mise à niveau continue du serveur, et les clients à l'aide des versions vDisk.
  - Provisioning Services 7.x ne prend pas en charge la création de nouveaux bureaux avec XenDesktop 5. Ainsi, bien que les bureaux existants continuent de fonctionner, vous ne pouvez pas utiliser Provisioning Services 7.x pour créer de nouveaux bureaux tant que vous n'avez pas effectué la mise à niveau de XenDesktop. Par conséquent, si vous envisagez d'utiliser un environnement mixte de sites XenDesktop 5.6 et 7.x, ne mettez pas à niveau Provisioning Services vers la version 7.
- Version d'hyperviseur hôte.
- StoreFront.
- Profile Management.
- Service d'authentification fédérée

Limitations

Les limites suivantes s'appliquent aux mises à niveau :

- **Installation sélective des composants :** si vous installez ou mettez à niveau les composants vers la nouvelle version, mais ne choisissez pas de mettre à niveau d'autres composants (sur différentes machines) qui nécessitent une mise à niveau, Studio vous le rappellera. Par exemple, supposons qu'une mise à niveau comprend de nouvelles versions de Controller et de Studio. Vous effectuez la mise à niveau du Controller, mais vous n'exécutez pas le programme d'installation sur la machine sur laquelle Studio est installé. Studio ne vous laissera pas continuer à gérer le site tant que vous n'aurez pas mis à niveau Studio.

Vous n'avez pas besoin de mettre à niveau les VDA, mais Citrix vous recommande de mettre à niveau tous les VDA pour vous permettre d'utiliser toutes les fonctionnalités disponibles.

- **Version XenApp antérieure à 7.5 :** vous ne pouvez pas mettre à niveau à partir d'une version de XenApp antérieure à la version 7.5. Vous pouvez effectuer la migration depuis XenApp 6.x ; consultez la section Migrer XenApp 6.x. Bien que vous ne puissiez pas mettre à niveau une batterie XenApp 6.5, vous pouvez remplacer le logiciel XenApp 6.5 sur une machine Windows Server 2008 R2 par un VDA pour OS de serveur actuel. Voir Mettre à niveau une tâche XenApp 6.5 vers un nouveau VDA.
- **Version XenDesktop antérieure à 5.6 :** vous ne pouvez pas mettre à niveau à partir d'une version de XenDesktop antérieure à la version 5.6.
- **XenDesktop Express Edition :** vous ne pouvez pas mettre à niveau XenDesktop Express Edition. Obtenez et installez une licence pour une édition actuellement prise en charge, puis effectuez une mise à niveau.
- **Versions préliminaires :** vous ne pouvez pas effectuer une mise à niveau à partir d'une version XenApp ou XenDesktop, Early Release ou Technology Preview.
- **Windows XP/Vista :** si des VDA sont déjà installés sur les machines Windows XP ou Windows Vista, consultez la section VDA sur les machines exécutant Windows XP ou Windows Vista.
- **Sélection de produit :** lorsque vous effectuez une mise à niveau à partir d'une version 7.x antérieure, vous ne choisissez pas ni ne spécifiez le produit (XenApp ou XenDesktop) qui a été défini lors de l'installation initiale.
- **Environnements/sites mixtes :** si vous devez continuer à exécuter des sites de version antérieure et des sites de version actuelle, consultez la section Considérations d'environnement mixte.

Préparation

Avant de procéder à une mise à niveau :

- **Choisissez le programme d'installation et l'interface à utiliser :** utilisez le programme

d'installation du produit entier depuis l'image ISO de XenApp ou XenDesktop pour mettre à niveau les composants principaux. Vous pouvez mettre à niveau les VDA à l'aide du programme d'installation du produit entier ou de l'un des programmes d'installation de VDA autonomes. Tous les programmes d'installation offrent des interfaces graphique et de ligne de commande. Pour de plus amples informations, consultez Programmes d'installation.

Vous ne pouvez pas mettre à niveau en important ou en migrant les données depuis une version qui peut être mise à niveau. (Remarque : certaines versions bien antérieures doivent être migrées plutôt que d'être mises à niveau ; consultez la section Mettre à niveau et migrer pour obtenir une liste des versions qui peuvent être mises à niveau).

Si vous avez installé un VDA de bureau avec le programme d'installation VDAWorkstationCoreSetup.exe, Citrix vous recommande de mettre à niveau à l'aide de ce programme d'installation. Si vous utilisez le programme d'installation VDA du produit entier ou le programme d'installation VDAWorkstationSetup.exe pour mettre à niveau le VDA, il est possible que les composants initialement exclus soient installés, sauf si vous les ignorez/excluez expressément de la mise à niveau.

Par exemple, si vous avez installé un VDA version 7.13 à l'aide de VDAWorkstationCoreSetup.exe, puis que vous avez utilisé le programme d'installation du produit entier pour mettre à niveau ce VDA vers la version 7.14, les composants exclus de l'installation d'origine (tels que Profile Management et Personal vDisk) peuvent être installés lors de la mise à niveau, si vous acceptez les paramètres par défaut ou que vous n'utilisez pas l'option de ligne de commande /exclude.

- **Vérifiez l'intégrité de votre site :** assurez-vous que le site est fonctionnel et stable avant de démarrer une mise à niveau. Si un site présente des problèmes, la mise à niveau ne résoudra pas ces problèmes, et peut laisser le site dans un état difficile à réparer. Pour tester le site, sélectionnez le **site** dans le panneau de navigation de Studio. Dans la section Configuration de site du panneau central, cliquez sur **Tester le site**.
- **Sauvegardez les bases de données de site, de contrôle et de journalisation de la configuration :** suivez les instructions dans CTX135207. Si vous rencontrez des problèmes après la mise à niveau, vous pouvez restaurer la sauvegarde.

  Si vous le souhaitez, vous pouvez sauvegarder les modèles et mettre à niveau les hyperviseurs, le cas échéant.

  Effectuez les tâches de préparation en fonction de votre plan de continuité des activités.
- **Assurez-vous que vos licences Citrix sont à jour :** avant la mise à niveau, assurez-vous que votre abonnement à Customer Success Services/Software Maintenance/Subscription Advantage est toujours valide pour la nouvelle version du produit. Si vous mettez à niveau depuis une version antérieure à la version 7.x du produit, la date doit être au moins 2017.0801. (Cette date s'applique à la version 7.15 LTSR, pas aux mises à jour cumulatives (UC) qui suivent.)

- **Assurez-vous que votre serveur de licences Citrix est compatible :** assurez-vous que votre serveur de licences Citrix est compatible avec la nouvelle version. Il existe deux façons de procéder :
  - Avant de procéder à la mise à niveau de tout autre composant Citrix, exécutez le programme d'installation sur la machine contenant le serveur de licences. Si une mise à niveau est requise, le programme d'installation l'initie.
  - À partir du répertoire d'installation XenDesktop sur le support d'installation, exécutez la commande `.\LicServ\Verify.exe -h <delivery-controller-fqdn> -p 27000 -v`. L'affichage résultant indique si le serveur de licences est compatible. Si le serveur de licences n'est pas compatible, exécutez le programme d'installation sur cette machine pour la mettre à niveau.
- **Fermez les applications et consoles :** avant de démarrer une mise à niveau, fermez tous les programmes qui pourraient entraîner des verrouillages de fichier, y compris les consoles d'administration et les sessions PowerShell. (Le redémarrage de la machine assure que tout verrouillage de fichier est annulé et qu'aucune mise à jour Windows n'est en attente.)

  Avant de démarrer une mise à niveau, arrêtez et désactivez tout service d'agent de surveillance tiers.
- **Vérifiez que vous disposez des autorisations adéquates :** en plus d'être un utilisateur du domaine, vous devez être un administrateur local sur les machines sur lesquelles vous mettez à niveau les composants du produit.

La base de données du site et le site peuvent être mis à niveau automatiquement ou manuellement. Pour une mise à niveau automatique de la base de données, les autorisations de l'utilisateur de Studio doivent inclure la possibilité de mettre à jour le schéma de base de données SQL Server (par exemple, le rôle de base de données db_securityadmin ou db_owner). Pour de plus amples informations, veuillez consulter l'article Bases de données. Si l'utilisateur Studio ne possède pas ces autorisations, l'initiation de la mise à niveau manuelle d'une base de données générera des scripts. L'utilisateur Studio exécute certains de ces scripts depuis Studio ; l'administrateur de la base de données exécute d'autres scripts à l'aide d'un outil tel que SQL Server Management Studio.

Considérations d'environnement mixte

Lorsque votre environnement contient des sites/batteries dont les versions de produits diffèrent (environnement mixte), Citrix recommande d'utiliser StoreFront pour regrouper les applications et les bureaux provenant de versions de produits différentes (par exemple, si vous disposez d'un site XenDesktop 7.13 et d'un site XenDesktop 7.14). Pour plus de détails, consultez la documentation StoreFront.

- Dans un environnement mixte, continuez à utiliser les versions de Studio et de Director pour chaque version, mais assurez-vous que les différentes versions sont installées sur des machines distinctes.
- Si vous voulez exécuter des sites XenDesktop 5.6 et 7.x simultanément et utiliser Provisioning Services pour les deux, déployez un nouveau Provisioning Services à utiliser avec le site 7.x, ou mettez à niveau Provisioning Services et soyez incapable de provisionner de nouvelles charges de travail dans le site XenDesktop 5.6.

Citrix vous recommande de mettre à niveau tous les composants dans chaque site. Bien que vous puissiez utiliser des versions antérieures de certains composants, certaines fonctionnalités de la version la plus récente risquent de ne pas être disponibles. Par exemple, bien que vous puissiez utiliser les VDA actuels dans les déploiements contenant des versions antérieures de Controller, les nouvelles fonctionnalités de la version actuelle peuvent ne pas être disponibles. Des problèmes d'enregistrement de VDA peuvent aussi se produire lors de l'utilisation de versions antérieures.

- Les sites ayant des Controller à la version 5.x et des VDA à la version 7.x ne devraient rester dans cet état que temporairement. Dans l'idéal, vous devez effectuer la mise à niveau de tous les composants dès que possible.
- Ne mettez pas à niveau une version autonome de Studio tant que vous n'êtes pas prêt à utiliser la nouvelle version.

VDA sur les machines exécutant Windows XP ou Windows Vista

Vous ne pouvez pas mettre à niveau les VDA installés sur les machines exécutant Windows XP ou Windows Vista vers une version 7.x. Vous devez utiliser le VDA 5.6 FP1 avec certaines corrections à chaud ; voir CTX140941 pour obtenir des instructions. Bien que les VDA de versions antérieures s'exécutent dans un site 7.x, ils ne peuvent utiliser la plupart de ses fonctionnalités, notamment :

- Les fonctionnalités mentionnées dans Studio qui nécessitent une nouvelle version du VDA.
- Configuration des applications App-V dans Studio.
- Configuration des adresses StoreFront dans Studio.
- Prise en charge automatique des licences KMS Microsoft Windows lors de l'utilisation de Machine Creation Services (MCS). Voir CTX128580.
- Informations de Director :
  - Temps d'ouverture de session et événements de fin d'ouverture de session qui ont un impact sur la durée d'ouverture de session dans les vues Tableau de bord, Tendances et Détails de l'utilisateur.
  - La répartition des détails de la durée d'ouverture de session pour la connexion HDX et la durée d'authentification, ainsi que les détails de la durée de chargement du profil, la charge GPO, le script d'ouverture de session et l'établissement de la session interactive.
  - Plusieurs catégories de machine et taux d'échec de connexion.

- Gestionnaire d'activités dans les vues Assistance et Détails de l'utilisateur.

Citrix vous recommande de réimager les machines Windows XP et Windows Vista vers une version de système d'exploitation pris en charge, puis d'installer la dernière version du VDA.

VDA sur les machines exécutant Windows 8.x et Windows 7

Pour mettre à niveau les VDA installés sur les machines exécutant Windows 8.x ou Windows 7 vers Windows 10, Citrix vous recommande de réimager les machines Windows 7 et Windows 8.x vers Windows 10, puis d'installer le VDA pour Windows 10. Si réimager n'est pas une option, désinstallez le VDA avant de mettre à niveau le système d'exploitation, sinon, le VDA sera dans un état non pris en charge.

Prise en charge de VDA mixte

Lorsque vous mettez à niveau le produit vers une version ultérieure, Citrix vous recommande de mettre à niveau tous les composants principaux et les VDA, vous pouvez accéder à toutes ses nouvelles fonctionnalités dans votre édition.

Dans certains environnements, vous risquez de ne pas pouvoir mettre à niveau tous les VDA vers la version la plus récente. Dans ce scénario, lorsque vous créez un catalogue de machines, vous pouvez spécifier la version du VDA installée sur les machines. Par défaut, ce paramètre spécifie la dernière version du VDA recommandée, vous devez tenir compte de la modification de ce paramètre uniquement si le catalogue de machines contient des machines avec des versions antérieures du VDA. Cependant, le mélange de versions VDA dans un catalogue de machines n'est pas recommandé.

Si un catalogue de machine est créé avec le paramètre de valeur par défaut de VDA recommandée, et toutes les machines du catalogue possèdent une version antérieure de VDA installée, ces machines ne pourront pas s'enregistrer auprès du Controller et ne fonctionneront pas.

Pour de plus amples informations, consultez la section Versions VDA et niveaux fonctionnels.

Controller sur des systèmes d'exploitation antérieurs

Citrix recommande que tous les Delivery Controller d'un site aient le même système d'exploitation. La séquence de mise à niveau suivante minimise l'intervalle lorsque différents Controller ont des systèmes d'exploitation différents.

1. Prenez un instantané de tous les Delivery Controller sur le site, puis sauvegardez la base de données du site.
2. Installez les nouveaux Delivery Controller sur des serveurs vierges avec système d'exploitation pris en charge
3. Ajoutez les nouveaux Controller au site.

4. Supprimez les Controller qui s'exécutent sur des systèmes d'exploitation qui ne sont pas valides pour la version la plus récente.

Pour plus d'informations sur l'ajout et la suppression de contrôleurs, voir Delivery Controller.

Procédure de mise à niveau

Pour exécuter l'interface graphique du programme d'installation du produit, ouvrez une session sur la machine, puis insérez le support ou montez le lecteur ISO pour la nouvelle version. Cliquez deux fois sur **Sélection automatique**. Pour utiliser l'interface de ligne de commande, consultez la section Installer à l'aide de la ligne de commande.

1. Si plus d'un composant principal est installé sur le même serveur (par exemple, le Controller, Studio et le serveur de licences) et plusieurs de ces composants possèdent de nouvelles versions disponibles, ils seront mis à niveau lorsque vous exécutez le programme d'installation sur le serveur.

   Si les composants principaux sont installés sur des machines autres que le Delivery Controller, exécutez le programme d'installation sur chacune de ces machines. L'ordre recommandé est : serveur de licences, StoreFront et Director.

   Si vous n'avez pas encore déterminé si votre serveur de licences est compatible avec la nouvelle version (voir Préparation), il est essentiel que vous exécutiez le programme d'installation sur le serveur de licences avant de procéder à la mise à niveau des autres composants principaux.

2. Si vous utilisez Provisioning Services, mettez à niveau les serveurs et les machines cibles PVS à l'aide des instructions de la documentation Provisioning Services.

3. Exécutez le programme d'installation du produit sur des machines contenant les VDA. (Voir l'étape 12 si vous utilisez des images principales et Machine Creation Services).

4. Exécutez le programme d'installation du produit sur la moitié des contrôleurs. (Cette opération met également à niveau les autres composants principaux installés sur ces serveurs). Par exemple, si votre site comporte quatre Controller, exécutez le programme d'installation sur deux d'entre eux.

   - Le fait de laisser la moitié des Controller actifs permet aux utilisateurs d'accéder au site. Les VDA peuvent s'enregistrer auprès des Controller restants. Il peut aussi arriver que le site dispose d'une capacité réduite car moins de Controller sont disponibles. La mise à niveau entraîne une brève interruption dans l'établissement de nouvelles connexions client au cours des dernières étapes de mise à niveau de la base de données. Le Controller mis à niveau ne peut pas traiter les demandes tant que l'intégralité du site n'a pas été mise à niveau.
   - Si votre site comporte un seul Controller, le site est inutilisable lors de la mise à niveau.

5. Si Studio est installé sur une machine différente de celle que vous avez déjà mise à niveau, exécutez le programme d'installation sur la machine sur laquelle Studio est installé.
6. Depuis la version de Studio nouvellement mise à niveau, mettez à niveau la base de données du site. Pour de plus amples informations, consultez la section Mettre à niveau les bases de données et le site.
7. Depuis la version de Studio nouvellement mise à niveau, sélectionnez **Citrix Studio** *nom-site* dans le volet de navigation. Sélectionnez l'onglet **Tâches courantes**. Sélectionnez **Mettre à niveau les Delivery Controller restants**.
8. Après avoir effectué la mise à niveau et confirmé l'achèvement sur les Controller restants, fermez puis rouvrez Studio. Studio peut demander une mise à niveau du site supplémentaire pour enregistrer les services du Controller sur le site ou pour créer un ID de zone s'il n'existe pas encore.
9. Dans la section Configuration du site de la page Tâches courantes, sélectionnez **Procéder à l'enregistrement**. L'inscription des Controller les rend disponibles pour le site.
10. Lorsque vous sélectionnez **Terminer** une fois la mise à niveau terminée, vous avez la possibilité de participer à des programmes de télémétrie Citrix qui collectent des informations relatives à votre déploiement. Ces informations sont utilisées pour améliorer la qualité, la fiabilité et les performances nos produits.
11. Après la mise à niveau des composants, de la base de données et du site, testez le site nouvellement mis à niveau. À partir de Studio, sélectionnez **Citrix Studio** *nom du site* dans le volet de navigation. Sélectionnez l'onglet **Tâches courantes**, puis sélectionnez **Tester le site**. Ces tests ont été exécutés automatiquement après que vous ayez mis à niveau la base de données, mais vous pouvez les exécuter à tout moment.

    La fonctionnalité de test du site peut échouer pour un Controller installé sur Windows Server 2016, lorsqu'une instance locale de SQL Server Express est utilisée pour la base de données du site, si le service SQL Server Browser ne démarre pas. Pour éviter ce problème, procédez comme suit.

    a) Activez le service SQL Server Browser (si nécessaire), puis redémarrez-le.

    b) Redémarrez le service SQL Server (SQLEXPRESS).
12. Si vous utilisez Machine Creation Services et souhaitez utiliser des VDA mis à niveau : une fois que vous avez mis à niveau et testé le déploiement, mettez à niveau le VDA utilisé dans les images principales (si ce n'est déjà fait). Mettez à jour les images principales qui utilisent ces VDA. Voir la section Mettre à jour ou créer une nouvelle image principale. Mettez ensuite à niveau les catalogues de machines qui utilisent ces images principales, et les groupes de mise à disposition qui utilisent ces catalogues.

Mettre à niveau les bases de données et le site

Après mise à niveau des composants principaux et des VDA, utilisez la version nouvellement mise à niveau de Studio pour initier une mise à niveau automatique ou manuelle de la base de données et du site.

Rappel : consultez la section Préparation ci-dessus pour prendre connaissance des autorisations requises.

- Pour une mise à niveau automatique de la base de données, les autorisations de l'utilisateur de Studio doivent inclure la possibilité de mettre à jour le schéma de base de données SQL Server.
- Pour une mise à niveau manuelle, l'utilisateur Studio exécute certains des scripts générés à partir de Studio. L'administrateur de base de données exécute d'autres scripts, à l'aide de l'utilitaire SQLCMD ou de SQL Server Management Studio en mode SQLCMD. Si ce n'est pas le cas, des erreurs peuvent se produire.

Citrix recommande fortement de sauvegarder la base de données avant de procéder à la mise à niveau. Voir CTX135207. Lors d'une mise à niveau de base de données, les services du produit sont désactivés. Pendant ce temps, les Controller ne peuvent pas initier de nouvelles connexions pour le site, ainsi effectuez une planification prudente.

Une fois la mise à niveau de la base de données terminée, et les services du produit activés, Studio teste l'environnement et la configuration, puis génère un rapport HTML. Si des problèmes sont identifiés, vous pouvez restaurer la sauvegarde de la base de données. Après avoir résolu les problèmes, vous pouvez effectuer la mise à niveau de la base de données à nouveau.

Mettre à niveau la base de données et le site automatiquement :

Lancez le logiciel Studio nouvellement mis à niveau. Lorsque vous choisissez de démarrer la mise à niveau du site automatiquement et confirmer que vous êtes prêt, la mise à niveau de la base de données et du site se poursuit.

Mettre à niveau la base de données et le site manuellement :

1. Lancez le logiciel Studio nouvellement mis à niveau. Choisissez de mettre le site à niveau manuellement. L'Assistant vérifie la compatibilité du serveur de licences et des demandes de confirmation. Après confirmation que vous avez sauvegardé la base de données, l'Assistant génère et affiche les scripts et une liste des étapes de mise à niveau.
2. Exécutez les scripts suivants dans l'ordre indiqué.
    - **DisableServices.ps1 :** script PowerShell à exécuter par l'utilisateur de Studio sur un Controller pour désactiver les services du produit.
    - **UpgradeSiteDatabase.sql :** script SQL à exécuter par l'administrateur de la base de données sur le serveur qui contient la base de données du site.
    - **UpgradeMonitorDatabase.sql :** script SQL à exécuter par l'administrateur de la base de données sur le serveur qui contient la base de données de surveillance.

- **UpgradeLoggingDatabase.sql :** script SQL à exécuter par l'administrateur de la base de données sur le serveur qui contient la base de données de journalisation de la configuration. Exécutez ce script uniquement si cette base de données change (par exemple, après l'application d'un correctif logiciel).
- **EnableServices.ps1 :** script PowerShell à exécuter par l'utilisateur de Studio sur un Controller pour activer les services du produit.

3. Après avoir effectué les tâches de la check-list, cliquez sur **Terminer la mise à niveau**.

Mise à niveau de Dbschema

Lorsque vous mettez à jour votre déploiement vers une nouvelle CU, plusieurs de vos schémas de base de données sont mis à niveau. Consultez le tableau suivant pour plus d'informations sur les schémas de base de données mis à niveau au cours de la procédure :

To / From	7.15 CU1	7.15 CU2	7.15 CU3
7.15 RTM	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config
7.15 CU1		Config	Site; Config
7.15 CU2			Site; Config

Définition des termes :

- Site = magasin de données de site ; la mise à jour de Dbschema est effectuée sur le magasin de données de site.
- Monitor = magasin de données de surveillance ; la mise à jour de Dbschema est effectuée dans le magasin de données de surveillance.
- Config = table de configuration ; la version de Desktop Studio, la version du serveur de licences ou les deux sont mises à jour dans le tableau de configuration.

Mettre à niveau une tâche XenApp 6.5 vers un nouveau VDA

November 6, 2018

Après avoir migré une batterie XenApp 6.5, vous pouvez utiliser vos serveurs XenApp 6.5 qui ont été configurés dans le mode Hôte de session uniquement (également appelé Session uniquement ou Serveurs de tâches) en supprimant les logiciels précédents et en installant un nouveau VDA pour OS de serveur.

REMARQUE : bien qu'il soit possible de mettre à niveau un serveur de tâches XenApp 6.5, l'installation du logiciel VDA actuel sur une nouvelle machine fournit une meilleure sécurité.

Pour mettre à niveau une tâche XenApp 6.5 vers un nouveau VDA :

1. Supprimez le Hotfix Rollup Pack 7 pour XenApp 6.5, en utilisant les instructions fournies dans le fichier Lisez-moi du Hotfix. Consultez l'article CTX202095.
2. Désinstaller XenApp 6.5, en suivant les instructions dans Suppression de rôles et de composants Ce processus nécessite plusieurs redémarrages. Si une erreur se produit lors de la désinstallation, consultez le journal des erreurs de désinstallation dont il est fait référence dans le message d'erreur. Ce fichier journal réside dans le dossier « %TEMP%\Citrix\XenDesktop Installation\XenApp 6.5 Uninstall Log Files\. »
3. Installez un VDA pour OS de serveur, à l'aide d'un programme d'installation fourni dans cette version. Consultez Installer des VDA ou Installer à l'aide de la ligne de commande.

Une fois que vous avez installé un nouveau VDA dans Studio, dans le nouveau site XenApp, créez des catalogues de machines (ou modifiez des catalogues existants) pour les tâches mises à niveau.

Résolution des problèmes

Symptômes : la suppression du logiciel XenApp 6.5 échoue. Le journal de désinstallation contient le message : « Erreur 25703. Une erreur s'est produite lors du branchement de XML dans Internet Information Server. Le programme d'installation ne peut pas copier des fichiers dans votre répertoire des scripts IIS. Vérifiez que votre installation d'IIS est correcte.

Cause : le problème se produit sur les systèmes sur lesquels (1) pendant la phase initiale de l'installation de XenApp 6.5, vous avez indiqué que le service XML Citrix (CtxHttp.exe) ne peut pas partager un port avec IIS, et (2) .NET Framework 3.5.1 est installé.

Résolution :

1. Supprimez le rôle de Serveur Web (IIS) à l'aide de l'Assistant Supprimer des rôles sur le serveur Windows. (Vous pouvez réinstaller le rôle Serveur Web (IIS) plus tard).
2. Redémarrez le serveur.
3. À l'aide de la fonctionnalité Ajout/suppression de programmes, désinstallez Citrix XenApp 6.5 et Microsoft Visual C++ 2005 Redistributable Package (x64), version 8.0.56336.
4. Redémarrez le serveur.
5. Installez le VDA pour OS de serveur Windows.

Migrer XenApp 6.x

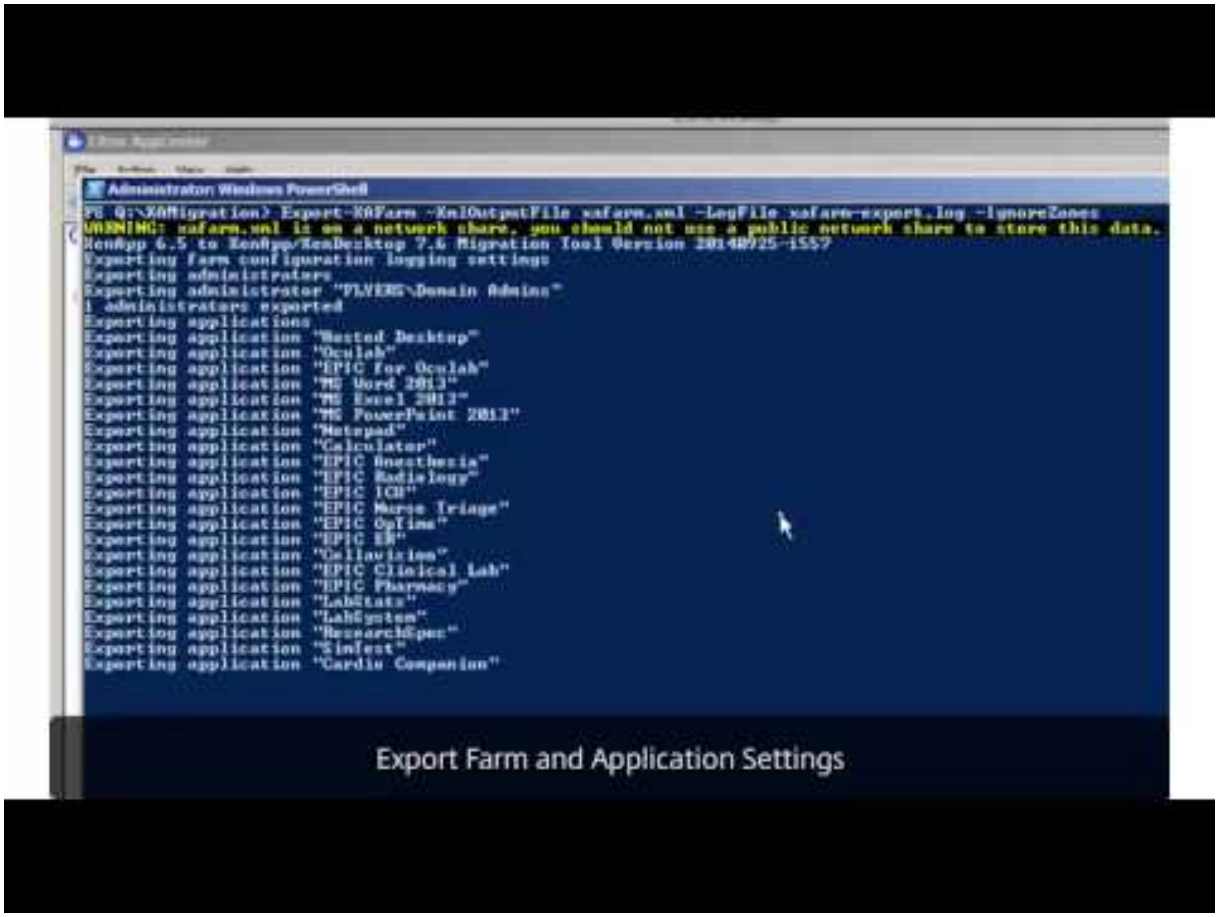
February 28, 2019

Remarque : vous ne pouvez pas utiliser le produit Citrix Smart Migrate avec cette version de XenApp et XenDesktop. Toutefois, l'outil de Migration est disponible.

Outil de migration XenApp 6.x

L'outil de migration XenApp 6.x est une collection de scripts PowerShell contenant des applets de commande qui migrent une stratégie et des données de batterie XenApp 6.x (6.0 ou 6.5). Sur le serveur de Controller XenApp 6.x, vous pouvez exécuter des applets de commande d'exportation qui collectent ces données dans des fichiers XML. Ensuite, depuis le Controller XenApp 7.6, exécutez les applets de commande d'importation qui créent des objets à l'aide des données collectées au cours de l'exportation.

Une présentation vidéo de l'outil de migration est disponible ici.



La séquence suivante résume le processus de migration ; des détails sont fournis plus tard.

1. Sur un Controller XenApp 6.0 ou 6.5 :
2. Importez les modules d'exportation PowerShell.
3. Exécuter les applets de commande d'exportation pour exporter des stratégies et/ou des données de batterie vers les fichiers XML.
4. Copiez les fichiers XML (et le dossier d'icônes si vous choisissez de ne pas les incorporer dans les fichiers XML lors de l'exportation) dans le Controller XenApp 7.6.
5. Sur un Controller XenApp 7.6 :
6. Importez les modules d'importation du PowerShell.
7. Exécutez les applets de commande d'importation pour importer la stratégie et/ou les données de la batterie de serveurs (applications), à l'aide des fichiers XML en entrée.
8. Terminez les étapes de post-migration.

Avant d'exécuter la migration, vous pouvez exporter vos paramètres XenApp 6.5, puis effectuer une importation de l'aperçu sur le site XenApp 7.6. L'aperçu identifie des points d'échec possibles pour vous permettre de résoudre les problèmes avant de procéder à l'importation elle-même. Par exemple, un aperçu peut détecter qu'une application du même nom existe déjà dans le nouveau site XenApp 7.6. Vous pouvez également utiliser les fichiers journaux générés à partir de l'aperçu en tant que guide de migration.

Sauf spécification contraire, le terme 6.x fait référence à XenApp 6.0 ou 6.5.

Nouveautés dans cette version

Cette version de décembre 2014 (version 20141125) contient les mises à jour suivantes :

- Si vous rencontrez des problèmes lors de l'utilisation de l'outil de migration sur une batterie XenApp 6.x, signalez-les au forum d'assistance https://discussions.citrix.com/forum/1411-xenapp-7x/, afin que Citrix puisse les examiner et potentiellement améliorer l'outil.
- Nouveau conditionnement : le fichier XAMigration.zip contient désormais deux packs distincts et indépendants : ReadIMA.zip et ImportFMA.zip. Pour effectuer l'exportation depuis un serveur XenApp 6.x, vous avez uniquement besoin de ReadIMA.zip. Pour effectuer l'importation vers un serveur XenApp 7.6, vous avez uniquement besoin d'ImportFMA.zip.
- L'applet de commande Export-XAFarm prend en charge un nouveau paramètre (EmbedIconData) qui élimine le besoin de copier les données d'icône pour séparer des fichiers.
- L'applet de commande d'Import-XAFarm prend en charge trois nouveaux paramètres :
- MatchServer : importez des applications depuis des serveurs dont les noms correspondent à une expression
- NotMatchServer : importez des applications depuis des serveurs dont les noms ne correspondent pas à une expression
- IncludeDisabledApps : importez des applications désactivées
- Les pré-démarrées ne sont pas importées.

- L'applet de commande Export-Policy fonctionne sur XenDesktop 7.x.

Pack outil de migration

L'outil de migration est disponible depuis le site de téléchargement Citrix sous XenApp 7.6. Le fichier XAMigration.zip contient deux packs séparés et indépendants :

- ReadIMA.zip : contient les fichiers utilisés pour exporter des données depuis votre batterie XenApp 6.x, plus les modules partagés.

Module ou fichier	Description
ExportPolicy.psm1	Module de script PowerShell pour l'exportation de stratégies XenApp 6.x vers un fichier XML.
ExportXAFarm.psm1	Module de script PowerShell pour l'exportation de paramètres de batterie XenApp 6.x vers un fichier XML.
ExportPolicy.psd1	Fichier manifeste PowerShell pour module de script ExportPolicy.psm1.
ExportXAFarm.psd1	Fichier manifeste PowerShell pour module de script ExportXAFarm.psm1.
LogUtilities.psm1	Module de script PowerShell partagé qui contient des fonctions de journalisation.
XmlUtilities.psd1	Fichier manifeste PowerShell pour le module de script XmlUtilities.psm1.
XmlUtilities.psm1	Module de script PowerShell partagé qui contient les fonctions XML.

- ImportFMA.zip : contient les fichiers utilisés pour importer des données vers votre batterie XenApp 7.6, plus les modules partagés.

Module ou fichier	Description
ImportPolicy.psm1	Module de script PowerShell pour l'importation de stratégies vers XenApp 7.6
ImportXAFarm.psm1	Module de script PowerShell pour l'importation des applications vers XenApp 7.6.
ImportPolicy.psd1	Fichier manifeste PowerShell pour module de script ImportPolicy.psm1.

Module ou fichier	Description
ImportXAFarm.psd1	Fichier manifeste PowerShell pour module de script ImportXAFarm.psm1.
PolicyData.xsd	Schéma XML pour les données de stratégie.
XAFarmData.xsd	Schéma XML pour les données de batterie XenApp.
LogUtilities.psm1	Module de script PowerShell partagé qui contient des fonctions de journalisation.
XmlUtilities.psd1	Fichier manifeste PowerShell pour le module de script XmlUtilities.psm1.
XmlUtilities.psm1	Module de script PowerShell partagé qui contient les fonctions XML.

Limitations

- Les paramètres de stratégie ne sont pas tous importés ; veuillez consulter la section Paramètres de stratégie non importés. Les paramètres qui ne sont pas pris en charge sont ignorés et affichés dans le fichier journal.
- Bien que tous les détails d'application soient collectés dans le fichier XML de sortie lors de l'opération d'exportation, seules les applications installées sur le serveur sont importées dans le site XenApp 7.6. Les bureaux, le contenu et la plupart des applications publiés livrés en streaming ne sont pas pris en charge (voir les paramètres de l'applet de commande Import-XAFarm dans Étapes détaillées : importer les données pour les exceptions).
- Les serveurs d'applications ne sont pas importés.
- La plupart des propriétés d'application ne sont pas importées en raison des différences entre les technologies XenApp 6.x Independent Management Architecture (IMA) et XenApp 7.6 FlexCast Management Architecture (FMA) ; voir Mappage des propriétés d'application.
- Un groupe de mise à disposition est créé lors de l'importation. Voir Utilisation avancée pour plus de détails sur l'utilisation des paramètres pour filtrer les éléments importés.
- Seuls les paramètres de stratégie Citrix créés avec la console de gestion AppCenter sont importés, les paramètres de stratégie Citrix créés avec les Objets de stratégie de groupe (GPO) ne sont pas importés.
- Les scripts de migration sont uniquement conçus pour les migrations de XenApp 6.x à XenApp 7.6.
- Les dossiers imbriqués contenant plus de cinq niveaux ne sont pas pris en charge par Studio et ne seront pas importés. Si votre structure de dossier d'applications contient plus de cinq niveaux, réduisez le nombre de dossiers imbriqués avant l'importation.

Considérations de sécurité

Les fichiers XML créés par les scripts d'exportation peuvent contenir des informations confidentielles sur votre environnement et votre organisation, telles que des noms d'utilisateurs, des noms de serveur et autres données de batteries, d'applications et de configuration de stratégies XenApp. Stockez et gérez ces fichiers dans des environnements sécurisés.

Lisez attentivement les fichiers XML avant de les utiliser comme entrée pour l'importation des stratégies et des applications pour vous assurer qu'ils ne contiennent pas de modifications non autorisées.

Les affectations des objets de stratégie (anciennement connus sous le nom de filtres de stratégie) contrôlent la manière dont les stratégies sont appliquées. Après avoir importé les stratégies, vérifiez l'affectation des objets de chaque stratégie pour vous assurer qu'il n'existe aucune faille de sécurité résultant de l'importation. Les différents groupes d'utilisateurs, d'adresses IP ou de noms de client peuvent être appliqués à la stratégie après l'importation. Les paramètres autoriser/refuser peuvent avoir différentes significations après l'importation.

Journalisation et gestion des erreurs

Les scripts fournissent une journalisation complète qui effectue le suivi de toutes les exécutions de l'applet de commande, des messages d'information, des résultats d'exécution de l'applet de commande, des avertissements et des erreurs.

- L'utilisation de la plupart des applets de commande PowerShell Citrix est journalisée. Toutes les applets de commande PowerShell des scripts d'importation qui créent de nouveaux objets de site sont journalisées.
- La progression de l'exécution du script est journalisée, y compris les objets en cours de traitement.
- Les actions principales qui affectent l'état du flux sont journalisées, y compris les flux effectués à partir de la ligne de commande.
- Tous les messages imprimés dans la console sont journalisés, y compris les avertissements et les erreurs.
- Chaque ligne est horodatée à la milliseconde près.

Citrix vous recommande de spécifier un fichier journal lorsque vous exécutez chacune des applets de commande d'importation et d'exportation.

Si vous ne spécifiez pas un nom de fichier journal, celui-ci est stocké dans le dossier de base de l'utilisateur actuel (spécifié dans la variable $HOME de PowerShell) si ce dossier existe ; sinon, il est placé dans le dossier d'exécution du script courant. Le nom de journal par défaut est « XFarmAAAAMMJJHHmmSS-xxxxxx » où les six derniers chiffres constituent un nombre aléatoire.

Par défaut, toutes les informations de progression sont affichées. Pour supprimer l'affichage, spécifiez le paramètre NoDetails dans l'applet de commande d'exportation et d'importation.

En général, un script arrête l'exécution lorsqu'une erreur est détectée, et vous pouvez réexécuter l'applet de commande après la suppression des conditions d'erreurs.

Les conditions qui ne sont pas considérées comme des erreurs sont journalisées ; la plupart sont considérées comme des avertissements et l'exécution du script continue. Par exemple, des types d'applications non pris en charge sont considérés comme des avertissements et ne sont pas importés. Les applications qui existent déjà dans le site XenApp 7.6 ne sont pas importées. Les paramètres de stratégie qui sont déconseillés dans XenApp 7.6 ne sont pas importés.

La migration des scripts utilise la plupart des applets de commande PowerShell, et toutes les erreurs possibles peuvent ne pas être journalisées. Pour de plus amples informations sur la journalisation, utilisez les fonctionnalités de journalisation du PowerShell. Par exemple, les transcriptions du PowerShell journalisent tout ce qui est imprimé à l'écran. Pour plus d'informations, consultez l'aide des applets de commande Start-Transcript et Stop-Transcript.

Configuration requise, préparation et meilleures pratiques

Pour effectuer la migration, vous devez utiliser le Kit de développement logiciel de Citrix XenApp 6.5. Téléchargez ce SDK à partir de https://www.citrix.com/downloads/xenapp/sdks/powershell-sdk.html.

Important : n'oubliez pas de consulter la totalité de cet article avant de commencer une migration.

Vous devez connaître les concepts de base sur la stratégie d'exécution, les modules, les applets de commande et les scripts PowerShell. Bien que des connaissances complètes liées aux scripts ne soient pas requises, vous devez comprendre les applets de commande que vous exécutez. Utilisez l'applet de commande Get-Help pour afficher l'aide de chaque applet de commande de migration avant de l'exécuter. Par exemple :

```
Get-Help -full Import-XAFarm
```

Spécifiez un fichier journal sur la ligne de commande et vérifiez toujours le fichier journal après l'exécution d'une applet de commande. Si un script échoue, vérifiez et corrigez les erreurs dans le fichier journal, puis réexécutez l'applet de commande.

À savoir:

- Pour optimiser la mise à disposition d'applications pendant l'exécution de deux déploiements (la batterie XenApp 6.x et le nouveau site XenApp 7.6), vous pouvez regrouper les deux déploiements dans StoreFront ou l'Interface Web. Consultez la documentation eDocs pour votre version de StoreFront ou de l'Interface Web (Gérer > Créer un magasin).
- Les données de l'icône d'application sont gérées de deux manières différentes :
- si vous spécifiez le paramètre EmbedIconData dans l'applet de commande Export-XAFarm, les données de l'icône d'application exportées sont incorporées dans le fichier XML de sortie.

- Si vous ne spécifiez pas le paramètre EmbedIconData dans l'applet de commande Export-XAFarm, les données de l'icône d'application exportées sont stockées dans un dossier nommé en ajoutant la chaîne « -icons » au nom de base du fichier XML de sortie. Par exemple, si le paramètre XmlOutputFile est « FarmData.xml », le dossier « FarmData-icons » est alors créé pour stocker les icônes de l'application.

  Les fichiers de données des icônes dans ce dossier sont des fichiers .txt qui sont nommés à l'aide du nom de navigateur de l'application publiée (bien que les fichiers soient des fichiers .txt, les données stockées sont des données d'icône binaires codées, qui peuvent être lues par le script d'importation pour recréer l'icône de l'application). Lors de l'opération d'importation, si le dossier d'icône ne se trouve pas dans le même emplacement que le fichier XML d'importation, des icônes génériques sont utilisées pour chaque application importée.

- Les noms des modules de script, des fichiers manifestes, des modules partagés et des applets de commande sont similaires. Utilisez la saisie semi-automatique avec précaution afin d'éviter des erreurs. Par exemple, Export-XAFarm est une applet de commande. ExportXAFarm.psd1 et ExportXAFarm.psm1 sont des fichiers qui ne peuvent pas être exécutés.

- Dans les sections détaillées ci-dessous, la plupart des valeurs de paramètre de affichent les guillemets. Ceux-ci sont facultatifs pour les chaînes à mot unique.

Pour exporter depuis le serveur XenApp 6.x :

- L'exportation doit être exécutée sur un serveur XenApp 6.x configuré avec le mode de serveur Controller et hôte de session (plus couramment appelé Controller).
- Pour exécuter les applets de commande d'exportation, vous devez être un administrateur XenApp avec la permission de lecture des objets. Vous devez également disposer de suffisamment de permissions Windows pour exécuter des scripts PowerShell ; les procédures détaillées ci-dessous contiennent les instructions.
- Vérifiez que la batterie XenApp 6.x se trouve dans un état d'intégrité normal avant de procéder à l'exportation. Sauvegardez la base de données de la batterie. Vérifiez l'intégrité de la batterie à l'aide de l'utilitaire Citrix IMA Helper (CTX133983) : à partir de l'onglet du magasin de données IMA, exécutez une vérification de base (puis utilisez l'option DSCheck pour résoudre les entrées non valides). La résolution des problèmes avant d'effectuer la migration vous aide à empêcher les échecs d'exportation. Par exemple, si un serveur n'a pas été correctement supprimé de la batterie, il se peut que ses données soient conservées dans la base de données, ce qui peut entraîner l'échec des applets de commande dans le script d'exportation (par exemple, Get-XAServer -ZoneName). Si les applets de commande échouent, le script échoue.
- Vous pouvez exécuter les applets de commande d'exportation sur une batterie de serveurs en direct qui possède des connexions utilisateur actives ; les scripts d'exportation ne lisent que la configuration statique de la batterie et les données de stratégie.

Pour effectuer l'importation vers le serveur XenApp 7.6 :

- Vous pouvez importer des données vers les déploiements XenApp 7.6 (et sur les versions ultérieures prises en charge). Vous devez installer un Controller XenApp 7.6 et Studio, puis créer un site avant d'importer les données que vous avez exportées depuis la batterie XenApp 6.x. Bien que les VDA ne soient pas nécessaires pour importer des paramètres, Ils autorisent les types de fichiers d'application à être mis à disposition.
- Pour exécuter les applets de commande d'importation XenApp, vous devez être un administrateur XenApp avec autorisation de lecture et de création des objets. Un administrateur complet possède ces autorisations. Vous devez également disposer de suffisamment de permissions Windows pour exécuter des scripts PowerShell ; les procédures détaillées ci-dessous contiennent les instructions.
- Aucune autre connexion utilisateur ne doit être active lors d'une importation. Les scripts d'importation créent beaucoup de nouveaux objets et des dysfonctionnements peuvent se produire si les autres utilisateurs modifient la configuration en même temps.

N'oubliez pas que vous pouvez exporter des données, puis utiliser le paramètre -Preview avec les applets de commande d'importation pour voir ce qui se passe réellement durant une importation, mais sans importer quoi que ce soit. Les journaux indiquent exactement ce qui se passe durant une importation réelle ; si des erreurs se produisent, vous pouvez les résoudre avant de démarrer une importation réelle.

Étapes détaillées : exporter des données

Une vidéo de la marche à suivre pour l'exportation est disponible ici.

Effectuez les étapes suivantes pour l'exportation de données à partir d'un Controller XenApp 6.x vers des fichiers XML.

1. Téléchargez le pack de l'outil de migration XAMigration.zip à partir du site de téléchargement de Citrix. Par commodité, placez-le dans un partage de fichiers réseau pouvant être accédé par la batterie XenApp 6.x et le site XenApp 7.6. Décompressez le fichier XAMigration.zip dans le partage de fichiers du réseau. Deux fichiers zip devraient être présents : ReadIMA.zip et ImportFMA.zip.
2. Ouvrez une session sur le Controller XenApp 6.x en tant qu'administrateur XenApp avec au moins une autorisation en lecture seule et une autorisation Windows pour exécuter des scripts PowerShell.
3. Copiez ReadIMA.zip depuis le partage de fichiers du réseau vers un ControllerXenApp 6.x. Décompressez et extrayez ReadIMA.zip sur le Controller dans un dossier (par exemple : C:\XAMigration).
4. Ouvrez une console PowerShell et définissez le répertoire courant à l'emplacement du script. Par exemple :


```
cd C:\XAMigration
```

5. Vérifiez la stratégie d'exécution de script en exécutant Get-ExecutionPolicy.
6. Définissez la stratégie d'exécution de script sur RemoteSigned au minimum pour autoriser les scripts à être exécutés. Par exemple :

   ```
   Set-ExecutionPolicy RemoteSigned
   ```

7. Importez les fichiers de définition des modules ExportPolicy.psd1 et ExportXAFarm.psd1 :

   ```
   Import-Module .\ExportPolicy.psd1
   ```

   ```
   Import-Module .\ExportXAFarm.psd1
   ```

   À savoir

   - Si vous souhaitez uniquement exporter des données de stratégie, vous ne pouvez importer que le fichier de définition du module ExportPolicy.psd1. De même, si vous souhaitez uniquement exporter des données de la batterie, importez uniquement ExportXAFarm.psd1.
   - L'importation des fichiers de définition de module ajoute également les composants enfichables PowerShell requis.
   - N'importez pas les fichiers de script .psm1.

8. Pour exporter des données de stratégie, exécutez l'applet de commande Export-Policy.

Paramètre	Description
-XmlOutputFile ".xml"	Nom de fichier de sortie XML ; ce fichier contient les données exportées. Doit posséder une extension .xml. Le fichier ne doit pas exister, mais si un chemin d'accès est spécifié, le chemin parent doit exister. Valeur par défaut : Aucun ; ce paramètre est requis.
-LogFile ""	Nom du fichier journal. Une extension est facultative. Le fichier est créé s'il n'existe pas. Si le fichier existe et que le paramètre NoClobber est également spécifié, une erreur est générée ; sinon, le contenu du fichier est remplacé. Valeur par défaut : consultez la section Journalisation et gestion des erreurs
-NoLog	Ne pas générer de sortie de journal. Ceci remplace le paramètre LogFile, s'il est également spécifié. Valeur par défaut : false; une sortie de journal est générée

Paramètre	Description
-NoClobber	Ne pas remplacer un fichier journal spécifié dans le paramètre LogFile. Si le fichier journal n'existe pas, ce paramètre n'a aucun effet. Valeur par défaut : false ; un fichier journal existant est remplacé
-NoDetails	Ne pas envoyer de rapports détaillés sur l'exécution du script à la console. Valeur par défaut : false ; des rapports détaillés sont envoyés à la console
-SuppressLogo	N'imprimez pas le message « Version de l'outil de migration XenApp 6.x vers XenApp/XenDesktop 7.6 #aaaaMMjj-hhmm# » sur la console. Ce message, qui identifie la version du script, peut être utile lors de la résolution des problèmes ; par conséquent, Citrix vous recommande d'omettre ce paramètre. Valeur par défaut : false ; le message est imprimé sur la console

Exemple : l'applet de commande suivante exporte des informations de stratégie pour le fichier XML appelé MyPolicies.xml. L'opération est journalisée dans le fichier appelé MyPolicies.log.

```
Export-Policy -XmlOutputFile ".\MyPolicies.XML"
-LogFile ".\MyPolicies.Log"
```

9. Pour exporter des données de batterie, exécutez la cmdlet Export-XAFarm en spécifiant un fichier journal et un fichier XML.

Paramètre	Description
-XmlOutputFile ".xml"	Nom de fichier de sortie XML ; ce fichier contient les données exportées. Doit posséder une extension .xml. Le fichier ne doit pas exister, mais si un chemin d'accès est spécifié, le chemin parent doit exister. Valeur par défaut : Aucun ; ce paramètre est requis.

Paramètre	Description
-LogFile “”	Nom du fichier journal. Une extension est facultative. Le fichier est créé s’il n’existe pas. Si le fichier existe et que le paramètre NoClobber est également spécifié, une erreur est générée ; sinon, le contenu du fichier est remplacé. Valeur par défaut : consultez la section Journalisation et gestion des erreurs
-NoLog	Ne pas générer de sortie de journal. Ceci remplace le paramètre LogFile, s’il est également spécifié. Valeur par défaut : false; une sortie de journal est générée
-NoClobber	Ne pas remplacer un fichier journal spécifié dans le paramètre LogFile. Si le fichier journal n’existe pas, ce paramètre n’a aucun effet. Valeur par défaut : false ; un fichier journal existant est remplacé
-NoDetails	Ne pas envoyer de rapports détaillés sur l’exécution du script à la console. Valeur par défaut : false ; des rapports détaillés sont envoyés à la console
-SuppressLogo	N’imprimez pas le message « Version de l’outil de migration XenApp 6.x vers XenApp/XenDesktop 7.6 #aaaaMMjj-hhmm# » sur la console. Ce message, qui identifie la version du script, peut être utile lors de la résolution des problèmes ; par conséquent, Citrix vous recommande d’omettre ce paramètre. Valeur par défaut : false ; le message est imprimé sur la console
-IgnoreAdmins	Ne pas exporter les informations de l’administrateur. Voir Utilisation avancée pour des informations supplémentaires. Valeur par défaut : false ; les informations administrateur sont exportées

Paramètre	Description
-IgnoreApps	Ne pas exporter les informations d'application. Voir Utilisation avancée pour des informations supplémentaires. Valeur par défaut : false ; les informations de l'application sont exportées
-IgnoreServers	Ne pas exporter les informations du serveur. Valeur par défaut : false ; les informations du serveur sont exportées
-IgnoreZones	Ne pas exporter les informations de zone. Valeur par défaut : false ; les informations de zone sont exportées.
-IgnoreOthers	Ne pas exporter les informations telles que la journalisation de la configuration, les calculateurs de charge, les stratégies d'équilibrage de charge, les pilotes d'imprimante et les groupes de tâches. Valeur par défaut : false ; d'autres informations sont exportées. **Remarque :** l'objectif du commutateur -IgnoreOthers est de vous autoriser à continuer l'exportation en cas d'erreur qui pourrait affecter les données actuellement utilisées dans le processus d'exportation ou d'importation.
-AppLimit	Nombre d'applications à exporter. Voir Utilisation avancée pour des informations supplémentaires. Valeur par défaut : toutes les applications sont exportées
-EmbedIconData	Incorporez les données de l'icône d'application dans le même fichier XML que les autres objets. Valeur par défaut : les icônes sont stockées séparément. Voir Configuration requise, préparation et meilleures pratiques pour plus d'informations.

Paramètre	Description
-SkipApps	Nombre d'applications à ignorer. Voir Utilisation avancée pour des informations supplémentaires. Valeur par défaut : aucune application n'est ignorée

Exemple : l'applet de commande suivante exporte les informations sur la batterie vers le fichier XML nommé MyFarm.xml. L'opération est journalisée sur le fichier MyFarm.log. Un dossier nommé « MyFarm-icons » est créé pour stocker les fichiers de données de l'icône de l'application ; ce dossier se trouve au même emplacement que MyFarm.XML.

```
Export-XAFarm -XmlOutputFile ".\MyFarm.XML"-LogFile ".\MyFarm.Log"
```

Une fois les scripts d'exportation terminés, les fichiers XML spécifiés sur la ligne de commande contiennent la stratégie et les données de la batterie XenApp. Les fichiers de l'icône de l'application contiennent des fichiers de données d'icône, et le fichier journal indique ce qui s'est passé lors de l'exportation.

Étapes détaillées : importer les données

Une vidéo de la marche à suivre pour l'importation est disponible ici.

N'oubliez pas que vous pouvez exécuter une importation d'aperçu (en émettant l'applet de commande Import-Policy ou Import-XAFarm avec le paramètre Preview) et consultez les fichiers journaux avant d'effectuer une importation.

Effectuez les étapes suivantes pour importer des données vers un site XenApp 7.6, en utilisant les fichiers XML générés lors de l'exportation.

1. Ouvrez une session sur le Controller XenApp 7.6 en tant qu'administrateur possédant des permissions en lecture et écriture et des permissions Windows pour exécuter des scripts PowerShell.
2. Si vous n'avez pas décompressé le pack de l'outil de migration XAMigration sur le partage de fichiers réseau, faites-le maintenant. Copiez ImportFMA.zip depuis le partage de fichiers du réseau vers un Controller XenApp 7.6. Décompressez et extrayez ImportFMA.zip sur le contrôleur dans un dossier (par exemple : C:\XAMigration).
3. Copiez les fichiers XML (les fichiers de sortie générés lors de l'exportation) depuis le Controller XenApp 6.x vers le même emplacement sur le Controller XenApp 7.6 sur lequel vous avez extrait les fichiers ImportFMA.zip.

Si vous choisissez de ne pas incorporer les données de l'icône d'application dans le fichier de sortie XML lorsque vous exécutez l'applet de commande Export-XAFarm, assurez-vous de copier le dossier et les fichiers de données d'icône sur le même emplacement sur le Controller XenApp 7.6 que le fichier XML de sortie contenant les données de l'application et les fichiers ImportFMA.zip extraits.

4. Ouvrez une console PowerShell et définissez le répertoire courant à l'emplacement du script.

   ```
   cd C:\XAMigration
   ```

5. Vérifiez la stratégie d'exécution de script en exécutant Get-ExecutionPolicy.
6. Définissez la stratégie d'exécution de script sur RemoteSigned au minimum pour autoriser les scripts à être exécutés. Par exemple :

   ```
   Set-ExecutionPolicy RemoteSigned
   ```

7. Importez les fichiers de définition de module PowerShell ImportPolicy.psd1 et ImportXAFarm.psd1 :

   ```
   Import-Module .\ImportPolicy.psd1
   ```

   ```
   Import-Module .\ImportXAFarm.psd1
   ```

   À savoir

   - Si vous souhaitez uniquement importer des données de stratégie, vous ne pouvez importer que le module et les fichiers de définition de module ImportPolicy.psd1. De même, si vous souhaitez uniquement importer des données de batterie, importez uniquement ImportXAFarm.psd1.
   - L'importation des fichiers de définition de module ajoute également les composants enfichables PowerShell requis.
   - N'importez pas les fichiers de script .psm1.

8. Pour importer des données de stratégie, exécutez l'applet de commande Import-Policy, en spécifiant le fichier XML contenant les données de stratégie exportées.

Paramètre	Description
-XmlInputFile ".xml"	Nom du fichier d'entrée XML ; ce fichier contient des données collectées à partir de l'exécution de l'applet de commande Export-Policy. Doit posséder une extension .xml. Valeur par défaut : Aucun ; ce paramètre est requis.

Paramètre	Description
-XsdFile “chaîne”	Nom du fichier XSD. Les scripts d’importation utilisent ce fichier pour valider la syntaxe du fichier d’entrée XML. Voir Utilisation avancée pour des informations supplémentaires. Valeur par défaut : PolicyData.XSD
-LogFile “”	Nom du fichier journal. Si vous avez copié les fichiers journaux d’exportation vers ce serveur, vous pouvez utiliser un autre nom de fichier journal avec l’applet de commande d’importation. Valeur par défaut : consultez la section Journalisation et gestion des erreurs
-NoLog	Ne pas générer de sortie de journal. Ce paramètre remplace le paramètre LogFile, si celui-ci est également spécifié. Valeur par défaut : false; une sortie de journal est générée
-NoClobber	Ne pas remplacer un fichier journal spécifié dans le paramètre LogFile. Si le fichier journal n’existe pas, ce paramètre n’a aucun effet. Valeur par défaut : false ; un fichier journal existant est remplacé
-NoDetails	Ne pas envoyer de rapports détaillés sur l’exécution du script à la console. Valeur par défaut : false ; des rapports détaillés sont envoyés à la console
-SuppressLogo	N’imprimez pas le message « Version de l’outil de migration XenApp 6.x vers XenApp/XenDesktop 7.6 #aaaaMMjj-hhmm# » sur la console. Ce message, qui identifie la version du script, peut être utile lors de la résolution des problèmes ; par conséquent, Citrix vous recommande d’omettre ce paramètre. Valeur par défaut : false ; le message est imprimé sur la console

Paramètre	Description
-Preview	Effectuez un aperçu de l'importation : lisez des données à partir du fichier d'entrée XML, mais n'importez pas d'objets dans le site. Le fichier journal et la console indiquent ce qui s'est passé lors de l'importation de l'aperçu. Un aperçu illustre auprès des administrateurs ce qui doit se passer durant une importation réelle. Valeur par défaut : false ; une importation réelle se produit

Exemple : l'applet de commande suivante importe des données de stratégie à partir du fichier XML nommé MyPolicies.xml. L'opération est journalisée dans le fichier appelé MyPolicies.log.

```
1 Import-Policy -XmlInputFile ".\MyPolicies.XML"
2 -LogFile ".\MyPolicies.Log"
```

9. Pour importer des applications, exécutez la cmdlet Import-XAFarm, en spécifiant un fichier journal et le fichier XML contenant les données de la batterie exportées.

Paramètre	Description
-XmlInputFile ".xml"	Nom du fichier d'entrée XML ; ce fichier contient des données collectées à partir de l'exécution de l'applet de commande Export-XAFarm. Doit posséder une extension .xml. Valeur par défaut : Aucun ; ce paramètre est requis.
-XsdFile "chaîne"	Nom du fichier XSD. Les scripts d'importation utilisent ce fichier pour valider la syntaxe du fichier d'entrée XML. Voir Utilisation avancée pour des informations supplémentaires. Valeur par défaut : XAFarmData.XSD
-LogFile ""	Nom du fichier journal. Si vous avez copié les fichiers journaux d'exportation vers ce serveur, vous pouvez utiliser un autre nom de fichier journal avec l'applet de commande d'importation. Valeur par défaut : consultez la section Journalisation et gestion des erreurs

Paramètre	Description
-NoLog	Ne pas générer de sortie de journal. Ce paramètre remplace le paramètre LogFile, si celui-ci est également spécifié. Valeur par défaut : false; une sortie de journal est générée
-NoClobber	Ne pas remplacer un fichier journal spécifié dans le paramètre LogFile. Si le fichier journal n'existe pas, ce paramètre n'a aucun effet. Valeur par défaut : false ; un fichier journal existant est remplacé
-NoDetails	Ne pas envoyer de rapports détaillés sur l'exécution du script à la console. Valeur par défaut : false ; des rapports détaillés sont envoyés à la console
-SuppressLogo	N'imprimez pas le message « Version de l'outil de migration XenApp 6.x vers XenApp/XenDesktop 7.6 #aaaaMMjj-hhmm# » sur la console. Ce message, qui identifie la version du script, peut être utile lors de la résolution des problèmes ; par conséquent, Citrix vous recommande d'omettre ce paramètre. Valeur par défaut : false ; le message est imprimé sur la console
-Preview	Effectuez un aperçu de l'importation : lisez des données à partir du fichier d'entrée XML, mais n'importez pas d'objets dans le site. Le fichier journal et la console indiquent ce qui s'est passé lors de l'importation de l'aperçu. Un aperçu illustre auprès des administrateurs ce qui doit se passer durant une importation réelle. Valeur par défaut : false ; une importation réelle se produit
-DeliveryGroupName ""	Nom du groupe de mise à disposition pour toutes les applications importées. Voir Utilisation avancée pour des informations supplémentaires. Par défaut : " - Delivery Group"

Paramètre	Description
-MatchFolder “”	Importer uniquement les applications dans des dossiers portant des noms qui correspondent à la chaîne. Voir Utilisation avancée pour des informations supplémentaires. Valeur par défaut : aucune correspondance ne se produit
-NotMatchFolder “”	Importer uniquement ces applications dans des dossiers portant des noms qui ne correspondent pas à celui de la chaîne. Voir Utilisation avancée pour des informations supplémentaires. Valeur par défaut : aucune correspondance ne se produit
-MatchServer “”	Importez uniquement ces applications depuis les serveurs dont les noms correspondent à la chaîne. Voir Utilisation avancée pour des informations supplémentaires.
-NotMatchServer “”	Importez uniquement ces applications depuis les serveurs dont les noms ne correspondent pas à la chaîne. Voir Utilisation avancée pour des informations supplémentaires. Valeur par défaut : aucune correspondance ne se produit
-MatchWorkerGroup “”	Importer uniquement les applications publiées vers des groupes de tâches avec des noms qui correspondent à la chaîne. Voir Utilisation avancée pour des informations supplémentaires. Valeur par défaut : aucune correspondance ne se produit
-NotMatchWorkerGroup “”	Importer uniquement les applications publiées vers des groupes de tâches avec des noms qui ne correspondent pas à la chaîne. Voir Utilisation avancée pour des informations supplémentaires. Valeur par défaut : aucune correspondance ne se produit

Paramètre	Description
-MatchAccount “”	Importer uniquement les applications publiées vers les comptes d’utilisateur avec des noms qui correspondent à la chaîne. Voir Utilisation avancée pour des informations supplémentaires. Valeur par défaut : aucune correspondance ne se produit
-NotMatchAccount “”	Importer uniquement les applications publiées vers des comptes d’utilisateur avec des noms qui ne correspondent pas à la chaîne. Voir Utilisation avancée pour des informations supplémentaires. Valeur par défaut : aucune correspondance ne se produit
-IncludeStreamedApps	Importer des applications de type « StreamedToClientOrServerInstalled ». (Aucune autre application streamée n’est importée.) Par défaut, les applications streamées ne sont pas importées.
-IncludeDisabledApps	Importez des applications qui ont été marquées comme désactivées. Valeur par défaut : les applications désactivées ne sont pas importées

Exemple : l’applet de commande suivante importe des applications à partir du fichier XML appelé MyFarm.xml. L’opération est journalisée dans le fichier appelé MyFarm.log.

```
Import-XAFarm -XmlInputFile ”.\MyFarm.XML”
-LogFile ”.\MyFarm.Log”
```

10. Une fois l’importation terminée, effectuez les tâches de post-migration.

Tâches d’après migration

Après l’importation réussie des stratégies XenApp 6.x et des paramètres de batterie dans un site XenApp 7.6, utilisez les instructions suivantes pour vous assurer que les données ont été importées correctement.

- **Stratégies et paramètres de stratégie**

L'importation des stratégies est fondamentalement une opération de copie, à l'exception des paramètres et des stratégies obsolètes qui ne sont pas importés. La vérification post-migration implique essentiellement la comparaison des deux côtés.

1. Le fichier journal répertorie toutes les stratégies et tous les paramètres importés et ignorés. Tout d'abord, consultez le fichier journal et identifiez les paramètres et les stratégies qui n'ont pas été importés.
2. Comparez les stratégies XenApp 6.x avec les stratégies importées dans XenApp 7.6. Les valeurs des paramètres doivent rester les mêmes (à l'exception des paramètres de stratégie obsolètes, comme indiqué dans l'étape suivante).
    - Si vous disposez d'un petit nombre de stratégies, vous pouvez réaliser une comparaison visuelle côte à côte des stratégies affichées dans l'AppCenter de XenApp 6.5 et des stratégies affichées dans Studio de XenApp 7.6.
    - Si vous disposez d'un nombre important de stratégies, une comparaison visuelle peut ne pas être possible. Dans de tels cas, utilisez l'applet de commande d'exportation de la stratégie (Export-Policy) pour exporter les stratégies XenApp 7.6 vers un fichier XML différent, puis utilisez un outil de comparaison de texte (comme windiff) pour comparer les données de ce fichier aux données du fichier XML utilisé lors de l'exportation de la stratégie à partir de XenApp 6.5.
3. Utilisez les informations dans la section Paramètres de stratégie non importés pour déterminer ce qui peut avoir changé lors de l'importation. Si une stratégie XenApp 6.x contient uniquement des paramètres obsolètes, comme une stratégie totale, elle n'est pas importée. Par exemple, si une stratégie XenApp 6.x ne contient que des paramètres de test HMR, cette stratégie est totalement ignorée, car il n'existe pas de paramètre équivalent pris en charge dans XenApp 7.6.

    Certains paramètres de stratégie XenApp 6.x ne sont plus pris en charge, mais les fonctionnalités équivalentes sont implémentées dans XenApp 7.6. Par exemple, dans XenApp 7.6, vous pouvez configurer un programme de redémarrage pour les machines avec OS de serveur en modifiant un groupe de mise à disposition ; cette fonctionnalité a été précédemment implémentée au travers des paramètres de stratégie.
4. Vérifiez et confirmez la manière dont les filtres sont appliqués à votre site XenApp 7.6 par rapport à leur utilisation dans XenApp 6.x ; des différences significatives entre la batterie XenApp 6.x et le site XenApp 7.6 pourraient changer l'effet des filtres.

- **Filtres**

Examinez attentivement les filtres pour chaque stratégie. Des modifications peuvent être nécessaires pour assurer qu'ils fonctionnent toujours dans XenApp 7.6 comme initialement prévu dans XenApp 6.x.

Filtre	Notions importantes
Access Control	Le contrôle d'accès doit contenir les mêmes valeurs que les filtres XenApp 6.x originaux et devrait fonctionner sans nécessiter de modifications.
Citrix CloudBridge	Une valeur booléenne simple ; devrait fonctionner sans nécessiter de modifications. (Ce produit est maintenant appelé NetScaler SD-WAN).
Adresse IP cliente	Affiche les plages d'adresses IP des clients ; chaque plage est soit autorisée soit refusée. Le script d'importation préserve les valeurs, mais elles peuvent nécessiter des modifications si d'autres clients se connectent aux machines de VDA XenApp 7.6.
Nom du client	Identique au filtre d'adresse IP client, le script d'importation préserve les valeurs, mais elles peuvent nécessiter des modifications si d'autres clients se connectent aux machines de VDA XenApp 7.6.

Filtre	Notions importantes
Unité d'organisation	Les valeurs peuvent être conservées, selon que les unités d'organisation peuvent être résolues ou non au moment où elles sont importées. Consultez ce filtre étroitement, particulièrement si les machines XenApp 6.x et XenApp 7.6 résident dans des domaines différents. Si vous ne configurez pas les valeurs de filtre correctement, il se peut que la stratégie soit appliquée à un ensemble d'unités d'organisation incorrect. Les unités d'organisation sont uniquement représentées par des noms, il existe donc un risque qu'un nom d'unité d'organisation soit résolu à une unité d'organisation contenant différents membres de l'unité d'organisation dans le domaine XenApp 6.5. Même si certaines valeurs du filtre de l'unité d'organisation sont conservées, vérifiez les valeurs attentivement.
Utilisateur ou groupe	Les valeurs peuvent être conservées, selon que les comptes peuvent être résolus ou non au moment où ils sont importés. Similaire à des unités d'organisation, les comptes sont résolus en utilisant uniquement les noms, ainsi, si le site XenApp 7.6 dispose d'un domaine avec les mêmes noms de domaine et d'utilisateur, mais qu'ils sont en fait deux domaines et utilisateurs différents, les comptes résolus peuvent être différents des utilisateurs de domaine XenApp 6.x. Si vous ne consultez et modifiez pas correctement les valeurs de filtre, des applications de stratégies incorrectes peuvent se produire.

Filtre	Notions importantes
Groupe de tâches	Les groupes de tâches ne sont pas pris en charge dans XenApp 7.6. Utilisez le groupe de mise à disposition, le type de groupe de mise à disposition et les filtres de balises, qui sont pris en charge dans XenApp 7.6 (et non pas dans XenApp 6.x). Groupe de mise à disposition : autorise l'application des stratégies en fonction des groupes de mise à disposition. Chaque entrée de filtre spécifie un groupe de mise à disposition et peut être autorisé ou refusé. Type de groupe de mise à disposition : autorise l'application des stratégies sur les types de groupes de mise à disposition. Chaque filtre spécifie un type de groupe de mise à disposition qui peut être autorisé ou refusé. Balise : spécifie l'application de stratégie basée sur les balises créées pour les machines du VDA. Chaque balise peut être autorisée ou refusée.

Pour récapituler, les filtres qui impliquent les modifications de l'utilisateur de domaine requièrent le plus d'attention si la batterie XenApp 6.x et le site XenApp 7.6 se trouvent dans des domaines différents. Étant donné que le script d'importation utilise uniquement des chaînes de noms de domaine et d'utilisateur pour résoudre les utilisateurs dans le nouveau domaine, certains comptes peuvent être résolus et d'autres non. Bien qu'il n'existe qu'un risque infime que des domaines et utilisateurs différents aient le même nom, vous devriez vérifier ces filtres attentivement pour vous assurer qu'ils contiennent des valeurs correctes.

- **Applications**

Les scripts d'importation d'application n'importent pas simplement des applications ; ils créent également des objets, tels que des groupes de mise à disposition. Si l'importation de l'application implique plusieurs itérations, les hiérarchies de dossier d'application originales peuvent changer de manière significative.

1. Tout d'abord, consultez les fichiers journaux de migration qui contiennent des informations sur les applications qui ont été importées, les applications qui ont été ignorées et les applets de commande qui ont été utilisées pour créer les applications.
2. Pour chaque application :

- Vérifiez visuellement pour vous assurer que les propriétés de base ont été conservées lors de l'importation. Utilisez les informations sous la section Mappage des propriétés d'application pour déterminer les propriétés qui ont été importées sans être modifiées, qui n'ont pas été importées ou qui ont été initialisées à l'aide des données d'applications XenApp 6.x.
- Vérifiez la liste des utilisateurs. Le script d'importation importe automatiquement la liste explicite des utilisateurs dans la liste de visibilité de limite de l'application dans XenApp 7.6. Vérifiez pour vous assurer que la liste reste la même.

3. Les serveurs d'applications ne sont pas importés. Cela signifie qu'aucune des applications importées n'est accessible à cet instant. Les groupes de mise à disposition qui contiennent ces applications doivent se voir attribuer les catalogues de machines qui contiennent les machines qui possèdent les images exécutables des applications publiées. Pour chaque application :
    - Assurez-vous que le nom de l'exécutable et le répertoire de travail pointent vers un exécutable qui existe sur les machines attribuées au groupe de mise à disposition (via les catalogues de machines).
    - Vérifiez un paramètre de ligne de commande (qui peut être quoi que ce soit, tel qu'un nom de fichier, une variable d'environnement ou un nom d'exécutable). Vérifiez que le paramètre est valide pour toutes les machines des catalogues de machines attribués au groupe de mise à disposition.

- **Fichiers journaux**

Les fichiers journaux sont les ressources de référence les plus importantes pour une importation et une exportation. C'est pourquoi les fichiers journaux existants ne sont pas remplacés par défaut, et les noms de fichier journal par défaut sont uniques.

Comme indiqué dans la section « Journalisation et gestion des erreurs », si vous choisissez d'utiliser la couverture de journalisation supplémentaire avec les applets de commande PowerShell Start-Transcript et Stop-Transcript (qui enregistrent tout ce que vous tapez et imprimez dans la console), cette sortie ainsi que le fichier journal, fournit une référence complète de l'activité d'importation et d'exportation.

À l'aide des horodatages des fichiers journaux, vous pouvez effectuer un diagnostic de certains problèmes. Par exemple, si une exportation ou une importation a été exécutée pour une très longue durée, vous pouvez déterminer si une connexion de base de données défaillante ou la résolution des comptes utilisateur a pris plus de temps.

Les commandes enregistrées dans les fichiers journaux vous indiquent également la manière dont certains objets sont lus ou créés. Par exemple, pour créer un groupe de mise à disposition, plusieurs commandes sont exécutées non seulement pour créer l'objet de groupe de mise à disposition, mais également d'autres objets, tels que les règles de stratégie d'accès qui permettent l'attribution d'objets d'application au groupe de mise à disposition.

Le fichier journal peut également être utilisé pour diagnostiquer une exportation ou une importation

en échec. En général, les dernières lignes du fichier journal indiquent ce qui a causé l'échec, le message d'erreur d'échec est également enregistré dans le fichier journal. Ensemble avec le fichier XML, le fichier journal peut être utilisé pour déterminer l'objet impliqué dans l'échec.

Après avoir vérifié et effectué le test de la migration, vous pouvez :

1. Effectuez la mise à niveau de vos serveurs de tâches XenApp 6.5 vers des Virtual Delivery Agents (VDA) actuels en exécutant le programme d'installation 7.6 sur le serveur, qui supprime le logiciel XenApp 6.5 puis installe automatiquement un VDA courant. Consultez la section Mettre à niveau une tâche XenApp 6.5 vers un VDA pour OS Windows Server pour des instructions.

   Pour les serveurs de tâches XenApp 6.0, vous devez désinstaller manuellement le logiciel XenApp 6.0 du serveur. Vous pouvez alors utiliser le programme d'installation 7.6 pour installer le VDA courant. Vous ne pouvez pas utiliser le programme d'installation 7.6 pour supprimer automatiquement le logiciel XenApp 6.0.

2. Dans Studio, dans le nouveau site XenApp, créez des catalogues de machines (ou modifiez des catalogues existants) pour les tâches mises à niveau.
3. Ajouter les machines mises à niveau du catalogue de machines aux groupes de mise à disposition contenant les applications installées sur ces VDA pour système d'exploitation Windows Server.

Utilisation avancée

Par défaut, l'applet de commande Export-Policy exporte toutes les données de stratégie dans un fichier XML. De même, Export-XAFarm exporte les données de la batterie dans un fichier XML. Vous pouvez utiliser des paramètres de ligne de commande pour contrôler de manière plus avancée quels éléments sont exportés et importés.

- **Exporter les applications partiellement :** si vous possédez un grand nombre d'applications et souhaitez contrôler combien sont exportées dans le fichier XML, utilisez les paramètres suivants :
- AppLimit : spécifie le nombre d'applications à exporter.
- SkipApps : spécifie le nombre d'applications à ignorer avant d'exporter les applications suivantes.

Vous pouvez utiliser ces deux paramètres pour exporter de grandes quantités d'applications par segments gérables. Par exemple, la première fois que vous exécutez Export-XAFarm, vous souhaitez exporter uniquement les 200 premières applications, vous spécifiez ainsi cette valeur dans le paramètre AppLimit.

```
1 Export-XAFarm -XmlOutputFile "Apps1-200.xml"
2 -AppLimit "200"
```


La prochaine fois que vous exécutez Export-XAFarm, vous souhaitez exporter les 100 applications suivantes, et vous utilisez le paramètre SkipApps pour ignorer les applications que vous avez déjà exporté (les 200 premières), et le paramètre AppLimit pour exporter les 100 applications suivantes.

```
Export-XAFarm -XmlOutputFile ”Apps201-300.xml”
-AppLimit ”100” -SkipApps ”200”
```

- **Ne pas exporter certains objets :** certains objets peuvent être ignorés et n'ont donc pas besoin d'être exportés, plus particulièrement les objets qui ne sont pas importés ; voir Paramètres de stratégie non importés et Mappage des propriétés d'application. Utilisez les paramètres suivants pour empêcher l'exportation des objets inutiles :
- IgnoreAdmins : ne pas exporter les objets de l'administrateur
- IgnoreServers : ne pas exporter les objets du serveur
- IgnoreZones : ne pas exporter les objets de zone
- IgnoreOthers : ne pas exporter la journalisation de la configuration, le calculateur de charge, la stratégie d'équilibrage de charge, le pilote d'imprimante et les objets des groupes de tâches
- IgnoreApps : ne pas exporter les applications ; cela vous permet d'exporter d'autres données dans un fichier de sortie XML, puis d'exécuter l'exportation à nouveau pour exporter des applications vers un fichier de sortie XML différent.

Vous pouvez également utiliser ces paramètres pour résoudre les problèmes qui pourraient provoquer l'échec de l'exportation. Par exemple, si vous possédez un serveur erroné dans une zone, il se peut que la zone d'exportation échoue ; si vous incluez le paramètre IgnoreZones, l'exportation continue avec d'autres objets.

- **Noms de groupe de mise à disposition :** si vous ne souhaitez pas placer toutes vos applications dans un seul groupe de mise à disposition (par exemple, car elles sont accédées par différents utilisateurs et publiées sur différents serveurs), vous pouvez exécuter Import-XAFarm plusieurs fois, en spécifiant différentes applications et un groupe de mise à disposition différent à chaque fois. Bien que vous puissiez utiliser les applets de commande PowerShell pour déplacer les applications d'un groupe de mise à disposition à un autre après la migration, l'importation de manière sélective vers des groupes de mise à disposition uniques peut réduire ou éliminer l'effort de déplacement des applications ultérieurement.

1. Utilisez l'applet de commande Import-XAFarm avec le paramètre DeliveryGroupName. Le script crée le groupe de mise à disposition spécifié s'il n'existe pas.
2. Utilisez les paramètres suivants dans les expressions régulières pour filtrer les applications devant être importées dans le groupe de mise à disposition, en fonction du dossier, du groupe de tâches, du compte utilisateur et/ou des noms de serveurs. Il est recommandé d'entourer l'expression régulière de guillemets simples ou doubles. Pour plus d'informations sur les expressions régulières, voir https://msdn.microsoft.com/en-us/library/hs600312(v=vs.110).aspx.

- MatchWorkerGroup et NotMatchWorkerGroup : par exemple, pour les applications publiées vers des groupes de tâches, l'applet de commande suivante importe des applications dans le groupe de tâches appelé « applications de productivité » vers un groupe de mise à disposition XenApp 7.6 du même nom :

```
Import-XAFarm -XmlInputFile XAFarm.xml -LogFile XAFarmImport.log
-MatchWorkerGroup 'Productivity Apps' -DeliveryGroupName '
    Productivity Apps'
```

- MatchFolder et NotMatchFolder : par exemple, pour les applications organisées dans des dossiers d'application, l'applet de commande suivante importe des applications dans le dossier nommé « applications de productivité » dans un groupe de mise à disposition XenApp 7.6 du même nom.

```
Import-XAFarm -XmlInputFile XAFarm.xml -LogFile XAFarmImport.log -
    MatchFolder 'Productivity Apps' -DeliveryGroupName 'Productivity
     Apps'
```

Par exemple, l'applet de commande suivante importe des applications dans tout dossier dont le nom contient « MS Office Apps » dans le groupe de mise à disposition par défaut.

```
Import-XAFarm -XmlInputFile .\THeFarmApps.XML -MatchFolder ".\*/MS
    Office Apps/.\*"
```

- MatchAccount et NotMatchAccount : par exemple, pour les applications publiées vers des utilisateurs ou des groupes d'utilisateurs Active Directory, l'applet de commande suivante importe des applications publiées vers le groupe d'utilisateurs nommé « groupe Finance » vers un groupe de mise à disposition XenApp 7.6 appelé « Finance ».

```
Import-XAFarm -XmlInputFile XAFarm.xml -LogFile XAFarmImport.log
-MatchAccount 'DOMAIN\Finance Group' -DeliveryGroupName 'Finance'
```

- MatchServer et NotMatchServer : par exemple, pour les applications organisées sur des serveurs, l'applet de commande suivante importe les applications associées au serveur qui n'est pas nommé « Courant » dans un groupe de mise à disposition XenApp appelé « Ancienne génération ».

```
Import-XAFarm -XmlInputFile XAFarm.xml -LogFile XAFarmImport.log
-NotMatchServer 'Current' -DeliveryGroupName 'Legacy'
```

- **Personnalisation :** les programmeurs PowerShell peuvent créer leurs propres outils. Par exemple, vous pouvez utiliser le script d'exportation en tant qu'outil d'inventaire pour le suivi des modifications dans une batterie XenApp 6.x. Vous pouvez également modifier les fichiers XSD

(ou créer vos propres fichiers XSD) pour stocker des données supplémentaires ou des données dans des formats différents dans les fichiers XML. Vous pouvez spécifier un fichier XSD non défaut avec chacune des applets de commande d'importation.

Remarque : bien que vous puissiez modifier les fichiers de script pour répondre à des besoins de migration spécifiques ou avancés, la prise en charge est limitée aux scripts dans leur état non modifié. Le support technique Citrix vous recommande de rétablir les scripts non modifiés pour déterminer le comportement attendu et fournir de l'assistance, le cas échéant.

Résolution des problèmes

- Si vous utilisez PowerShell version 2.0 et que vous avez ajouté le composant logiciel enfichable du fournisseur PowerShell de stratégie de groupe Citrix ou le composant logiciel enfichable de l'outil Citrix Common Commands à l'aide de l'applet de commande Add-PSSnapIn, vous pouvez voir le message d'erreur « La référence d'objet n'est pas définie à une instance d'un objet » lorsque vous exécutez les applets de commande d'importation ou d'exportation. Cette erreur n'affecte pas l'exécution du script et peut être ignorée.
- Évitez d'ajouter ou de supprimer le composant logiciel enfichable du fournisseur PowerShell de stratégie de groupe Citrix dans la même session de console dans laquelle les modules de script d'importation et d'exportation sont utilisés, car ces modules de script ajoutent automatiquement le composant logiciel enfichable. Si vous ajoutez ou supprimez le composant logiciel enfichable séparément, il se peut que vous aperceviez les erreurs suivantes :
- « A drive with the name 'LocalGpo' already exists (Un lecteur appelé 'LocalGpo' existe déjà) ». Cette erreur s'affiche lorsque le composant logiciel enfichable est ajouté deux fois ; le composant tente de monter le lecteur LocalGpo lorsqu'il est chargé, puis signale l'erreur.
- « A parameter cannot be found that matches parameter name 'Controller' (Un paramètre qui correspond au nom de paramètre 'Controller' est introuvable) ». Cette erreur s'affiche lorsque le composant logiciel enfichable n'a pas été ajouté, mais que le script tente de monter le lecteur. Le script ne sait pas que le composant logiciel enfichable a été supprimé. Fermez la console et démarrez une nouvelle session. Dans la nouvelle session, importez les modules de script ; n'ajoutez pas ou ne supprimez pas le composant logiciel enfichable séparément.
- When importing the modules, if you right-click a .psd1 file and select Open or Open with PowerShell, the PowerShell console window will rapidly open and close until you stop the process. Pour éviter cette erreur, saisissez le nom de module du script PowerShell directement dans la fenêtre de la console PowerShell (par exemple, Import-Module.\ExportPolicy.psd1).
- Si vous recevez une erreur de permission lors de l'exécution d'une importation ou exportation, assurez-vous que vous êtes un administrateur XenApp avec permission de lecture des objets (pour l'exportation) ou de lecture et de création des objets (pour l'importation). Vous devez également disposer de suffisamment de permissions Windows pour exécuter des scripts PowerShell.

- Si une exportation échoue, vérifiez que la batterie XenApp 6.x se trouve dans un état d'intégrité normal en exécutant les outils DSMAINT et DSCHECK sur le serveur Controller XenApp 6.x.
- Si vous exécutez un aperçu de l'importation, puis ultérieurement exécutez les applets de commande d'importation pour une migration, mais découvrez que rien n'a été importé, vérifiez que vous avez supprimé le paramètre Preview des applets de commande d'importation.

Paramètres de stratégie non importés

Les paramètres de stratégie ordinateur et utilisateur suivants ne sont pas importés, car ils ne sont plus pris en charge. Veuillez noter que les stratégies non filtrées ne sont jamais importées. Les fonctionnalités et composants qui prennent en charge ces paramètres ont été remplacés par de nouvelles technologies/nouveaux composants ou elles ne s'appliquent plus à cause de modifications apportées à l'architecture et à la plate-forme.

Paramètres de stratégie Ordinateur non importés

- Type d'accès des connexions
- Niveau du serveur de gestion UC
- Résolution d'adresse DNS
- Nom de la batterie
- Mise en cache d'icône complète
- Contrôle de l'intégrité, Tests de contrôle de l'intégrité
- Nom d'hôte du serveur de licences, port du serveur de licences
- Limiter les sessions utilisateur, Limite sur les sessions administrateur
- Nom du calculateur de charge
- Journalisation des événements des limites d'ouvertures de session
- Pourcentage maximal de serveurs avec contrôle de l'ouverture de session
- Optimisation de la mémoire, Liste d'exclusion d'applications pour l'optimisation de mémoire, Intervalle d'optimisation de la mémoire, Programme d'optimisation de mémoire : jour du mois, Programme d'optimisation de mémoire : jour de la semaine, Programme d'optimisation de mémoire : heure
- Approbation de client d'applications en mode déconnecté, Journalisation des événements des applications en mode déconnecté, Période de validité de la licence d'applications en mode déconnecté, Utilisateurs d'applications en mode déconnecté
- Demander le mot de passe
- Avertissement de redémarrage personnalisé, Texte d'avertissement de redémarrage personnalisé, Horaire de désactivation des ouvertures de session pour le redémarrage, Fréquence de programmation du redémarrage, Intervalle de randomisation du programme de redémarrage, Date de début de la programmation du redémarrage, Horaire de programmation du redémarrage, In-

tervalle d'avertissement de redémarrage, Horaire de début de l'avertissement de redémarrage, Avertissement du redémarrage auprès des utilisateurs, Redémarrages programmés
- Observation *
- Requêtes d'approbation XML (configurées dans StoreFront)
- Filtrage d'adaptateur d'adresse IP virtuelle, Liste de programmes de compatibilité d'adresse IP virtuelle, Compatibilité d'adresse IP virtuelle améliorée, Liste de programmes d'adresses de l'adaptateur de filtre d'adresse IP virtuelle
- Nom de charge de travail
- Édition de produit XenApp, Modèle de produit XenApp
- Port du service XML

* Remplacé(s) par l'Assistance à distance Windows

Paramètres de stratégie Utilisateur non importés

- Connecter automatiquement les ports COM du client, Connecter automatiquement les ports LPT du client
- Redirection de port COM client, Redirection de port LPT client
- Noms des imprimantes clientes
- Limite d'ouvertures de session simultanées
- Entrée depuis des connexions observées *
- Intervalle d'horloge de déconnexion de persistance, Intervalle d'horloge de fin de persistance
- Journaliser les tentatives d'observation *
- Notifier l'utilisateur de connexions observées en attente *
- Intervalle d'horloge de déconnexion de pré-lancement, Intervalle d'horloge de fin de pré-lancement
- Importance de session
- Single Sign-On, Magasin central Single Sign-On
- Utilisateurs qui peuvent observer d'autres utilisateurs, Utilisateurs qui ne peuvent pas observer d'autres utilisateurs *

* Remplacé(s) par l'Assistance à distance Windows

Types d'application non importés

Les types d'application suivants ne sont pas importés.

- Bureaux de serveur
- Contenu
- Applications livrées en streaming (App-V est la nouvelle méthode utilisée pour les applications livrées en streaming)

Mappage des propriétés d'application

Le script d'importation des données de la batterie importe uniquement des applications. Les propriétés d'application suivantes sont importées sans modification.

Propriété IMA	Propriété FMA
AddToClientDesktop	ShortcutAddedToDesktop
AddToClientStartMenu	ShortcutAddedToStartMenu
ClientFolder	ClientFolder
CommandLineExecutable	CommandLineExecutable
CpuPriorityLevel	CpuPriorityLevel
Description	Description
DisplayName	PublishedName
Activée	Activée
StartMenuFolder	StartMenuFolder
WaitOnPrinterCreation	WaitForPrinterCreation
WorkingDirectory	WorkingDirectory
FolderPath	AdminFolderName

Remarque : IMA et FMA possèdent des restrictions différentes sur la longueur du nom de dossier. Dans IMA, la limite du nom de dossier est de 256 caractères ; la limite FMA est de 64 caractères. Lors de l'importation, les applications possédant un chemin d'accès contenant un nom de dossier de plus de 64 caractères sont ignorées. La limite s'applique uniquement au nom du dossier dans le chemin d'accès au dossier ; le chemin d'accès entier vers le dossier peut être plus long que les limites notées. Pour éviter que des applications soient ignorées lors de l'importation, Citrix vous recommande de vérifier la longueur du nom de dossier d'application et de la raccourcir, si nécessaire, avant l'exportation.

Les propriétés d'applications suivantes sont initialisées ou non initialisées par défaut, ou définies sur des valeurs fournies dans les données XenApp 6.x :

Propriété FMA	Valeur
Name	Initialisé pour le nom de chemin complet, qui contient les propriétés IMA FolderPath et DisplayName, mais sans la chaîne de préfixe « Applications\ »

Propriété FMA	Valeur
ApplicationType	HostedOnDesktop
CommandLineArguments	Initialisé à l'aide des arguments de ligne de commande XenApp 6.x
IconFromClient	Non initialisée ; la valeur par défaut est false.
IconUid	Initialisé à un objet d'icône créé à l'aide de données d'icônes XenApp 6.x
SecureCmdLineArgumentsEnabled	Non initialisée ; la valeur par défaut est true.
UserFilterEnabled	Non initialisée ; la valeur par défaut est false.
UUID	En lecture seule, affecté par le Controller
Visible	Non initialisée ; la valeur par défaut est true.

Les propriétés d'application suivantes sont partiellement migrées :

Propriété IMA	Commentaires
Types de fichiers	Seuls les types de fichiers qui existent sur le nouveau site XenApp sont migrés. Les types de fichiers qui n'existent pas sur le nouveau site sont ignorés. Les types de fichiers sont importés uniquement après que les types de fichier du nouveau site aient été mis à jour.
IconData	Les nouveaux objets d'icône sont créés si les données d'icône ont été fournies pour les applications exportées.
Comptes	Les comptes d'utilisateur d'une application sont partagés entre la liste des utilisateurs du groupe de mise à disposition et l'application. Les utilisateurs explicites sont utilisés pour initialiser la liste des utilisateurs de l'application. En outre, le compte « Utilisateurs de domaine » pour le domaine des comptes utilisateur est ajouté à la liste des utilisateurs du groupe de mise à disposition.

Les propriétés de XenApp 6.x suivantes ne sont pas importées :

Propriété IMA	Commentaires
ApplicationType	Ignorée.
HideWhenDisabled	Ignorée.
AccessSessionConditions	Remplacée par les stratégies d'accès du groupe de mise à disposition.
AccessSessionConditionsEnabled	Remplacée par les stratégies d'accès du groupe de mise à disposition.
ConnectionsThroughAccessGatewayAllowed	Remplacée par les stratégies d'accès du groupe de mise à disposition.
OtherConnectionsAllowed	Remplacée par les stratégies d'accès du groupe de mise à disposition.
AlternateProfiles	FMA ne prend pas en charge les applications livrées en streaming.
OfflineAccessAllowed	FMA ne prend pas en charge les applications livrées en streaming.
ProfileLocation	FMA ne prend pas en charge les applications livrées en streaming.
ProfileProgramArguments	FMA ne prend pas en charge les applications livrées en streaming.
ProfileProgramName	FMA ne prend pas en charge les applications livrées en streaming.
RunAsLeastPrivilegedUser	FMA ne prend pas en charge les applications livrées en streaming.
AnonymousConnectionsAllowed	FMA utilise une technologie différente pour prendre en charge les connexions (anonymes) non authentifiées.
ApplicationId, SequenceNumber	Données uniques à IMA
AudioType	FMA ne prend pas en charge les options de connexion clientes avancées.
EncryptionLevel	SecureICA est activé/désactivé dans les groupes de mise à disposition.
EncryptionRequired	SecureICA est activé/désactivé dans les groupes de mise à disposition.

Propriété IMA	Commentaires
SslConnectionEnabled	FMA utilise une implémentation TLS différente.
ContentAddress	FMA ne prend pas en charge le contenu publié.
ColorDepth	FMA ne prend pas en charge les apparences de fenêtre avancées.
MaximizedOnStartup	FMA ne prend pas en charge les apparences de fenêtre avancées.
TitleBarHidden	FMA ne prend pas en charge les apparences de fenêtre avancées.
WindowsType	FMA ne prend pas en charge les apparences de fenêtre avancées.
InstanceLimit	FMA ne prend pas en charge les limites d'application.
MultipleInstancesPerUserAllowed	FMA ne prend pas en charge les limites d'application.
LoadBalancingApplicationCheckEnabled	FMA utilise une technologie différente pour prendre en charge l'équilibrage de charge.
PreLaunch	FMA utilise une technologie différente pour la prise en charge du pré-lancement de session.
CachingOption	FMA utilise une technologie différente pour la prise en charge du pré-lancement de session.
ServerNames	FMA utilise une technologie différente.
WorkerGroupNames	FMA ne prend pas en charge les groupes de tâches.

Sécuriser

November 8, 2018

XenApp et XenDesktop offre une solution sécurisée de par sa conception qui vous permet de configurer votre environnement selon vos besoins en termes de sécurité.

Un problème de sécurité souvent rencontré en informatique concerne la perte ou le vol des données des travailleurs mobiles. En hébergeant les applications et les bureaux, XenApp et XenDesktop sépare les données sensibles et la propriété intellectuelle des machines de point de terminaison de manière

sécurisée en conservant les données dans un centre de données. Lorsque des stratégies sont activées pour autoriser le transfert des données, toutes les données sont cryptées.

Les centres de données XenDesktop et XenApp facilitent également les réponses aux incidents avec un service de contrôle et de gestion centralisé. Director permet au département informatique de surveiller et d'analyser les données qui sont accédées sur le réseau et Studio permet au département informatique d'appliquer des correctifs logiciels et de remédier à la plupart des vulnérabilités dans le centre de données au lieu de résoudre les problèmes localement sur chaque machine utilisateur.

XenApp et XenDesktop simplifie également les audits et assure la conformité à la règlementation car les enquêteurs peuvent utiliser une piste d'audit centralisée pour déterminer les personnes qui ont accès aux applications et aux données. Director collecte des données d'historique concernant les mises à jour du système et l'utilisation des données utilisateur en accédant à la journalisation de la configuration et l'API OData.

L'administration déléguée vous permet de configurer des rôles administrateur pour contrôler l'accès à XenDesktop et XenApp à un niveau plus précis. Ceci permet une plus grande souplesse dans votre organisation pour fournir à certains administrateurs un accès complet aux tâches, opérations et étendues alors que d'autres administrateurs ont un accès limité.

XenApp et XenDesktop fournit un contrôle plus précis aux administrateurs sur les utilisateurs en appliquant des stratégies à différents niveaux du réseau (à partir du niveau local de l'unité d'organisation). Ce contrôle des stratégies détermine si un utilisateur, une machine ou des groupes d'utilisateurs et de périphériques peuvent se connecter, imprimer, copier/coller, ou mapper les lecteurs locaux, ce qui peut réduire les problèmes de sécurité causés par des travailleurs tiers intérimaires. Les administrateurs peuvent également utiliser la fonctionnalité Desktop Lock, les utilisateurs finaux peuvent alors uniquement utiliser le bureau virtuel tout en empêchant tout accès au système d'exploitation local de la machine utilisateur.

Les administrateurs peuvent améliorer la sécurité de XenApp ou XenDesktop en configurant le site pour utiliser le protocole de sécurité TLS (Transport Layer Security) du Controller ou entre utilisateurs finaux et Virtual Delivery Agents (VDA). Le protocole peut également être activé sur un site pour fournir l'authentification de serveur, le cryptage du flux de données et le contrôle de l'intégrité des messages pour une connexion TCP/IP.

XenApp et XenDesktop fournit également l'authentification multi-facteurs pour Windows ou une application spécifique. L'authentification multi-facteurs peut également être utilisée pour gérer toutes les ressources mises à disposition par XenApp et XenDesktop. Ces méthodes comprennent :

- Jetons
- Cartes à puce
- RADIUS
- Kerberos
- Biométrie

XenDesktop peut être intégré à plusieurs des solutions de sécurité tierces, allant de la gestion de l'identité à un logiciel antivirus. Une liste des produits pris en charge peut être obtenue à l'adresse https://www.citrix.com/ready.

Les versions Premium de XenApp et XenDesktop sont certifiées pour la norme des critères communs. Pour consulter la liste de ces normes, accédez à https://www.commoncriteriaportal.org/cc/.

Considérations de sécurité et meilleures pratiques

January 23, 2019

> **Remarque :**
>
> Votre entreprise peut être tenue de satisfaire à certaines normes de sécurité pour remplir ses obligations réglementaires. Ce document ne traite pas de ce sujet, car ces normes de sécurité évoluent continuellement. Pour obtenir les informations les plus récentes sur les normes de sécurité et les produits Citrix, consultez https://www.citrix.com/security/.

Bonnes pratiques en matière de sécurité

Maintenez à jour toutes les machines de votre environnement avec des correctifs de sécurité. L'un des avantages est de pouvoir utiliser des clients légers comme terminaux, ce qui vous simplifie énormément la tâche.

Protégez toutes les machines de votre environnement avec un logiciel antivirus.

Envisagez d'utiliser un logiciel anti-malware spécifique à la plate-forme tel que la Trousse à outils EMET de Microsoft pour les machines Windows. Certaines autorités recommandent d'utiliser la dernière version de EMET prise en charge par Microsoft dans leurs environnements qui sont soumis à des réglementations strictes. D'après Microsoft, EMET peut ne pas être compatible avec certains logiciels, par conséquent il doit faire l'objet de tests rigoureux avec vos applications avant le déploiement dans un environnement de production. XenApp et XenDesktop ont été testés avec EMET 5.5 dans sa configuration par défaut. Pour le moment, nous ne recommandons pas d'utiliser EMET sur une machine sur laquelle est installé un Virtual Delivery Agent (VDA).

Protégez toutes les machines de votre environnement avec des pare-feu de périmètre, y compris aux limites des enclaves.

Si vous faites migrer un environnement classique vers cette version, il peut être nécessaire de repositionner un pare-feu de périmètre existant ou d'en ajouter de nouveaux. Supposons, par exemple, qu'un pare-feu de périmètre soit positionné entre un client classique et un serveur de base de données dans le centre de données. Avec cette version, ce pare-feu de périmètre doit être positionné de façon telle que le bureau virtuel et la machine utilisateur se trouvent d'un côté du pare-feu, et les

serveurs de bases de données et les Delivery Controller du centre de données de l'autre côté. Envisagez par conséquent de créer une enclave dans votre centre de données qui contiendra les serveurs de bases de données et les Controller. Il peut également être recommandé de mettre en place une protection entre la machine utilisateur et le bureau virtuel.

Toutes les machines de votre environnement devraient être protégées par un pare-feu personnel. Lorsque vous installez des composants principaux et des VDA (Virtual Delivery Agents), vous pouvez choisir que les ports requis pour le composant de la fonctionnalité de communication soient ouverts automatiquement si le service Pare-feu Windows est détecté (même si le pare-feu n'est pas activé). Vous pouvez également configurer ces ports des pare-feu manuellement. Si vous utilisez un autre pare-feu, vous devez configurer le pare-feu manuellement.

Remarque : les ports TCP 1494 et 2598 sont utilisés par les protocoles ICA et CGP. Ils sont donc susceptibles d'être ouverts afin que les utilisateurs se trouvant hors du centre de données puissent y accéder. Citrix vous recommande de ne pas utiliser ces ports à d'autres fins pour éviter tout risque d'attaque des interfaces d'administration. Les ports 1494 et 2598 sont officiellement enregistrés auprès de l'IANA (Internet Assigned Number Authority, voir https://www.iana.org/).

Toutes les communications réseau doivent être correctement sécurisées et cryptées pour répondre à votre stratégie de sécurité. Vous pouvez sécuriser toutes les communications entre vos ordinateurs Microsoft Windows avec IPSec ; reportez-vous à la documentation de votre système d'exploitation pour plus d'informations à ce sujet. De plus, les communications entre les machines utilisateurs et les bureaux sont sécurisées via Citrix SecureICA, configuré par défaut sur un cryptage 128 bits. Vous pouvez configurer SecureICA lorsque vous créez ou mettez à jour un groupe de mise à disposition.

Appliquez les recommandations Windows pour la gestion de comptes. Ne créez pas de compte sur un modèle ou une image avant sa duplication par Machine Creation Services ou Provisioning Services. Ne planifiez pas de tâches à l'aide de comptes de domaine privilégiés stockés. Ne créez pas manuellement de comptes de machines Active Directory partagés. Ces recommandations permettront d'éviter une attaque de machines par l'obtention des mots de passe de compte persistants locaux et leur utilisation pour se connecter à des images partagées MCS et PVS appartenant à d'autres utilisateurs.

Gérer les privilèges utilisateur

Accordez aux utilisateurs uniquement les droits qui leur sont nécessaires. Les privilèges Microsoft Windows sont toujours appliqués aux bureaux de la manière habituelle : vous configurez les privilèges à l'aide de l'attribution des droits utilisateur et de l'appartenance aux groupes via la stratégie de groupe. L'un des avantages de cette version est qu'il est possible d'octroyer à un utilisateur des droits d'administration sur un bureau sans lui accorder le contrôle physique de l'ordinateur qui héberge ce bureau.

Lorsque vous planifiez les privilèges des bureaux, veuillez noter ce qui suit.

- Par défaut, lorsque des utilisateurs non privilégiés se connectent à un bureau, ils voient le fuseau horaire du système exécutant le bureau au lieu de celui de leur propre machine utilisateur. Pour savoir comment autoriser les utilisateurs à voir leur heure locale lorsqu'ils utilisent des bureaux, veuillez consulter la section Modifier les paramètres de base.
- Un utilisateur qui est administrateur d'un bureau dispose d'un contrôle total sur ce dernier. S'il s'agit d'un bureau regroupé et non d'un bureau dédié, tous les autres utilisateurs de ce bureau, y compris les utilisateurs futurs, doivent lui faire confiance. Tous les utilisateurs doivent être conscients que ce genre de situation peut représenter un risque potentiel permanent pour la sécurité de leurs données. Cette remarque ne s'applique pas aux bureaux dédiés, qui n'ont qu'un seul utilisateur ; celui-ci ne doit être l'administrateur d'aucun autre bureau.
- Un utilisateur qui est administrateur d'un bureau peut généralement installer des logiciels sur ce bureau, y compris des logiciels potentiellement malveillants. Il a aussi la possibilité de surveiller ou de contrôler le trafic sur tout réseau connecté au bureau.

Certaines applications requièrent des privilèges de bureau, même si elles sont destinées aux utilisateurs plutôt qu'aux administrateurs. Les utilisateurs peuvent ne pas être aussi conscients des risques de sécurité.

Traitez ces applications comme des applications hautement sensibles, même si leurs données ne sont pas sensibles. Ces approches peuvent être utiles pour réduire le risque de sécurité :

- Appliquez l'authentification à deux facteurs et désactivez tout mécanisme de connexion unique pour l'application.
- Appliquez des règles d'accès contextuel.
- Publiez l'application sur un bureau dédié. Si l'application doit être publiée sur un bureau hébergé partagé, ne publiez aucune autre application sur ce bureau hébergé partagé.
- Assurez-vous que les privilèges du bureau ne sont appliqués qu'à ce bureau et non aux autres ordinateurs.
- Activez l'enregistrement de session pour l'application. Activez également d'autres fonctionnalités de journalisation de la sécurité dans l'application et dans Windows même.
- Configurez XenApp et XenDesktop pour limiter les fonctionnalités utilisées avec l'application (par exemple, Presse-papiers, imprimante, lecteur client et redirection USB).
- Activez toutes les fonctionnalités de sécurité de l'application. Appliquez des limites correspondant strictement aux besoins des utilisateurs - pas plus.
- Configurez les fonctionnalités de sécurité de Windows pour répondre strictement aux besoins des utilisateurs. La configuration sera plus simple si cette seule application est publiée sur le bureau ; par exemple, une configuration AppLocker restrictive peut être utilisée. Contrôlez l'accès au système de fichiers.
- Planifiez la reconfiguration, la mise à niveau ou le remplacement de l'application afin que les privilèges de bureau ne soient plus nécessaires à l'avenir.

Ces approches n'éliminent pas tous les risques de sécurité des applications nécessitant des privilèges

de bureau.

Gérer les droits d'ouverture de session

Des droits d'ouverture de session sont requis pour les comptes d'utilisateur et les comptes d'ordinateur. À l'instar des privilèges Microsoft Windows, les droits d'ouverture de session sont toujours appliqués aux bureaux de la manière habituelle : vous configurez les droits d'ouverture de session à l'aide de l'attribution des droits utilisateur et de l'appartenance aux groupes via la stratégie de groupe.

Les droits d'ouverture de session Windows sont les suivants : ouverture de session locale, ouverture de session via les Services Bureau à distance, ouverture de session sur le réseau (accès à cet ordinateur depuis le réseau), ouverture de session en tant que traitement par lots et ouverture de session en tant que service.

Pour les comptes d'ordinateur, accordez aux ordinateurs uniquement les droits d'ouverture de session dont ils ont besoin. Le droit d'ouverture de session « Accéder à cet ordinateur à partir du réseau » est obligatoire :

- Sur les VDA, pour les comptes d'ordinateur des Delivery Controller.
- Sur les Delivery Controller, pour les comptes d'ordinateur des VDA. Voir Découverte de Controller basée sur unité d'organisation Active Directory.
- Sur les serveurs StoreFront, pour les comptes d'ordinateur des autres serveurs dans le même groupe de serveurs StoreFront.

Pour les comptes d'utilisateur, accordez aux utilisateurs uniquement les droits d'ouverture de session dont ils ont besoin.

Selon Microsoft, le droit d'ouverture de session « Autoriser l'ouverture de session par les services Bureau à distance » est accordé par défaut au groupe Utilisateurs du Bureau à distance (excepté sur les contrôleurs de domaine).

La stratégie de sécurité de votre organisation peut stipuler explicitement que ce groupe soit supprimé de ce droit d'ouverture de session. Considérez l'approche suivante :

- Le Virtual Delivery Agent (VDA) de l'OS de serveur utilise les Services Bureau à distance Microsoft. Vous pouvez configurer le groupe Utilisateurs du Bureau à distance en tant que groupe restreint, et contrôler l'appartenance au groupe via des stratégies de groupe Active Directory. Référez-vous à la documentation Microsoft pour plus d'informations.
- Pour les autres composants de XenApp et XenDesktop, y compris le VDA pour OS de bureau, le groupe Utilisateurs du Bureau à distance n'est pas requis. Étant donné que le groupe Utilisateurs du Bureau à distance ne nécessite pas le droit d'ouverture de session « Autoriser l'ouverture de session au travers des services Bureau à distance » pour ces composants, vous pouvez le supprimer. Autres tâches :

  - Si vous administrez ces ordinateurs via les Services Bureau à distance, assurez-vous que tous les administrateurs sont déjà membres du groupe Administrateurs.
  - Si vous n'administrez pas ces ordinateurs via les Services Bureau à distance, vous pouvez désactiver les Services Bureau à distance sur ces ordinateurs.

Bien qu'il soit possible d'ajouter des utilisateurs et des groupes au droit d'ouverture de session « Interdire l'ouverture de session par les services Bureau à distance », l'interdiction de droits d'ouverture de session n'est généralement pas recommandée. Référez-vous à la documentation Microsoft pour plus d'informations.

Configurer les droits des utilisateurs

L'installation de Delivery Controller crée les services Windows suivants :

- Citrix AD Identity Service (NT SERVICE\CitrixADIdentityService Microsoft) : gère les comptes d'ordinateurs Active Directory pour les machines virtuelles.
- Citrix Analytics (NT SERVICE\CitrixAnalytics) : collecte des informations sur l'utilisation de la configuration du site, si cette collecte a été approuvée par l'administrateur du site. Ces informations sont ensuite envoyées à Citrix pour aider à améliorer le produit.
- Citrix App Library (NT SERVICE\CitrixAppLibrary) : prend en charge la gestion et le provisioning d'AppDisks, l'intégration d'AppDNA et la gestion d'App-V.
- Citrix Broker Service (NT SERVICE\CitrixBrokerService) : sélectionne les applications ou bureaux virtuels qui sont disponibles pour les utilisateurs.
- Citrix Configuration Logging Service (NT SERVICE\CitrixConfigurationLogging) : enregistre toutes les modifications de configuration et d'autres modifications apportées par les administrateurs du site.
- Citrix Configuration Service (NT SERVICE\CitrixConfigurationService) : référentiel à l'échelle du site pour la configuration partagée.
- Citrix Delegated Administration Service (NT SERVICE\CitrixDelegatedAdmin) : gère les autorisations accordées aux administrateurs.
- Citrix Environment Test Service (NT SERVICE\CitrixEnvTest) : gère les auto-tests des autres services Delivery Controller.
- Citrix Host Service (NT SERVICE\CitrixHostService) : stocke des informations sur les infrastructures d'hyperviseur utilisées dans un déploiement XenApp ou XenDesktop, et offre également des fonctionnalités utilisées par la console pour énumérer les ressources dans un pool d'hyperviseurs.
- Citrix Machine Creation Service (NT SERVICE\CitrixMachineCreationService) : orchestre la création de machines virtuelles de bureau.
- Citrix Monitor Service (NT SERVICE\CitrixMonitor) : collecte des métriques pour XenApp ou XenDesktop, stocke les données d'historique, et fournit une interface de requête pour la résolution des problèmes et les outils de reporting.

- Citrix Storefront Service (NT SERVICE\CitrixStorefront) : prend en charge la gestion de StoreFront. (Ne fait pas partie du composant StoreFront).
- Citrix Storefront Privileged Administration Service (NT SERVICE\CitrixPrivilegedService) : prend en charge les opérations d'administration privilégiée de StoreFront. (Ne fait pas partie du composant StoreFront).
- Citrix Config Synchronizer Service (NT SERVICE\CitrixConfigSyncService) : propage les données de configuration depuis la base de données du site principal vers le cache d'hôte local.
- Citrix High Availability Service (NT SERVICE\CitrixHighAvailabilityService) : sélectionne les applications ou bureaux virtuels qui sont disponibles pour les utilisateurs, lorsque la base de données du site principal n'est pas disponible.

L'installation de Delivery Controller crée également les services Windows suivants. Ces services sont également créés lorsqu'ils sont installés avec d'autres composants Citrix :

- Citrix Diagnostic Facility COM Server (NT SERVICE\CdfSvc) : prend en charge la collecte d'informations de diagnostic destinées au support technique de Citrix.
- Service de télémétrie Citrix (NT SERVICE\CitrixTelemetryService) : collecte des informations de diagnostic à des fins d'analyse par Citrix, de façon à ce que les résultats de l'analyse et les recommandations puissent être consultés par les administrateurs pour diagnostiquer les problèmes avec le site.

L'installation de Delivery Controller crée également le service Windows suivant. Il n'est pas utilisé pour le moment. S'il est activé, désactivez-le.

- Citrix Remote Broker Provider (NT SERVICE\XaXdCloudProxy)

L'installation de Delivery Controller crée également les services Windows suivants. Ces derniers ne sont pas utilisés actuellement, mais doivent être activés. Ne les désactivez pas.

- Citrix Orchestration Service (NT SERVICE\CitrixOrchestration)
- Citrix Trust Service (NT SERVICE\CitrixTrust)

À l'exception du service Citrix Storefront Privileged Administration Service, le droit d'ouverture de session Ouvrir une session en tant que service et les privilèges Ajuster les quotas de mémoire pour un processus, Générer des audits de sécurité et Remplacer un jeton de niveau processus sont accordés à ces services. Vous n'avez pas besoin de changer ces droits d'utilisateur. Ces privilèges ne sont pas utilisés par le Delivery Controller et sont automatiquement désactivés.

Configurer les paramètres du service

À l'exception du service Citrix StoreFront Privileged Administration Service et du Service de télémétrie Citrix, les services Windows Delivery Controller répertoriés ci-dessus dans la section Configurer les droits des utilisateurs sont configurés pour ouvrir une session sous l'identité NETWORK SERVICE. Ne modifiez pas ces paramètres de service.

Le service Citrix StoreFront Privileged Administration Service est configuré pour ouvrir une session sous l'identité Système local (NT AUTHORITY\SYSTEM). Ceci est requis pour les opérations de Delivery Controller et de StoreFront qui ne sont normalement pas disponibles pour les services (y compris la création de sites IIS Microsoft). Ne modifiez pas ses paramètres de service.

Le Service de télémétrie Citrix est configuré pour ouvrir une session sous sa propre identité spécifique au service.

Vous pouvez désactiver le Service de télémétrie Citrix. Outre ce service, et les services qui sont déjà désactivés, ne désactivez aucun des autres services Windows Delivery Controller.

Configurer les paramètres de registre

Il n'est plus nécessaire d'activer la création de noms de fichiers et de dossiers au format 8.3 sur le système de fichiers du VDA. La clé de registre **NtfsDisable8dot3NameCreation** peut être configurée pour désactiver la création de noms de fichiers et de dossiers au format 8.3. Vous pouvez également configurer ce comportement à l'aide de la commande **fsutil.exe behavior set disable8dot3**.

Implications en termes de sécurité du scénario de déploiement

Votre environnement utilisateur peut se composer soit de machines utilisateur non gérées par votre entreprise et totalement sous le contrôle de l'utilisateur, soit de machines utilisateur gérées et administrées par votre entreprise. Les considérations de sécurité pour ces deux environnements sont généralement différentes.

Machines utilisateur gérées

Les machines utilisateur gérées font l'objet d'un contrôle administratif ; elles sont soit sous votre propre contrôle, soit sous celui d'une autre organisation à laquelle vous faites confiance. Vous pouvez configurer et fournir directement aux utilisateurs les machines utilisateur ; vous pouvez également fournir des terminaux sur lesquels un seul bureau s'exécute en mode plein écran seulement. Suivez les bonnes pratiques générales en matière de sécurité décrites ci-dessous pour toutes les machines utilisateur gérées. Cette version présente l'avantage de n'exiger qu'un minimum de logiciels sur une machine utilisateur.

Une machine utilisateur gérée peut être configurée pour être utilisée en mode plein écran seulement ou en mode fenêtre.

- Mode plein écran uniquement : les utilisateurs ouvrent une session sur celle-ci à partir de l'écran d'ouverture de session Windows habituel. Les mêmes informations d'identification de l'utilisateur sont alors utilisées pour ouvrir automatiquement une session sur cette version.

- Les utilisateurs voient leur bureau dans une fenêtre : les utilisateurs doivent d'abord ouvrir une session sur la machine utilisateur, puis sur cette version via le site Web fourni avec le produit.

Machines utilisateur non gérées

Les machines utilisateur qui ne sont pas gérées et administrées par une organisation de confiance ne peuvent pas être considérées comme des machines sous contrôle administratif. Vous pouvez, par exemple, autoriser les utilisateurs à se procurer et à configurer leurs propres machines, mais ceux-ci peuvent ne pas respecter les bonnes pratiques générales en matière de sécurité décrites ci-dessus. Cette version présente l'avantage de mettre, en toute sécurité, des bureaux à la disposition des machines utilisateur non gérées. Ces machines doivent tout de même disposer d'une protection antivirus de base capable d'arrêter les enregistreurs de frappes et les attaques similaires axées sur la saisie.

Considérations sur le stockage de données

Lorsque vous utilisez cette version, vous pouvez empêcher les utilisateurs de stocker des données sur les machines utilisateur qui sont sous leur contrôle physique. Toutefois, vous devez encore envisager les conséquences de l'enregistrement, par les utilisateurs, de données sur leurs bureaux. Enregistrer des données sur les bureaux n'est pas une bonne pratique ; celles-ci doivent être stockées sur des serveurs de fichiers, des serveurs de bases de données ou d'autres référentiels où elles feront l'objet d'une protection appropriée.

Votre environnement peut être composé de différents types de bureaux, tels que des bureaux regroupés ou dédiés. Les utilisateurs ne doivent jamais stocker de données sur des bureaux partagés, tels que les bureaux regroupés. S'ils stockent des données sur des bureaux dédiés, celles-ci doivent être supprimées si les bureaux sont ensuite mis à la disposition d'autres utilisateurs.

Environnements à versions mixtes

Les environnements à versions mixtes sont inévitables lors de certaines mises à niveau. Suivez les recommandations et réduisez la durée pendant laquelle les composants Citrix de versions différentes co-existent. Dans les environnements à versions mixtes, la stratégie de sécurité, par exemple, peut ne pas être appliquée de façon uniforme.

Remarque : ce comportement est caractéristique d'autres produits logiciels ; l'utilisation d'une version antérieure d'Active Directory n'applique que partiellement la stratégie de groupe avec les versions ultérieures de Windows.

Le scénario suivant décrit un problème de sécurité qui peut se produire dans un environnement Citrix à versions mixtes spécifique. Lorsque Citrix Receiver 1.7 est utilisé pour se connecter à un bureau virtuel exécutant le VDA dans XenApp et XenDesktop 7.6 Feature Pack 2, le paramètre de stratégie

Autoriser le transfert de fichiers entre les bureaux et le client est activée dans le site, mais ne peut pas être désactivée par un Delivery Controller exécutant XenApp et XenDesktop 7.1. Il ne reconnaît pas le paramètre de stratégie, qui est disponible dans la version ultérieure du produit. Ce paramètre de stratégie permet aux utilisateurs de télécharger des fichiers sur leur bureau virtuel, ce qui cause le problème de sécurité. Pour contourner ce problème, mettez à niveau le Delivery Controller ou une instance autonome de Studio vers la version 7.6 Feature Pack 2, puis utilisez la stratégie de groupe pour désactiver le paramètre de stratégie. Vous pouvez également utiliser la stratégie locale sur tous les bureaux virtuels concernés.

Considérations de sécurité Remote PC Access

Remote PC Access implémente les fonctionnalités de sécurité suivantes :

- La carte à puce est prise en charge.
- Lorsqu'une session à distance se connecte, le moniteur du PC de bureau affiche un écran noir.
- Remote PC Access redirige toutes les entrées de claviers et de souris vers la session à distance, sauf la combinaison CTRL+ALT+SUPPR et les cartes à puce et les périphériques biométriques USB.
- SmoothRoaming est prise en charge uniquement pour un seul utilisateur.
- Lorsqu'un utilisateur a ouvert une session distante connectée à un PC de bureau, seul cet utilisateur peut reprendre l'accès local sur le PC de bureau. Pour reprendre l'accès local, l'utilisateur appuie sur Ctrl+Alt+Suppr sur le PC local et ouvre une session avec les mêmes informations d'identification utilisées par la session à distance. L'utilisateur peut également reprendre l'accès local en insérant une carte à puce ou en tirant parti de la biométrie, si votre système possède une intégration fournisseur des informations d'identification tierces appropriées. Ce comportement par défaut peut être substitué par l'activation de changement rapide d'utilisateur via des objets de stratégie de groupe (GPO) ou en modifiant le registre.

Remarque : Citrix recommande de ne pas attribuer de privilèges d'administrateur VDA aux utilisateurs de sessions.

Assignations automatiques

Par défaut, Remote PC Access prend en charge l'assignation automatique de plusieurs utilisateurs à un VDA. Dans XenDesktop 5.6 Feature Pack 1, les administrateurs peuvent modifier ce comportement en utilisant le script PowerShell RemotePCAccess.ps1. Cette version utilise une entrée du Registre pour autoriser ou interdire plusieurs affectations de PC distants automatiques, ce paramètre s'applique à l'intégralité du site.

Avertissement : toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possi-

bilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Pour restreindre les affectations automatiques pour un utilisateur unique :

Sur chaque Controller du site, définissez la clé de registre suivante :

```
HKEY\_LOCAL\_MACHINE\Software\Citrix|DesktopServer

Nom : AllowMultipleRemotePCAssignments

Type : REG\_DWORD

Données : 0 = Désactiver l'attribution de plusieurs utilisateurs, 1 =
    Activer l'affectation de plusieurs utilisateurs (valeur par défaut).
```

S'il existe une ou plusieurs affectations d'utilisateur, supprimez-les à l'aide des commandes du kit de développement afin que le VDA puisse ensuite être admissible pour une seule affectation automatique.

- Supprimez tous les utilisateurs affectés à partir du VDA :
  $machine.AssociatedUserNames | %{ Remove-BrokerUser-Name $_ -Machine $machine
- Supprimez le VDA du groupe de mise à disposition :
  $machine | Remove-BrokerMachine -DesktopGroup $desktopGroup

Redémarrez le PC de bureau physique.

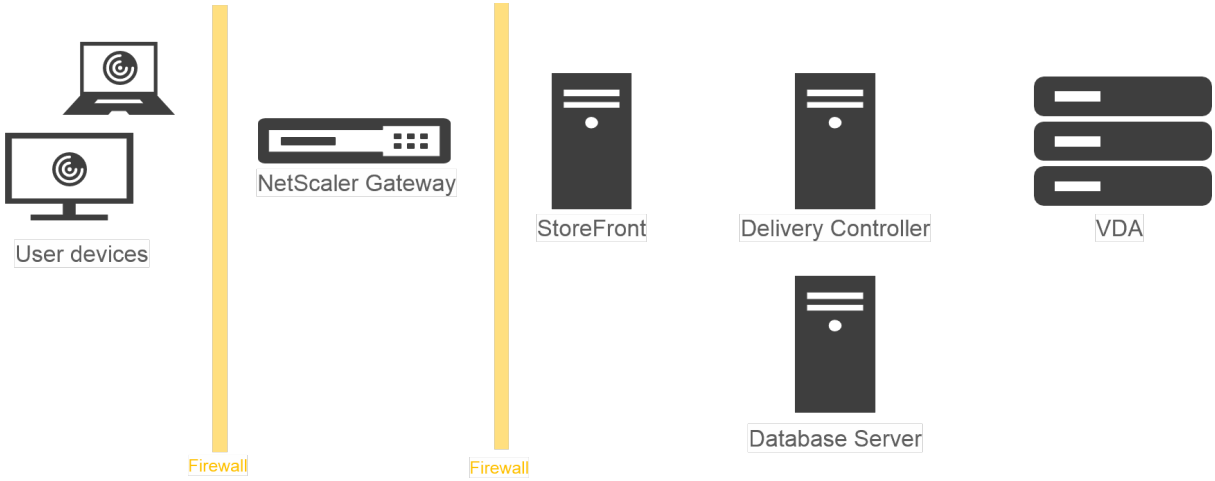
Intégrer XenApp et XenDesktop avec NetScaler Gateway

January 23, 2019

Les serveurs StoreFront sont déployés et configurés pour gérer l'accès aux données et ressources publiées. Pour un accès distant, il est recommandé d'ajouter NetScaler Gateway devant StoreFront.

> **Remarque :**
>
> Pour obtenir la procédure détaillée de configuration de l'intégration de XenApp et XenDesktop avec NetScaler Gateway, consultez la documentation de StoreFront.

Le diagramme suivant illustre un exemple d'un déploiement de Citrix simplifié qui inclut NetScaler Gateway. NetScaler Gateway communique avec StoreFront pour protéger les applications et les données fournies par XenApp et XenDesktop. Les machines utilisateur exécutent Citrix Receiver pour créer une connexion sécurisée et accéder à leurs applications, postes de travail et fichiers.



Les utilisateurs se connectent et s'authentifient à l'aide de NetScaler Gateway. NetScaler Gateway est déployé et sécurisé dans la DMZ. L'authentification à deux facteurs est configurée. En fonction des informations d'identification qu'ils saisissent, les utilisateurs recevront les ressources et applications auxquelles ils sont autorisés à accéder. Les applications et les données sont sur des serveurs appropriés (non illustrés dans le diagramme). Séparez les serveurs utilisés pour des applications et des données sensibles.

Administration déléguée

January 23, 2019

Grâce à l'utilisation d'un contrôle basé sur des objets et des rôles, le modèle d'administration déléguée vous offre une souplesse permettant d'adapter les activités d'administration déléguée aux besoins de votre entreprise. L'administration déléguée prend en charge les déploiements de toutes les tailles et vous permet d'affiner la granularité des autorisations à mesure que votre déploiement gagne en complexité. L'administration déléguée utilise trois concepts : les administrateurs, les rôles et les étendues.

- **Administrateurs** : un administrateur représente une personne ou un groupe de personnes identifié par leur compte Active Directory. Chaque administrateur est associé à un ou plusieurs rôles et à des paires d'étendues.
- **Rôles** : un rôle représente une fonction de tâche à laquelle des permissions sont associées. Par exemple, le rôle Administrateur du groupe de mise à disposition possède des autorisations telles que « Créer un groupe de mise à disposition » et « Supprimer le bureau d'un groupe de mise à disposition ». Un administrateur peut avoir plusieurs rôles pour un même site, donc une personne peut être administrateur du groupe de mise à disposition et administrateur du catalogue de machines. Les rôles peuvent être intégrés ou personnalisés.

  Les rôles intégrés sont :

Rôle	Autorisations
Administrateur complet	Peut effectuer toutes les tâches et toutes les opérations. Un administrateur complet est toujours associé à l'étendue Tout.
Administrateur en lecture seule	Peut afficher tous les objets dans les étendues spécifiées ainsi que les informations générales, mais ne peut rien modifier. Par exemple, un administrateur en lecture seule avec l'étendue = Londres peut voir tous les objets globaux (tels que la journalisation de la configuration) et les objets associés à Londres (par exemple, les groupes de mise à disposition Londres). Toutefois, cet administrateur ne peut pas afficher d'objets dans l'étendue New York (en supposant que les étendues Londres et New York ne se chevauchent pas).
Administrateur du service d'assistance	Peut afficher des groupes de mise à disposition et gérer les sessions et les machines associées à ces groupes. Peut afficher le catalogue de machines et les informations d'hôte des groupes de mise à disposition en cours de surveillance et peut également effectuer des opérations de gestion de session et de gestion de l'alimentation de la machine pour les machines figurant dans ces groupes de mise à disposition.
Administrateur du catalogue de machines	Peut créer et de gérer des catalogues de machines et y provisionner des machines. Peut créer des catalogues de machines à partir de l'infrastructure de virtualisation, Provisioning Services et des machines physiques. Ce rôle peut gérer les images de base et installer le logiciel, mais ne peut pas assigner les applications ou bureaux aux utilisateurs.

Rôle	Autorisations
Administrateur de groupe de mise à disposition	Peut mettre à disposition des applications, bureaux et machines ; peut également gérer les sessions associées. Il peut également gérer les configurations d'applications et de bureaux, telles que les stratégies et les paramètres de gestion de l'alimentation.
Administrateur d'hôte	Peut gérer les connexions hôtes et leurs paramètres de ressources associés. Impossible de mettre à disposition des machines, applications ou bureaux aux utilisateurs.

Dans certaines éditions du produit, vous pouvez créer des rôles personnalisés correspondants aux besoins de votre organisation, et déléguer des autorisations avec plus de détails. Vous pouvez utiliser les rôles personnalisés pour allouer des autorisations à la précision d'une action ou d'une tâche dans la console.

- **Étendues** : une étendue représente une collection d'objets. Les étendues sont utilisées pour grouper les objets de manière pertinente pour votre organisation (par exemple, l'ensemble de groupes de mise à disposition utilisé par l'équipe des ventes). Les objets peuvent appartenir à plus d'une étendue ; par exemple, un objet peut être marqué comme appartenant à une ou plusieurs étendues. Il existe une étendue intégrée appelée « Tout » qui contient tous les objets. Le rôle d'administrateur complet est toujours associé à l'étendue Tout.

Exemple

La société XYZ a décidé de gérer les applications et bureaux en fonction de leur département (Comptabilité, Ventes et Production) et de leur système d'exploitation de bureau (Windows 7 ou Windows 8). L'administrateur a créé cinq étendues, puis a attribué deux étendues à chaque groupe de mise à disposition : une pour le département où ils sont utilisés et une pour le système d'exploitation qu'ils utilisent.

Les administrateurs suivants ont été créés :

Administrateur	Rôles	Étendues
domaine/fred	Administrateur complet	Tous (le rôle Administrateur complet a toujours la portée Tout)

Administrateur	Rôles	Étendues
domaine/rob	Administrateur en lecture seule	Toutes
domaine/heidi	Administrateur en lecture seule, Administrateur du service d'assistance	Toutes les ventes
domaine/warehouseadmin	Administrateur du service d'assistance	Distribution
domaine/peter	Administrateur du groupe de mise à disposition, Administrateur du catalogue de machines	Win7

- Fred est un administrateur complet qui peut afficher, modifier et supprimer tous les objets dans le système.
- Rob peut afficher tous les objets dans le site mais ne peut pas les modifier ou les supprimer.
- Heidi peut afficher tous les objets et peut effectuer des tâches de support technique sur les groupes de mise à disposition dans l'étendue Ventes. Cela lui permet de gérer les sessions et les machines associées à ces groupes ; elle ne peut pas effectuer de modifications dans le groupe de mise à disposition, telles que l'ajout ou la suppression de machines.
- Toute personne qui est membre du groupe de sécurité Active Directory admindistribution peut afficher et effectuer des tâches d'assistance sur des machines dans l'étendue Distribution.
- Peter est un spécialiste Windows 7 et peut gérer tous les catalogues de machines Windows 7 et mettre à disposition des applications, bureaux et machines Windows 7, quelle que soit l'étendue du département auquel elles appartiennent. L'administrateur a envisagé de donner à Peter le rôle d'administrateur complet pour l'étendue Win7 ; elle en a décidé autrement, car un administrateur complet a également des droits complets sur tous les objets qui ne sont pas inclus dans l'étendue, tels que « Site » et « Administrateur ».

Comment utiliser l'administration déléguée

En général, le nombre d'administrateurs et la granularité de leurs autorisations dépendent de la taille et de la complexité du déploiement.

- Dans les déploiements de petite taille ou de preuve de concept, toutes les tâches sont effectuées par un ou plusieurs administrateurs ; il n'y a pas de délégation. Dans ce cas, créez chaque administrateur avec le rôle Administrateur complet intégré, qui a la portée Tout.

- Dans les déploiements plus importants avec plus d'ordinateurs, d'applications et de bureaux, une plus grande délégation est nécessaire. Plusieurs administrateurs ont peut-être des responsabilités fonctionnelles plus spécifiques (rôles). Par exemple, deux sont des administrateurs complets et les autres sont des administrateurs du service d'assistance. En outre, un administrateur peut ne gérer que certains groupes d'objets (étendues), tels que des catalogues de machines. Dans ce cas, créez de nouvelles étendues, ainsi que des administrateurs avec l'un des rôles intégrés et les étendues appropriées.
- Même les déploiements plus importants peuvent nécessiter plus (ou plus spécifiques) d'étendues, ainsi que des administrateurs différents dotés de rôles non conventionnels. Dans ce cas, modifiez ou créez des étendues supplémentaires, créez des rôles personnalisés et créez chaque administrateur avec un rôle personnalisé ou intégré, ainsi que des étendues existantes et nouvelles.

Pour garantir une souplesse et facilité de configuration, vous pouvez créer de nouvelles étendues lorsque vous créez un administrateur. Vous pouvez également spécifier des étendues lors de la création ou de la modification de catalogues de machines ou de connexions.

Créer et gérer des administrateurs

Lorsque vous créez un site en tant qu'administrateur local, votre compte d'utilisateur devient automatiquement un administrateur complet avec autorisations complètes sur tous les objets. Après la création d'un site, les administrateurs locaux n'ont pas de privilèges spéciaux.

Le rôle administrateur complet a toujours l'étendue Tout ; vous ne pouvez pas le modifier.

Par défaut, un administrateur est activé. La désactivation d'un administrateur peut être nécessaire si vous créez le nouvel administrateur maintenant, mais cette personne ne possèdera des droits d'administration que bien plus tard. Pour les administrateurs activés existants, il se peut que vous souhaitiez désactiver plusieurs d'entre eux pendant que vous réorganisez vos objets/étendues, puis les réactiver lorsque vous êtes prêt à utiliser la configuration mise à jour dans votre environnement de production. Vous ne pouvez pas désactiver un administrateur complet si cela a pour conséquence qu'il n'existe plus d'administrateur complet activé. La case à cocher activer/désactiver est disponible lors de la création, de la copie ou de la modification d'un administrateur.

Lorsque vous supprimez une paire rôle/étendue lors de la copie, la modification ou la suppression d'un administrateur, il supprime uniquement la relation entre le rôle et l'étendue de cet administrateur ; il ne peut pas supprimer le rôle ou l'étendue et n'affecte aucun autre administrateur qui est configuré avec cette paire rôle/étendue.

Pour gérer des administrateurs, cliquez sur
Configuration > Administrateurs dans le panneau de navigation de Studio, puis cliquez sur l'onglet Administrateurs dans la partie supérieure du panneau central.

- Pour créer un administrateur, cliquez sur Créer un nouvel administrateur dans le volet Actions. Entrez le nom ou recherchez le nom du compte d'utilisateur, sélectionnez ou créez une étendue, et sélectionnez un rôle. Le nouvel administrateur est activé par défaut, vous pouvez le modifier.
- Pour copier un administrateur, sélectionnez l'administrateur dans le panneau du milieu, puis cliquez sur Copier l'administrateur dans le volet Actions. Entrez le nom ou recherchez le nom de compte de l'utilisateur. Vous pouvez sélectionner puis modifier les paires rôle/étendue et vous pouvez en ajouter de nouvelles. Le nouvel administrateur est activé par défaut, vous pouvez le modifier.
- Pour modifier un administrateur, sélectionnez l'administrateur dans le panneau du milieu, puis cliquez sur Modifier l'administrateur dans le volet Actions. Vous pouvez modifier ou supprimer les paires rôle/étendue et en ajouter de nouvelles.
- Pour supprimer un administrateur, sélectionnez l'administrateur dans le panneau du milieu, puis cliquez sur Supprimer l'administrateur dans le volet Actions. Vous ne pouvez pas supprimer un administrateur complet si cela a pour conséquence qu'il n'existe plus d'administrateur complet.

Créer et gérer les rôles

Les noms de rôles peuvent contenir jusqu'à 64 caractères Unicode ; ils ne peuvent pas contenir les caractères suivants : \ (barre oblique inverse) / (barre oblique) ; (point-virgule) : (deux-points), # (symbole de la livre) , (virgule), * (astérisque), ? (point d'interrogation), = (signe égal), < (flèche gauche), > (flèche droite), | (barre verticale), [ ] (crochet droit ou gauche), ( ) (parenthèse droite ou gauche), " (guillemets) et ' (apostrophe). Les descriptions peuvent contenir jusqu'à 256 caractères unicode.

Vous ne pouvez pas modifier ou supprimer un rôle intégré. Vous ne pouvez pas supprimer un rôle personnalisé si un administrateur l'utilise.

Remarque : seules certaines éditions de produit prennent en charge les rôles personnalisés. Les éditions qui ne prennent pas en charge les rôles personnalisés n'ont aucune entrée dans le volet Actions.

Pour gérer les rôles, cliquez sur Configuration > Administrateurs dans le panneau de navigation de Studio, puis cliquez sur l'onglet Rôles en haut du panneau central.

- Pour afficher les détails d'un rôle, sélectionnez le rôle dans le volet central. La partie inférieure du panneau central répertorie les types d'objets et les autorisations associées pour le rôle. Cliquez sur l'onglet Administrateurs dans le volet inférieur pour afficher une liste des administrateurs détiennent actuellement ce rôle.
- Pour créer un rôle personnalisé, cliquez sur Créer un nouveau rôle dans le volet Actions. Entrez un nom et une description. Sélectionnez les types d'objets et les autorisations.
- Pour copier un rôle, sélectionnez le rôle dans le volet central, puis cliquez sur Copier un rôle dans le volet Actions. Modifiez le nom, la description, les types d'objet et les autorisations nécessaires.

- Pour modifier un rôle personnalisé, sélectionnez le rôle dans le volet central, puis cliquez sur Modifier un rôle dans le volet Actions. Modifiez le nom, la description, les types d'objet et les autorisations nécessaires.
- Pour supprimer un rôle personnalisé, sélectionnez le rôle dans le volet central, puis cliquez sur Supprimer un rôle dans le volet Actions. Lorsque vous y êtes invité, confirmez la suppression.

Créer et gérer des étendues

Lorsque vous créez un site, la seule étendue disponible est l'étendue 'Tout', qui ne peut pas être supprimée.

Vous pouvez créer des étendues à l'aide de la procédure ci-dessous. Vous pouvez également créer des étendues lorsque vous créez un administrateur ; chaque administrateur doit être associé à au moins une paire de un rôle/étendue. Lorsque vous créez ou modifiez des bureaux, des catalogues de machines, des applications ou des hôtes, vous pouvez les ajouter à une étendue existante ; si vous ne les ajoutez pas à une étendue, ils restent dans l'étendue 'Toute'.

La création d'un site ne peut faire être incluse à une étendue, ni les objets d'administration déléguée (étendues et rôles). Cependant, les objets ne pouvant pas être inclus à une étendue sont inclus dans l'étendue « Tout ». (Les administrateurs complets disposent toujours de l'étendue Toute.) Les machines, actions d'alimentation, bureaux et sessions ne sont pas directement inclus à une étendue ; des permissions sur ces objets peuvent être accordées aux administrateurs via les catalogues de machines ou groupes de mise à disposition associés.

Les noms d'étendues peuvent contenir jusqu'à 64 caractères Unicode ; ils ne peuvent pas contenir les caractères suivants : \ (barre oblique inverse) / (barre oblique) ; (point-virgule) : (deux-points), # (symbole de la livre) , (virgule), * (astérisque), ? (point d'interrogation), = (signe égal), < (flèche gauche), > (flèche droite), | (barre verticale), [ ] (crochet droit ou gauche), ( ) (parenthèse droite ou gauche), " (guillemets) et ' (apostrophe). Les descriptions peuvent contenir jusqu'à 256 caractères unicode.

Lorsque vous copiez ou modifier une étendue, n'oubliez pas que la suppression des objets dans l'étendue peut rendre ces objets inaccessibles à l'administrateur. Si l'étendue modifiée est associée à un ou plusieurs rôles, assurez-vous que les mises à jour que vous apportez à l'étendue ne rendent pas une paire rôle/étendue inutilisable.

Pour gérer des étendues, cliquez sur Configuration > Administrateurs dans le panneau de navigation de Studio, puis cliquez sur l'onglet Étendues dans la partie supérieure du panneau central.

- Pour créer une étendue, cliquez sur Créer une nouvelle étendue dans le volet Actions. Entrez un nom et une description. Pour inclure tous les objets d'un type particulier (par exemple, les groupes de mise à disposition), sélectionnez le type d'objet. Pour inclure des objets spécifiques, développez le type, puis sélectionnez les objets individuels (par exemple, les groupes de mise à disposition individuels utilisés par l'équipe des Ventes).

- Pour copier une étendue, sélectionnez l'étendue dans le volet central, puis cliquez sur Copier étendue dans le volet Actions. Entrez un nom et une description. Modifiez les types d'objets et les objets, si nécessaire.
- Pour modifier une étendue, sélectionnez l'étendue dans le volet central, puis cliquez sur Modifier l'étendue dans le volet Actions. Modifiez le nom, la description, les types d'objet et les objets, si nécessaire.
- Pour supprimer une étendue, sélectionnez l'étendue dans le volet central, puis cliquez sur Supprimer l'étendue dans le volet Actions. Lorsque vous y êtes invité, confirmez la suppression.

Créer des rapports

Vous pouvez créer deux types de rapports d'administration déléguée :

- Ce rapport HTML indique les paires rôle/étendue associées à un administrateur et dresse la liste des autorisations individuelles pour chaque type d'objet (par exemple, les groupes de mise à disposition et les catalogues de machines). Vous pouvez générer ce rapport à partir de Studio.

  Pour créer ce rapport, cliquez sur Configuration > Administrateurs dans le volet de navigation. Sélectionnez un administrateur dans le panneau du milieu, puis cliquez sur Créer un rapport dans le volet Actions.

  Vous pouvez également demander ce rapport lors de la création, de la copie ou de la modification d'un administrateur.

- Un rapport HTML ou CSV qui mappe tous les rôles personnalisés et intégrés à des autorisations. Vous pouvez générer ce rapport en exécutant le script PowerShell nommé OutputPermissionMapping.ps1.

  Pour exécuter ce script, vous devez être un administrateur complet, un administrateur en lecture seule ou un administrateur personnalisé avec autorisation de lecture des rôles. Le script se trouve dans : Program Files\Citrix\DelegatedAdmin\SnapIn\Citrix.DelegatedAdmin.Admin.V1\Scripts\.

  Syntaxe :

  OutputPermissionMapping.ps1 [-Help] [-Csv] [-Path <string>] [-AdminAddress <string>] [-Show] [<CommonParameters>]

Paramètre	Description
-Help	Affiche l'aide du script.
-Csv	Spécifie le fichier CSV de sortie. Valeur par défaut = HTML
-Path	Où écrire la sortie. Valeur par défaut = stdout

Paramètre	Description
-AdminAddress	Adresse IP ou nom d'hôte du Delivery Controller auquel se connecter. Valeur par défaut = XA
-Show	(Valide uniquement lorsque le paramètre -Path est également spécifié). Lorsque vous écrivez la sortie vers un fichier, ce paramètre entraîne l'ouverture de la sortie dans un programme approprié, tel qu'un navigateur Web.
	Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer et OutVariable. Pour plus d'informations, veuillez consulter la documentation Microsoft.

L'exemple suivant écrit une table HTML sur un fichier appelé Roles.html et ouvre la table dans un navigateur Web.

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"
-Path Roles.html  - Show
```

L'exemple suivant écrit une table CSV sur un fichier appelé Roles.csv. La table n'est pas affichée.

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"
 - CSV -Path Roles.csv
```

À partir d'une invite de commande Windows, l'exemple de commande précédente est :

```
powershell -command "& '%ProgramFiles%\Citrix\DelegatedAdmin\SnapIn\
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1'
-CSV -Path Roles.csv"
```

Cartes à puce

February 28, 2019

Les cartes à puce et les technologies équivalentes sont prises en charge selon les indications décrites dans cet article. Pour utiliser des cartes à puce avec XenApp ou XenDesktop :

- Il est important de bien comprendre la stratégie de sécurité de votre organisation concernant l'utilisation des cartes à puce. Ces stratégies peuvent, par exemple, déterminer comment les cartes à puce sont délivrées et comment les utilisateurs doivent les protéger. Il peut être nécessaire de réévaluer certains aspects de ces stratégies dans un environnement XenApp ou XenDesktop.
- Déterminez les types de machine utilisateur, les systèmes d'exploitation et les applications publiées qui doivent être utilisés avec des cartes à puce.
- Familiarisez-vous avec la technologie de carte à puce ainsi que le matériel et les logiciels de votre fournisseur de carte à puce.
- Déterminez comment déployer des certificats numériques dans un environnement distribué.

Types de cartes à puce

Les cartes à puce d'entreprise et de consommateur ont les mêmes dimensions et connecteurs électriques et utilisent les mêmes lecteurs de carte à puce.

Les cartes à puce d'entreprise contiennent des certificats numériques. Ces cartes à puce prennent en charge l'ouverture de session Windows et peuvent également être utilisées avec des applications pour la signature numérique et le cryptage de documents et d'e-mails. XenApp et XenDesktop prennent en charge ces utilisations.

Les cartes à puce de consommateur ne contiennent pas de certificats numériques ; elles contiennent un secret partagé. Ces cartes à puce peuvent prendre en charge les paiements (par carte de crédit avec puce et signature ou avec puce et code PIN). Elles ne prennent pas en charge l'ouverture de session Windows ou les applications Windows standard. Des applications Windows spécialisées et une infrastructure logicielle adaptée (notamment, par exemple, une connexion à un réseau de carte de paiement) sont requises pour utiliser ces cartes à puce. Contactez votre conseiller Citrix pour de plus amples informations sur la prise en charge de ces applications spécialisées sur XenApp ou XenDesktop.

Pour les cartes à puce d'entreprise, il existe des équivalents compatibles qui peuvent être utilisés de manière similaire.

- Un jeton USB équivalent à une carte à puce se connecte directement à un port USB. Ces jetons USB sont généralement de la taille d'un lecteur flash USB, mais peuvent être aussi petits qu'une carte SIM utilisée dans un téléphone mobile. Ils se présentent comme une combinaison d'une carte à puce et d'un lecteur de carte à puce USB.
- Une carte à puce virtuelle utilisant un module de plateforme sécurisée Windows (TPM) s'affiche en tant que carte à puce. Ces cartes à puce virtuelles sont prises en charge pour Windows 8 et Windows 10, à l'aide de Citrix Receiver 4.3 minimum.
  - Les versions de XenApp et XenDesktop antérieures à 7.6 FP3 ne prennent pas en charge les cartes à puce virtuelles.

- Pour de plus amples informations sur les cartes à puce virtuelles, consultez la section Virtual Smart Card Overview.

Remarque : le terme « carte à puce virtuelle » est également utilisé pour décrire un certificat numérique simplement stocké sur l'ordinateur de l'utilisateur. Ces certificats numériques ne sont pas réellement similaires aux cartes à puce.

La prise en charge des cartes à puce de XenApp et XenDesktop repose sur les spécifications standard PC/SC (Personal Computer/Smart Card) de Microsoft. La configuration minimale requise exige que les cartes à puce et les lecteurs de carte à puce soient pris en charge par le système d'exploitation Windows sous-jacent et soient certifiés WHQL (laboratoires Microsoft de contrôle qualité du matériel conçu pour Windows). Consultez la documentation Microsoft pour obtenir des informations supplémentaires sur le matériel PC/SC conformité. D'autres types de machines utilisateur peuvent respecter les normes PS/SC. Pour plus d'informations, reportez-vous au programme Citrix Ready à l'adresse https://www.citrix.com/ready/.

En règle générale, un pilote de périphérique séparé est nécessaire pour la carte à puce ou équivalent de chaque fournisseur. Cependant, si des cartes à puce sont conformes à une norme telle que la norme NIST Personal Identity Verification (PIV), il est possible d'utiliser un seul pilote de périphérique pour une gamme de cartes à puce. Le pilote de périphérique doit être installé sur la machine utilisateur et le Virtual Delivery Agent (VDA). Le pilote de périphérique est souvent fourni dans le cadre du package de middleware de la carte à puce, disponible auprès d'un partenaire Citrix ; le package de middleware de carte à puce propose des fonctionnalités avancées. Le pilote de périphérique peut également être décrit comme fournisseur de service cryptographique (CSP), fournisseur de stockage de clés (KSP) ou minipilote.

Les combinaisons carte à puce et logiciel intermédiaire suivantes ont été testées par Citrix comme exemples représentatifs de leur type. Cependant, d'autres cartes à puce et middleware peuvent également être utilisés. Pour de plus amples informations sur les cartes à puce et middleware compatibles avec Citrix, consultez https://www.citrix.com/ready.

Logiciels intermédiaires	Correspondance des cartes
ActivClient 7.0 (mode DoD activé)	Carte DoD CAC
ActivClient 7.0 en mode PIV	Carte NIST PIV
Mini-pilote Microsoft	Carte NIST PIV
GemAlto Mini Driver pour carte .NET	GemAlto .NET v2+
Pilote natif Microsoft	Cartes à puce virtuelles (TPM)

Pour de plus amples informations sur l'utilisation de cartes à puce avec d'autres types de périphériques, consultez la documentation relative à Citrix Receiver pour ce périphérique.

Pour de plus amples informations sur l'utilisation de cartes à puce avec d'autres types de périphériques, consultez la documentation relative à Citrix Receiver pour ce périphérique.

Remote PC Access

Les cartes à puce sont uniquement prises en charge pour l'accès à distance vers les postes de travail physiques exécutant Windows 10, Windows 8 ou Windows 7 ; les cartes à puce ne sont pas prises en charge par les postes de travail exécutant Windows XP.

Les cartes à puce suivantes ont été testées avec Remote PC Access :

Logiciels intermédiaires	Correspondance des cartes
Minipilote Gemalto .NET	Gemalto .NET v2+
ActivIdentity ActivClient 6.2	NIST PIV
ActivIdentity ActivClient 6.2	CAC
Minipilote Microsoft	NIST PIV
Pilote natif Microsoft	Cartes à puce virtuelles

Types de lecteurs de carte à puce

Un lecteur de carte à puce peut être intégré à la machine utilisateur, ou être connecté séparément à la machine utilisateur (généralement via USB ou Bluetooth). Les lecteurs de carte avec contact qui sont conformes à la spécification USB CCID sont pris en charge. Ils contiennent une fente dans laquelle l'utilisateur insère la carte à puce. La norme Deutsche Kreditwirtschaft (DK) définit quatre catégories de lecteurs de carte de contact.

- Les lecteurs de carte à puce de classe 1 sont les plus courants et sont généralement dotés d'une seule fente. Les lecteurs de carte à puce de classe 1 sont pris en charge, généralement avec un pilote de périphérique CCID standard fourni avec le système d'exploitation.
- Les lecteurs de carte à puce de classe 2 présentent également un pavé numérique sécurisé qui n'est pas accessible par la machine utilisateur. Les lecteurs de carte à puce de classe 2 peuvent être intégrés à un clavier avec un pavé numérique sécurisé. Pour les lecteurs de carte à puce de classe 2, contactez votre conseiller Citrix ; un pilote de périphérique spécifique au lecteur peut être nécessaire pour activer la fonctionnalité de pavé numérique sécurisé.
- Les lecteurs de carte à puce de classe 3 contiennent également un écran sécurisé. Les lecteurs de carte à puce de classe 3 ne sont pas pris en charge.
- Les lecteurs de carte à puce de classe 4 contiennent également un module de transaction sécurisé. Les lecteurs de carte à puce de classe 4 ne sont pas pris en charge.

Remarque : la classe du lecteur de carte à puce n'est pas liée à la classe du périphérique USB.

Les lecteurs de carte à puce doivent être installés avec un pilote de périphérique correspondant sur la machine utilisateur.

Pour plus d'informations sur les lecteurs de carte pris en charge, consultez la documentation correspondant au Citrix Receiver que vous utilisez. Dans la documentation de Citrix Receiver, les versions prises en charge sont généralement répertoriées dans une section sur les cartes à puce où dans la section sur la configuration système requise.

Expérience utilisateur

La prise en charge des cartes à puce est intégrée dans XenApp et XenDesktop, à l'aide d'un canal virtuel de carte à puce ICA/HDX spécifique qui est activé par défaut.

Important : n'utilisez pas la redirection USB générique pour les lecteurs de carte à puce. Cette option est désactivée par défaut pour les lecteurs de carte à puce et n'est pas prise en charge si elle est activée.

Il est possible d'utiliser plusieurs cartes à puce et plusieurs lecteurs sur la même machine utilisateur, mais si l'authentification unique est en service, une seule carte à puce doit être insérée lorsque l'utilisateur démarre une application ou un bureau virtuel. En cas d'utilisation d'une carte à puce dans une application (par exemple pour les fonctions de signature numérique ou de cryptage), des messages supplémentaires invitant à insérer la carte à puce ou à saisir un code PIN peuvent s'afficher. Cela peut se produire si plusieurs cartes à puce sont insérées en même temps.

- Si les utilisateurs sont invités à insérer une carte à puce alors que celle-ci se trouve déjà dans le lecteur, ils doivent sélectionner Annuler.
- Si les utilisateurs sont invités à entrer le code PIN, ils doivent le saisir à nouveau.

Si vous utilisez des applications hébergées s'exécutant sur Windows Server 2008 ou 2008 R2 et avec des cartes à puce exigeant Microsoft Base Smart Card Cryptographic Service Provider, vous constaterez peut-être que tous les autres utilisateurs qui utilisent une carte à puce dans le processus d'ouverture de session sont bloqués. Pour plus de détails et pour obtenir une correction pour ce problème, veuillez consulter l'article https://support.microsoft.com/kb/949538.

Vous pouvez réinitialiser les codes confidentiels à l'aide d'un système de gestion de carte ou d'un outil du fournisseur.

> **Important**
>
> Dans une session XenApp ou XenDesktop, l'utilisation d'une carte à puce avec l'application Connexion Bureau à distance Microsoft n'est pas prise en charge. Ceci est parfois décrit comme un scénario « double-hop ».

Avant de déployer les cartes à puce

- Vous devez vous procurer un pilote de périphérique pour le lecteur de carte à puce et l'installer sur la machine utilisateur. De nombreux lecteurs de carte à puce peuvent utiliser le pilote de périphérique CCID fourni par Microsoft.
- Vous devez vous procurer un pilote de périphérique et un logiciel de fournisseur de services de chiffrement (CSP) depuis votre fournisseur de carte à puce et les installer sur les machines utilisateur et les bureaux virtuels. Le pilote et le logiciel CSP doivent être compatibles avec XenApp et XenDesktop, consultez la documentation du fournisseur de compatibilité. Pour les bureaux virtuels utilisant des cartes à puce qui prennent en charge et utilisent le modèle minipilote, les minipilotes de carte à puce devraient se télécharger automatiquement, mais vous pouvez les obtenir à partir de https://catalog.update.microsoft.com ou auprès votre fournisseur. En outre, si des middlewares PKCS #11 sont requis, obtenez-les auprès de votre fournisseur de carte.
- Important : Citrix recommande d'installer et de tester les pilotes et le logiciel CSP sur un ordinateur physique avant d'installer le logiciel Citrix.
- Ajoutez l'adresse URL de Receiver pour Web à la liste Sites de confiance pour les utilisateurs qui travaillent avec des cartes à puce dans Internet Explorer avec Windows 10. Dans Windows 10, Internet Explorer n'est pas exécuté par défaut en mode protégé pour les sites de confiance.
- Assurez-vous que votre infrastructure de clé publique (PKI) est configurée correctement. Cela assure que le mappage de certificat vers le compte est correctement configuré pour l'environnement Active Directory et que la validation du certificat utilisateur peut être effectuée avec succès.
- Assurez-vous que votre déploiement répond à la configuration système requise des autres composants Citrix utilisé avec des cartes à puce, y compris Citrix Receiver et StoreFront.
- Vérifiez l'accès aux serveurs suivants de votre site :
  - Le contrôleur de domaine Active Directory pour le compte d'utilisateur associé à un certificat d'ouverture de session sur la carte à puce
  - Delivery Controller
  - Citrix StoreFront
  - Citrix NetScaler Gateway/Citrix Access Gateway 10.x
  - VDA
  - (Facultatif pour Remote PC Access) : Microsoft Exchange Server

Activer l'authentification par carte à puce

Étape 1 – Problème de cartes à puce pour les utilisateurs en fonction de votre stratégie d'émission de carte.

Étape 2 – (Facultatif) Définissez des cartes à puce pour activer les utilisateurs pour Remote PC Access.

Étape 3 – Installez et configurez le Delivery Controller et StoreFront (s'ils ne sont pas déjà installés

pour l'utilisation des cartes à puce à distance).

Étape 4 – Activez StoreFront pour l'utilisation des cartes à puce. Pour de plus amples informations, consultez la section Configurer l'authentification par carte à puce dans la documentation de StoreFront.

Étape 5 – Activez NetScaler Gateway/Access Gateway pour utiliser la carte à puce. Pour de plus amples informations, consultez la section Configuration de l'authentification et de l'autorisation et Configuration de l'accès par carte à puce avec l'Interface Web dans la documentation NetScaler.

Étape 6 – Activez VDAs pour l'utilisation des cartes à puce.

- Assurez-vous que le VDA possède les applications et les mises à jour requises.
- Installez les logiciels intermédiaires.
- Définissez l'utilisation d'une carte à puce à distance, l'activation de la communication des données de carte à puce entre Receiver sur une machine utilisateur et une session de bureau virtuel.

Étape 7 – Activez les machines utilisateur (y compris les machines appartenant à un domaine ou non) pour utiliser la carte à puce. Consultez la section Configurer l'authentification par carte à puce dans la documentation de StoreFront pour plus de détails.

- Importez le certificat racine de l'autorité de certification et le certificat émis par l'autorité de certificat dans le magasin de clés de la machine.
- Installez le middleware de carte à puce de votre fournisseur.
- Installez et configurez Citrix Receiver pour Windows, en vous assurant d'importer le fichier icaclient.adm à l'aide de la console de gestion des stratégies de groupe et d'activer l'authentification par carte à puce.

Étape 8 – Testez le déploiement. Assurez-vous que votre déploiement est correctement configuré en démarrant un bureau virtuel avec une carte à puce d'utilisateur test. Testez tous les mécanismes d'accès possibles (par exemple, accès au bureau via Internet Explorer et Citrix Receiver).

Déploiements de carte à puce

November 8, 2018

Les types de déploiements de carte à puce suivants sont pris en charge par cette version du produit et par les environnements mixtes contenant cette version. D'autres configurations peuvent fonctionner mais ne sont pas prises en charge.

Type	Connectivité StoreFront
Ordinateurs appartenant à un domaine local	Directement connectés

Type	Connectivité StoreFront
Accès à distance à partir d'ordinateurs appartenant à un domaine	Connectés au travers de NetScaler Gateway
Ordinateurs n'appartenant pas à un domaine	Directement connectés
Accès à distance depuis des ordinateurs n'appartenant pas à un domaine	Connectés au travers de NetScaler Gateway
Ordinateurs n'appartenant pas à un domaine et clients légers accédant au site Desktop Appliance	Connectés au travers des sites Desktop Appliance
Ordinateurs appartenant à un domaine et clients légers accédant à StoreFront au travers de l'adresse URL XenApp Services	Connectés via les adresses URL XenApp Services

Les types de déploiement sont définis par les caractéristiques de la machine utilisateur sur laquelle le lecteur de carte à puce est connecté :

- Indique si la machine appartient à un domaine ou n'appartient pas à un domaine.
- Comment le périphérique est-il connecté à StoreFront.
- Quel logiciel est utilisé pour afficher les applications et les bureaux virtuels.

En outre, les applications compatibles avec les cartes à puce, telles que Microsoft Word et Microsoft Excel, peuvent être utilisées dans ces déploiements. Ces applications permettent aux utilisateurs de signer numériquement ou de crypter des documents.

Authentification bimodale

Lorsque cela est possible dans chacun de ces déploiements, Receiver prend en charge l'authentification bimodale en offrant à l'utilisateur le choix d'utilisation d'une carte à puce ou de saisie de leur nom d'utilisateur et mot de passe. Ceci est utile si la carte à puce ne peut pas être utilisé (par exemple, si l'utilisateur l'a laissé chez lui, ou que le certificat d'ouverture de session a expiré).

Étant donné que les utilisateurs de machines n'appartenant pas à un domaine ouvrent une session sur Receiver pour Windows directement, vous pouvez autoriser les utilisateurs à revenir à l'authentification explicite. Si vous configurez l'authentification bimodale, les utilisateurs sont initialement invités à ouvrir une session à l'aide de leurs cartes à puce et codes PIN mais ont la possibilité de sélectionner l'authentification explicite s'ils rencontrent des problèmes avec leurs cartes à puce.

Si vous déployez NetScaler Gateway, les utilisateurs ouvrent une session sur leurs machines et sont invités par Receiver pour Windows à s'authentifier auprès de NetScaler Gateway. Cela s'applique

aussi bien aux machines appartenant à un domaine qu'à celles n'appartenant pas à un domaine. Les utilisateurs peuvent ouvrir une session sur NetScaler Gateway à l'aide de leurs cartes à puce et codes PIN, ou avec des informations d'identification explicites. Cela vous permet de fournir aux utilisateurs une authentification bimodale pour l'ouverture de session NetScaler Gateway. Configurez l'authentification pass-through via NetScaler Gateway à StoreFront et déléguez la validation des informations d'identification à NetScaler Gateway pour les utilisateurs de cartes à puce de façon à ce que les utilisateurs soient authentifiés auprès de StoreFront de manière silencieuse.

Considérations relatives à la forêt Active Directory

Dans un environnement Citrix, les cartes à puce sont prises en charge dans une forêt unique. Les ouvertures de session par carte à puce entre les forêts nécessitent une approbation de forêt bidirectionnelle pour tous les comptes d'utilisateur. Les déploiements plus complexes de forêts multiples impliquant des cartes à puce (c'est-à-dire, où les approbations sont uniquement à sens unique ou de types différents) ne sont pas pris en charge.

Vous pouvez utiliser des cartes à puce dans un environnement Citrix qui comprend des bureaux distants. Cette fonctionnalité peut être installée localement (sur la machine utilisateur à laquelle la carte à puce est connectée) ou à distance (sur le bureau distant à laquelle la machine utilisateur se connecte).

Stratégie de retrait de carte à puce

La stratégie définie pour le retrait de la carte à puce sur le produit détermine ce qui se passe lorsque vous retirez la carte à puce du lecteur au cours d'une session. Cette stratégie est configurée et gérée par le système d'exploitation Windows.

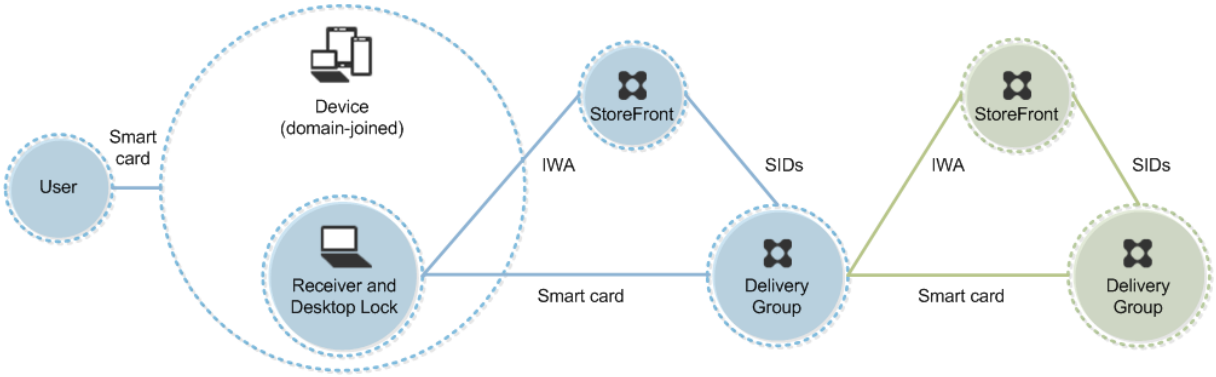
Paramètre de stratégie	Comportement du Bureau
Aucune action	Aucune action.
Verrouiller la station de travail	La session de bureau est déconnectée et le bureau virtuel est verrouillé.
Forcer la fermeture de session	L'utilisateur est obligé de fermer la session. Si la connexion réseau est interrompue et que ce paramètre est activé, la session peut être fermée et l'utilisateur peut perdre des données.
Déconnecter en cas de session Terminal Server	La session est déconnectée et le bureau virtuel est verrouillé.

Vérification de la révocation des certificats

Si la vérification de la révocation des certificats est activée et qu'un utilisateur insère une carte à puce avec un certificat non valide dans un lecteur de carte, l'utilisateur ne peut pas authentifier ou accéder au bureau ou à l'application associée à ce certificat. Par exemple, si le certificat non valide est utilisé pour le déchiffrement de messagerie, l'e-mail reste crypté. Si d'autres certificats sur la carte, tels que ceux utilisées pour l'authentification, sont toujours valides, ces fonctions restent actives.

Exemple de déploiement : ordinateurs appartenant à un domaine

Ce déploiement implique des machines utilisateur appartenant à un domaine qui exécutent Desktop Viewer et se connectent directement à StoreFront.

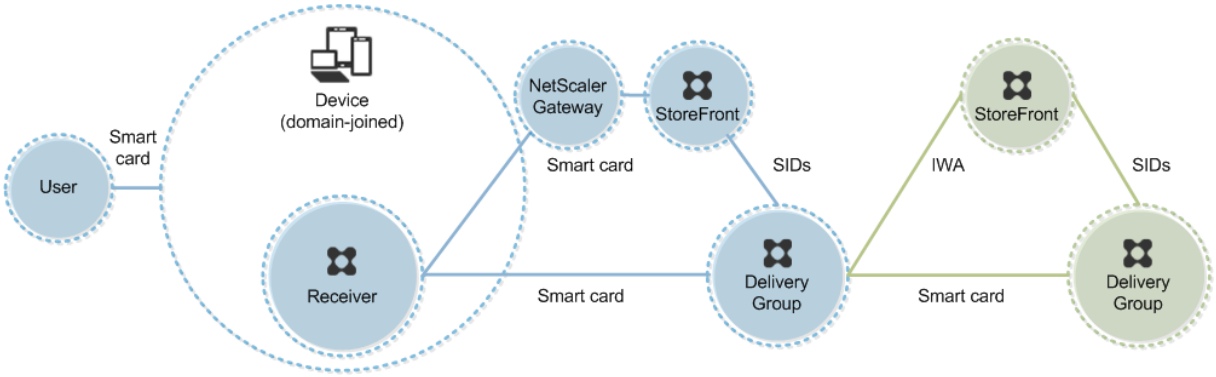


Un utilisateur ouvre une session sur une machine à l'aide d'une carte à puce et du code confidentiel. Receiver authentifie l'utilisateur à un serveur StoreFront à l'aide de l'authentification Windows intégrée (IWA). StoreFront transmet les identificateurs de sécurité (SID) de l'utilisateur à XenApp ou XenDesktop. Lorsque l'utilisateur démarre un bureau virtuel ou une application, l'utilisateur n'est pas invité à entrer un code confidentiel, car la fonctionnalité d'authentification unique est configurée sur Receiver.

Ce déploiement peut être étendu à une DMZ double avec l'ajout d'un deuxième serveur StoreFront et un serveur hébergeant des applications. Un Receiver depuis le bureau virtuel s'authentifie sur le deuxième serveur StoreFront. Toute méthode d'authentification peut être utilisée pour cette seconde connexion. La configuration indiquée pour le premier hop peut être réutilisée dans le deuxième hop ou utilisée dans le deuxième hop uniquement.

Exemple de déploiement : accès à distance à partir d'ordinateurs appartenant à un domaine

Ce déploiement implique des machines utilisateur appartenant à un domaine qui exécutent Desktop Viewer et se connectent à StoreFront via NetScaler Gateway/Access Gateway.



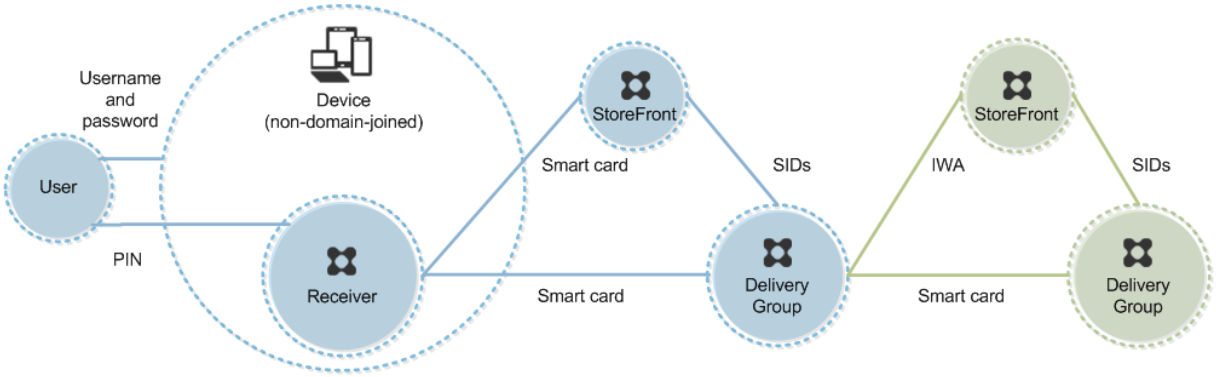
Un utilisateur ouvre une session sur une machine à l'aide d'une carte à puce et d'un code confidentiel, puis ouvre une session sur NetScaler Gateway/Access Gateway. Cette seconde ouverture de session peut être effectuée avec la carte à puce et un code confidentiel ou un nom d'utilisateur et un mot de passe car Receiver permet l'authentification bimodale dans ce déploiement.

L'utilisateur ouvre automatiquement une session sur StoreFront, qui transmet les identificateurs de sécurité (SID) de l'utilisateur à XenApp ou XenDesktop. Lorsque l'utilisateur démarre un bureau ou une application virtuel(le), l'utilisateur n'est pas invité à entrer à nouveau un code confidentiel, car la fonctionnalité d'authentification unique est configurée sur Receiver.

Ce déploiement peut être étendu à une DMZ double avec l'ajout d'un deuxième serveur StoreFront et un serveur hébergeant des applications. Un Receiver depuis le bureau virtuel s'authentifie sur le deuxième serveur StoreFront. Toute méthode d'authentification peut être utilisée pour cette seconde connexion. La configuration indiquée pour le premier hop peut être réutilisée dans le deuxième hop ou utilisée dans le deuxième hop uniquement.

Exemple de déploiement : ordinateurs n'appartenant pas à un domaine

Ce déploiement implique des machines utilisateur n'appartenant pas au domaine qui exécutent Desktop Viewer et se connectent directement à StoreFront.



Un utilisateur ouvre une session sur une machine. En général, l'utilisateur entre un nom d'utilisateur et un mot de passe, mais puisque la machine n'appartient pas à un domaine, les informations

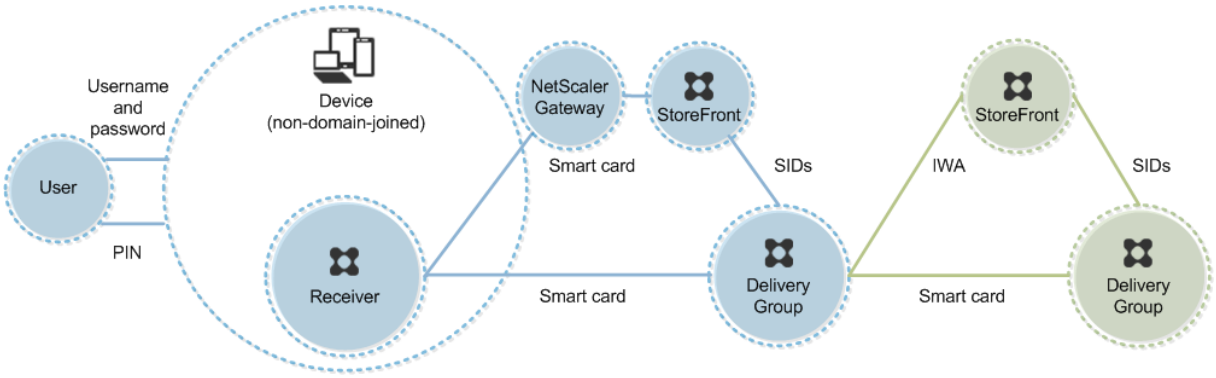
d'identification de cette ouverture de session sont facultatives. Comme l'authentification bimodale est possible dans ce déploiement, Receiver invite l'utilisateur à entrer une carte à puce et un code confidentiel ou un nom d'utilisateur et un mot de passe. Receiver s'authentifie ensuite auprès de StoreFront.

StoreFront transmet les identificateurs de sécurité (SID) de l'utilisateur à XenApp ou XenDesktop. Lorsque l'utilisateur démarre un bureau virtuel ou une application, l'utilisateur est invité à entrer un code confidentiel, car la fonctionnalité d'authentification unique n'est pas disponible dans ce déploiement.

Ce déploiement peut être étendu à une DMZ double avec l'ajout d'un deuxième serveur StoreFront et un serveur hébergeant des applications. Un Receiver depuis le bureau virtuel s'authentifie sur le deuxième serveur StoreFront. Toute méthode d'authentification peut être utilisée pour cette seconde connexion. La configuration indiquée pour le premier hop peut être réutilisée dans le deuxième hop ou utilisée dans le deuxième hop uniquement.

Exemple de déploiement : accès à distance à partir d'ordinateurs n'appartenant pas à un domaine

Ce déploiement implique des machines utilisateur n'appartenant pas au domaine qui exécutent Desktop Viewer et se connectent directement à StoreFront.



Un utilisateur ouvre une session sur une machine. En général, l'utilisateur entre un nom d'utilisateur et un mot de passe, mais puisque la machine n'appartient pas à un domaine, les informations d'identification de cette ouverture de session sont facultatives. Comme l'authentification bimodale est possible dans ce déploiement, Receiver invite l'utilisateur à entrer une carte à puce et un code confidentiel ou un nom d'utilisateur et un mot de passe. Receiver s'authentifie ensuite auprès de StoreFront.

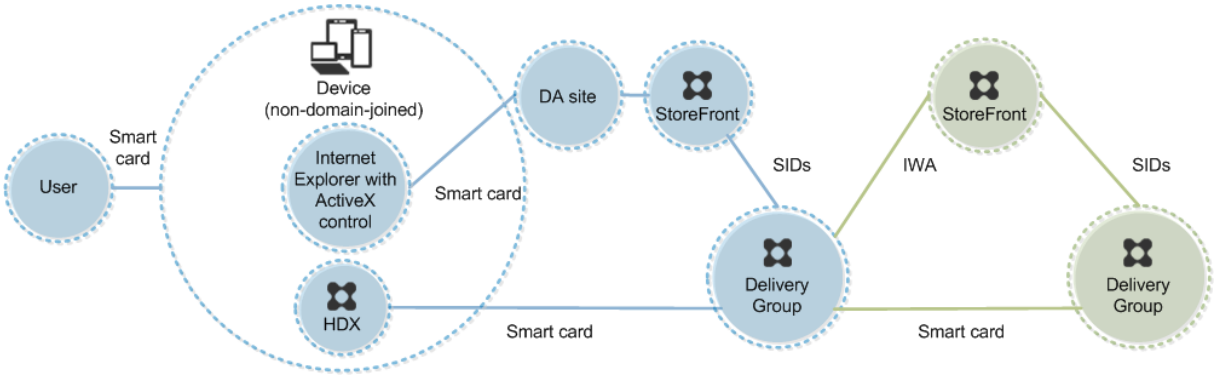
StoreFront transmet les identificateurs de sécurité (SID) de l'utilisateur à XenApp ou XenDesktop. Lorsque l'utilisateur démarre un bureau virtuel ou une application, l'utilisateur est invité à entrer un code confidentiel, car la fonctionnalité d'authentification unique n'est pas disponible dans ce déploiement.

Ce déploiement peut être étendu à une DMZ double avec l'ajout d'un deuxième serveur StoreFront et un serveur hébergeant des applications. Un Receiver depuis le bureau virtuel s'authentifie sur le deuxième serveur StoreFront. Toute méthode d'authentification peut être utilisée pour cette seconde connexion. La configuration indiquée pour le premier hop peut être réutilisée dans le deuxième hop ou utilisée dans le deuxième hop uniquement.

Exemple de déploiement : ordinateurs n'appartenant pas à un domaine et clients légers accédant au site Desktop Appliance

Ce déploiement implique des machines utilisateur n'appartenant pas au domaine pouvant exécuter Desktop Lock et se connecter à StoreFront via des sites Desktop Appliance.

Desktop Lock est un composant distinct fourni avec XenApp, XenDesktop et VDI-in-a-Box. Il constitue une alternative à Desktop Viewer et il est conçu principalement pour les ordinateurs Windows réaffectés et les clients légers Windows. Desktop Lock remplace le shell Windows et le Gestionnaire des tâches dans ces machines utilisateur, ce qui empêche les utilisateurs d'accéder à des machines sous-jacentes. Grâce à Desktop Lock, les utilisateurs peuvent accéder aux bureaux Windows Server Machine et aux bureaux Windows Desktop Machine. l'installation de Desktop Lock est facultative.



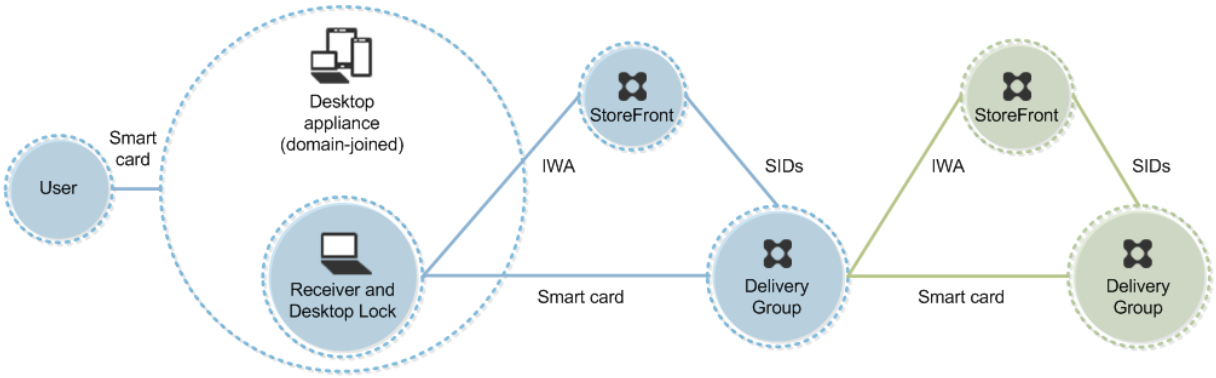
Un utilisateur ouvre une session sur une machine avec une carte à puce. Si Desktop Lock est en cours d'exécution sur la machine, celle-ci est configurée pour démarrer un site Desktop Appliance au travers d'Internet Explorer exécuté en mode Kiosque. Un contrôle ActiveX présent sur le site invite l'utilisateur à entrer un code confidentiel, et l'envoie à StoreFront. StoreFront transmet les identificateurs de sécurité (SID) de l'utilisateur à XenApp ou XenDesktop. Le premier bureau disponible de la liste alphabétique d'un groupe de bureaux attribué démarre.

Ce déploiement peut être étendu à une DMZ double avec l'ajout d'un deuxième serveur StoreFront et un serveur hébergeant des applications. Un Receiver depuis le bureau virtuel s'authentifie sur le deuxième serveur StoreFront. Toute méthode d'authentification peut être utilisée pour cette seconde connexion. La configuration indiquée pour le premier hop peut être réutilisée dans le deuxième hop ou utilisée dans le deuxième hop uniquement.

Exemple de déploiement : ordinateurs appartenant à un domaine et clients légers accédant à StoreFront via l'adresse URL XenApp Services

Ce déploiement implique des machines utilisateur appartenant à un domaine qui exécutent Desktop Lock et se connectent à StoreFront via les adresses URL XenApp Services.

Desktop Lock est un composant distinct fourni avec XenApp, XenDesktop et VDI-in-a-Box. Il constitue une alternative à Desktop Viewer et il est conçu principalement pour les ordinateurs Windows réaffectés et les clients légers Windows. Desktop Lock remplace le shell Windows et le Gestionnaire des tâches dans ces machines utilisateur, ce qui empêche les utilisateurs d'accéder à des machines sous-jacentes. Grâce à Desktop Lock, les utilisateurs peuvent accéder aux bureaux Windows Server Machine et aux bureaux Windows Desktop Machine. l'installation de Desktop Lock est facultative.



Un utilisateur ouvre une session sur une machine à l'aide d'une carte à puce et du code confidentiel. Si Desktop Lock est en cours d'exécution sur la machine, il authentifie l'utilisateur à un serveur StoreFront à l'aide de l'authentification Windows intégrée (IWA). StoreFront transmet les identificateurs de sécurité (SID) de l'utilisateur à XenApp ou XenDesktop. Lorsque l'utilisateur démarre un bureau virtuel, l'utilisateur n'est pas invité à entrer un code confidentiel, car la fonctionnalité d'authentification unique est configurée sur Receiver.

Ce déploiement peut être étendu à une DMZ double avec l'ajout d'un deuxième serveur StoreFront et un serveur hébergeant des applications. Un Receiver depuis le bureau virtuel s'authentifie sur le deuxième serveur StoreFront. Toute méthode d'authentification peut être utilisée pour cette seconde connexion. La configuration indiquée pour le premier hop peut être réutilisée dans le deuxième hop ou utilisée dans le deuxième hop uniquement.

Authentification unique et single sign-on avec des cartes à puce

February 28, 2019

Authentification pass-through

L'authentification pass-through avec des cartes à puce sur les bureaux virtuels est prise en charge sur les machines utilisateur exécutant Windows 10, Windows 8 et Windows 7 SP1, éditions Enterprise et Professional.

L'authentification pass-through avec des cartes à puce sur les applications hébergées est prise en charge sur les serveurs exécutant Windows Server 2016, Windows Server 2012 R2, Windows Server 2012 et Windows Server 2008 R2 SP1

Pour utiliser l'authentification unique avec des applications hébergées sur des cartes à puce, vous devez activer l'utilisation de Kerberos lorsque vous configurez Authentification unique avec carte à puce comme méthode d'authentification pour le site.

Remarque : la disponibilité de l'authentification pass-through avec des cartes à puce dépend de nombreux facteurs, notamment, mais pas exclusivement :

- les stratégies de sécurité de votre organisation concernant l'authentification pass-through.
- Type et configuration de logiciels intermédiaires.
- Types de lecteur de carte à puce.
- Stratégie de mise en cache du code confidentiel de logiciels intermédiaires.

L'authentification pass-through avec des cartes à puce est configurée sur Citrix StoreFront. Consultez la documentation StoreFront pour plus de détails.

Single Sign-On

Citrix Single Sign-On est une fonctionnalité qui implémente l'authentification unique lors du lancement de bureaux virtuels et d'applications. Vous pouvez utiliser cette fonctionnalité dans des déploiements de carte à puce, appartenant à un domaine, direct-to-StoreFront et appartenant à un domaine, NetScaler-to-StoreFront pour réduire le nombre de fois où les utilisateurs entrent leur code confidentiel. Pour utiliser l'authentification unique dans ces types de déploiement, modifiez les paramètres suivants dans le fichier default.ica, qui se trouve sur le serveur StoreFront :

- Déploiements de carte à puce appartenant à un domaine, directement vers StoreFront : définissez DisableCtrlAltDel sur Off
- Déploiements de carte à puce appartenant à un domaine, NetScaler vers StoreFront : définissez UseLocalUserAndPassword sur On

Pour obtenir des instructions sur la configuration de ces paramètres, consultez la documentation de StoreFront ou NetScaler Gateway.

La disponibilité de la fonctionnalité d'authentification unique dépend de nombreux facteurs, notamment, mais pas exclusivement :

- Les stratégies de sécurité de votre organisation relatives à l'authentification unique.
- Type et configuration de logiciels intermédiaires.
- Types de lecteur de carte à puce.
- Stratégie de mise en cache du code confidentiel de logiciels intermédiaires.

Remarque : lorsque l'utilisateur ouvre une session sur Virtual Delivery Agent (VDA) sur une machine lorsqu'un lecteur de carte à puce est connecté, une mosaïque Windows peut sembler représenter le mode d'authentification précédent réussi, tel qu'une carte à puce ou un mot de passe. Par conséquent, lorsque l'authentification unique est activée, la mosaïque d'authentification unique peut s'afficher. Pour ouvrir une
session, l'utilisateur doit sélectionner Changer d'utilisateurs pour sélectionner une autre mosaïque car la mosaïque d'authentification unique ne fonctionne pas.

Transport Layer Security (TLS)

January 23, 2019

La configuration d'un site XenApp ou XenDesktop pour utiliser le protocole TLS (Transport Layer Security) de sécurité inclut les procédures suivantes :

- Obtenez, installez et enregistrez un certificat de serveur sur tous les Delivery Controller, et configurer un port avec le certificat TLS. Pour de plus amples informations, consultez la rubrique Installer les certificats de serveur TLS sur des Controller.

  Si vous le souhaitez, vous pouvez modifier les ports que le Controller utilise pour écouter le trafic HTTP et HTTPS.

- Activez les connexions TLS entre les utilisateurs et Virtual Delivery Agents (VDA) en renseignant les tâches suivantes :

  - Configurez TLS sur les machines où le VDA est installé. (Par commodité, les références supplémentaires sur les machines sur lesquelles les VDA sont installés sont simplement appelées « VDA ») Vous pouvez utiliser un script PowerShell fourni par Citrix, ou le configurer manuellement. Pour de plus amples informations, consultez la section À propos des paramètres TLS sur les VDA. Pour de plus amples informations, consultez la section Configurer TLS sur un VDA à l'aide du script PowerShell et Configurer manuellement TLS sur un VDA.
  - Configurez TSL dans les groupes de mise à disposition contenant les VDA en exécutant un jeu de cmdlets PowerShell dans Studio. Pour de plus amples informations, consultez la section Configurer TLS sur les groupes de mise à disposition.

  Configuration requise et considérations :

- L'activation des connexions TLS entre les utilisateurs et les VDA est valide uniquement pour les sites XenApp 7.6 et XenDesktop 7.6, ainsi que les versions ultérieures prises en charge.
- Configurez TLS dans les groupes de mise à disposition et le VDA après l'installation de composants, créez un site, créez des catalogues de machines, et créez des groupes de mise à disposition.
- Pour configurer TLS dans les groupes de mise à disposition, vous devez disposer de l'autorisation de modification des règles d'accès de Controller ; un administrateur complet possède ces permissions.
- Pour configurer TLS sur les VDA, vous devez être un administrateur Windows sur la machine sur laquelle le VDA est installé.
- Si vous prévoyez de configurer TLS sur les VDA qui ont été mis à niveau à partir de versions antérieures, désinstallez tous les relais SSL sur ces machines avant de les mettre à niveau.
- Le script PowerShell permet de configurer TLS sur les VDA statiques ; il ne configure pas TLS sur les VDA regroupés qui sont provisionnés par Machine Creation Services ou Provisioning Services, où l'image de la machine cliente est réinitialisée à chaque redémarrage.

> **Avertissement**
>
> Pour les tâches qui incluent l'utilisation du Registre Windows, la modification du Registre peut entraîner de sérieux problèmes qui pourraient nécessiter la réinstallation de votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Pour plus d'informations sur l'activation de TLS pour la base de données du site, consultez la section CTX137556.

> **Remarque :**
>
> Si TLS et UDT sont tous les deux activés sur le VDA :
>
> - Pour un accès direct au VDA, Citrix Receiver utilise toujours TLS sur TCP (et non UDP et UDT).
> - Pour un accès indirect au VDA à l'aide de NetScaler Gateway, Citrix Receiver utilise DTLS sur UDP pour les communications avec NetScaler Gateway. Les communications entre NetScaler Gateway et le VDA utilisent UDP sans DTLS. UDT est utilisé.

Installer les certificats de serveur TLS sur des Controller

Pour HTTPS, Le service XML prend en charge les fonctionnalités TLS par le biais de certificats de serveur mais pas de certificats de client. Pour obtenir, installer et enregistrer un certificat sur un Controller, et pour configurer un port avec le certificat TLS :

Si IIS est installé sur le Controller, suivez les instructions dans https://technet.microsoft.com/en-us/library/cc771438%28v=ws.10%29.aspx.

Si IIS n'est pas installé sur le Controller, le certificat pourrait être configuré comme suit :

1. Procurez-vous un certificat de serveur TLS et installez-le sur le Controller en suivant les instructions de https://blogs.technet.com/b/pki/archive/2009/08/05/how-to-create-a-web-server-ssl-certificate-manually.aspx. Pour de plus amples informations sur l'outil certreq, consultez https://technet.microsoft.com/en-us/library/cc736326(WS.10).aspx.

   Si vous prévoyez d'utiliser le script PowerShell pour configurer TLS sur VDA, et sauf si vous prévoyez de spécifier l'empreinte numérique du certificat TLS, vérifiez que le certificat est présent dans la zone Ordinateur local > Personnel > Certificats du magasin de certificats. Si plusieurs certificats résident à cet emplacement, le premier détecté sera utilisé.

2. Configurez un port avec le certificat ; consultez https://msdn.microsoft.com/en-us/library/ms733791%28v=vs.110%29.aspx.

Si le Controller est installé sur Windows Server 2016 et que StoreFront est installé sur Windows Server 2012, une modification de la configuration est nécessaire au niveau du Controller, pour modifier l'ordre des suites de chiffrement TLS.

> **Remarque :**
>
> Cette modification de la configuration n'est pas nécessaire pour le Controller et StoreFront avec d'autres combinaisons de versions de Windows Server.

La liste des suites de chiffrement doit contenir les suites de chiffrement TLS_ECDHE_RSA_WITH_AES_256*CBC_SHA3*
ou TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (ou les deux), et ces suites de chiffrement doivent précéder toute suite de chiffrement TLS_DHE.

> **Remarque :**
>
> Windows Server 2012 ne prend pas en charge les suites de chiffrement TLS_ECDHE_RSA_WITH_AES_256_GCM_S
> ou TLS_ECDHE_RSA_WITH_AES_128_GCM _SHA256.

1. Dans l'éditeur de stratégie de groupe Microsoft, accédez à Configuration ordinateur > Modèles d'administration > Réseau > Paramètres de configuration SSL.
2. Modifiez la stratégie « Ordre des suites de chiffrement SSL ». Par défaut, cette stratégie est définie sur « Non configuré ». Définissez cette stratégie sur Activé.
3. Organisez les suites dans l'ordre approprié ; supprimez les suites de chiffrement que vous ne souhaitez pas utiliser.

Assurez-vous que TLS_ECDHE_RSA_WITH_AES_256*CBC_SHA384 ou TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256*
précède toute suite de chiffrement TLS_DHE.

Sur Microsoft MSDN, consultez également Priorité des suites de chiffrement Schannel.

Modifier les ports HTTP ou HTTPS

Par défaut, le service XML du Controller écoute le trafic HTTP sur le port 80 et le trafic HTTPS sur le port 443. Bien que vous puissiez utiliser des ports différents de ceux par défaut, n'oubliez pas les risques de sécurité relatifs à l'exposition d'un Controller à des réseaux non approuvés. Le déploiement d'un serveur StoreFront autonome est préférable à la modification des valeurs par défaut.

Pour modifier la valeur par défaut des ports HTTP ou HTTPS utilisés par le Controller, exécutez la commande suivante à partir de Studio :

BrokerService.exe -WIPORT <*http-port*> -WISSLPORT <*https-port*>

où <*http-port*> est le numéro de port pour le trafic HTTP et <*https-port*> le numéro de port pour le trafic HTTPS.

> **Remarque :**
>
> Après avoir modifié un port, il se peut que Studio affiche un message sur la compatibilité et la mise à niveau des licences. Pour résoudre le problème, ré-enregistrez les instances de service à l'aide de la séquence de l'applet de commande PowerShell suivante :
>
> Get-ConfigRegisteredServiceInstance -ServiceType Broker -Binding XML_HTTPS |
>
> Unregister-ConfigRegisteredServiceInstance
>
> Get-BrokerServiceInstance | where Binding -eq "XML_HTTPS" |
> Register-ConfigServiceInstance

Appliquer le trafic HTTPS uniquement

Si vous souhaitez que le service XML ignore le trafic HTTP, créez le paramètre de registre suivant sur le Controller dans HKLM\Software\Citrix\DesktopServer\ et redémarrez le service Broker.

Pour ignorer le trafic HTTP, créez un DWORD XmlServicesEnableNonSsl et définissez-le sur 0.

Il existe une valeur de registre DWORD correspondante que vous pouvez créer pour ignorer le trafic HTTPS : DWORD XmlServicesEnableSsl. Assurez-vous qu'elle n'est pas définie sur 0.

Paramètres TLS sur les VDA

Un groupe de mise à disposition ne peut pas avoir un mélange d'un VDA avec TLS configuré et d'autres VDA sans TLS configuré. Lorsque vous configurez le protocole TLS pour un groupe de mise à disposition, vous devez avoir déjà configuré TLS pour tous les VDA dans ce groupe de mise à disposition.

Lorsque vous configurez le protocole TLS sur les VDA, les autorisations sur le certificat TLS installé sont modifiées, offrant au service ICA un accès en lecture à la clé privée du certificat, et informant le service ICA des opérations suivantes :

- **Quel certificat utiliser dans le magasin de certificat à utiliser pour TLS**.
- **Quel numéro de port TCP utiliser pour les connexions TLS**.

Le Pare-feu Windows (s'il est activé) doit être configuré pour autoriser les connexions entrantes sur ce port TCP. Cette configuration est effectuée pour vous si vous utilisez le script PowerShell.

- **Quelles sont les versions du protocole TLS à autoriser.**

> **Important**
>
> Citrix vous recommande de vérifier leur utilisation de SSLv3 et de reconfigurer ces déploiements pour supprimer la prise en charge de SSLv3, le cas échéant. Consultez l'article CTX200238.

Les versions prises en charge du protocole TLS suivent une hiérarchie (de la plus basse à la plus élevée) : SSL 3.0, TLS 1.0, TLS 1.1 et TLS 1.2. Vous devez spécifier la version minimale autorisée ; toutes les connexions de protocole utilisant cette version ou une version supérieure sont autorisées.

Par exemple, si vous spécifiez TLS 1.1 comme version minimale, les connexions de protocole TLS 1.1 et TLS 1.2 sont autorisées. Si vous spécifiez SSL 3.0 en tant que version minimale, les connexions pour toutes les versions prises en charge sont alors autorisées. Si vous spécifiez TLS 1.2 comme version minimale, seules les connexions TLS 1.2 sont autorisées.

- **Quelles suites de chiffrement TLS sont autorisées.**

Une suite de chiffrement sélectionne le cryptage qui sera utilisé pour une connexion. Les clients et les VDA peuvent prendre en charge plusieurs ensembles de suites de chiffrement. Lorsqu'un client (Citrix Receiver ou StoreFront) se connecte et envoie une liste des suites de chiffrement TLS pris en charge, le VDA fait correspondre une des suites de chiffrement du client avec l'une de suites de chiffrement de sa liste configurée et accepte la connexion. S'il n'existe aucune correspondance de suite de chiffrement, le VDA rejette la connexion.

Trois ensembles de suites de chiffrement (également appelés modes de conformité) sont pris en charge par le VDA : GOV (gouvernement), COM (commercial) et ALL (tout). Les suites de chiffrement acceptables dépendent du mode FIPS Windows ; voir `https://support.microsoft.com/kb/811833` pour plus d'informations sur le mode FIPS Windows. Le tableau suivant répertorie les suites de chiffrement compris dans chaque ensemble :

Suite de chiffrement TLS	GOV	COM	ALL	GOV	COM	ALL
Mode FIPS	Désactivé	Désactivé	Désactivé	Activé	Activé	Activé
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	x		x	x		x
TLS_ECDHE_[illegible]	x		x	x		x
TLS_RSA_WITH_AES_256_GCM_SHA384	x		x	x		x

Suite de chiffrement TLS	GOV	COM	ALL	GOV	COM	ALL
TLS_RSA_WIT	x	x	x	x	x	x
TLS_RSA_WITH	x	_AES_256_CBC_SHA256	x	x		x
TLS_RSA_WIT	x		x	x		x
TLS_RSA_WITH_AES_128_CBC		_SHA	x		x	x
TLS_RSA_WIT		x	x			
TLS_RSA_WITH_RC4_128_MD		5	x			
TLS_RSA_WIT	x		x	x		x

> **Important**
>
> Une étape supplémentaire est nécessaire lorsque le VDA se trouve sur un serveur Windows Server 2012 R2, Windows Server 2016 ou Windows 10 Anniversary Edition ou une version ultérieure prise en charge. Cela affecte les connexions à partir de Citrix Receiver pour Windows (version 4.6 à 4.9), Citrix Receiver pour HTML5 et Citrix Receiver pour Chrome. Cela inclut également les connexions via NetScaler Gateway.
>
> Cette étape est également requise pour toutes les connexions utilisant NetScaler Gateway, pour toutes les versions de VDA, si TLS est configuré entre NetScaler Gateway et le VDA. Cela affecte toutes les versions de Citrix Receiver.

Sur le VDA (Windows Server 2016 ou Windows 10 Anniversary Edition ou version ultérieure), à l'aide de l'éditeur de stratégie de groupe, accédez à Configuration ordinateur > Modèles d'administration > Réseau > Paramètres de configuration SSL > Ordre des suites de chiffrement SSL. Sélectionnez l'ordre suivant :

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA

> **Remarque :**
>
> Les quatre premiers éléments spécifient également la courbe elliptique, P384 ou P256. Assurez-vous que l'option « curve25519 » n'est pas sélectionnée. Le mode FIPS n'empêche pas l'utilisation de l'option « curve25519 ».

Lorsque ce paramètre de stratégie de groupe est configuré, le VDA sélectionnera une suite de chiffrement uniquement si elle apparaît dans les deux listes : la liste Stratégies de groupe et la liste pour le mode de conformité sélectionné (COM, GOV ou ALL). La suite de chiffrement doit également s'afficher dans la liste envoyée par le client (Citrix Receiver ou StoreFront).

Cette configuration de stratégie de groupe affecte également d'autres applications et services TLS sur le VDA. Si vos applications requièrent des suites de chiffrement spécifiques, vous devez les ajouter à la liste Stratégie de groupe.

> **Important**
>
> Même si les modifications de stratégie de groupe sont affichées lorsqu'elles sont appliquées, les modifications de stratégie de groupe pour la configuration TLS ne prennent effet qu'après le redémarrage du système d'exploitation. Par conséquent, pour les bureaux regroupés, appliquez les modifications de stratégie de groupe pour la configuration TLS à l'image de base.

Configurer TLS sur un VDA à l'aide du script PowerShell

Le script Enable-VdaSSL.ps1 active ou désactive l'écouteur TLS sur un VDA. Ce script est disponible dans le dossier Support > Tools > SslSupport sur le support d'installation.

Lorsque vous activez le protocole TLS, le script désactive toutes les règles du Pare-feu Windows existantes pour le port TCP spécifié avant d'ajouter une règle qui permet au service ICA d'accepter des connexions entrantes sur le port TCP TLS uniquement. Cela désactive également les règles du Pare-feu Windows pour :

- Citrix ICA 1494 (valeur par défaut : 8008)
- Citrix CGP 2598 (valeur par défaut : 8008)
- Citrix WebSocket 8008 (valeur par défaut : 8008)

Les utilisateurs peuvent uniquement se connecter en utilisant TLS ; ils ne peuvent pas utiliser ICA/HDX, ICA/HDX avec fiabilité de session ou HDX sur WebSocket, sans TLS.

Voir Ports réseau.

Le script contient des descriptions de la syntaxe suivante, ainsi que d'autres exemples ; vous pouvez utiliser un outil tel que le Bloc-notes++ pour consulter ces informations.

> **Important**
>
> Spécifiez soit le paramètre Enable ou Disable de même que le paramètre CertificateThumbPrint. Les autres paramètres sont facultatifs.

Syntaxe

```
Enable-VdaSSL {
 -Enable | -Disable }
  -CertificateThumbPrint "<thumbprint>"
[ - SSLPort <port>] [-SSLMinVersion "<min-ssl-version>"] [-
    SSLCipherSuite"<suite>"]
```

Paramètre	Description
Activer	Installe et active l'écouteur TLS sur le VDA. Soit ce paramètre ou le paramètre Disable est requis.
Désactiver	Désactive l'écouteur TLS sur le VDA. Soit ce paramètre ou le paramètre Enable est requis. Si vous spécifiez ce paramètre, aucun autre paramètre n'est valide.
CertificateThumbPrint "<empreinte>"	Empreinte numérique du certificat TLS dans le magasin de certificats, entourée de guillemets. Le script utilise l'empreinte numérique spécifiée pour sélectionner le certificat que vous voulez utiliser. Si ce paramètre est omis, un certificat incorrect est sélectionné.
SSLPort <port>	Port TLS. Valeur par défaut : 443
SSLMinVersion "<version>"	Version minimale du protocole TLS, entourés de guillemets. Valeurs valides : "SSL_3.0", "TLS_1.0" (défaut), "TLS_1.1" et "TLS_1.2". **Important :** Citrix recommande aux clients de vérifier leur utilisation de SSLv3 et de prendre des mesures pour reconfigurer leurs déploiements pour supprimer la prise en charge de SSLv3, le cas échéant. Consultez l'article CTX200238.

Paramètre	Description
SSLCipherSuite “<suite>”	Suite de chiffrement TLS, entourés de guillemets. Valeurs valides : « GOV », « COM » et « ALL » (par défaut)

Exemples

Le script suivant installe et active la version de protocole TLS 1.2. L’empreinte numérique (représentée en tant que « 12345678987654321 » dans cet exemple) est utilisée pour sélectionner le certificat à utiliser.

Enable-VdaSSL –Enable -CertificateThumbPrint “12345678987654321”

Le script suivant installe et active l’écouteur TLS et spécifie le port TLS 400, la suite de chiffrement GOV et une valeur de protocole minimale de TLS 1.2. L’empreinte numérique (représentée en tant que « 12345678987654321 » dans cet exemple) est utilisée pour sélectionner le certificat à utiliser.

Enable-VdaSSL – Enable
-CertificateThumbPrint “12345678987654321”
–SSLPort 400 ‘SSLMinVersion “TLS_1.2”
–SSLCipherSuite “GOV”

Le script suivant désactive l’écouteur TLS sur le VDA.

Enable-VdaSSL –Disable

Configurer manuellement TLS sur un VDA

Lors de la configuration manuelle de TLS sur un VDA, vous offrez un accès en lecture générique à la clé privée du certificat TLS pour le service approprié sur chaque VDA : NT SERVICE\PorticaService pour un VDA pour OS Windows Desktop, ou NT SERVICE\TermService pour un VDA pour OS Windows Server. Sur la machine sur laquelle le VDA est installé :

ÉTAPE 1. Lancez la console MMC (Microsoft Management Console) : Démarrer > Exécuter > mmc.exe.

ÉTAPE 2. Ajouter le composant logiciel enfichable Certificats à la console MMC :

1. Sélectionnez Fichier > Ajouter/Supprimer un composant logiciel enfichable.
2. Sélectionnez Certificats et cliquez sur Ajouter.
3. Lorsque vous y êtes invité par « Ce composant logiciel enfichable gérera toujours les certificats pour : », choisissez « Le compte d’ordinateur », puis cliquez sur Suivant.
4. Lorsque vous y êtes invité par « Sélectionnez l’ordinateur à gérer par ce composant logiciel enfichable », choisissez « Ordinateur local », puis cliquez sur Terminer.

ÉTAPE 3. Sous Certificats (Ordinateur local) > Personnel > Certificats, cliquez avec le bouton droit de la souris sur le certificat, puis sélectionnez Toutes les tâches > Gérer les clés privées.

ÉTAPE 4. L'Éditeur de liste de contrôle d'accès affiche « Autorisations pour les clés privées (NomConvivial) » où (NomConvivial) est le nom de votre certificat TLS. Ajoutez l'un des services suivants et accordez-lui un accès en lecture :

- Pour un VDA pour OS Windows Desktop, « PORTICASERVICE »
- Pour un VDA pour OS de serveur Windows, « TERMSERVICE »

ÉTAPE 5. Cliquez deux fois sur le certificat TLS installé. Dans la boîte de dialogue du certificat, sélectionnez l'onglet Détails, puis faites défiler vers le bas. Cliquez sur Empreinte numérique.

ÉTAPE 6. Exécutez la commande regedit et rendez-vous sur HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd.

1. Modifier la clé d'empreinte numérique SSL et copiez la valeur de l'empreinte numérique du certificat TLS dans cette valeur binaire. Vous pouvez ignorer sans risque les éléments inconnus dans la boîte de dialogue Modifier la valeur binaire (tels que '0000' et les caractères spéciaux).
2. Modifier la clé SSLEnabled et modifiez la valeur DWORD sur 1. (Pour désactiver SSL ultérieurement, changez la valeur DWORD sur 0).
3. Si vous souhaitez modifier les paramètres par défaut (facultatif), utilisez les informations suivantes dans le même chemin d'accès du Registre :

SSLPort DWORD : numéro de port SSL. Valeur par défaut : 443.

SSLMinVersion DWORD : 1 = SSL 3.0, 2 = TLS 1.0, 3 = TLS 1.1, 4 = TLS 1.2. Valeur par défaut : 2 (TLS 1.0).

SSLCipherSuite DWORD : 1 = GOV, 2 = COM, 3 = ALL. Valeur par défaut : 3 (ALL).

ÉTAPE 7. Assurez-vous que le port TCP TLS est ouvert dans le Pare-feu Windows s'il n'est pas la valeur par défaut (443). (Lors de la création de la règle de trafic entrant dans le Pare-feu Windows, assurez-vous que ses propriétés possèdent les entrées sélectionnées « Autoriser la connexion » et « Activé ».)

ÉTAPE 8. Assurez-vous qu'aucune autre application ou service (tel que IIS) utilisent le port TCP TLS.

ÉTAPE 9. Pour les VDA pour OS Windows Server, redémarrez la machine pour que les modifications prennent effet. (Il n'est pas nécessaire de redémarrer les machines contenant des VDA pour OS Windows Desktop).

Configurer TLS sur les groupes de mise à disposition

Effectuez cette procédure pour chaque groupe de mise à disposition qui contient les VDA vous avez configurés pour les connexions TLS.

1. À partir de Studio, ouvrez la console PowerShell.
2. Exécutez **asnp Citrix.*** pour charger les applets de commande du produit Citrix.

3. Exécutez **Get-BrokerAccessPolicyRule -DesktopGroupName '*<groupe-mise-à-disposition>*' | Set-BrokerAccessPolicyRule -HdxSslEnabled $true**.
4. Exécutez **Set-BrokerSite -DnsResolutionEnabled $true**.

Résolution des problèmes

Si une erreur de connexion se produit, consultez le journal des événements système du VDA.

Lorsque vous utilisez Citrix Receiver pour Windows, si vous recevez une erreur de connexion (comme 1030) qui indique une erreur TLS, désactivez Desktop Viewer et essayez de vous reconnecter. Bien que la connexion échoue toujours, une description du problème TLS sous-jacent peut être fournie. Par exemple, vous avez spécifié un modèle incorrect lors de la demande d'un certificat à partir de l'autorité de certification.

Communications entre le Controller et le VDA

Les communications entre le Controller et le VDA sont sécurisées par la protection des messages de Windows Communication Framework (WCF). Une protection supplémentaire au niveau du transport à l'aide de TLS n'est pas requise. La configuration WCF utilise Kerberos pour l'authentification mutuelle entre le Controller et le VDA. Le cryptage utilise AES en mode CBC avec une clé 256 bits. L'intégrité des messages est assurée par SHA-1.

Selon Microsoft, les protocoles de sécurité utilisés par WCF sont conformes aux normes OASIS (Organization for the Advancement of Structured Information Standards), y compris la stratégie WS-SecurityPolicy 1.2. En outre, Microsoft indique que WCF prend en charge tous les jeux d'algorithmes répertoriés dans la stratégie de sécurité 1.2.

Les communications entre les Controller et les VDA utilisent le jeu d'algorithmes basic256, dont les algorithmes sont indiqués ci-dessus.

TLS et redirection vidéo HTML5

Vous pouvez utiliser la redirection vidéo HTML5 pour rediriger les sites Web HTTPS. Le code JavaScript injecté sur ces sites Web doit établir une connexion TLS avec le service de redirection vidéo Citrix HDX HTML5 qui s'exécute sur le VDA. Pour ce faire, deux certificats personnalisés sont générés dans le magasin de certificats sur le VDA.

La redirection vidéo HTML5 est désactivée par défaut.

Pour plus d'informations sur la redirection de la vidéo pour HTML5, consultez la section Paramètres de stratégie multimédia.

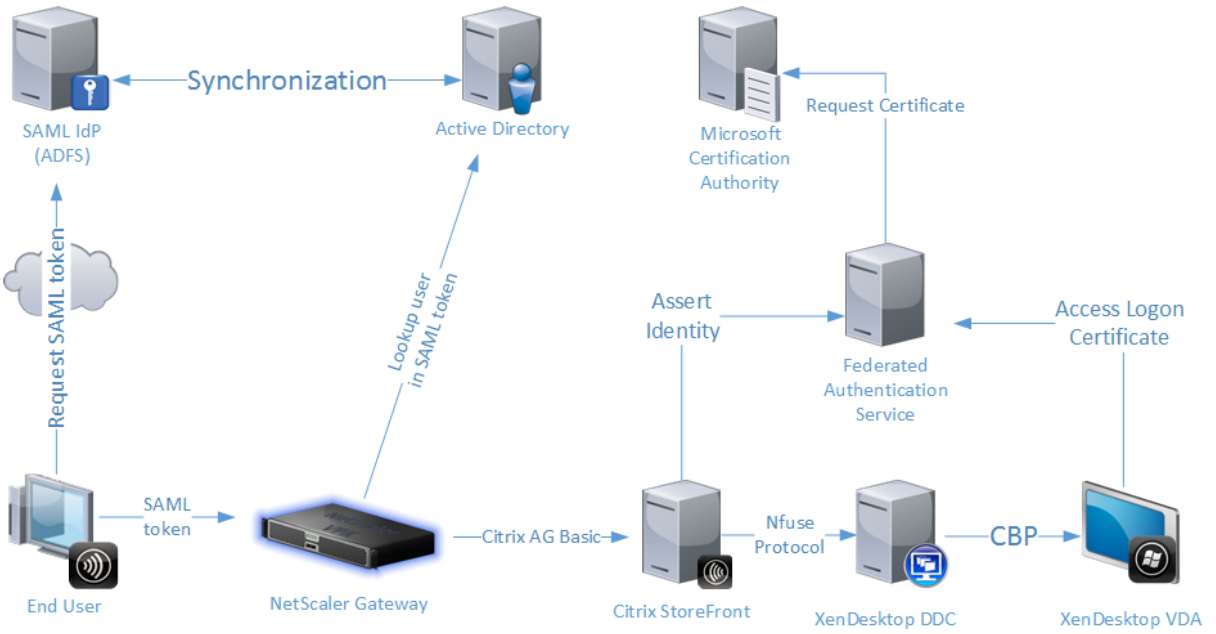
> **Remarque :**
>
> Si vous n'avez pas l'intention d'utiliser la redirection vidéo HTML5, nous vous recommandons de supprimer les deux certificats du magasin de certificats de l'ordinateur local.
>
> Ces certificats sont :
>
> - Pour l'autorité de certification (racine) : **Citrix XenApp/XenDesktop HDX In-Product CA** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp/XenDesktop Engineering; CN = Citrix XenApp/XenDesktop HDX In-Product CA)
>   Emplacement : Certificats (ordinateur local) > Autorités de certification racines de confiance > Certificats.
> - Pour l'entité de fin (feuille) : **Citrix XenApp/XenDesktop HDX Service** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp/XenDesktop Engineering; CN = Citrix XenApp/XenDesktop HDX Service)
>   Emplacement : Certificats (ordinateur local) > Personnel > Certificats.
>
> Nous vous recommandons de configurer le service de redirection vidéo Citrix HDX HTML5 pour qu'il ne démarre pas automatiquement.
> L'arrêt de ce service supprime également les certificats.

Service d'authentification fédérée

February 28, 2019

Le Service d'authentification fédérée de Citrix est un composant doté de privilèges conçu pour s'intégrer avec les Services de certificats Active Directory. Il émet des certificats pour les utilisateurs de manière dynamique, ce qui leur permet de se connecter à un environnement Active Directory comme s'ils avaient une carte à puce. Cela permet à StoreFront d'utiliser un éventail plus large d'options d'authentification, telles que les assertions SAML (Security Assertion Markup Language). SAML est généralement utilisé comme une alternative aux comptes utilisateur Windows traditionnels sur Internet.

Le diagramme suivant illustre l'intégration du Service d'authentification fédérée avec une autorité de certification Microsoft, ainsi que la fourniture de services de support à StoreFront et aux VDA XenApp et XenDesktop.



Les serveurs StoreFront approuvés contactent le Service d'authentification fédérée (FAS) lorsque les utilisateurs demandent accès à l'environnement Citrix. Le FAS accorde un ticket qui permet à une seule session XenApp ou XenDesktop de s'authentifier avec un certificat pour cette session. Lorsqu'un VDA doit authentifier un utilisateur, il se connecte au FAS utilise le ticket. Seul le FAS a accès à la clé privée du certificat de l'utilisateur ; le VDA doit envoyer au FAS chaque opération de signature et de décryptage opération qu'il doit effectuer avec le certificat.

Exigences

Le Service d'authentification fédérée est pris en charge sur les serveurs Windows (Windows Server 2008 R2 ou version supérieure).

- Citrix vous recommande d'installer le FAS sur un serveur qui ne contient pas d'autres composants Citrix.
- Le serveur Windows doit être sécurisé. Il aura accès à un certificat d'autorité d'inscription et à une clé privée qui lui permettent d'émettre automatiquement des certificats pour les utilisateurs du domaine, et il aura accès à ces certificats utilisateur et clés privées.

Dans le site XenApp ou XenDesktop :

- Les Delivery Controller doivent être à la version minimale 7.9.
- Les VDA doivent être à la version minimale 7.9. Vérifiez que la configuration de la stratégie de groupe Service d'authentification fédérée a été correctement appliquée aux VDA avant de créer le catalogue de machines de la manière habituelle ; consultez la section Configurer une stratégie de groupe pour plus de détails.

- Le serveur StoreFront doit être à la version minimale 3.6 (il s'agit de la version fournie avec l'ISO XenApp et XenDesktop 7.9).

Lors de la planification de votre déploiement de ce service, veuillez consulter la section Considérations de sécurité.

Références :

- Services de certificats Active Directory

https://technet.microsoft.com/en-us/library/hh831740.aspx

- Configuration de Windows pour l'ouverture de session par certificat

https://support.citrix.com/article/CTX206156

Séquence d'installation et de configuration

1. Installer le Service d'authentification fédérée
2. Activer le plug-in Service d'authentification fédérée sur les serveurs StoreFront
3. Configurer une stratégie de groupe
4. Utilisez la console d'administration Service d'authentification fédérée pour : (a) Déployer les modèles fournis, (b) Définir des autorités de certification, et (c) Autoriser le Service d'authentification fédérée à utiliser votre autorité de certification
5. Configurer des règles d'utilisateur

Installer le Service d'authentification fédérée

Pour des raisons de sécurité, Citrix recommande d'installer le FAS sur un serveur dédié qui est sécurisé de la même manière qu'un contrôleur de domaine ou une autorité de certification. Le FAS peut être installé à partir du bouton **Service d'authentification fédérée** sur l'écran de démarrage autorun lorsque l' ISO est inséré.

Les composants suivants vont être installés :

- Service d'authentification fédérée
- Applets de commande du composant logiciel enfichable PowerShell pour configurer à distance le Service d'authentification fédérée
- Console d'administration du Service d'authentification fédérée.
- Modèles de stratégie de groupe du Service d'authentification fédérée (CitrixFederatedAuthenticationService.admx/adml)
- Fichiers de modèle de certificat pour la configuration de l'autorité de certification
- Compteurs de performances et journaux d'événements

Activer le plug-in Service d'authentification fédérée sur un magasin StoreFront

Pour activer l'intégration du Service d'authentification fédérée sur un magasin StoreFront, exécutez les applets de commande PowerShell suivantes sous un compte d'administrateur. Si vous disposez de plus d'un magasin, ou si le magasin a un autre nom, le texte du chemin d'accès ci-dessous peut différer.

```
```
Get-Module "Citrix.StoreFront.*" -ListAvailable | Import-Module

$StoreVirtualPath = "/Citrix/Store"

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

$auth = Get-STFAuthenticationService -StoreService $store

Set-STFClaimsFactoryNames -AuthenticationService $auth -
    ClaimsFactoryName "FASClaimsFactory"

Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider "
    FASLogonDataProvider"
```
```

Pour arrêter d'utiliser le FAS, utilisez le script PowerShell suivant :

```
```
Get-Module "Citrix.StoreFront.*" -ListAvailable | Import-Module

$StoreVirtualPath = "/Citrix/Store"

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

$auth = Get-STFAuthenticationService -StoreService $store

Set-STFClaimsFactoryNames -AuthenticationService $auth -
    ClaimsFactoryName "standardClaimsFactory"

Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider ""
```
```


Configurer le Delivery Controller

Pour utiliser le Service d'authentification fédérée, configurez le Delivery Controller XenApp ou XenDesktop de manière à approuver les serveurs StoreFront qui peuvent s'y connecter : exécutez l'applet de commande PowerShell **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true**.

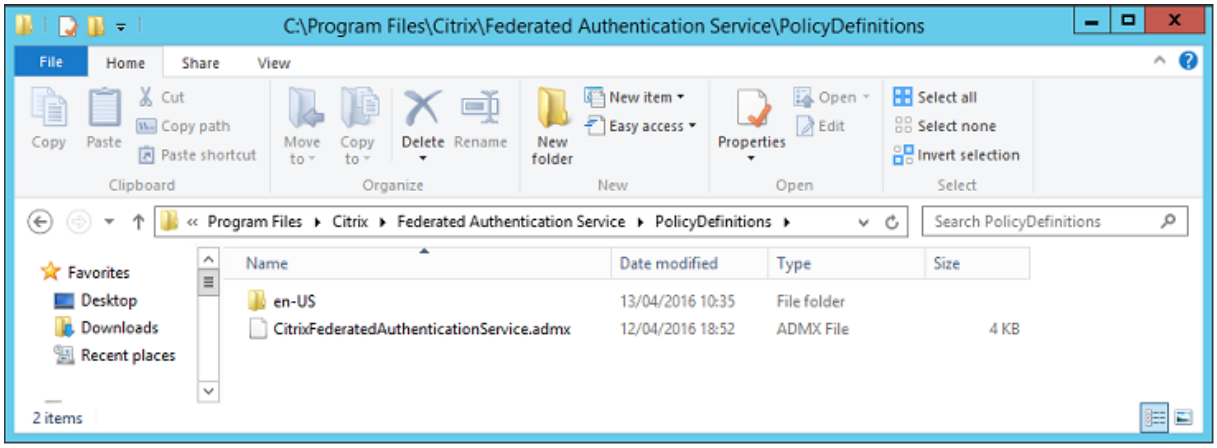
Configurer une stratégie de groupe

Après avoir installé le Service d'authentification fédérée, vous devez spécifier les adresses DNS complètes des serveurs FAS dans une stratégie de groupe à l'aide des modèles de stratégie de groupe fournis dans le cadre de l'installation.

Important : assurez-vous que les serveurs StoreFront qui demandent des tickets et les VDA utilisant des tickets disposent d'adresses DNS identiques, y compris l'attribution automatique de numéros appliquée aux serveurs par l'objet de stratégie de groupe.

À des fins de simplicité, les exemples suivants configurent une seule stratégie au niveau du domaine qui s'applique à toutes les machines ; cependant, cela n'est pas requis. Le FAS fonctionnera tant que les serveurs StoreFront, les VDA, et la machine exécutant la console d'administration FAS voient la même liste d'adresses DNS. Veuillez noter que l'objet de stratégie de groupe ajoute un numéro d'index pour chaque entrée, qui doit également correspondre si plusieurs objets sont utilisés.

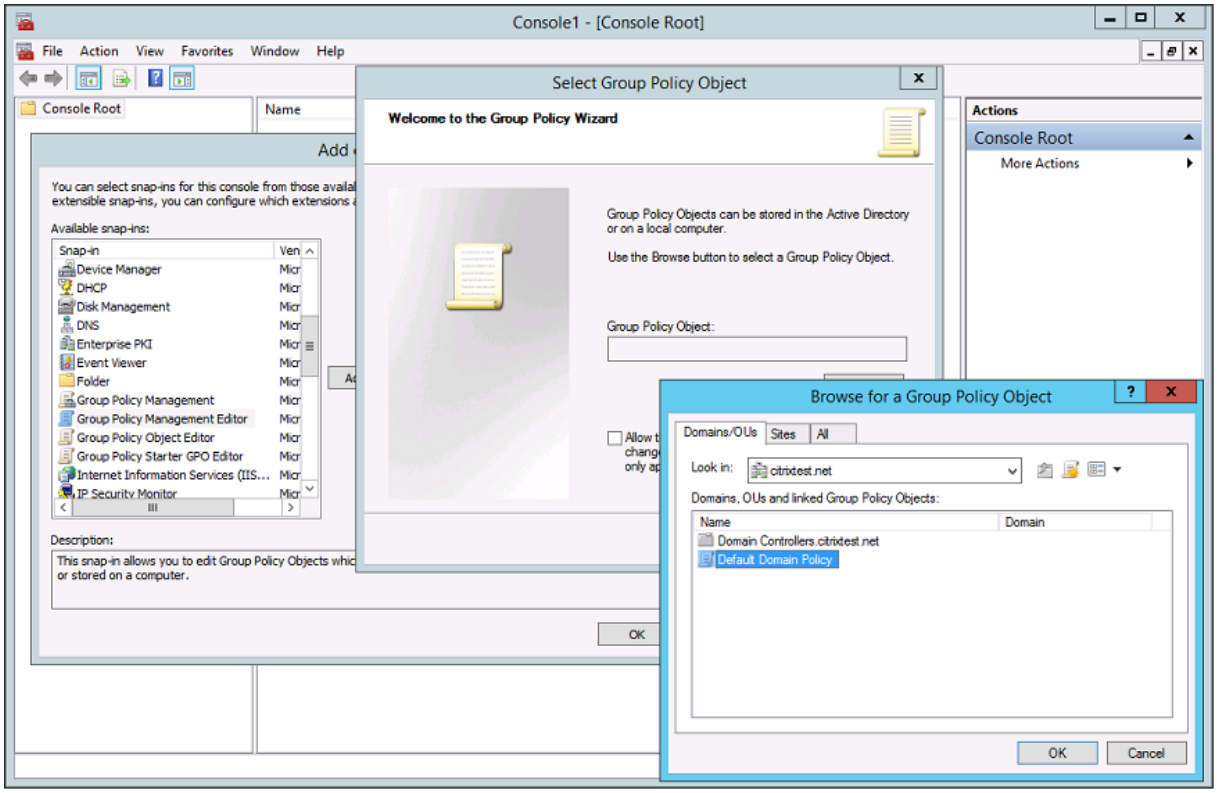
Étape 1 – Sur le serveur sur lequel vous avez installé le FAS, localisez le fichier C:\Program Files\Citrix\Federated Authentication Service\PolicyDefinitions\CitrixFederatedAuthenticationService.admx et le dossier en-US.



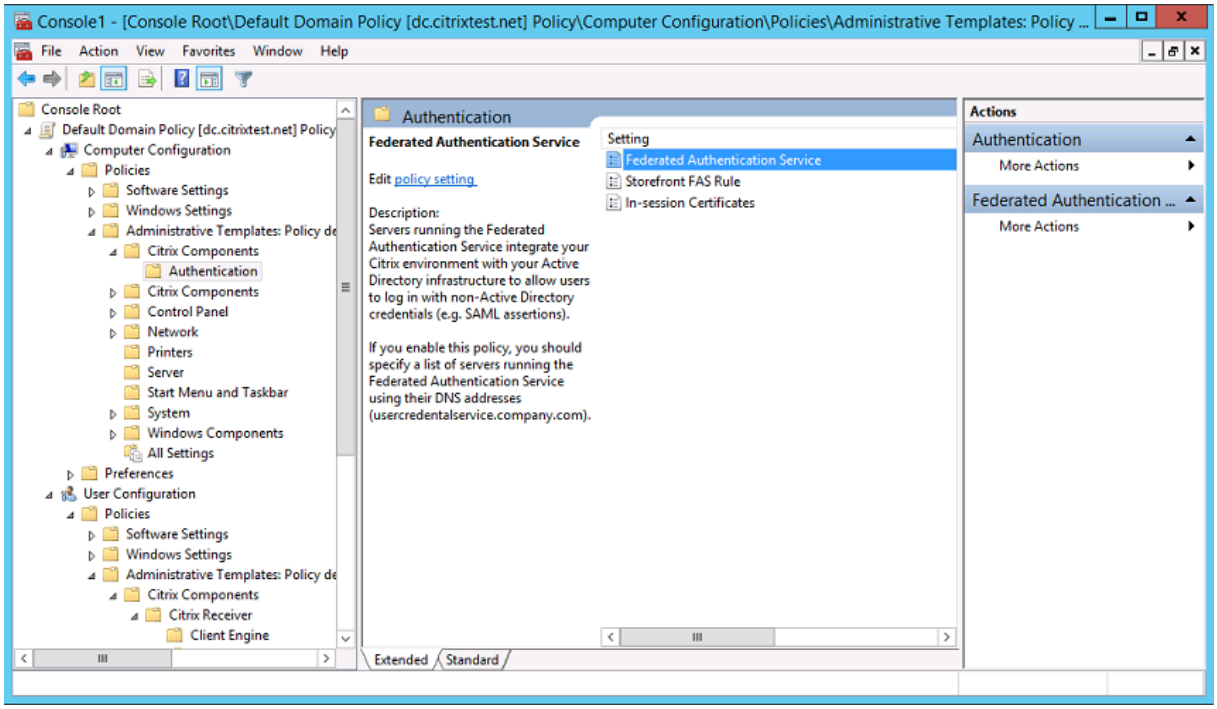
Étape 2 – Copiez ces derniers sur votre contrôleur de domaine et placez-les dans C:\Windows\PolicyDefinitions et le sous-dossier en-US.

Étape 3 – Exécutez la console Microsoft Management Console (mmc.exe à partir de la ligne de commande). À partir de la barre de menu, sélectionnez **Fichier > Ajouter/Supprimer un composant logiciel enfichable**. Ajoutez **Éditeur d'objets de stratégie de groupe**.

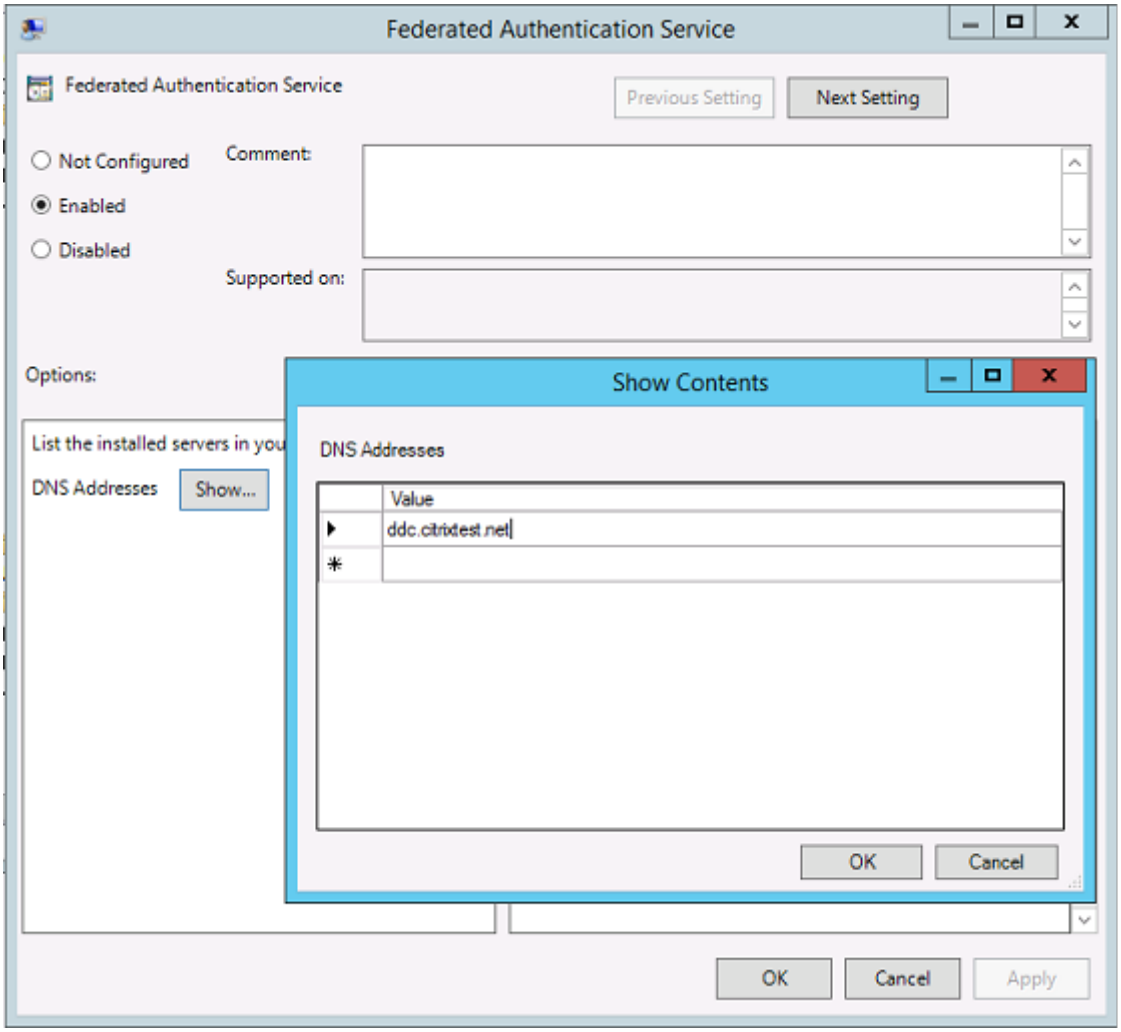
Lorsque vous y êtes invité par un objet de stratégie de groupe, sélectionnez **Parcourir**, puis sélectionnez la **stratégie de domaine par défaut**. Éventuellement, vous pouvez créer et sélectionner un objet de stratégie approprié pour votre environnement, à l'aide des outils de votre choix. La stratégie doit être appliquée à toutes les machines exécutant des logiciels Citrix affectés (VDA, serveurs StoreFront, outils d'administration).



Étape 4 – Accédez à la stratégie Service d'authentification fédérée située dans Configuration ordinateur/Stratégies/Modèles d'administration/Composants Citrix/Authentification.



Étape 5 – Ouvrez la stratégie Service d'authentification fédérée et sélectionnez **Activé**. Cela vous permet de sélectionner le bouton **Afficher**, dans lequel vous pouvez configurer les adresses DNS de vos serveurs FAS.



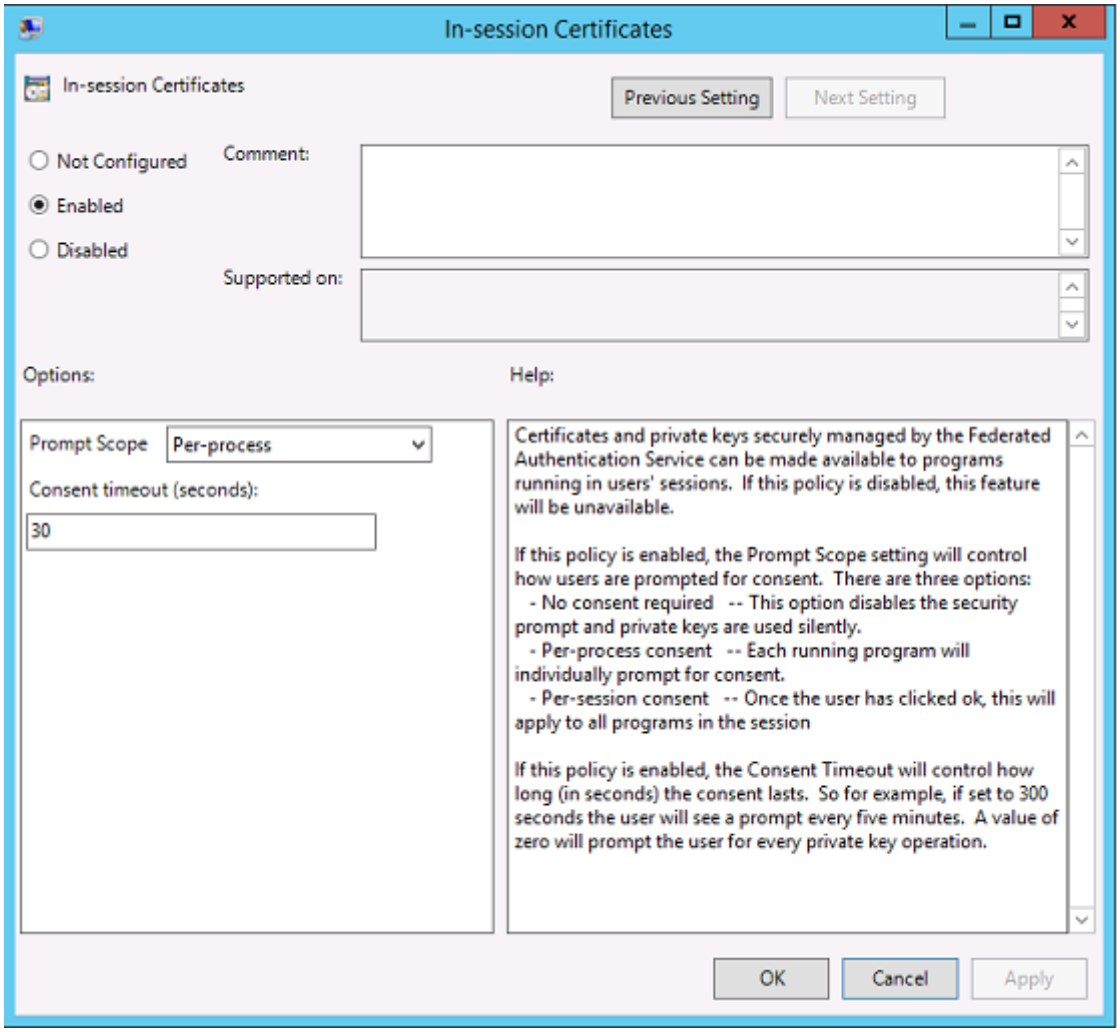
Étape 6 – Entrez les adresses DNS des serveurs hébergeant votre Service d'authentification fédérée.

Rappel : si vous entrez plusieurs adresses, l'ordre de la liste doit être cohérent entre les serveurs StoreFront et les VDA. Cela comprend des entrées vides ou non utilisées.

Étape 7 – Cliquez sur **OK** pour quitter l'assistant de stratégie de groupe et appliquer les modifications à la stratégie de groupe. Vous devrez peut-être redémarrer les machines (ou exécuter **gpupdate/force** à partir de la ligne de commande) pour que les modifications prennent effet.

Activer la prise en charge du certificat dans la session

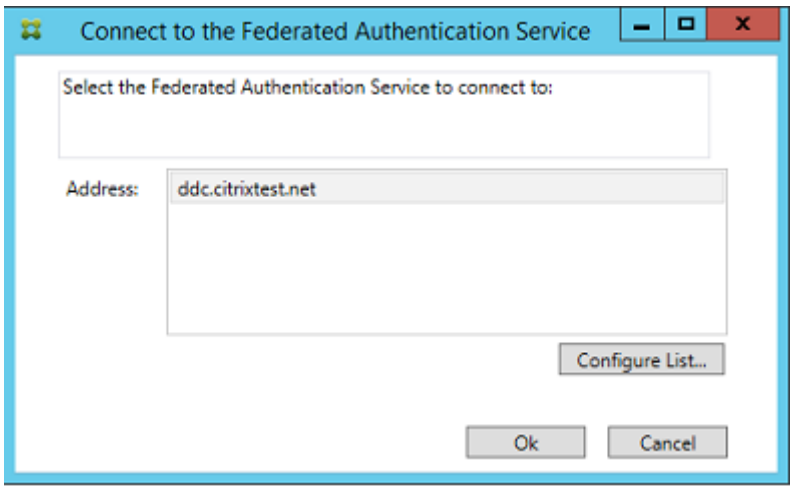
Le modèle de stratégie de groupe prend en charge la configuration du système pour les certificats dans la session. Ceci place les certificats dans le magasin de certificats personnel de l'utilisateur après l'ouverture de session afin que les applications puissent les utiliser. Par exemple, si vous exigez l'authentification TLS pour accéder aux serveurs Web dans la session VDA, le certificat peut être utilisé par Internet Explorer. Par défaut, les VDA n'autoriseront pas l'accès aux certificats après l'ouverture de session.



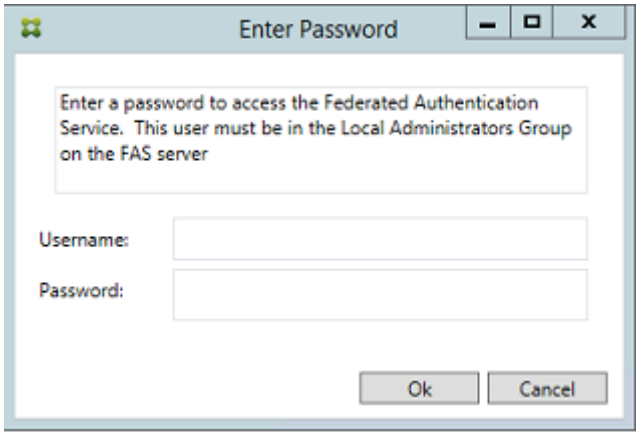
Utilisation de la console d'administration du Service d'authentification fédérée

Le console d'administration du Service d'authentification fédérée est installée dans le cadre du Service d'authentification fédérée. Une icône (Service d'authentification fédérée de Citrix) est placée dans le menu Démarrer.

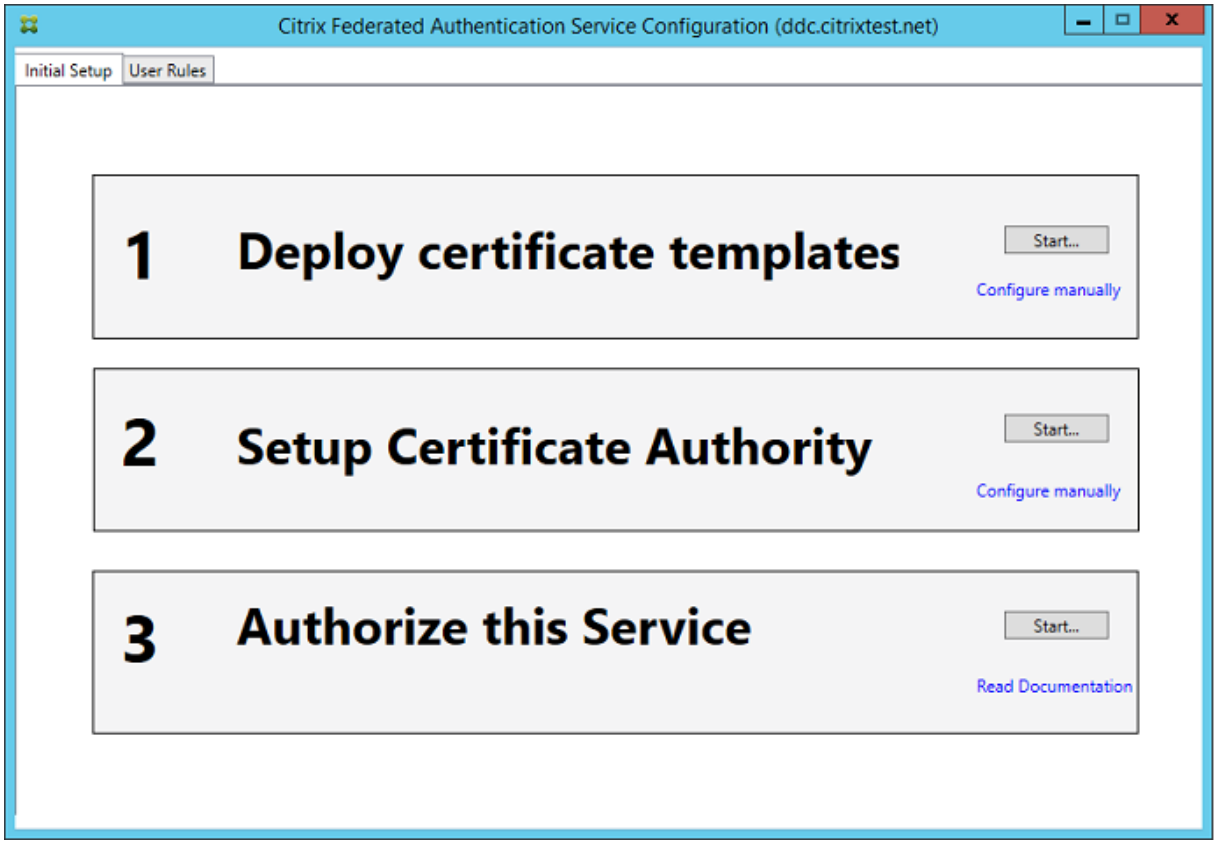
La console tente de localiser automatiquement les serveurs FAS dans votre environnement à l'aide de la configuration de la stratégie de groupe. Si cela échoue, consultez la section Configurer une stratégie de groupe.



Si votre compte utilisateur n'est pas membre du groupe Administrateurs sur la machine exécutant le Service d'authentification fédérée, vous serez invité à entrer des informations d'identification.



La première fois que la console d'administration est utilisée, elle vous guide au travers d'un processus en trois étapes qui déploie les modèles de certificat, configure l'autorité de certification et autorise le Service d'authentification fédérée à utiliser l'autorité de certification. Certaines des étapes peuvent également être effectuées manuellement à l'aide des outils de configuration du système d'exploitation.

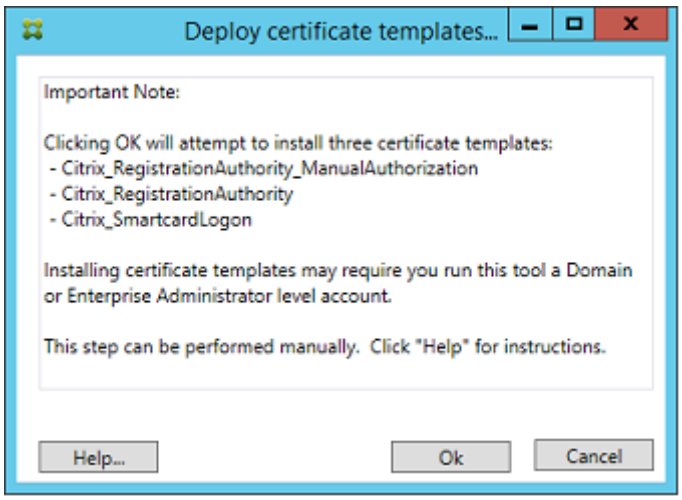


Déployer des modèles de certificat

Pour éviter des problèmes d'interopérabilité avec d'autres logiciels, le Service d'authentification fédérée offre trois modèles de certificats Citrix pour son propre usage.

- Citrix_RegistrationAuthority_ManualAuthorization
- Citrix_RegistrationAuthority
- Citrix_SmartcardLogon

Ces modèles doivent être enregistrés auprès d'Active Directory. Si la console ne peut pas les trouver, l'outil **Déployer des modèles de certificat** peut les installer. Cet outil doit être exécuté sous un compte disposant des autorisations nécessaires pour gérer votre forêt d'entreprise.



La configuration des modèles peut être trouvée dans les fichiers XML avec l'extension .certificatetemplate qui sont installés avec le service d'authentification fédérée dans :

C:\Program Files\Citrix\Federated Authentication Service\CertificateTemplates

Si vous ne disposez pas des autorisations nécessaires pour installer ces fichiers modèles, donnez-les à votre administrateur Active Directory.

Pour installer manuellement les modèles, vous pouvez utiliser les commandes PowerShell suivantes :

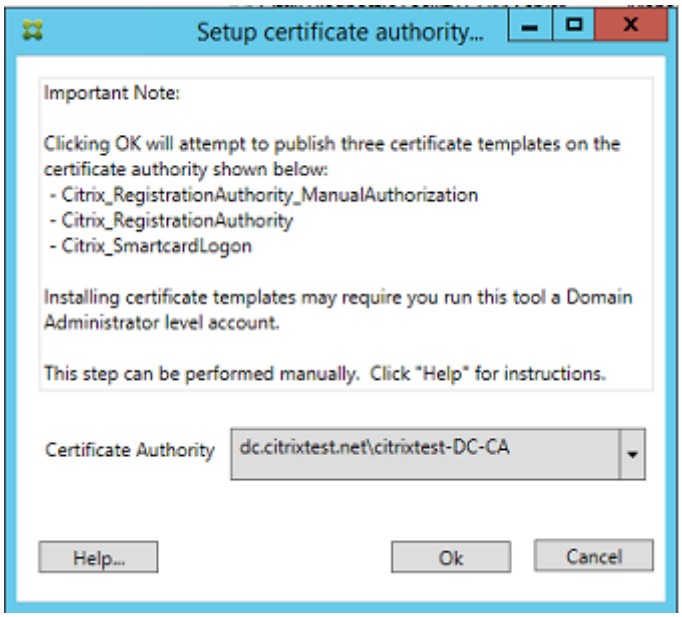
```
‘‘‘
$template = [System.IO.File]::ReadAllBytes(”$Pwd\Citrix_SmartcardLogon.certificatetemplate”)

 $CertEnrol = New-Object -ComObject X509Enrollment.CX509EnrollmentPolicyWebService

 $CertEnrol.InitializeImport($template)

 $comtemplate = $CertEnrol.GetTemplates().ItemByIndex(0)
$writabletemplate = New-Object -ComObject X509Enrollment.CX509CertificateTemplateADWritable

 $writabletemplate.Initialize($comtemplate)

 $writabletemplate.Commit(1, $NULL)
 ‘‘‘
```


Configurer des services de certificats Active Directory

Après l'installation de modèles de certificats Citrix, ils doivent être publiés sur un ou plusieurs serveurs d'autorité de certification Microsoft. Reportez-vous à la documentation Microsoft sur la manière de déployer des services de certificats Active Directory.

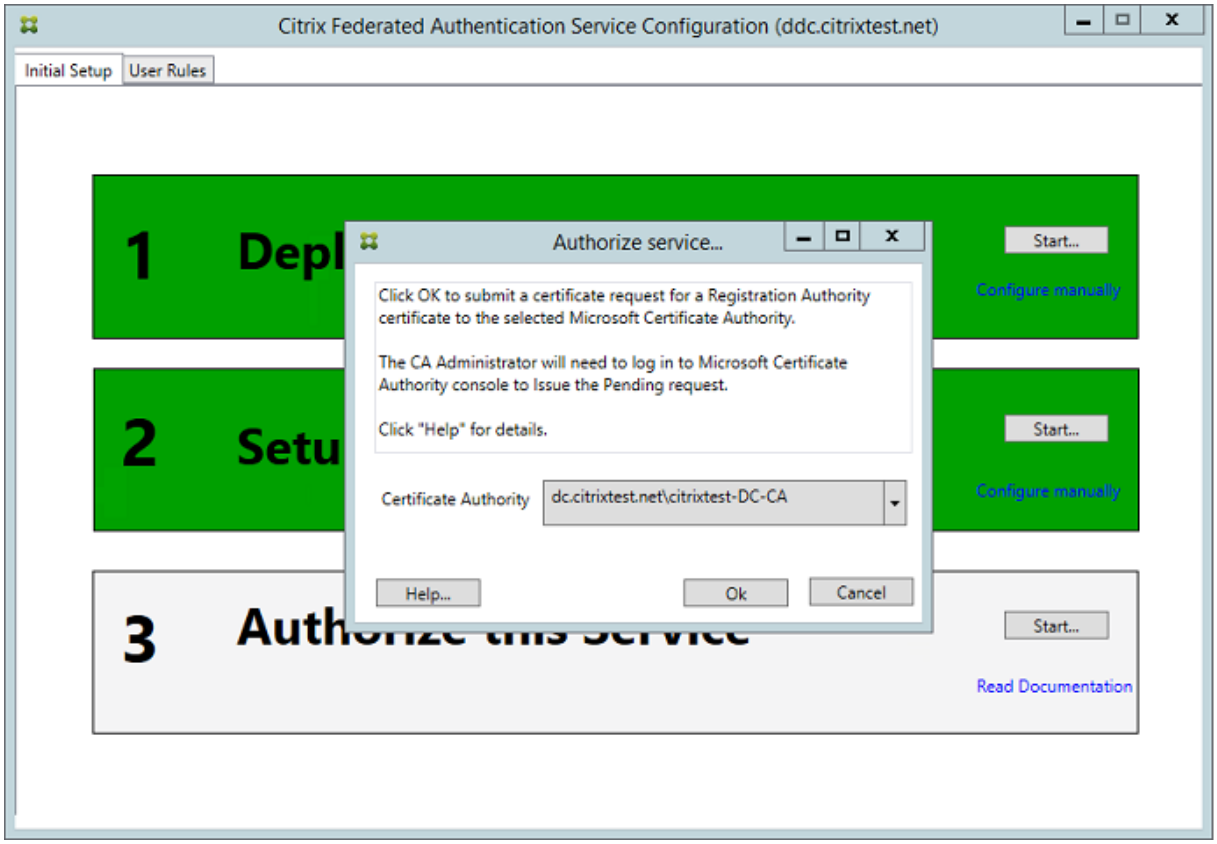
Si les modèles ne sont pas publiés sur au moins un serveur, l'outil **Configurer une autorité de certification** permet de les publier. Vous devez exécuter cet outil en tant qu'utilisateur disposant d'autorisations suffisantes pour gérer l'autorité de certification.

(Les modèles de certificats peuvent également être publiés à l'aide de la console Autorité de certification de Microsoft.

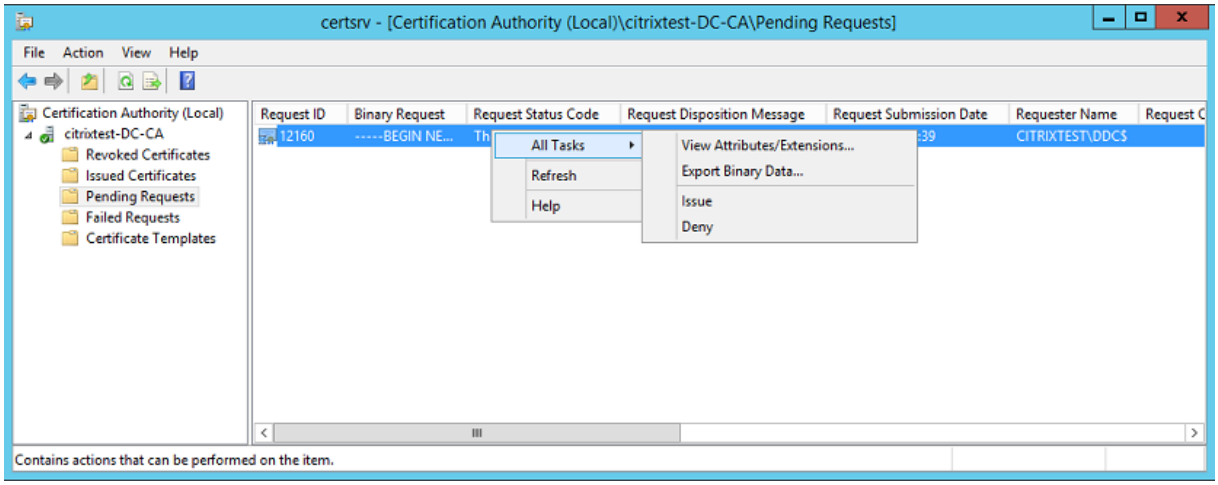


Autoriser le Service d'authentification fédérée

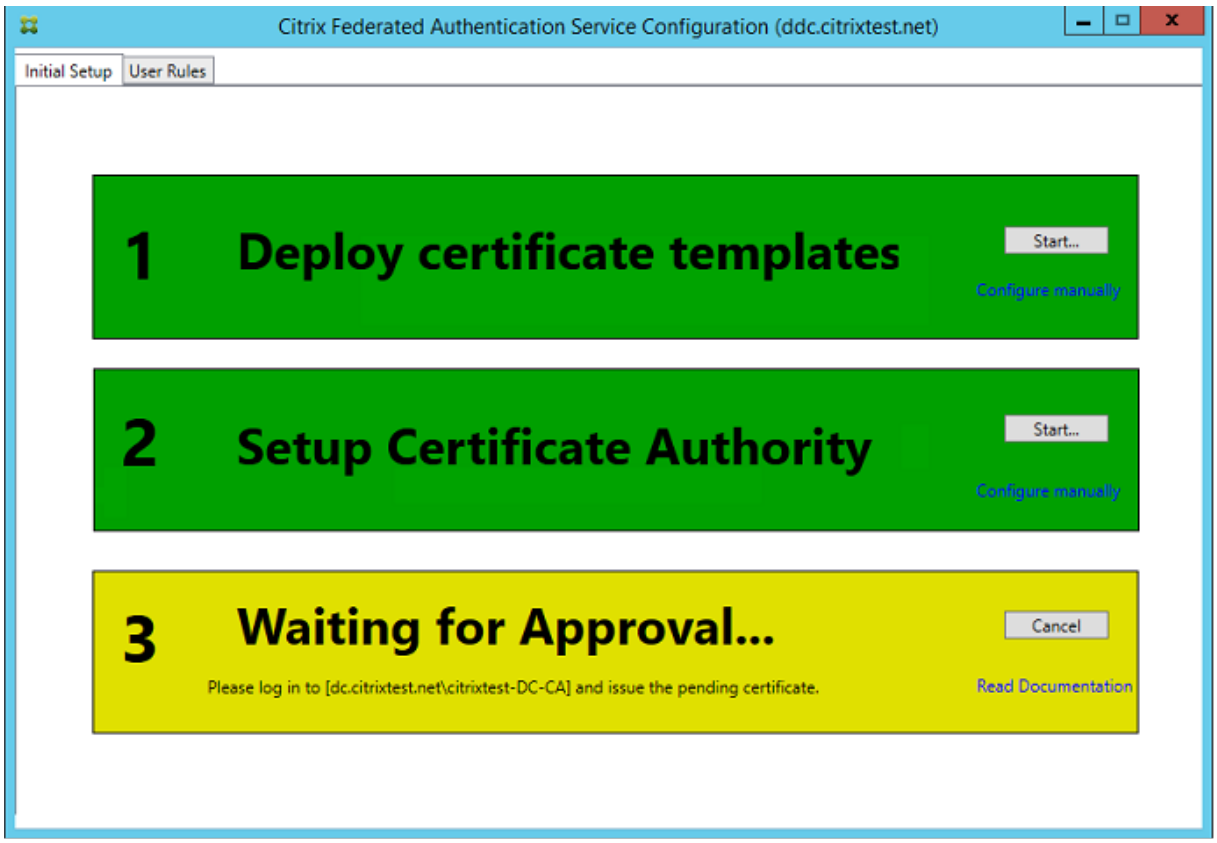
La dernière étape de configuration dans la console initie l'autorisation du Service d'authentification fédérée. La console d'administration utilise le modèle Citrix_RegistrationAuthority_ManualAuthorization pour générer une requête de certificat, puis l'envoie à l'une des autorités de certification qui publient ce modèle.



Une fois la requête envoyée, elle apparaît dans la liste **Demandes en attente** de la console Autorité de certification de Microsoft. L'administrateur de l'autorité de certification doit choisir d'**émettre** ou de **rejeter** la requête avant que la configuration du Service d'authentification fédérée puisse continuer. Veuillez noter que la demande d'autorisation s'affiche en tant que **Demande en attente** depuis le compte de la machine FAS.



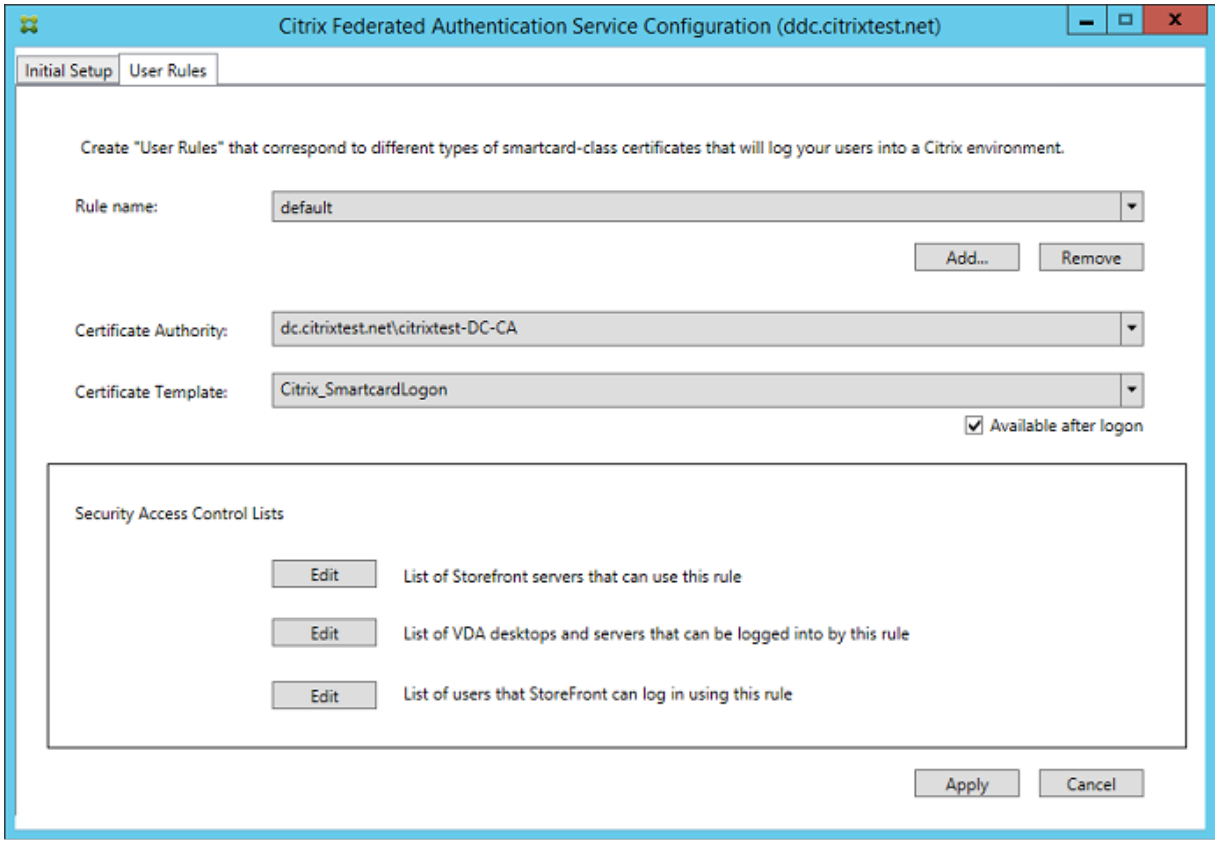
Cliquez avec le bouton droit sur **Toutes les tâches**, puis sélectionnez **Émettre** ou **Rejeter** pour la demande de certificat. La console d'administration du Service d'authentification fédérée détecte automatiquement lorsque ce processus est terminé. Cette opération peut prendre plusieurs minutes.



Configurer des règles d'utilisateur

Une règle d'utilisateur autorise l'émission de certificats pour l'ouverture de session sur des VDA et l'utilisation dans la session, conformément aux instructions de StoreFront. Chaque règle spécifie les serveurs StoreFront qui sont approuvés pour demander des certificats, les utilisateurs pour lesquels ils peuvent être demandés, et les VDA autorisés à les utiliser.

Pour terminer la configuration du Service d'authentification fédérée, l'administrateur doit définir la règle par défaut en basculant sur l'onglet User Rules de la console d'administration FAS, en sélectionnant une autorité de certification sur laquelle publier le modèle Citrix_SmartcardLogon et en modifiant la liste des serveurs StoreFront. La liste des VDA est par défaut Ordinateurs du domaine et la liste des utilisateurs est par défaut Utilisateurs du domaine ; ces informations peuvent être modifiées si les valeurs par défaut ne sont pas appropriées.



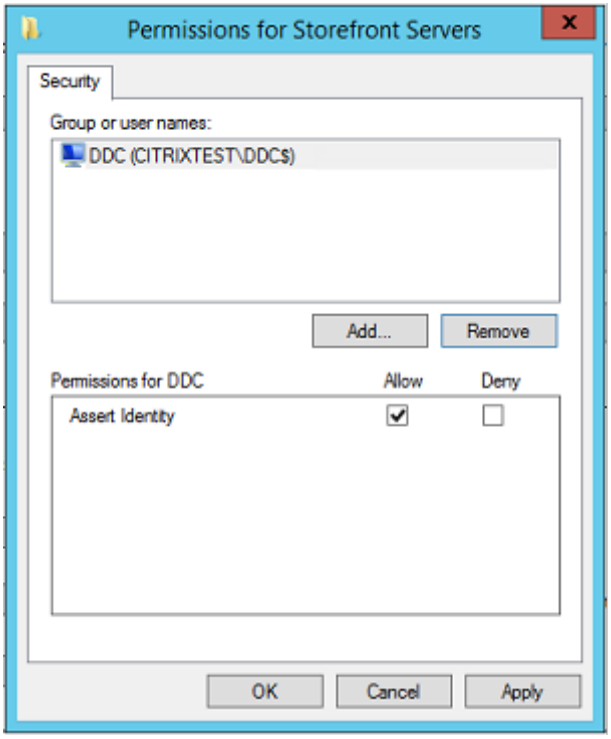
Champs :

Certificate Authority et Certificate Template : le modèle de certificat et l'autorité de certification qui seront utilisés pour émettre des certificats utilisateur. Il doit s'agir du modèle Citrix_SmartcardLogon, ou d'une copie modifiée de ce dernier, sur l'une des autorités de certification sur laquelle le modèle est publié.

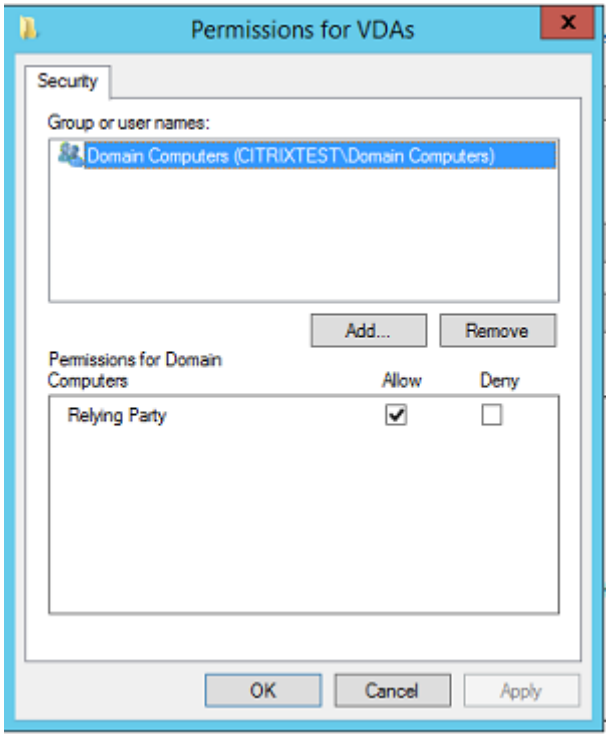
La console FAS prend en charge l'ajout de multiples autorités de certification à des fins de basculement et d'équilibrage de charge, à l'aide de commandes PowerShell. De même, des options de création de certificats plus avancées peuvent être configurées à l'aide de la ligne de commande et des fichiers de configuration. Consultez les sections PowerShell et Modules matériels de sécurité.

In-Session Certificats : la case à cocher **Available after logon** détermine si un certificat peut également être utilisé en tant que certificat dans la session. Si cette case n'est pas sélectionnée, le certificat sera utilisé uniquement pour l'ouverture de session ou la reconnexion, et l'utilisateur n'aura pas accès au certificat après l'authentification.

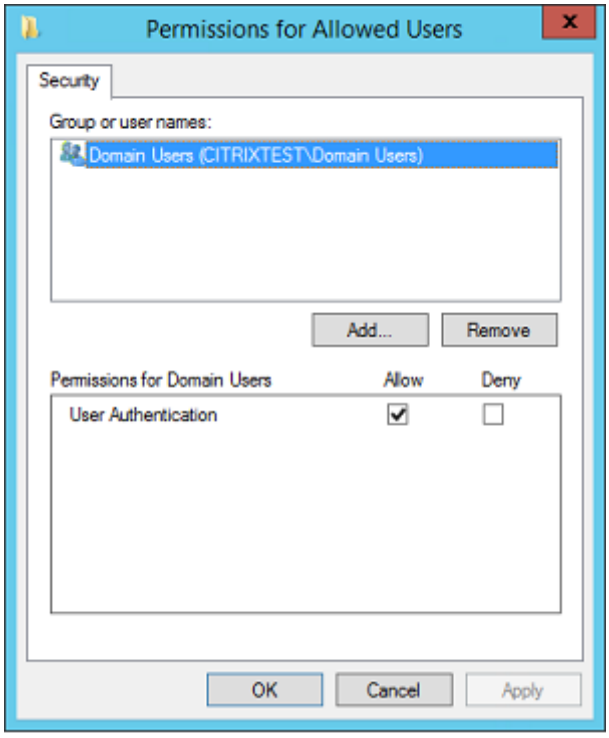
List of StoreFront servers that can use this rule : liste des serveurs StoreFront approuvés qui sont autorisés à demander des certificats pour l'ouverture de session ou la reconnexion des utilisateurs. Notez que ce paramètre est critique à la sécurité et doit être géré avec soin.



List of VDA desktops and servers that can be logged into by this rule : liste des machines VDA qui peuvent connecter les utilisateurs à l'aide du système FAS.



List of users that StoreFront can log in using this rule : liste des utilisateurs pour lesquels des certificats peuvent être émis par le Service d'authentification fédérée.



Utilisation avancée

Vous pouvez créer des règles supplémentaires pour référencer des autorités et des modèles de certificat différents, qui peuvent être configurés pour avoir des propriétés et des autorisations différentes. Ces règles peuvent être configurées pour être utilisées par différents serveurs StoreFront, qui devront être configurés pour demander la nouvelle règle par nom. Par défaut, StoreFront requiert les **valeurs par défaut** lors du contact du Service d'authentification fédérée. Cela peut être modifié à l'aide des options de configuration de la stratégie de groupe.

Pour créer un nouveau modèle de certificat, dupliquez le modèle Citrix_SmartcardLogon dans la console Autorité de certification de Microsoft, renommez-le (par exemple, Citrix_SmartcardLogon2) et modifiez-le si nécessaire. Créez une nouvelle règle d'utilisateur en cliquant sur **Add** afin de référencer le nouveau modèle de certificat.

Notions importantes sur la mise à niveau

- Tous les paramètres du serveur du service d'authentification fédérée sont conservés lorsque vous effectuez une mise à niveau sur place.
- Mettez à niveau le service d'authentification fédérée en exécutant le programme d'installation du produit complet de XenApp et XenDesktop.
- Avant de mettre à niveau le service d'authentification fédérée de 7.15 LTSR à 7.15 LTSR CU2 (ou

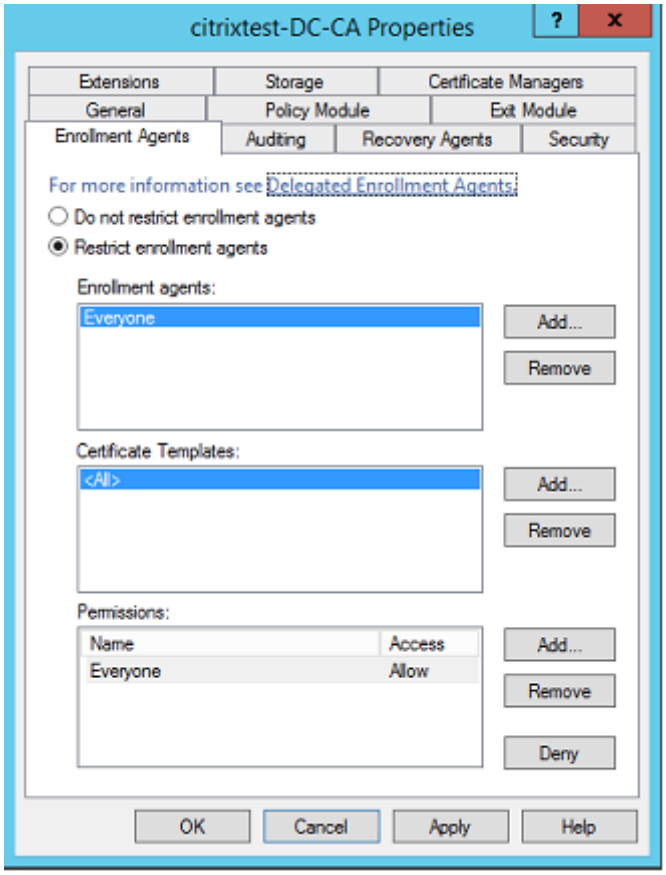
une CU ultérieure prise en charge), mettez à niveau le contrôleur et les VDA (et autres composants principaux) vers la version requise.
- Assurez-vous que la console du service d'authentification fédérée est fermée avant de mettre à niveau le service d'authentification fédérée.
- Assurez-vous qu'au moins un serveur du service d'authentification fédérée est disponible à tout moment. Si aucun serveur n'est accessible par un serveur StoreFront activé par le service d'authentification de fédération, les utilisateurs ne peuvent pas se connecter ni démarrer d'applications.

Considérations de sécurité

Le Service d'authentification fédérée dispose d'un certificat d'autorité d'inscription qui lui permet d'émettre des certificats de manière autonome de la part de vos utilisateurs de domaine. C'est la raison pour laquelle il est important de développer et d'appliquer une stratégie de sécurité pour protéger les serveurs FAS et limiter leurs autorisations.

Agents d'inscription délégués

L'autorité de certification Microsoft permet de contrôler les modèles que le serveur FAS peut utiliser, ainsi que de limiter les utilisateurs pour lesquels le serveur FAS peut émettre des certificats.



Citrix recommande fortement de configurer ces options de façon à ce que le Service d'authentification fédérée puisse uniquement émettre des certificats pour les utilisateurs visés. Par exemple, il est conseillé d'empêcher le Service d'authentification fédérée d'émettre des certificats aux utilisateurs d'un groupe d'utilisateurs protégés ou d'un groupe d'administration.

Configuration de la liste de contrôle d'accès

Comme indiqué dans la section Configurer des rôles utilisateur, vous devez configurer une liste de serveurs StoreFront autorisés à assumer des identités utilisateur sur le Service d'authentification fédérée lorsque des certificats sont émis. De même, vous pouvez restreindre les utilisateurs pour lesquels des certificats seront émis, et les machines VDA auprès desquelles ils peuvent s'authentifier. Cela vient s'ajouter à tout Active Directory standard ou toute fonctionnalité de sécurité d'autorité de certification que vous configurez.

Paramètres de pare-feu

Toutes les communications avec les serveurs FAS utilisent des connexions réseau Kerberos WCF authentifiées mutuellement sur le port 80.

Analyse du journal des événements

Le Service d'authentification fédérée et le VDA écrivent des informations dans le journal d'événements Windows. Ces informations peuvent être utilisées à des fins de contrôle et d'audit. La section Journaux d'événements dresse la liste des entrées de journal d'événements qui peuvent être générées.

Modules matériels de sécurité

Toutes les clés privées, y compris celles des certificats utilisateur émis par le Service d'authentification fédérée, sont stockées en tant que clés privées non exportables par le Compte de service réseau. Le Service d'authentification fédérée prend en charge l'utilisation d'un module matériel de sécurité cryptographique, si votre stratégie de sécurité l'exige.

Une configuration cryptographique de faible niveau est disponible dans le fichier FederatedAuthenticationService.exe.config. Ces paramètres s'appliquent lorsque les clés privées sont créées. Par conséquent, des paramètres différents peuvent être utilisés pour les clés privées d'autorité d'inscription (par exemple, 4 096 bits, Module de plateforme sécurisée protégé) et les certificats utilisateur d'exécution.

Paramètre	Description
ProviderLegacyCsp	Lorsque cette option est définie sur true, FAS utilisera l'API CryptoAPI (CAPI) de Microsoft. Sinon, FAS utilisera l'API Cryptography Next Generation (CNG) de Microsoft.
ProviderName	Nom du fournisseur CAPI ou CNG à utiliser.
ProviderType	Fait référence à la propriété Microsoft KeyContainerPermissionAccessEntry.ProviderType PROV_RSA_AES 24. Doit être toujours 24, sauf si vous utilisez un HSM avec CAPI et que le fournisseur HSM en décide autrement.
KeyProtection	Contrôle l'indicateur « Exportable » des clés privées. Permet également l'utilisation du stockage de clé TMP (Module de plateforme sécurisée), s'il est pris en charge par le matériel.
KeyLength	Longueur de clé des clés privées RSA. Les valeurs prises en charge sont 1024, 2048 et 4096 (valeur par défaut : 2048).

SDK PowerShell

Bien que la console d'administration Service d'authentification fédérée convienne aux déploiements simples, l'interface PowerShell offre des options plus avancées. Lorsque vous utilisez des options qui ne sont pas disponibles dans la console, Citrix recommande d'utiliser uniquement PowerShell pour la configuration.

La commande suivante ajoute les applets de commande PowerShell :

Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1

Utilisez **Get-Help** <*nom cmdlet*> pour afficher l'aide de l'applet de commande. Le tableau suivant dresse la liste de plusieurs commandes où * représente un verbe PowerShell standard (comme New, Get, Set, Remove).

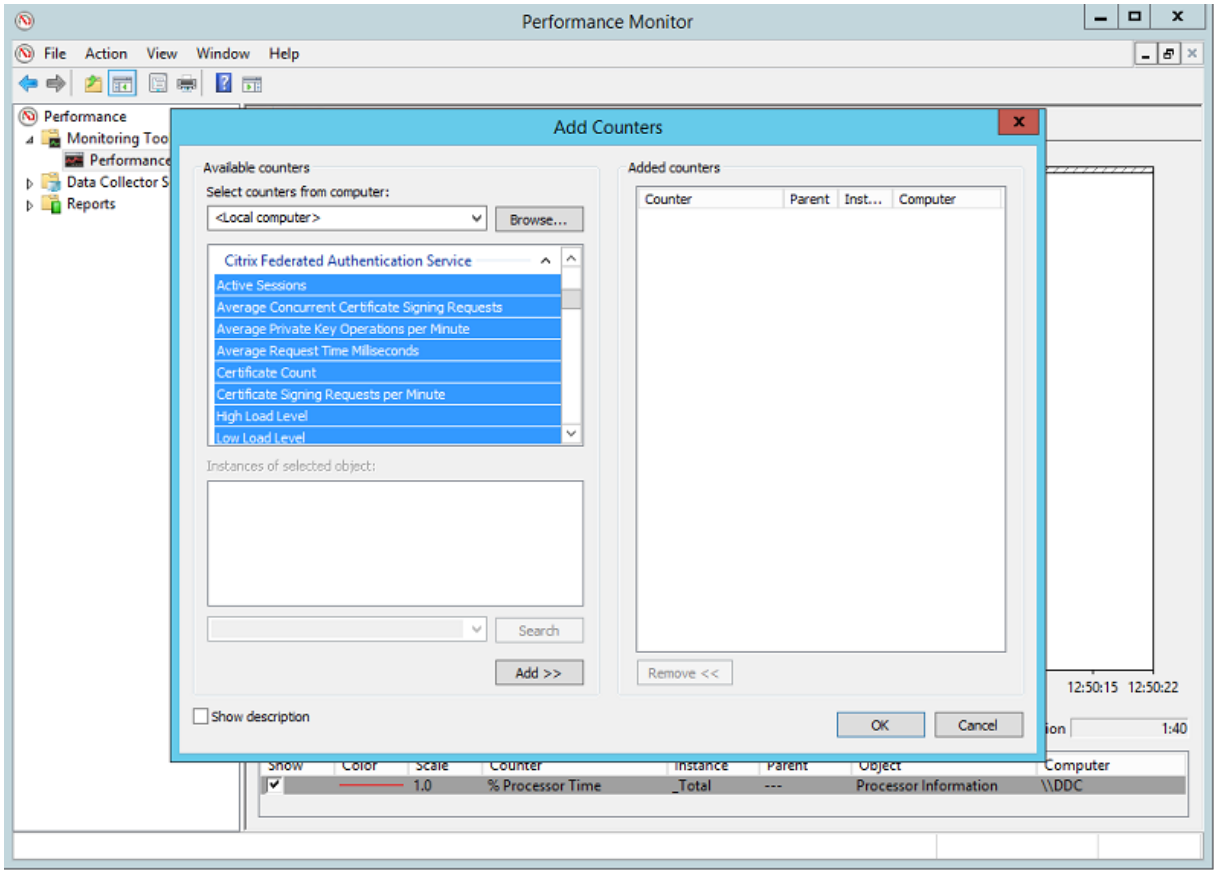
Commandes	Généralités
*-FasServer	Dresse la liste des serveurs FAS et les reconfigure dans l'environnement actuel.
*-FasAuthorizationCertificate	Gère le certificat d'autorité d'inscription.
*-FasCertificateDefinition	Contrôle les paramètres que le FAS utilise pour générer des certificats.
*-FasRule	Gère les règles d'utilisateurs configurées sur le Service d'authentification fédérée.
*-FasUserCertificate	Dresse la liste et gère les certificats mis en cache par le Service d'authentification fédérée.

Des applets de commande PowerShell peuvent être utilisées à distance en spécifiant l'adresse d'un serveur FAS.

Vous pouvez également télécharger un fichier zip contenant tous les fichiers d'aide de l'applet de commande du SDK PowerShell du Service d'authentification fédérée ; consultez l'article SDK PowerShell.

Compteurs de performances

Le Service d'authentification fédérée inclut un jeu de compteurs de performances conçus pour surveiller la charge.



Le tableau suivant répertorie les compteurs disponibles. La plupart des compteurs sont des moyennes mobiles de cinq minutes.

Name	Description
Sessions actives	Nombre de connexions surveillées par le Service d'authentification fédérée.
Concurrent CSRs	Nombre de demandes de certificat traitées simultanément.
Private Key ops	Nombre d'opérations de clé privée effectuées par minute.
Request time	Durée requise pour générer et signer un certificat.
Certificate Count	Nombre de certificats mis en cache dans le Service d'authentification fédérée.
CSR per minute	Nombre de demandes CRS traitées par minute.

Name	Description
Low/Medium/High	Estimations de la charge que le Service d'authentification fédérée peut accepter en termes de « demandes CSR par minute ». Le dépassement du seuil « High Load » peut entraîner l'échec du lancement de sessions.

Journaux d'événements

Les tableaux suivants répertorient les entrées de journal d'événements générées par le Service d'authentification fédérée.

Événements d'administration

[Source de l'événement : Citrix.Authentication.FederatedAuthenticationService]

Ces événements sont consignés en réponse à une modification de la configuration du serveur Service d'authentification fédérée.

Codes de journal
[S001] ACCESS DENIED: User [{0}] is not a member of Administrators group
[S002] ACCESS DENIED: User [{0}] is not an Administrator of Role [{1}]
[S003] Administrator [{0}] setting Maintenance Mode to [{1}]
[S004] Administrator [{0}] enrolling with CA [{1}] templates [{2} and {3}]
[S005] Administrator [{0}] de-authorizing CA [{1}]
[S006] Administrator [{0}] creating new Certificate Definition [{1}]
[S006] Administrator [{0}] creating new Certificate Definition [{1}]
[S008] Administrator [{0}] deleting Certificate Definition [{1}]
[S009] Administrator [{0}] creating new Role [{1}]
[S010] Administrator [{0}] updating Role [{1}]
[S011] Administrator [{0}] deleting Role [{1}]
[S012] Administrator [{0}] creating certificate [upn: {0} sid: {1} role: {2}][Certificate Definition: {3}]
[S013] Administrator [{0}] deleting certificates [upn: {0} role: {1} Certificate Definition: {2}]

Codes de journal
[S401] Performing configuration upgrade – [From version {0}][to version {1}]
[S402] ERROR: The Citrix Federated Authentication Service must be run as Network Service [currently running as: {0}]

Création d'assertions d'identité [Service d'authentification fédérée]

Ces événements sont journalisés au moment de l'exécution sur le serveur du Service d'authentification fédérée lorsqu'un serveur approuvé assume l'ouverture de session d'un utilisateur.

Codes de journal
[S101] Server [{0}] is not authorized to assert identities in role [{1}]
[S102] Server [{0}] failed to assert UPN [{1}] (Exception: {2}{3})
[S103] Server [{0}] requested UPN [{1}] SID {2}, but lookup returned SID {3}
[S104] Server [{0}] failed to assert UPN [{1}] (UPN not allowed by role [{2}])
[S105] Server [{0}] issued identity assertion [upn: {0}, role {1}, Security Context: [{2}]
[S120] Issuing certificate to [upn: {0} role: {1} Security Context: [{2}]]
[S121] Issuing certificate to [upn: {0} role: {1}] on behalf of account {2}
[S122] Warning: Server is overloaded [upn: {0} role: {1}][Requests per minute {2}].

Agissant en tant que partie de confiance [Service d'authentification fédérée]

Ces événements sont journalisés au moment de l'exécution sur le serveur du Service d'authentification fédérée lorsqu'un VDA connecte un utilisateur.

Codes de journal
[S201] Relying party [{0}] does not have access to a password.
[S202] Relying party [{0}] does not have access to a certificate.
[S203] Relying party [{0}] does not have access to the Logon CSP
[S204] Relying party [{0}] accessing the Logon CSP [Operation: {1}]
[S205] Calling account [{0}] is not a relying party in role [{1}]

Codes de journal
[S206] Calling account [{0}] is not a relying party
[S207] Relying party [{0}] asserting identity [upn: {1}] in role: [{2}]
[S208] Private Key operation failed [Operation: {0}][upn: {1} role: {2} certificateDefinition {3}][Error {4} {5}].

Serveur de certificats dans la session [Service d'authentification fédérée]

Ces événements sont journalisés sur le serveur du Service d'authentification fédérée lorsqu'un utilisateur utilise un certificat dans la session.

Codes de journal
[S301] Access Denied: User [{0}] does not have access to a Virtual Smart Card
[S302] User [{0}] requested unknown Virtual Smart Card [thumbprint: {1}]
[S303] User [{0}] does not match Virtual Smart Card [upn: {1}]
[S304] User [{1}] running program [{2}] on computer [{3}] using Virtual Smart Card [upn: {4} role: {5}] for private key operation: [{6}]
[S305] Private Key operation failed [Operation: {0}][upn: {1} role: {2} containerName {3}][Error {4} {5}].

Ouverture de session [VDA]

[Source de l'événement : Citrix.Authentication.IdentityAssertion]

Ces événements sont journalisés sur le VDA durant la phase d'ouverture de session.

Codes de journal
[S101] Identity Assertion Logon failed. Unrecognised Federated Authentication Service [id: {0}]
[S102] Identity Assertion Logon failed. Could not lookup SID for {0} [Exception: {1}{2}]
[S103] Identity Assertion Logon failed. User {0} has SID {1}, expected SID {2}
[S104] Identity Assertion Logon failed. Failed to connect to Federated Authentication Service: {0} [Error: {1} {2}]
[S105] Identity Assertion Logon. Logging in [Username: {0}][Domain: {1}]

Codes de journal
[S106] Identity Assertion Logon. Logging in [Certificate: {0}]
[S107] Identity Assertion Logon failed. [Exception: {1}{2}]
[S108] Identity Assertion Subsystem. ACCESS_DENIED [Caller: {0}]

Certificats dans la session [VDA]

Ces événements sont journalisés sur le VDA lorsqu'un utilisateur tente d'utiliser un certificat dans la session.

Codes de journal
[S201] Virtual Smart Card Authorized [User: {0}][PID: {1} Name:{2}][Certificate {3}]
[S202] Virtual Smart Card Subsystem. No smart cards available in session {0}
[S203] Virtual Smart Card Subsystem. Access Denied [caller: {0}, session {1}, expected: {2}]
[S204] Virtual Smart Card Subsystem. Smart card support disabled.

Demande de certificat et génération de codes [Service d'authentification fédérée]

[Source de l'événement : Citrix.TrustFabric]

Ces événements de bas niveau sont journalisés lorsque le serveur du Service d'authentification fédérée effectue des opérations cryptographiques au niveau du journal.

Codes de journal
[S0001]TrustArea::TrustArea: Installed certificate chain
[S0002]TrustArea::Join: Callback has authorized an untrusted certificate
[S0003]TrustArea::Join: Joining to a trusted server
[S0004]TrustArea::Maintain: Renewed certificate
[S0005]TrustArea::Maintain: Retrieved new certificate chain
[S0006]TrustArea::Export: Exporting private key
[S0007]TrustArea::Import: Importing Trust Area
[S0008]TrustArea::Leave: Leaving Trust Area

Codes de journal
[S0009]TrustArea::SecurityDescriptor: Setting Security Descriptor
[S0010]CertificateVerification: Installing new trusted certificate
[S0011]CertificateVerification: Uninstalling expired trusted certificate
[S0012]TrustFabricHttpClient: Attempting single sign-on to {0}
[S0013]TrustFabricHttpClient: Explicit credentials entered for {0}
[S0014]Pkcs10Request::Create: Created PKCS10 request
[S0015]Pkcs10Request::Renew: Created PKCS10 request
[S0016]PrivateKey::Create
[S0017]PrivateKey::Delete
[S0018]TrustArea::TrustArea: Waiting for Approval
[S0019]TrustArea::Join: Delayed Join
[S0020]TrustArea::Join: Delayed Join
[S0021]TrustArea::Maintain: Installed certificate chain

Codes de journal
[S0101]TrustAreaServer::Create root certificate
[S0102]TrustAreaServer::Subordinate: Join succeeded
[S0103]TrustAreaServer::PeerJoin: Join succeeded
[S0104]MicrosoftCertificateAuthority::GetCredentials: Authorized to use {0}
[S0104]MicrosoftCertificateAuthority::SubmitCertificateRequest Error {0}
[S0105]MicrosoftCertificateAuthority::SubmitCertificateRequest Issued cert {0}
[S0106]MicrosoftCertificateAuthority::PublishCRL: Published CRL
[S0107]MicrosoftCertificateAuthority::ReissueCertificate Error {0}
[S0108]MicrosoftCertificateAuthority::ReissueCertificate Issued Cert {0}
[S0109]MicrosoftCertificateAuthority::CompleteCertificateRequest - Still waiting for approval
[S0110]MicrosoftCertificateAuthority::CompleteCertificateRequest - Pending certificate refused
[S0111]MicrosoftCertificateAuthority::CompleteCertificateRequest Issued certificate
[S0112]MicrosoftCertificateAuthority::SubmitCertificateRequest - Waiting for approval

Codes de journal
[S0120]NativeCertificateAuthority::SubmitCertificateRequest Issued cert {0}
[S0121]NativeCertificateAuthority::SubmitCertificateRequest Error
[S0122]NativeCertificateAuthority::RootCARollover New root certificate
[S0123]NativeCertificateAuthority::ReissueCertificate New certificate
[S0124]NativeCertificateAuthority::RevokeCertificate
[S0125]NativeCertificateAuthority::PublishCRL

Informations connexes

- Les déploiements FAS courants sont décrits dans l'article Vue d'ensemble des architectures du Service d'authentification fédérée.
- Des informations pratiques sont disponibles dans l'article Configuration et gestion du Service d'authentification fédérée.

Vue d'ensemble des architectures du Service d'authentification fédérée

January 23, 2019

Introduction

Le Service d'authentification fédérée (FAS) est un composant Citrix qui s'intègre avec votre autorité de certification (CA) Active Directory, qui permet aux utilisateurs d'être authentifiés dans un environnement Citrix. Ce document présente les différentes architectures d'authentification susceptibles d'être appropriées à votre déploiement.

Lorsqu'il est activé, le FAS délègue l'authentification utilisateur aux serveurs StoreFront approuvés. StoreFront est doté d'un ensemble complet d'options d'authentification articulées autour de technologies Web modernes. En outre, il peut être étendu facilement grâce au SDK StoreFront ou à des plug-ins IIS tiers. L'objectif de base est que toute technologie d'authentification qui peut authentifier un utilisateur sur un site Web peut maintenant être utilisée pour la connexion à un déploiement Citrix XenApp ou XenDesktop.

Ce document décrit certaines architectures de déploiement de haut niveau, par complexité croissante.

- Déploiement interne

- Déploiement NetScaler Gateway
- ADFS SAML
- Mappage de compte B2B
- Jonction à un domaine Azure AD (Azure AD Join) avec Windows 10

Des liens vers les articles FAS sont fournis. Pour toutes les architectures, l'article Service d'authentification fédérée est le document de référence principal pour la configuration du FAS.

Fonctionnement

Le FAS est autorisé à émettre des certificats de classe de carte à puce automatiquement à la place des utilisateurs Active Directory qui sont authentifiés par StoreFront. Il utilise des API similaires aux outils qui permettent aux administrateurs de provisionner des cartes à puce physiques.

Lorsqu'un utilisateur est connecté à un VDA Citrix XenApp ou XenDesktop, le certificat est attaché à la machine, et le domaine Windows interprète l'ouverture de session en tant qu'authentification par carte à puce standard.

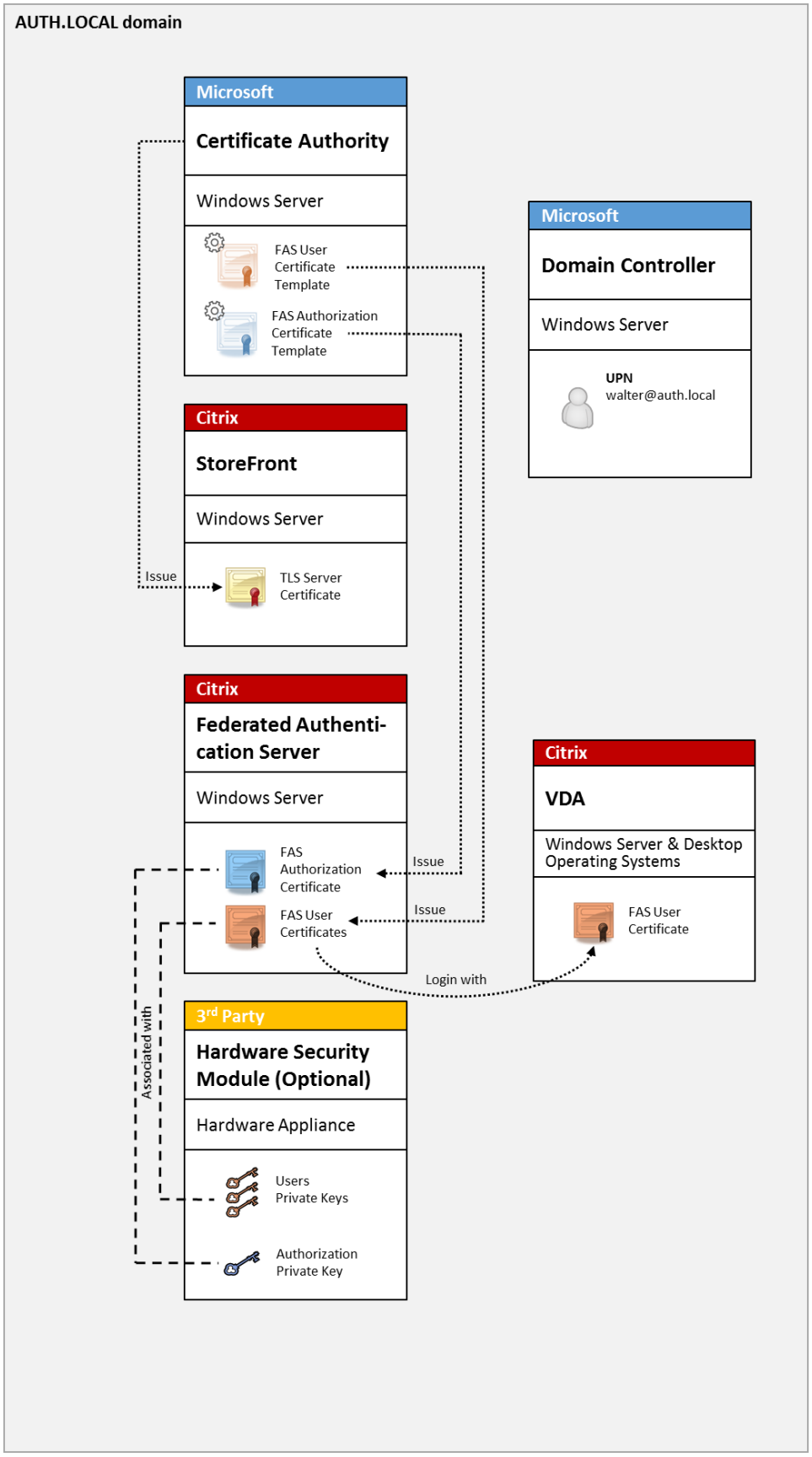
Déploiement interne

Le FAS permet aux utilisateurs de s'authentifier en toute sécurité auprès de StoreFront à l'aide de plusieurs options d'authentification (y compris l'authentification unique Kerberos) et de se connecter à une session Citrix HDX authentifiée.

Cela rend possible l'authentification Windows sans invite de saisie d'informations d'identification ou de codes PIN de carte à puce et sans l'utilisation de fonctionnalités de « gestion des mots de passe enregistrés » telles que le service Single Sign-On. Cela peut être utilisé pour remplacer les fonctionnalités d'ouverture de session de la délégation Kerberos contrainte disponibles dans les versions précédentes de XenApp.

Tous les utilisateurs ont accès aux certificats PKI dans leur session, qu'ils se soient connectés ou non aux machines de point de terminaison avec une carte à puce. Ceci permet une migration fluide vers des modèles d'authentification à deux facteurs, et ce, même à partir de périphériques tels que des smartphones et tablettes qui ne disposent pas d'un lecteur de carte à puce.

Ce déploiement ajoute un nouveau serveur exécutant le FAS, qui est autorisé à émettre des certificats de classe de carte à puce pour le compte d'utilisateurs. Ces certificats sont alors utilisés pour se connecter à des sessions utilisateur dans un environnement Citrix HDX comme si une ouverture de session par carte à puce était utilisée.



L'environnement XenApp ou XenDesktop doit être configuré de la même manière que l'ouverture de session par carte à puce à, ce qui est décrit dans l'article CTX206156.

Dans un déploiement existant, cela implique généralement de s'assurer qu'une autorité de certification (CA) Microsoft appartenant au domaine soit disponible, et que des certificats de contrôleur de domaine ont été attribués aux contrôleurs de domaine. (Consultez la section « Émission de certificats de contrôleur de domaine » dans l'article CTX206156).

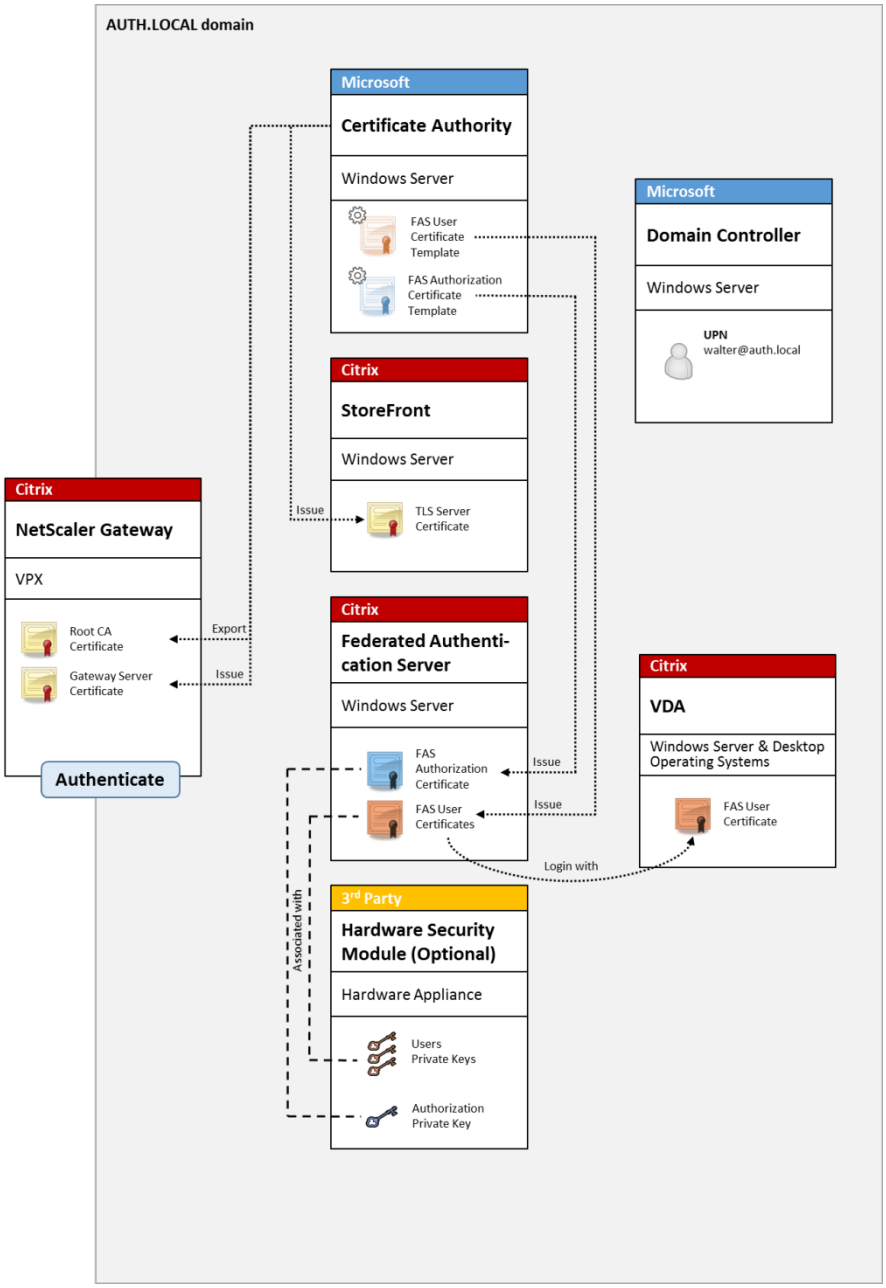
Informations connexes :

- Les clés peuvent être stockées dans un module de sécurité matériel (HSM) ou un module de plateforme sécurisée (TPM). Pour de plus amples informations, consultez l'article Protection des clés privées du Service d'authentification fédérée.
- L'article Service d'authentification fédérée décrit comment installer et configurer le FAS.

Déploiement NetScaler Gateway

Le déploiement NetScaler est similaire au déploiement interne, mais ajoute Citrix NetScaler Gateway couplé avec StoreFront, et déplace le point principal d'authentification sur NetScaler. Citrix NetScaler comprend des options d'authentification et d'autorisation avancées qui peuvent être utilisées pour sécuriser l'accès à distance aux sites Web d'une entreprise.

Ce déploiement peut être utilisé pour éviter l'affichage de plusieurs invites de saisie de code PIN qui se produisent lors de l'authentification auprès de NetScaler, puis de la connexion à une session utilisateur. Il permet également d'utiliser les technologies d'authentification NetScaler avancées sans nécessiter de mots de passe Active Directory ou de cartes à puce.

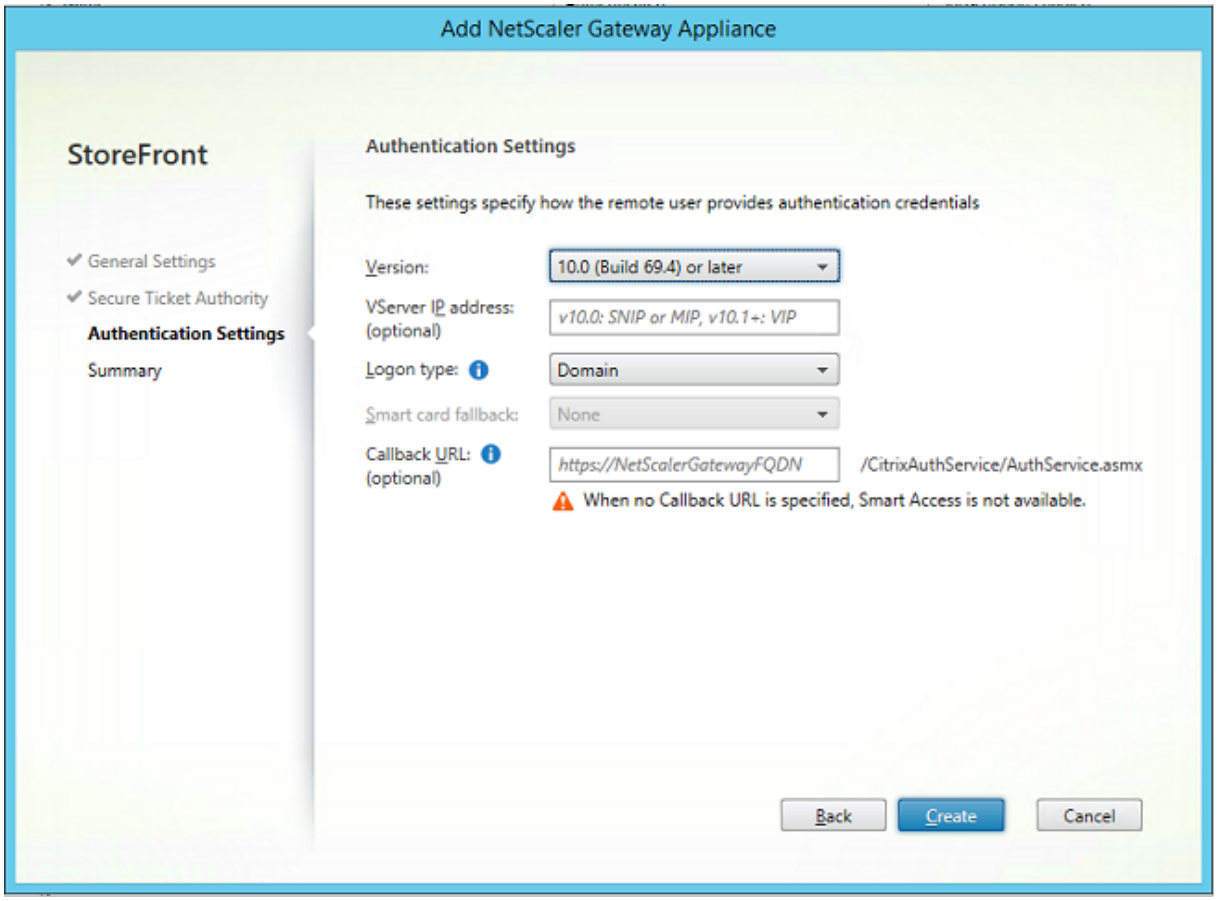


L'environnement XenApp ou XenDesktop doit être configuré de la même manière que l'ouverture de session par carte à puce à, ce qui est décrit dans l'article CTX206156.

Dans un déploiement existant, cela implique généralement de s'assurer qu'une autorité de certification (CA) Microsoft appartenant au domaine soit disponible, et que des certificats de contrôleur de domaine ont été attribués aux contrôleurs de domaine. (Consultez la section « Émission de certificats de contrôleur de domaine » dans l'article CTX206156).

Lors de la configuration de NetScaler Gateway en tant que système d'authentification principal, assurez-vous que toutes les connexions entre NetScaler et StoreFront sont sécurisées à l'aide du protocole TLS. En particulier, assurez-vous que l'URL de rappel est correctement configurée pour

pointer vers le serveur NetScaler, car cela peut être utilisé pour authentifier le serveur NetScaler dans ce déploiement.

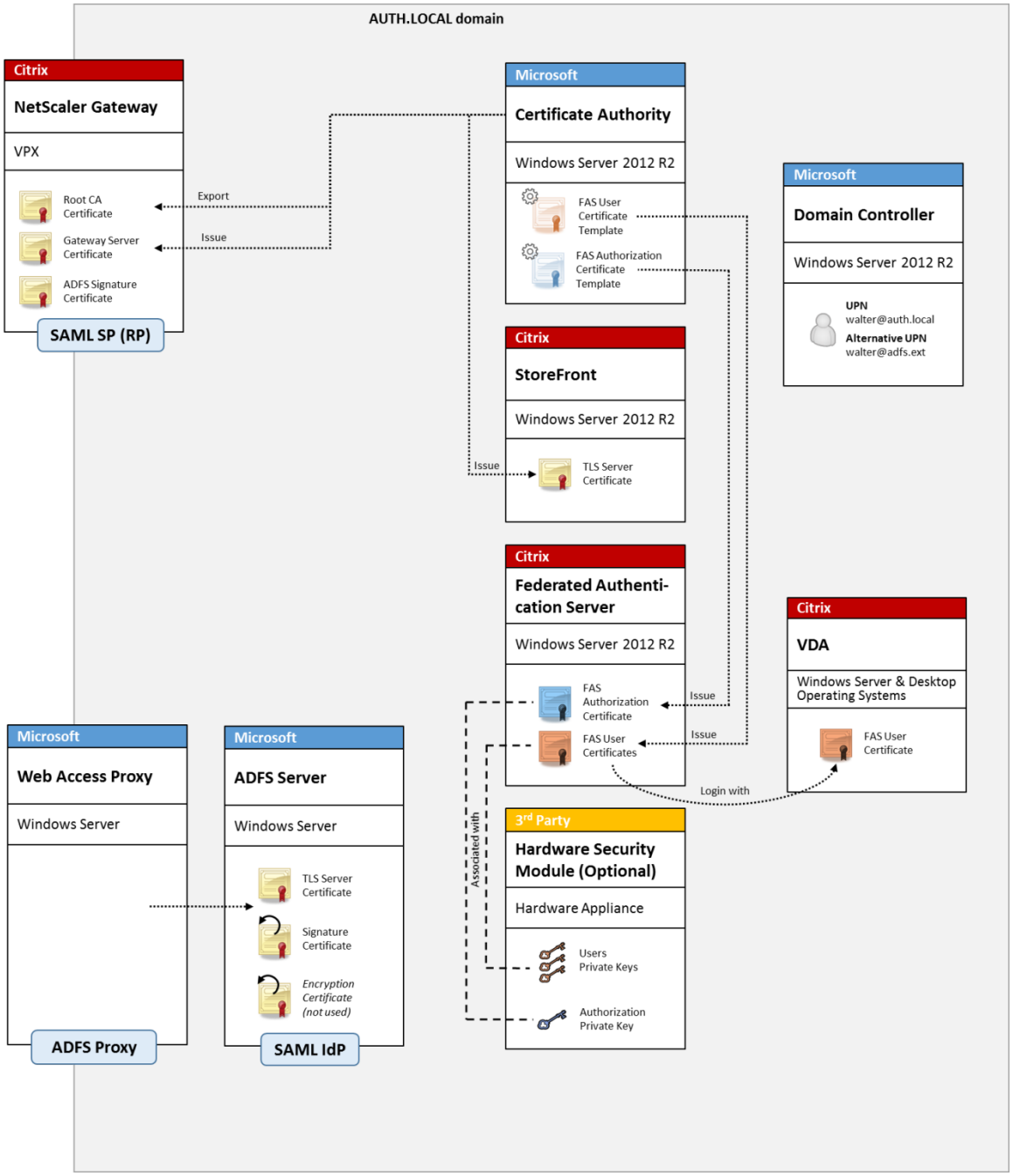


Informations connexes :

- Pour configurer NetScaler Gateway, consultez la section Comment configurer NetScaler Gateway 10.5 pour l'utiliser avec StoreFront 3.6 et XenDesktop 7.6.
- L'article Service d'authentification fédérée décrit comment installer et configurer le FAS.

Déploiement SAML ADFS

Une technologie d'authentification NetScaler clé permet l'intégration avec Microsoft ADFS, qui peut agir en tant que fournisseur d'identité SAML (IdP). Une assertion SAML est un bloc XML signé de manière cryptographique émis par un fournisseur d'identité approuvé qui autorise un utilisateur à ouvrir une session sur un ordinateur. Cela signifie que le serveur FAS permet maintenant de déléguer l'authentification d'un utilisateur au serveur Microsoft ADFS (ou d'autres fournisseurs d'identité SAML).



ADFS est généralement utilisé pour authentifier de manière sécurisée les utilisateurs auprès des ressources d'entreprise à distance via Internet ; par exemple, il est souvent utilisé pour l'intégration à Office 365.

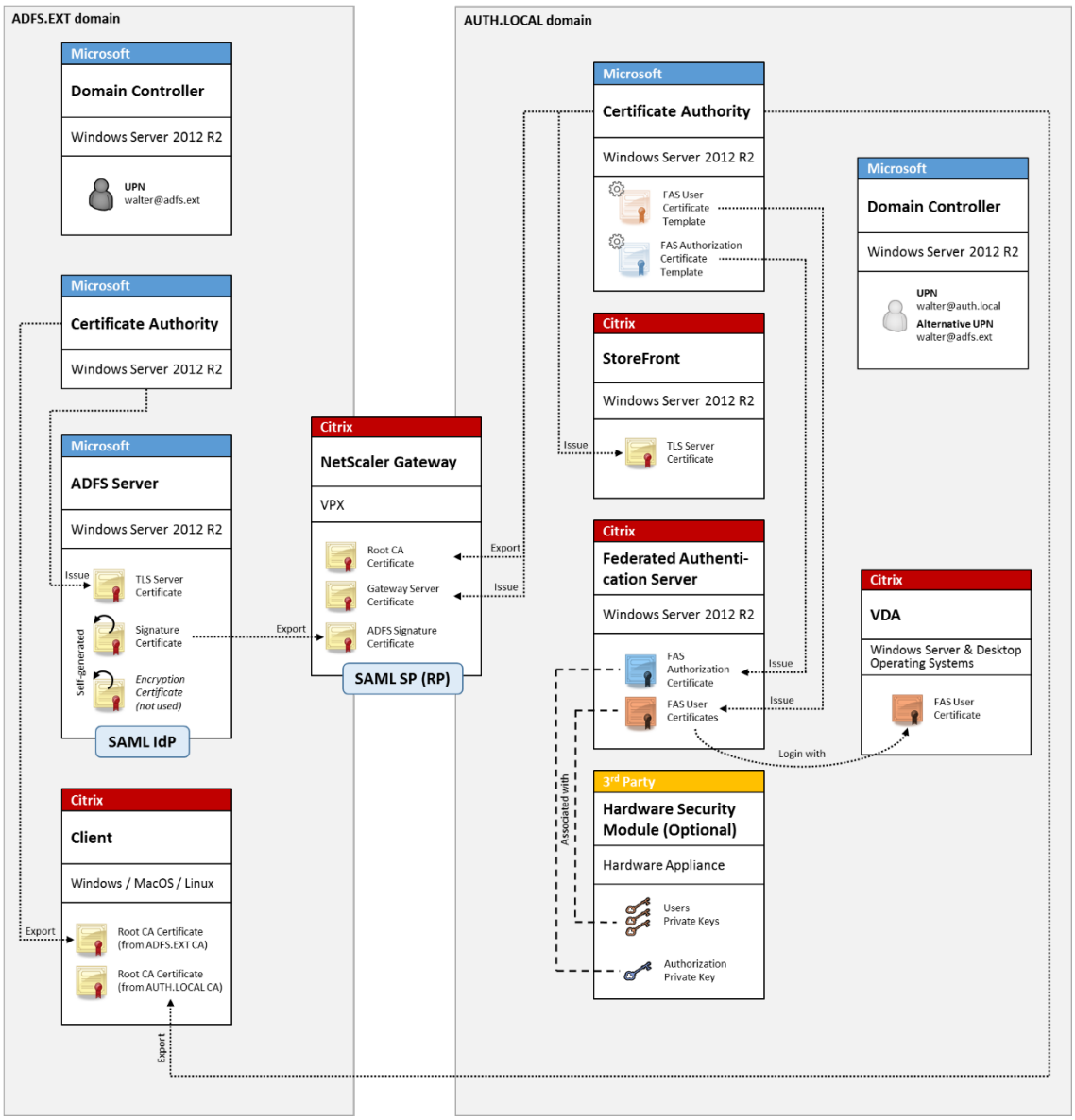
Informations connexes :

- L'article Déploiement ADFS du Service d'authentification fédérée contient des détails.
- L'article Service d'authentification fédérée décrit comment installer et configurer le FAS.
- La section Déploiement NetScaler Gateway dans cet article contient des recommandations en

matière de configuration.

Mappage de compte B2B

Si deux entreprises souhaitent utiliser réciproquement leurs systèmes informatiques, une option courante consiste à configurer un serveur Active Directory Federation Service (ADFS) avec une relation d'approbation. Cela permet aux utilisateurs d'une entreprise de s'authentifier en toute transparence auprès de l'environnement Active Directory (AD) d'une autre entreprise. Lors de l'ouverture de session, chaque utilisateur utilise ses propres informations d'identification d'ouverture de session d'entreprise ; ADFS mappe automatiquement ces dernières à un « compte fantôme » dans l'environnement Active Directory de l'entreprise homologue.

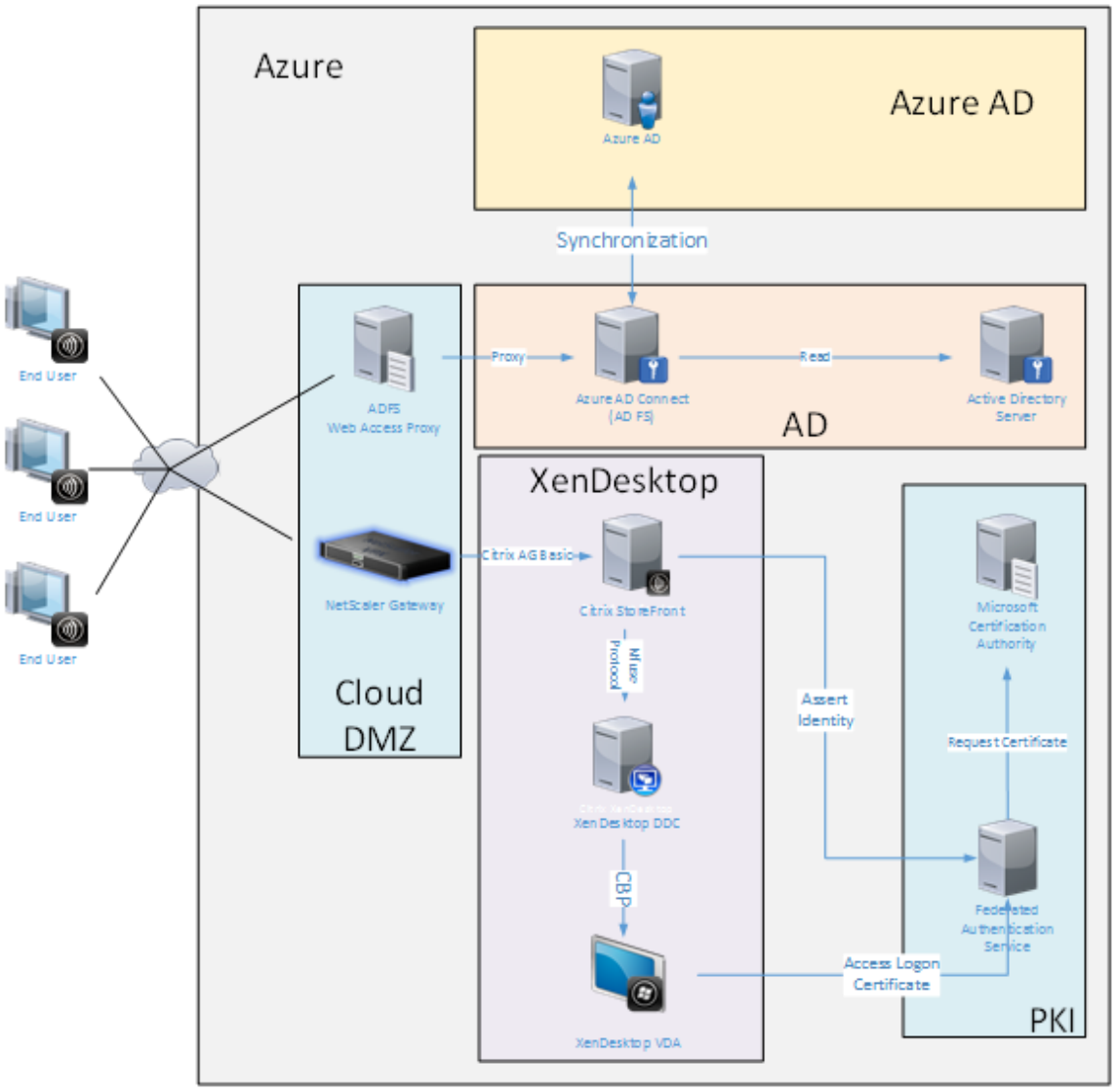


Informations connexes :

- L'article Service d'authentification fédérée décrit comment installer et configurer le FAS.

Jonction à un domaine Azure AD (Azure AD Join) avec Windows 10

Windows 10 a introduit le concept de « Azure AD Join » (Jonction à un domaine Azure AD), qui est d'un point de vue conceptuel similaire à la jointure de domaine Windows traditionnelle mais ciblé pour les scénarios « via Internet ». Ce concept convient tout particulièrement aux ordinateurs portables et tablettes. Comme avec la jonction de domaine Windows traditionnelle, Azure AD est équipé de fonctionnalités permettant d'utiliser des modèles d'authentification unique pour la connexion aux sites Web et aux ressources de l'entreprise. Ces derniers sont tous « compatibles Internet », ils fonctionnent donc à partir de n'importe quel emplacement connecté à Internet, et pas seulement sur le réseau local du bureau.



Ce déploiement est un exemple dans lequel il n'existe pas de concept « utilisateurs au bureau. » Les ordinateurs portables sont inscrits et s'authentifient via Internet à l'aide des fonctionnalités modernes d'Azure AD.

Veuillez noter que l'infrastructure dans ce déploiement peut s'exécuter partout où une adresse IP est disponible : en interne, fournisseur hébergé, Azure ou un autre fournisseur de cloud. Le synchronisateur Azure AD Connect se connectera automatiquement à Azure AD. Le graphique utilise des VM Azure à des fins de simplicité.

Informations connexes :

- L'article Service d'authentification fédérée décrit comment installer et configurer le FAS.
- L'article Intégration d'Azure AD au Service d'authentification fédérée contient des détails.

Déploiement ADFS du Service d'authentification fédérée

January 23, 2019

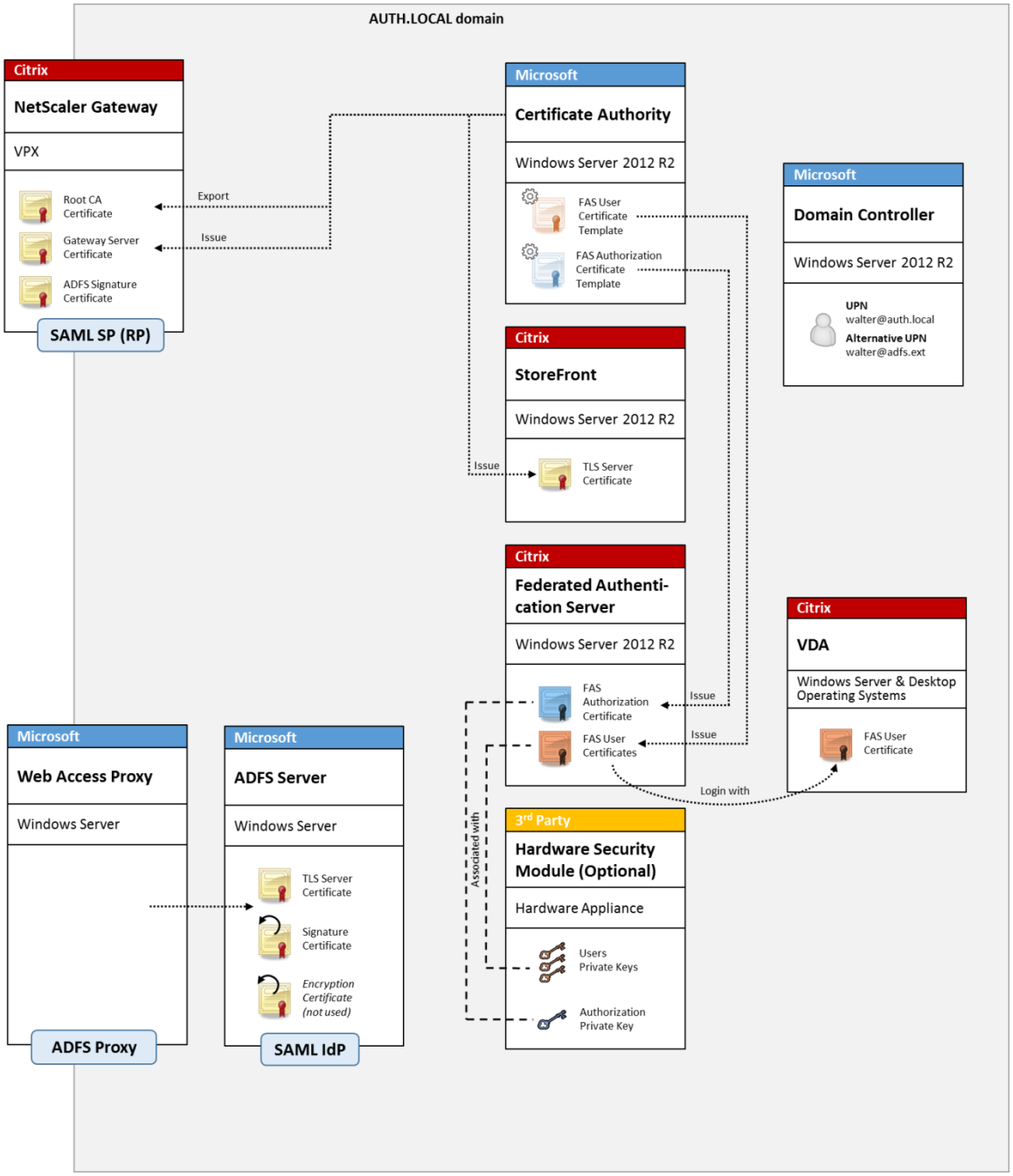
Introduction

Ce document décrit comment intégrer un environnement Citrix avec Microsoft ADFS.

De nombreuses organisations utilisent ADFS pour gérer l'accès sécurisé aux sites Web qui requièrent un seul point d'authentification. Par exemple, une entreprise peut disposer de contenu et de téléchargements supplémentaires disponibles pour les employés ; ces emplacements doivent être protégés avec des informations d'identification d'ouverture de session Windows standard.

Le Service d'authentification fédérée (FAS) permet également d'intégrer Citrix NetScaler et Citrix StoreFront avec le système d'ouverture de session ADFS, ce qui réduit toute confusion potentielle pour le personnel de l'entreprise.

Ce déploiement intègre NetScaler en tant que partie de confiance pour Microsoft ADFS.



Présentation SAML

SAML (Security Assertion Markup Language) est un système d'ouverture de session sur navigateur Web de « redirection vers une page d'ouverture de session ». La configuration comprend les éléments suivants :

URL de redirection [URL du service Single Sign-On]

Lorsque NetScaler découvre qu'un utilisateur a besoin d'être authentifié, il indique au navigateur Web de l'utilisateur d'utiliser un HTTP POST vers une page Web d'ouverture de session SAML sur le serveur ADFS. C'est généralement une adresse `https://` au format : `https://adfs.mycompany.com/adfs/ls`.

Cette page Web POST comprend d'autres informations, notamment « l'adresse de retour » à laquelle ADFS renverra l'utilisateur lorsque l'ouverture de session est terminée.

Identificateur [Nom de l'émetteur/EntityID]

EntityId est un identificateur unique que NetScaler inclut dans ses données POST à ADFS. Il renseigne ADFS sur le service auquel l'utilisateur tente de se connecter et applique différentes stratégies d'authentification le cas échéant. S'il est émis, le fichier XML d'authentification SAML pourra uniquement être utilisé pour ouvrir une session sur le service identifié par EntityId.

En règle générale, EntityID est l'adresse URL de la page d'ouverture de session du serveur NetScaler, mais une quelconque autre adresse peut être utilisée, à condition que NetScaler et ADFS l'acceptent : `https://ns.mycompany.com/application/logonpage`.

Adresse de retour [URL de réponse]

Si l'authentification réussit, ADFS indique au navigateur Web de l'utilisateur de publier un fichier ADFS d'authentification SAML sur l'une des URL de réponse qui sont configurées pour EntityId. Il s'agit généralement d'une adresse `https://` sur le serveur NetScaler d'origine au format : `https://ns.mycompany.com/cgi/samlauth`.

S'il existe plusieurs URL de réponse configurées, NetScaler peut en choisir une dans sa publication d'origine sur ADFS.

Certificat de signature [Certificat IDP]

ADFS signe de manière cryptographique les objets blob XML d'authentification SAML à l'aide de sa clé privée. Pour valider cette signature, NetScaler doit être configuré pour vérifier ces signatures à l'aide de la clé publique incluse dans un fichier de certificat. Le fichier de certificat sera généralement un fichier texte obtenu à partir du serveur ADFS.

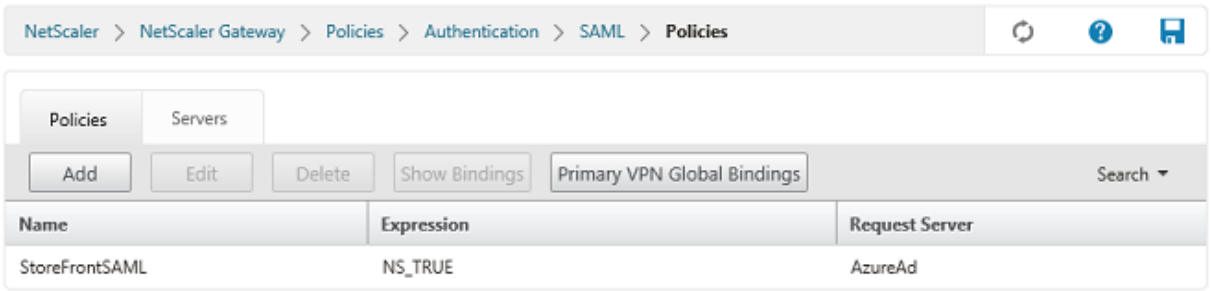
URL d'authentification unique [URL de déconnexion unique]

ADFS et NetScaler prennent en charge un système de « déconnexion centrale ». Il s'agit d'une adresse URL que NetScaler interroge parfois pour vérifier que l'objet blob XML d'authentification SAML représente toujours une session actuellement connectée.

Cette fonctionnalité est facultative et n'a pas besoin d'être configurée. C'est généralement une adresse `https://` au format `https://adfs.mycompany.com/adfs/logout`. (Notez que cette dernière peut être la même que l'URL d'ouverture de session unique).

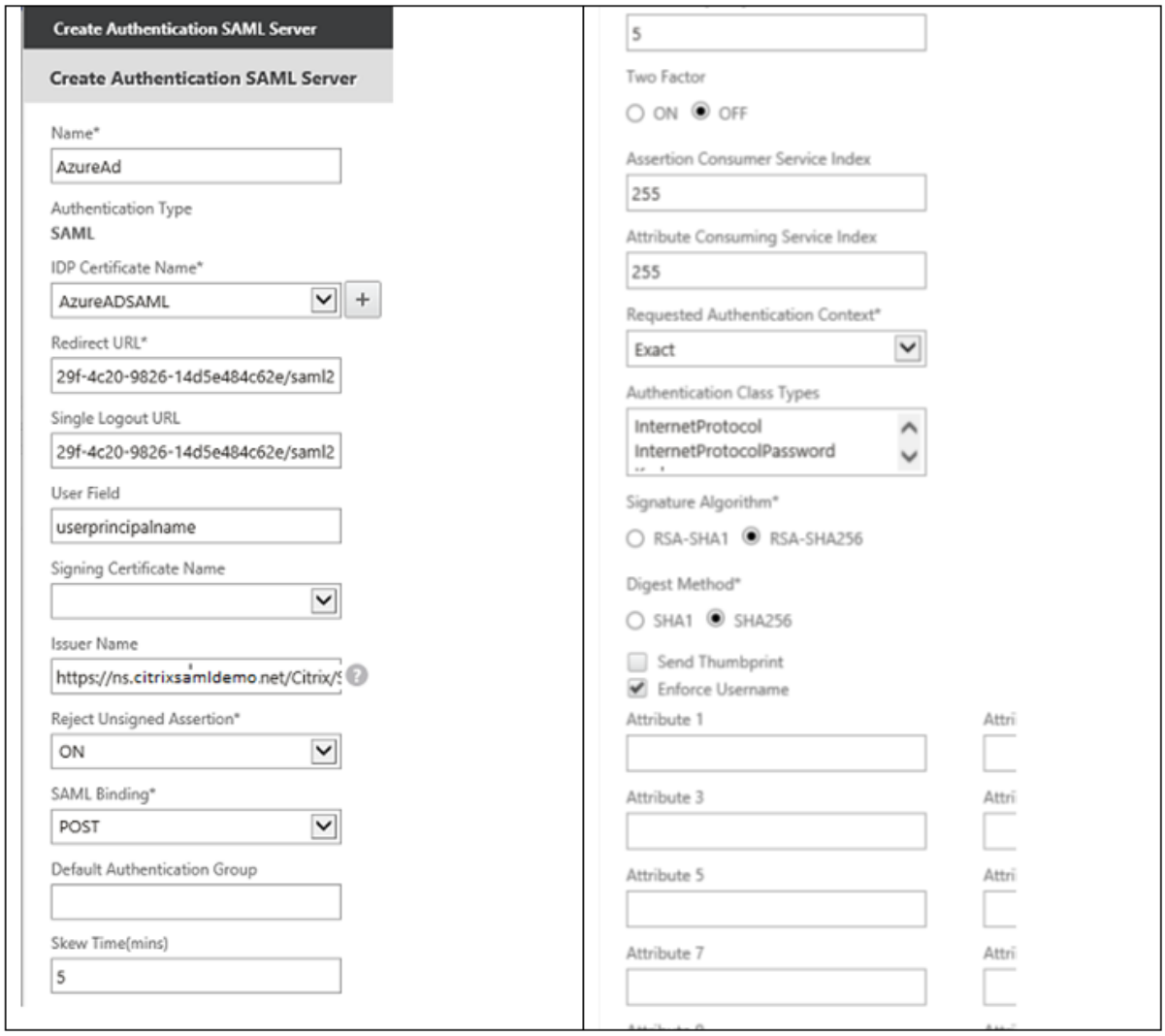
Configuration

La section Déploiement NetScaler Gateway de l'article Architectures du Service d'authentification fédérée explique comment configurer NetScaler Gateway afin de gérer les options d'authentification LDAP standard, à l'aide de l'assistant d'installation de XenApp et XenDesktop NetScaler. Une fois la configuration terminée, vous pouvez créer une nouvelle stratégie d'authentification sur NetScaler qui autorise l'authentification SAML. Cela peut remplacer la stratégie LDAP par défaut utilisée par l'assistant d'installation de NetScaler.



Renseigner la stratégie SAML

Configurez le nouveau serveur IdP SAML à l'aide des informations obtenues précédemment dans la console de gestion ADFS. Lorsque cette stratégie est appliquée, NetScaler redirige l'utilisateur vers ADFS pour l'ouverture de session, et accepte un jeton d'authentification SAML signé par ADFS.



Informations connexes

- L'article Service d'authentification fédérée est le document de référence principal pour obtenir des informations sur l'installation et la configuration du FAS.
- Les déploiements FAS courants sont décrits dans l'article Vue d'ensemble des architectures du Service d'authentification fédérée.
- Des informations pratiques sont disponibles dans l'article Configuration et gestion du Service d'authentification fédérée.

Intégration d'Azure AD au Service d'authentification fédérée

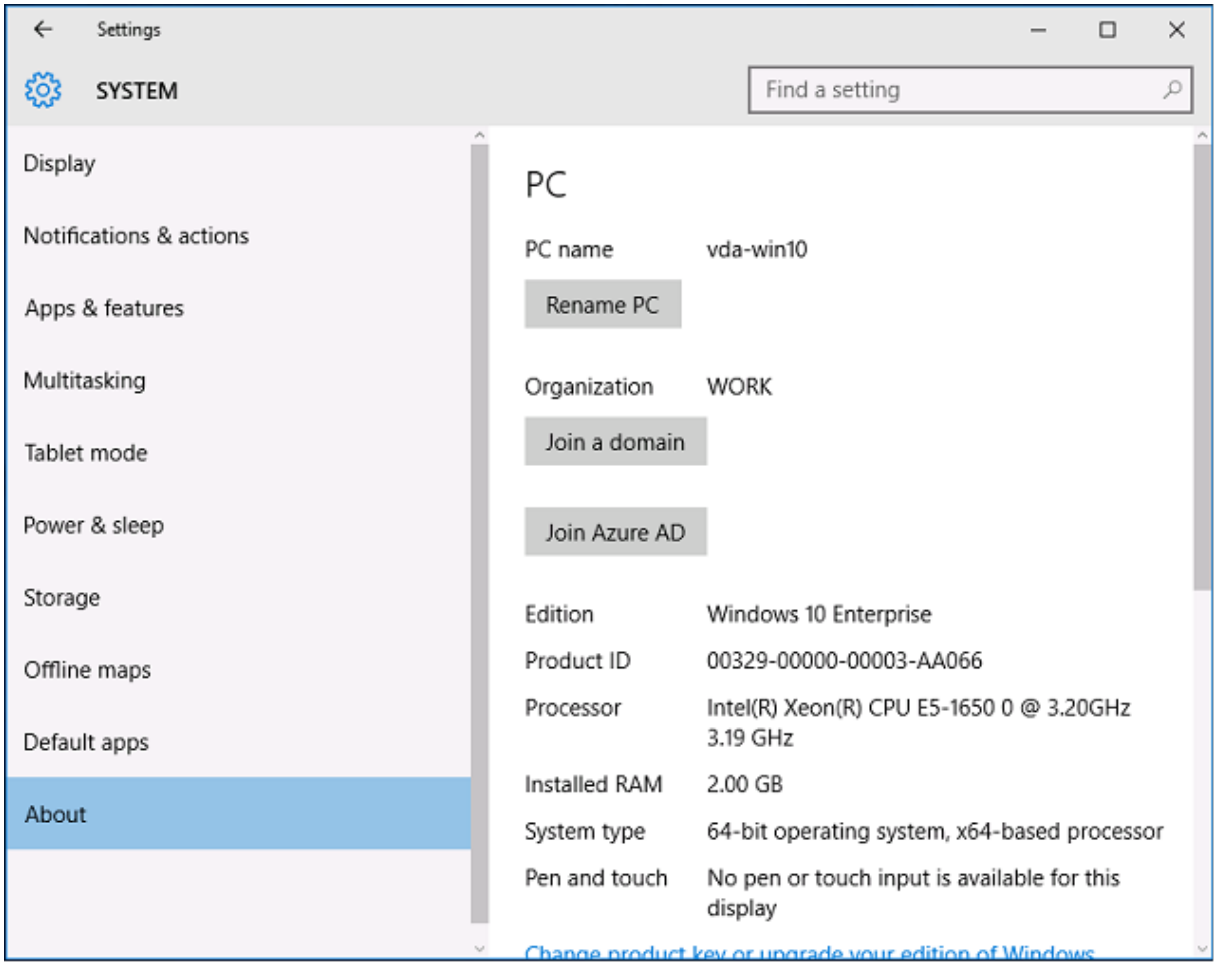
January 23, 2019

Introduction

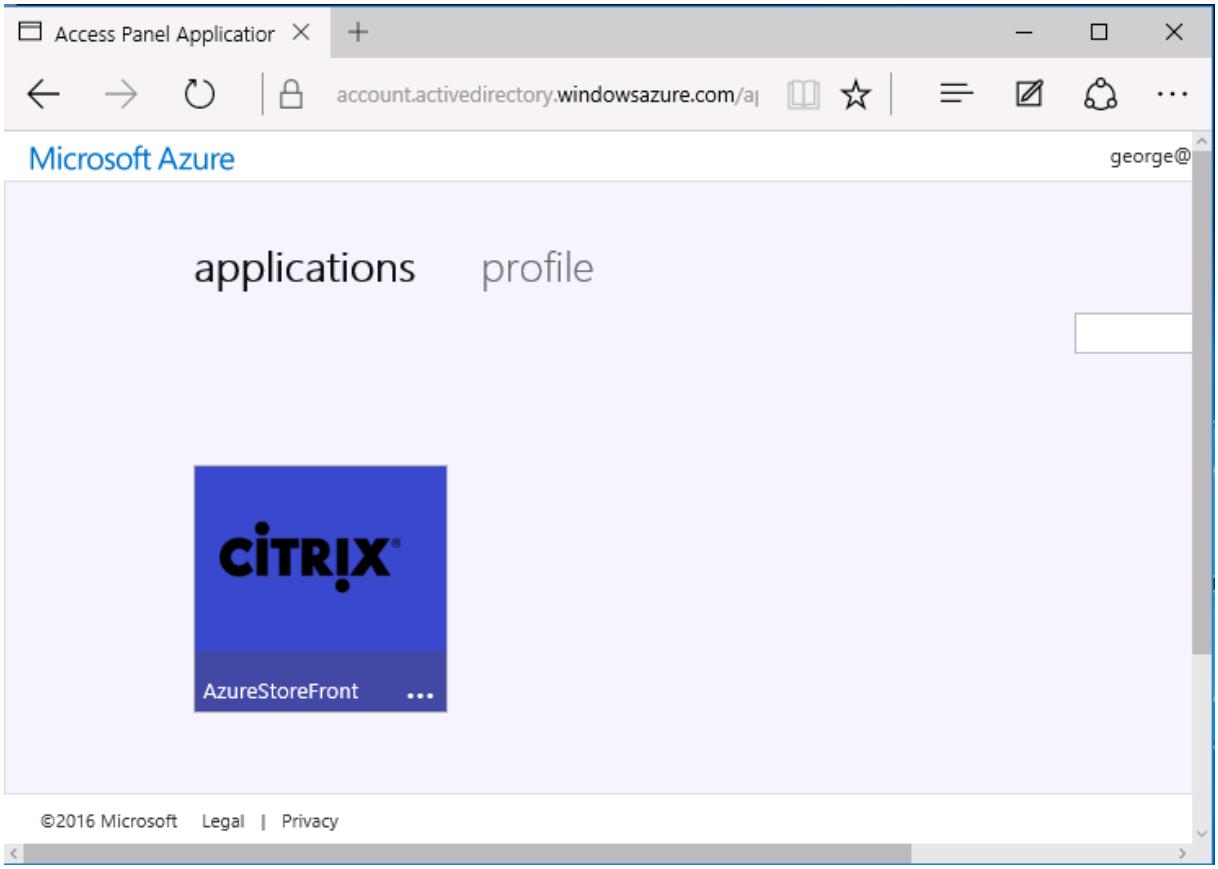
Ce document décrit comment intégrer un environnement Citrix avec la fonctionnalité Azure AD de Windows 10.

Windows 10 a introduit Azure AD, qui est un nouveau modèle de jonction de domaine dans lequel les ordinateurs portables itinérants peuvent être joints à un domaine d'entreprise via Internet à des fins de gestion et d'authentification unique.

L'exemple de déploiement dans ce document décrit un système dans lequel l'informatique fournit aux nouveaux utilisateurs une adresse de messagerie d'entreprise et un code d'inscription pour leurs ordinateurs portables Windows 10 personnels. Les utilisateurs accèdent à ce code via **Système** > **À propos de** > **Connecter à Azure AD** dans le volet **Paramètres**.



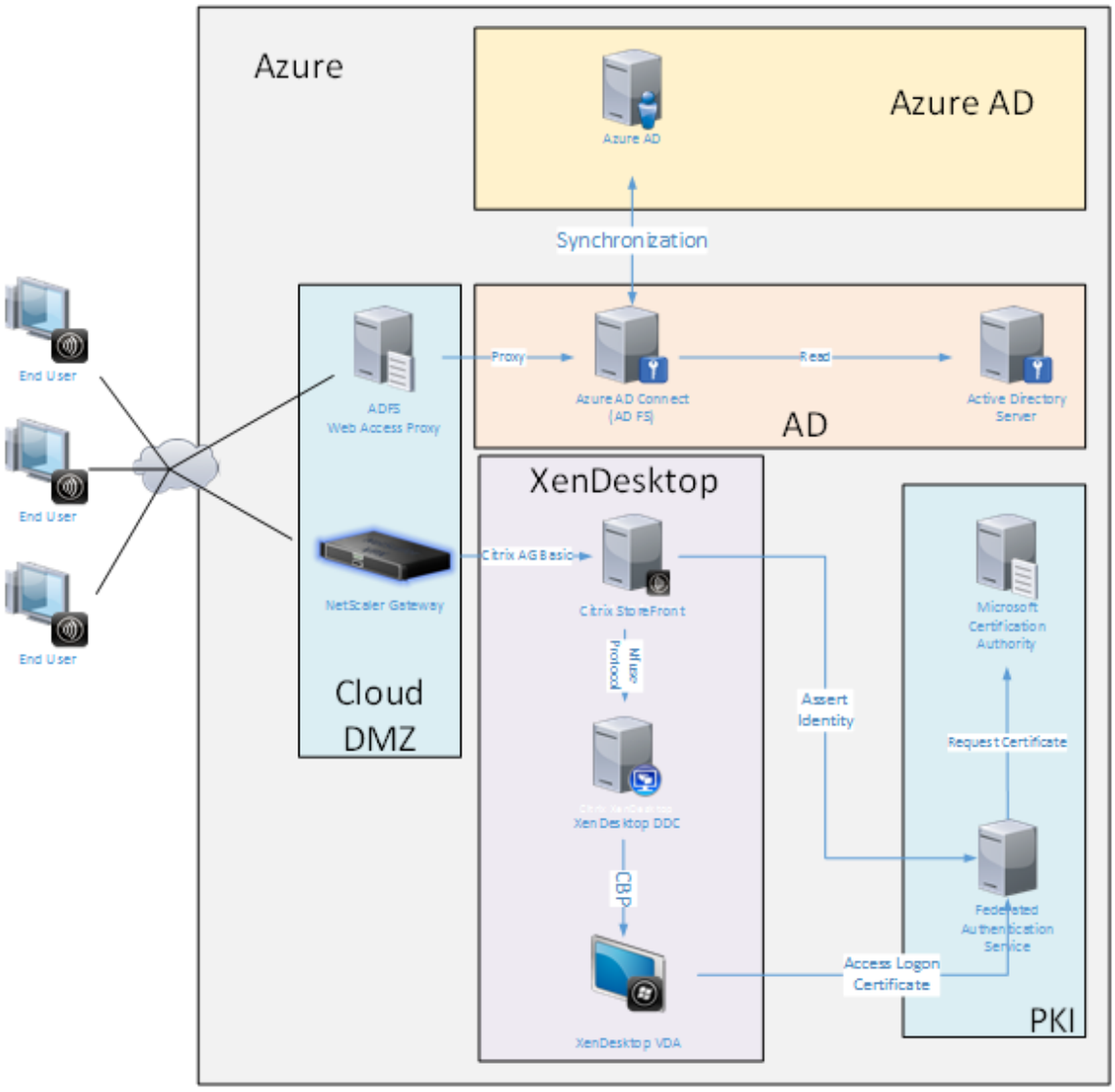
Une fois que l'ordinateur portable est inscrit, le navigateur Web Microsoft Edge se connecte automatiquement aux sites Web de l'entreprise et aux applications publiées Citrix via la page Web d'applications Azure SAAS, avec d'autres applications Azure telles que Microsoft Office 365.



Architecture

Cette architecture réplique un réseau d'entreprise traditionnel dans Azure, tout en intégrant des technologies de cloud modernes telles que Azure AD et Office 365. Les utilisateurs sont considérés comme des travailleurs distants, et la notion d'intranet n'a pas lieu.

Le modèle peut être appliqué aux entreprises disposant déjà de systèmes locaux, car le service de synchronisation Azure AD Connect peut établir un lien à Azure via Internet.



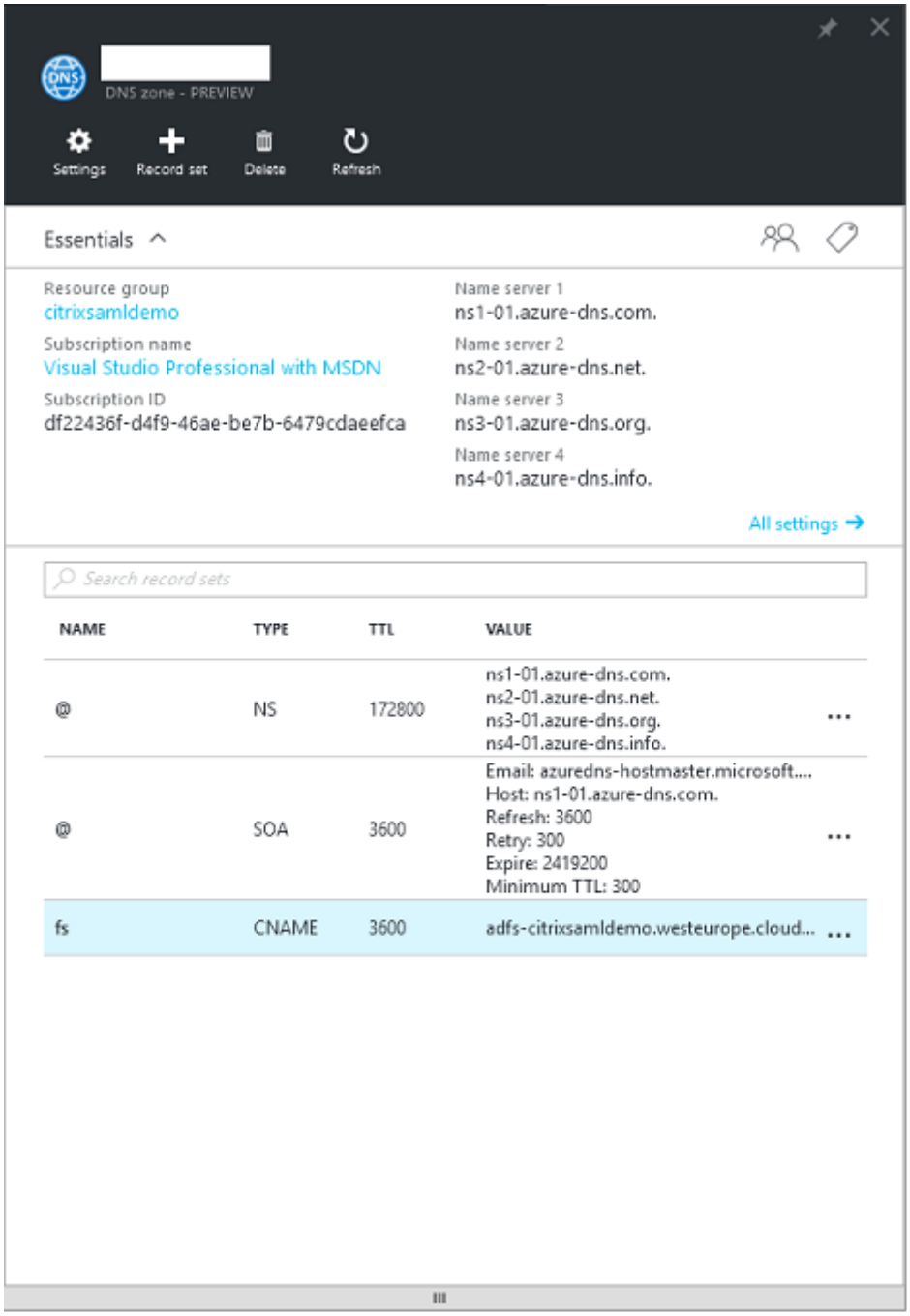
Les connexions sécurisées et l'authentification unique, qui sont traditionnellement derrière un pare-feu sur le LAN et l'authentification NTLM/ Kerberos, sont remplacées dans cette architecture par des connexions TLS à Azure et SAML. Des nouveaux services sont créés à mesure que des applications Azure sont jointes à Azure AD. Les applications existantes qui nécessitent Active Directory (telles qu'une base de données SQL Server) peuvent être exécutées à l'aide d'une VM de serveur Active Directory standard dans la partie IAAS du Azure Cloud Service.

Lorsqu'un utilisateur lance une application traditionnelle, elle est accessible à l'aide des applications publiées XenApp et XenDesktop. Les différents types d'applications sont compilés via la page **Applications Azure** de l'utilisateur, à l'aide des fonctionnalités d'authentification unique de Microsoft Edge. Microsoft fournit également des applications Android et iOS qui peuvent énumérer et lancer des applications Azure.

Créer une zone DNS

Azure AD requiert que l'administrateur ait enregistré une adresse DNS publique et qu'il contrôle la zone de délégation pour le suffixe de nom de domaine. Pour ce faire, l'administrateur peut utiliser la fonctionnalité de zone DNS d'Azure.

Cet exemple utilise le nom de zone DNS « citrixsamldemo.net. »



La console affiche les noms des serveurs de noms DNS Azure. Ces derniers doivent être référencés

dans les entrées NS du bureau d'enregistrement DNS pour la zone (par exemple, citrixsamldemo.net. NS n1-01.azure-dns.com)

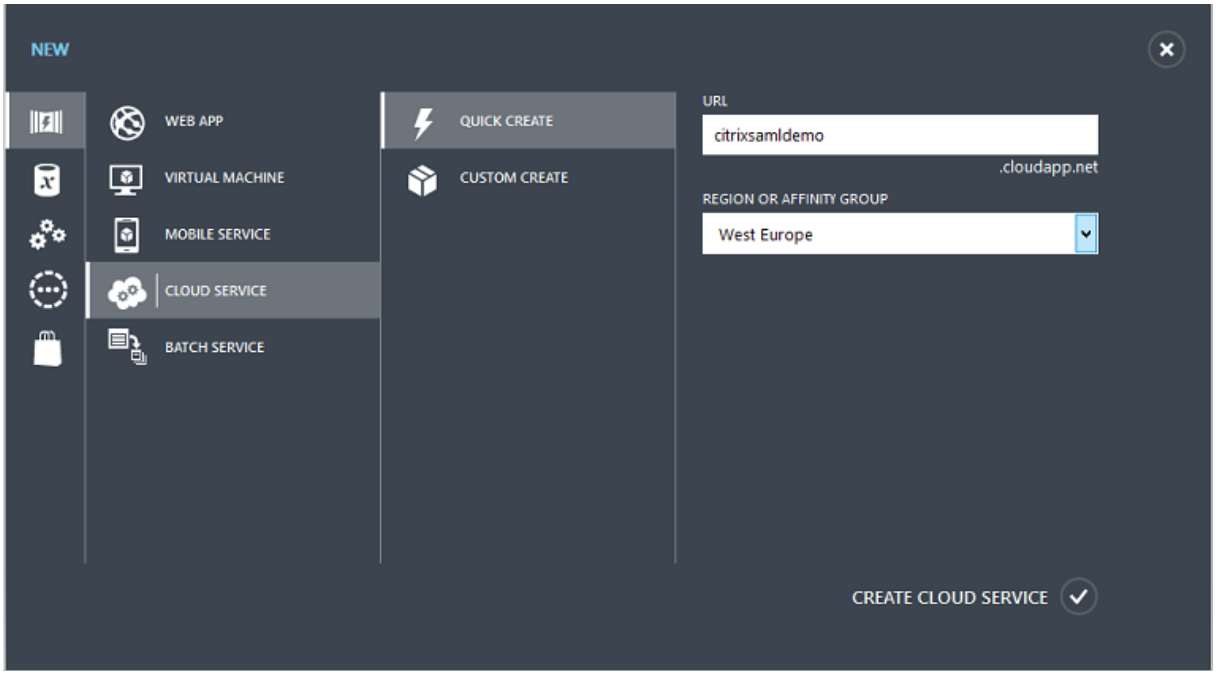
Lors de l'ajout de références aux VM exécutées dans Azure, il est plus facile d'utiliser un pointeur CNAME vers l'enregistrement DNS géré par Azure pour la VM. Si l'adresse IP de la VM change, vous n'aurez pas besoin de mettre à jour manuellement le fichier de la zone DNS.

Les suffixes des adresses DNS internes et externes correspondront pour ce déploiement. Le domaine est citrixsamldemo.net, et utilise un split DNS (10.0.0.* en interne).

Ajoutez une entrée « fs.citrixsamldemo.net » qui fait référence au serveur proxy d'application Web. Il s'agit du service de fédération pour cette zone.

Créer un service de cloud

Cet exemple configure un environnement Citrix comprenant un environnement Active Directory avec un serveur ADFS exécuté dans Azure. Un service de cloud appelé « citrixsamldemo » est créé.

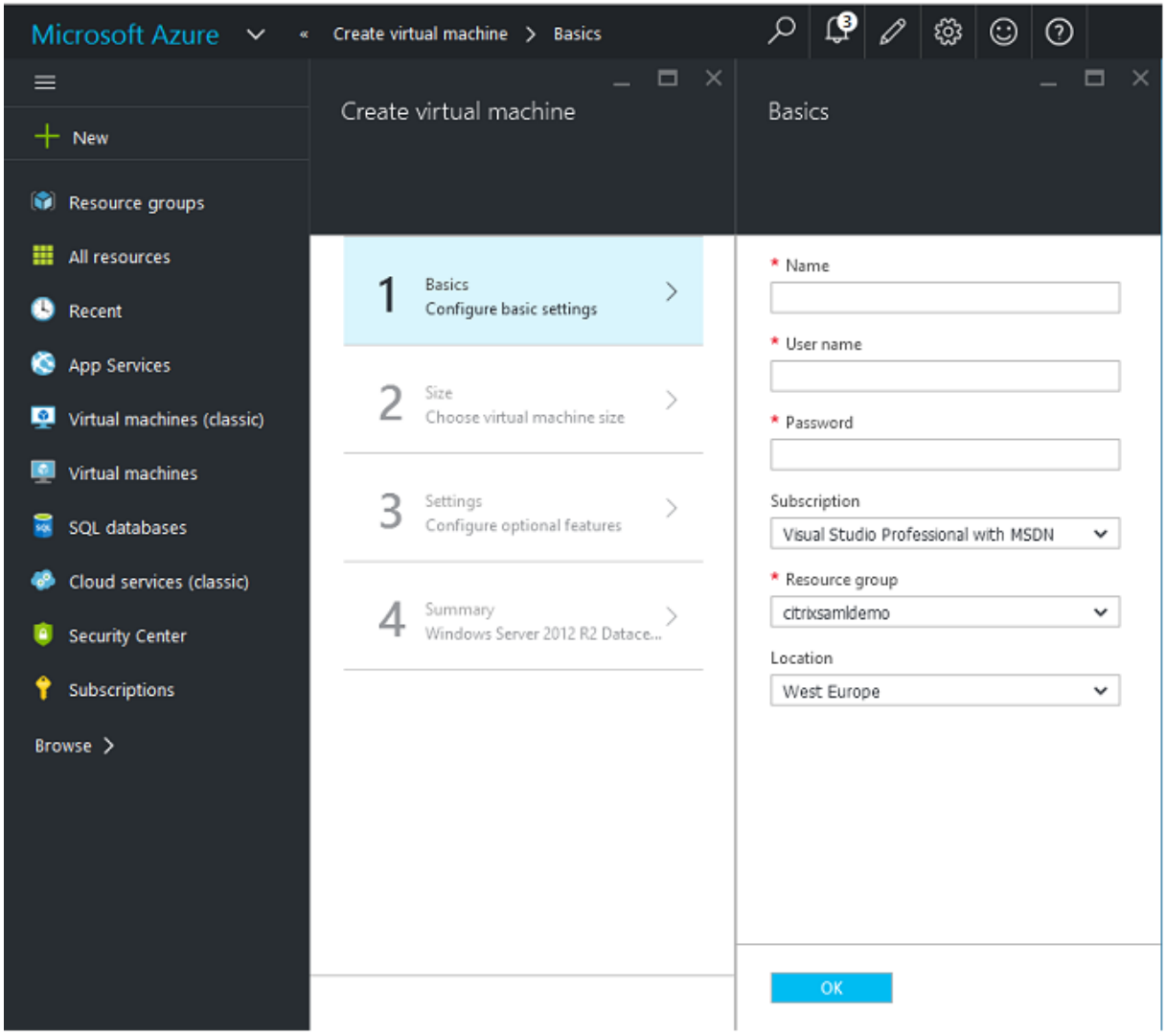


Créer des machines virtuelles Windows

Créez cinq VM Windows exécutées dans le service de cloud :

- Contrôleur de domaine (domaincontrol)
- Serveur ADFS Azure Connect (adfs)
- Proxy d'accès Web ADFS (proxy d'application Web, non joint à un domaine)
- Citrix XenDesktop Delivery Controller (ddc)

- les Agents Virtual Desktop Citrix (VDA) ;



Contrôleur de domaine

- Ajoutez les rôles **Serveur DNS** et **Services de domaine Active Directory** pour créer un déploiement Active Directory standard (dans cet exemple, citrixsamldemo. net). Une fois la promotion de domaine terminée, ajoutez le rôle **Services de certification Active Directory**.
- Créez un compte d'utilisateur normal pour le test (par exemple, George@citrixsamldemo.net).
- Étant donné que ce serveur exécutera le DNS interne, tous les serveurs doivent faire référence à ce serveur pour la résolution DNS. Cette opération peut être effectuée au travers de la page des **paramètres Azure DNS**. (Pour de plus amples informations, consultez la section Annexe dans ce document).

Contrôleur ADFS et serveur proxy d'application Web

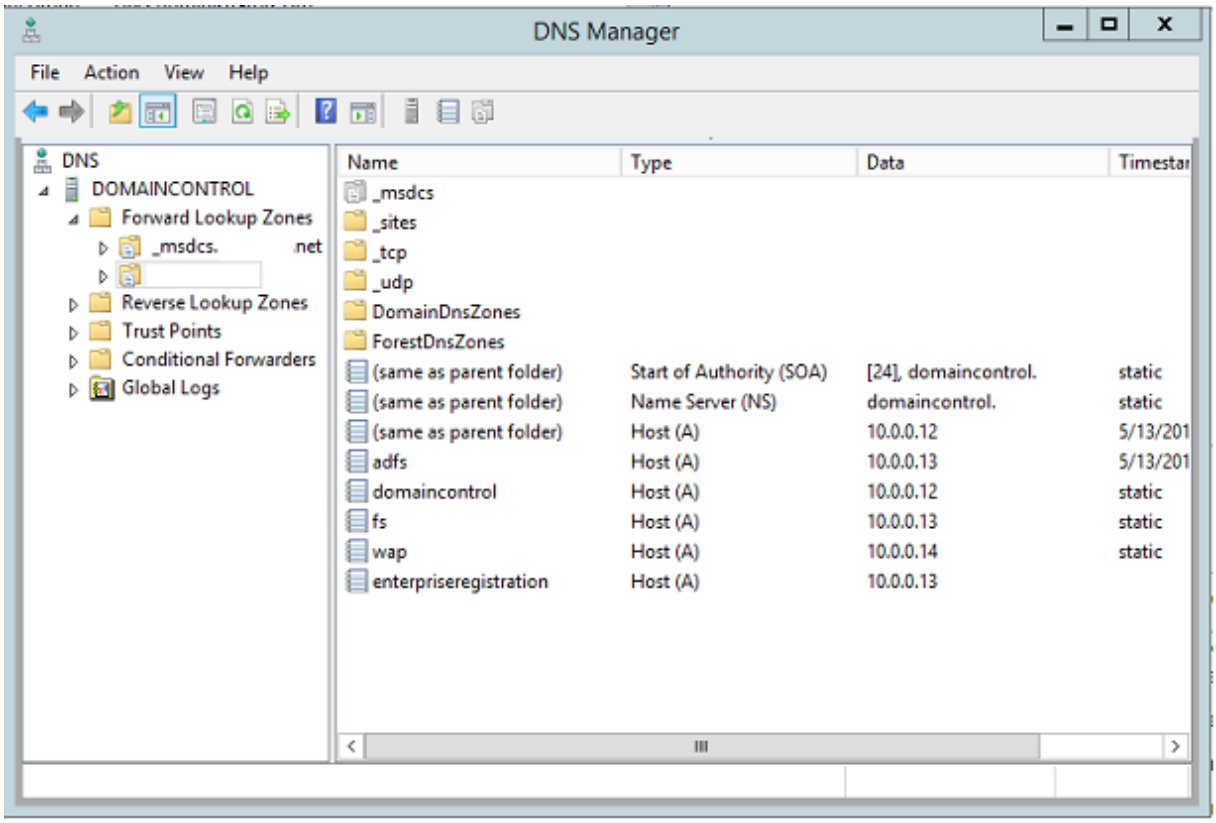
- Joignez le serveur ADFS au domaine citrixsamldemo. Le serveur proxy d'application Web doit rester dans un groupe de travail isolé, vous devez donc enregistrer une adresse DNS manuellement avec le DNS AD.
- Exécutez l'applet de commande **Enable-PSRemoting –Force** sur ces serveurs afin d'autoriser l'accès à distance PowerShell via les pare-feu depuis l'outil Azure AD Connect.

Delivery Controller et VDA XenDesktop

- Installez XenApp ou XenDesktop Delivery Controller et le VDA sur les deux autres serveurs Windows joints à citrixsamldemo.

Configurer un DNS interne

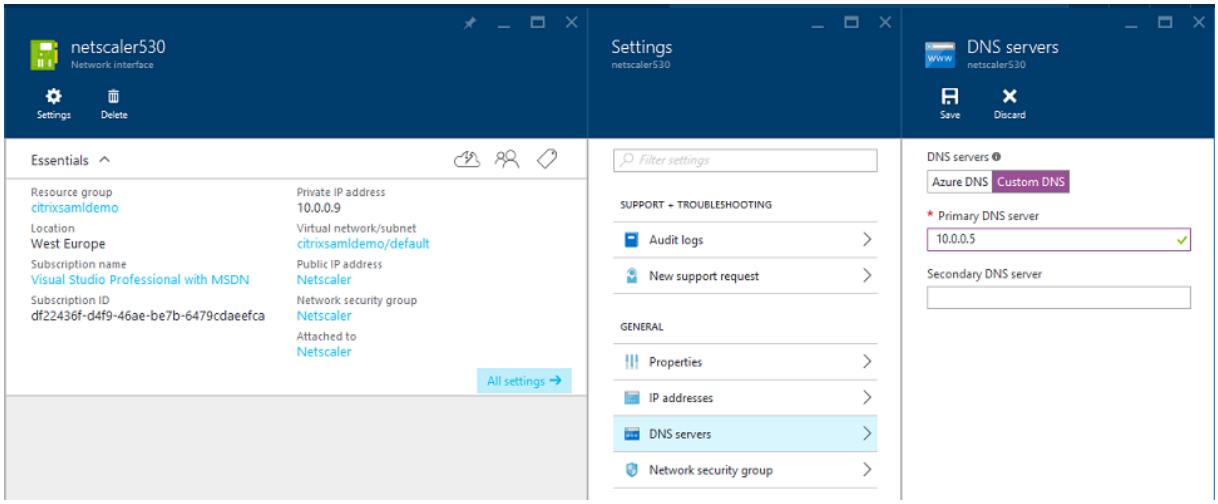
Une fois le contrôleur de domaine installé, configurez le serveur DNS afin de gérer l'affichage interne de citrixsamldemo.net, et d'agir en tant que redirecteur vers un serveur DNS externe (par exemple : 8.8.8.8).



Ajoutez un enregistrement statique pour :

- wap.citrixsamldemo.net [la VM du proxy d'application Web ne sera pas jointe au domaine]
- fs.citrixsamldemo.net [adresse du serveur de fédération interne]
- enterpriseregistration.citrixsaml.net [identique à fs.citrixsamldemo.net]

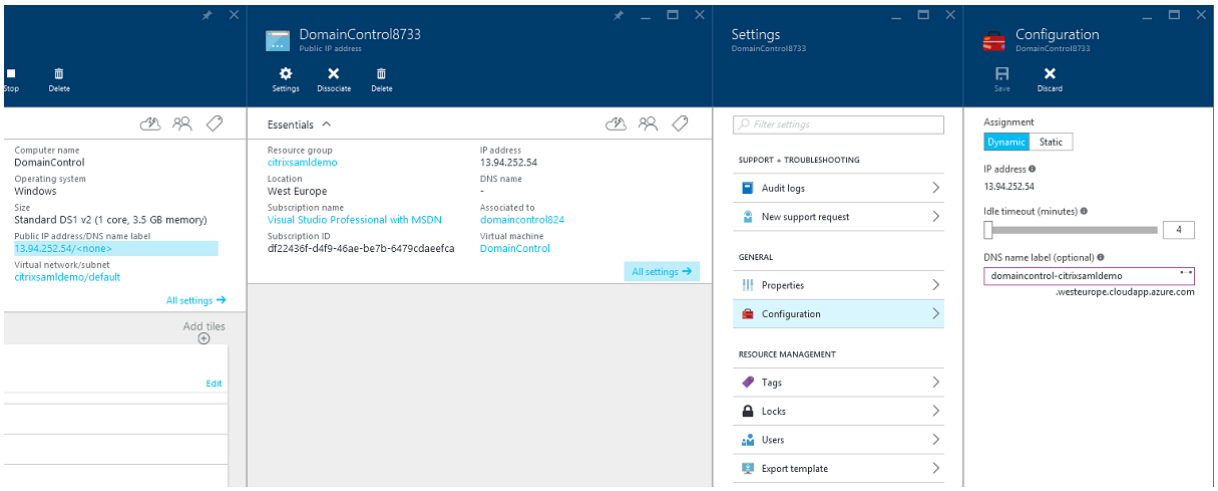
Toutes les VM exécutées dans Azure doivent être configurées pour utiliser uniquement ce serveur DNS. Vous pouvez effectuer cette opération à l'aide de l'interface réseau.



Par défaut, l'adresse IP interne (10.0.0.9) est attribuée de manière dynamique. Vous pouvez utiliser le paramètre d'adresses IP pour attribuer l'adresse IP de manière permanente. Ceci doit être effectué pour le serveur proxy d'application Web et le contrôleur de domaine.

Configurer une adresse DNS externe

Lorsqu'une VM est en cours d'exécution, Azure gère son propre serveur de zone DNS qui pointe vers l'adresse IP publique attribuée à la VM. Il est utile d'activer cette fonctionnalité car Azure attribue par défaut des adresses IP au démarrage de chaque VM.

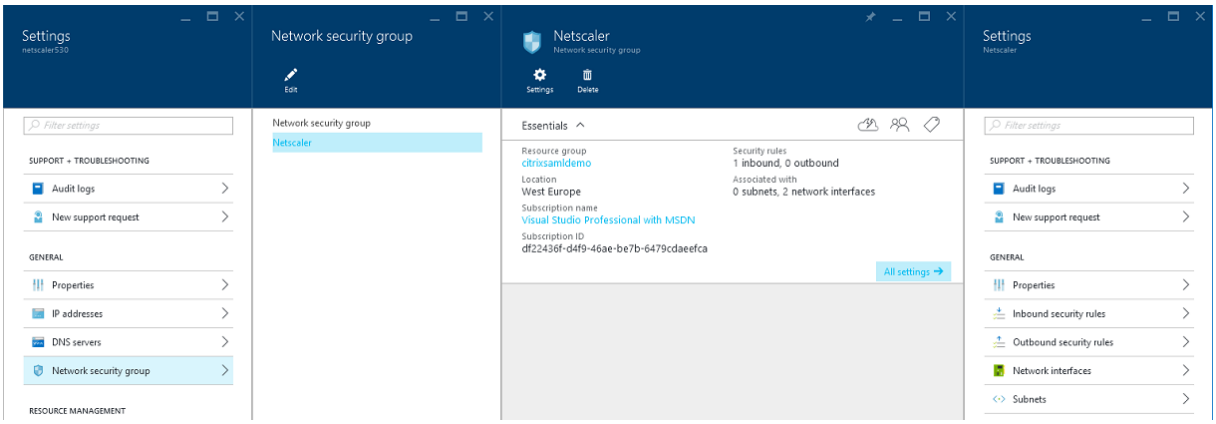


Cet exemple attribue l'adresse DNS domaincontrol-citrixsamldemo.westeurope.cloudapp.azure.com au contrôleur de domaine.

Notez que lorsque la configuration distante est terminée, seuls le proxy d'application Web et les VM NetScaler doivent disposer d'adresses IP publiques. (Lors de la configuration, l'adresse IP publique est utilisée pour accéder à distance à l'environnement).

Configurer des groupes de sécurité

Le cloud Azure gère les règles de pare-feu pour l'accès TCP/UDP aux VM à partir d'Internet à l'aide de groupes de sécurité. Par défaut, toutes les VM autorisent l'accès RDP. Les serveurs NetScaler et proxy d'application Web doivent également autoriser TLS sur le port 443.

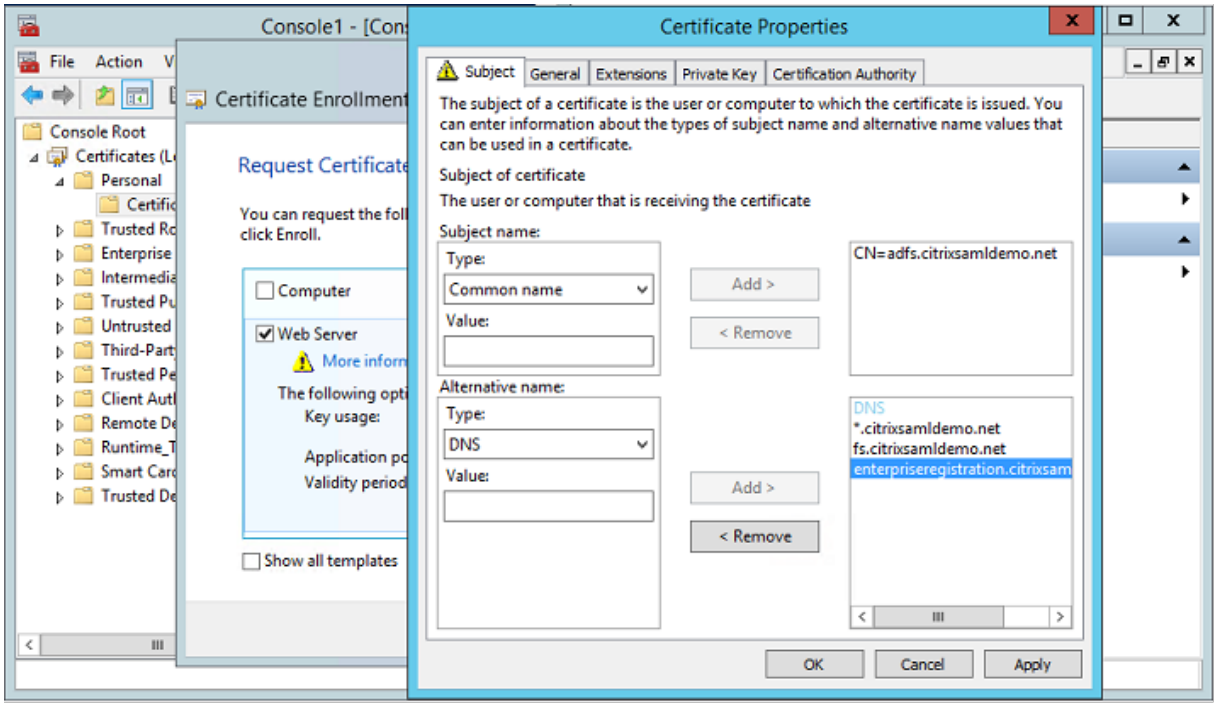


Créer un certificat d'ADFS

Activez le modèle de certificat **Serveur Web** sur l'autorité de certification Microsoft (CA). Ceci permet la création d'un certificat avec des adresses DNS personnalisées qui peuvent être exportées (y compris la clé privée) sur un fichier pfx. Vous devez installer ce certificat sur les serveurs ADFS et proxy d'applications Web, par conséquent le fichier pfx est l'option préférée.

Émettez un certificat de serveur Web avec les noms de sujets suivants :

- Commonname:
  - adfs.citrixsamldemo.net [nom d'ordinateur]
- SubjectAltname:
  - *.citrixsamldemo.net [nom de zone]
  - fs.citrixsamldemo. net [entrée dans le DNS]
  - enterpriseregistration.citrixsamldemo.net



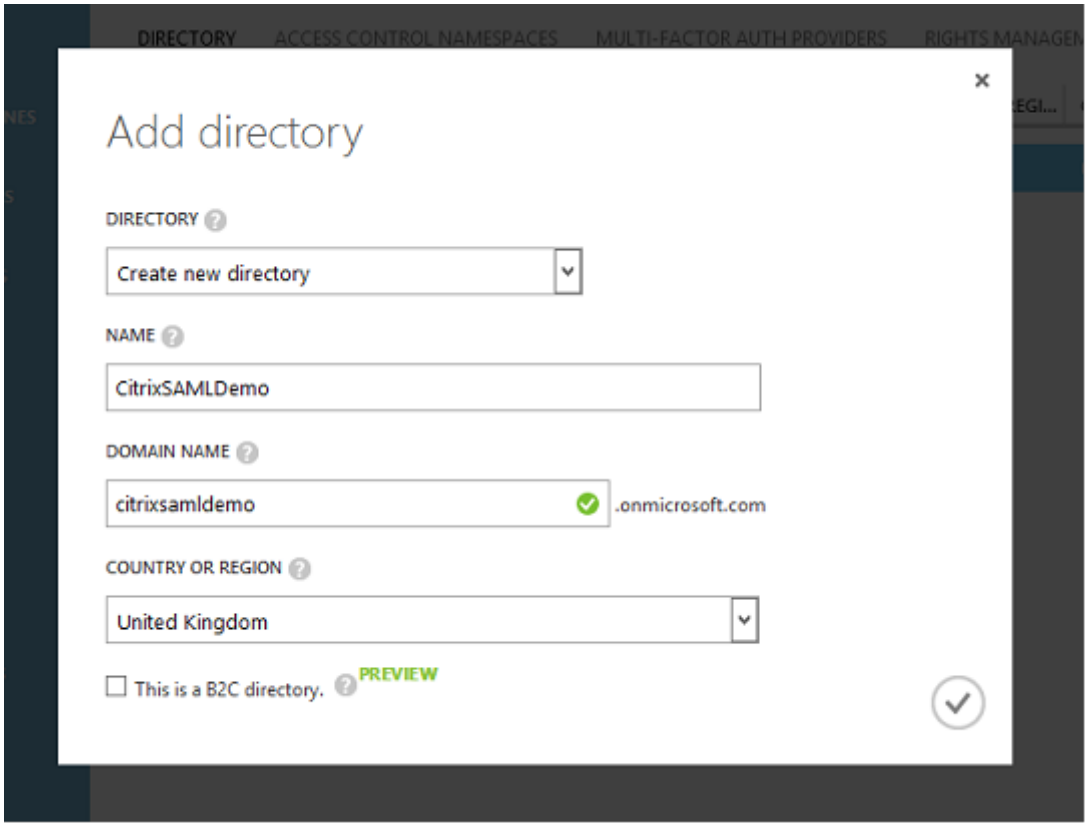
Exportez le certificat sur un fichier pfx, y compris une clé privée protégée par mot de passe.

Configurer Azure AD

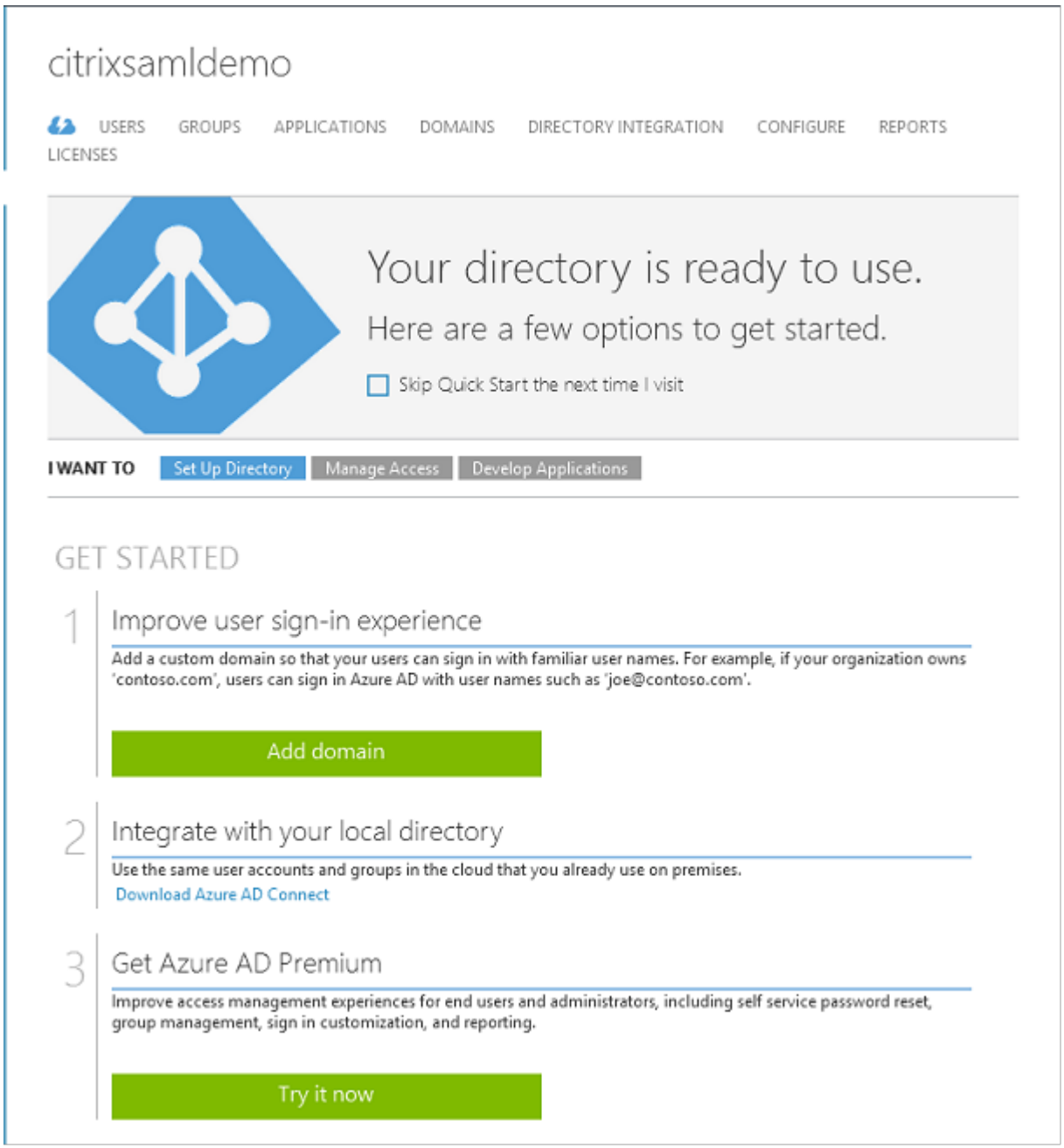
Cette section décrit en détail la création d'une nouvelle instance Azure AD et la création d'identités utilisateur qui peuvent être utilisées pour joindre Windows 10 à Azure AD.

Créer un nouveau répertoire

Ouvrez une session sur le portail Azure et créez un nouveau répertoire.

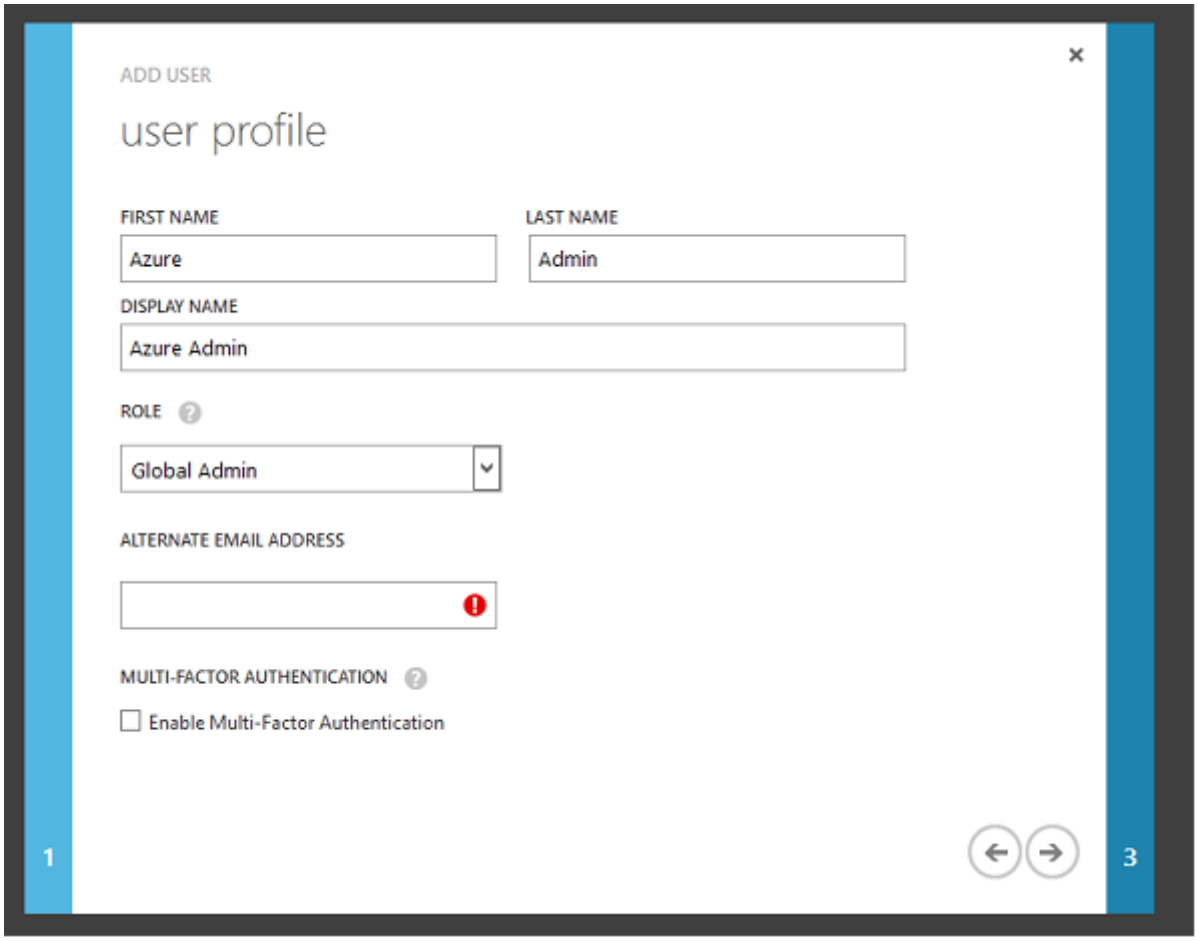


Une fois le répertoire créé, une page de résumé apparaît.



Créer un utilisateur administrateur global (AzureAdmin)

Créez un administrateur global dans Azure (dans cet exemple, AzureAdmin@citrixsamldemo.onmicrosoft.com) et ouvrez une session avec le nouveau compte pour définir un mot de passe.



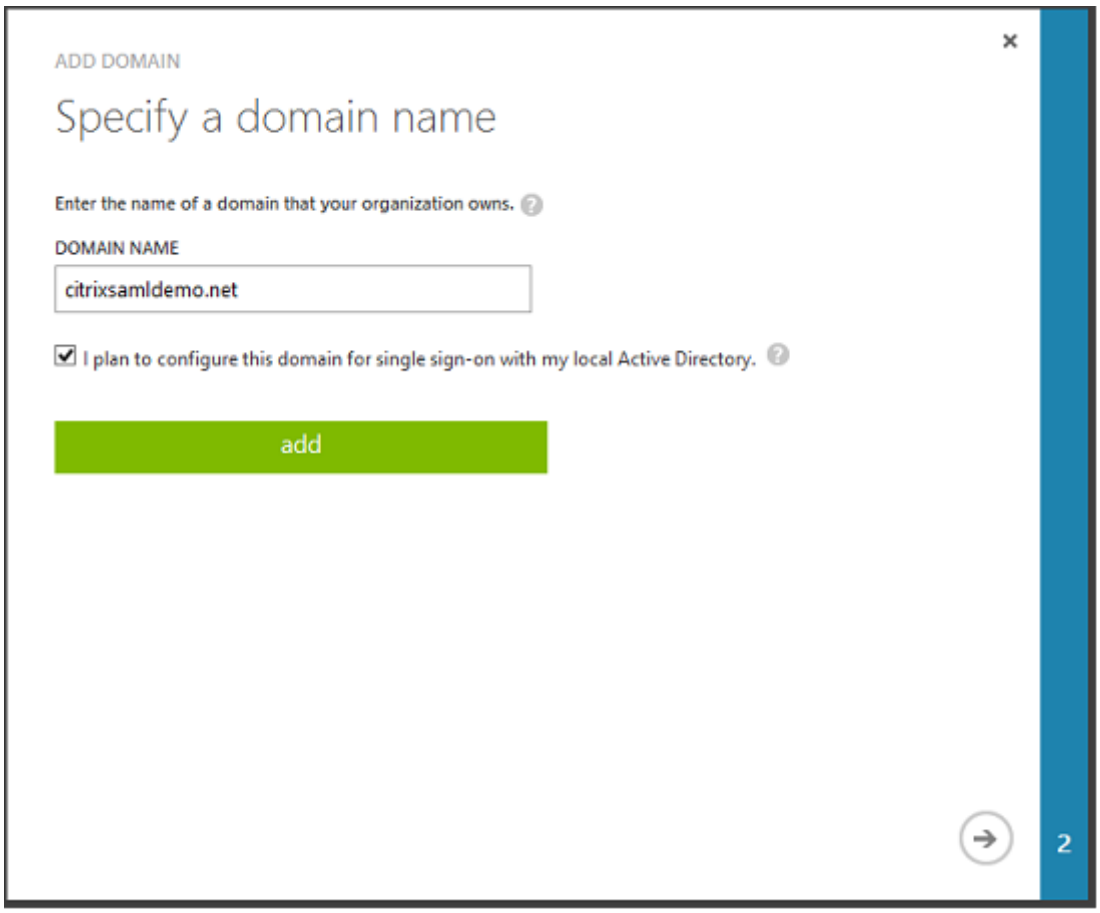
Enregistrer votre domaine avec Azure AD

Par défaut, les utilisateurs sont identifiés avec une adresse e-mail au format : *<user.name>@<company>.onmicroso*

Bien que cela fonctionne sans configuration supplémentaire, une adresse e-mail au format standard est préférable, de préférence une qui correspond au compte de messagerie de l'utilisateur final : @.com

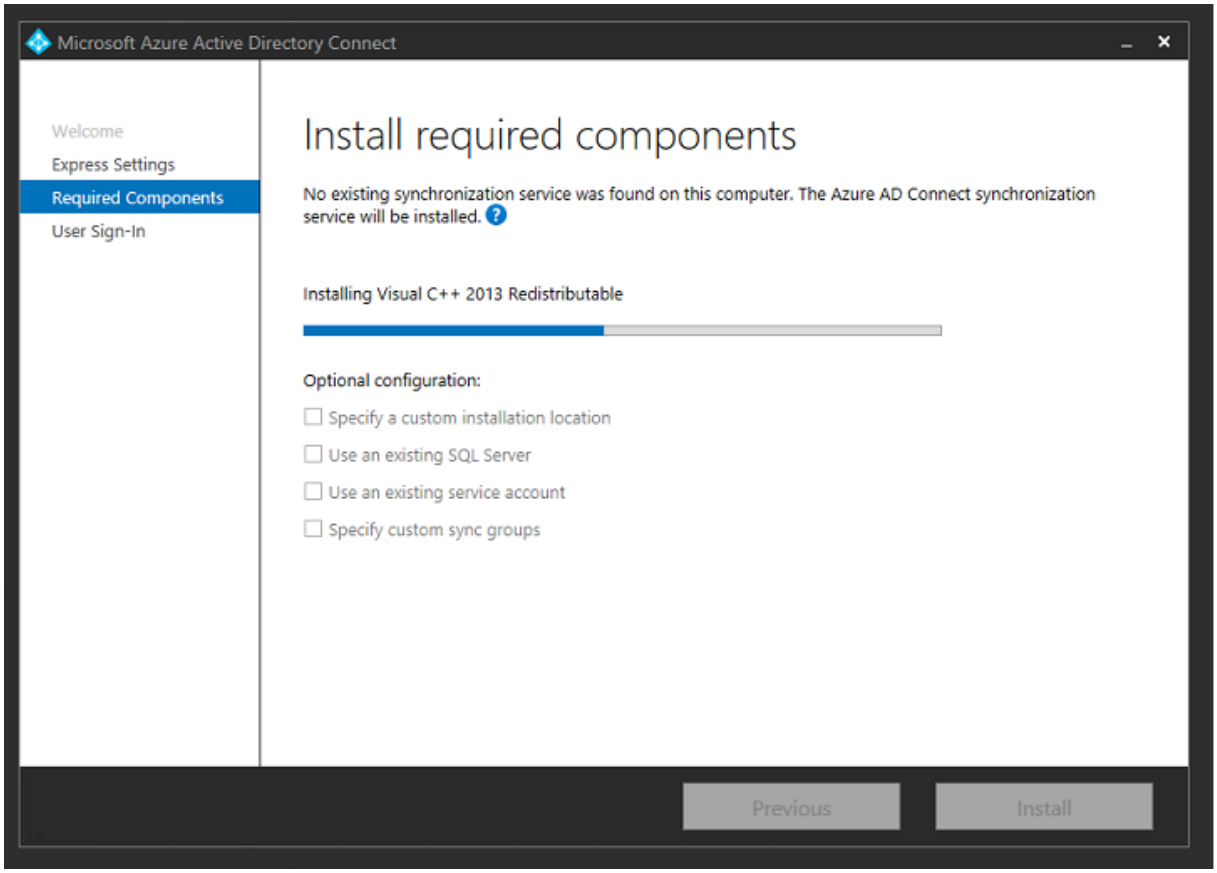
L'action **Ajouter un domaine** configure une redirection de votre domaine d'entreprise réel. Cet exemple utilise citrixsamldemo.net.

Si vous configurez ADFS pour l'authentification unique, activez la case à cocher.

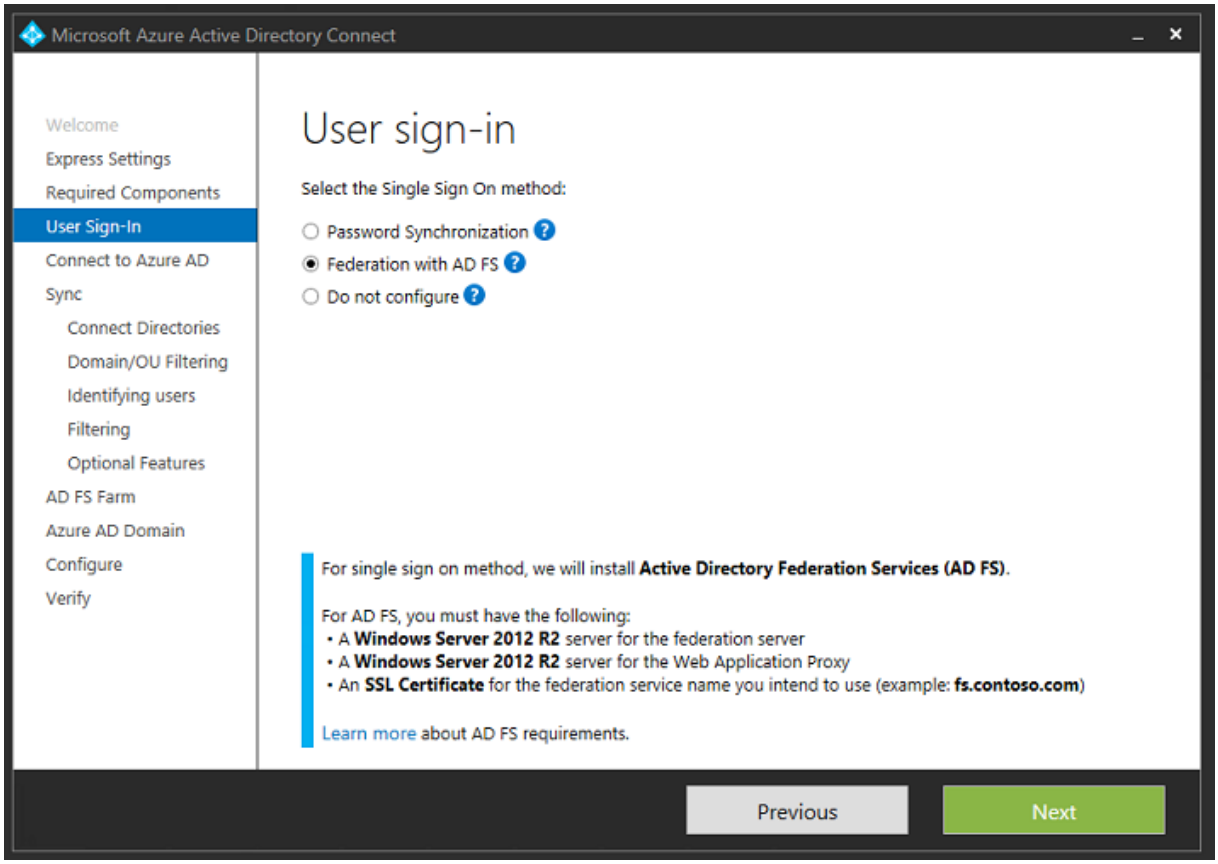


Installer Azure AD Connect

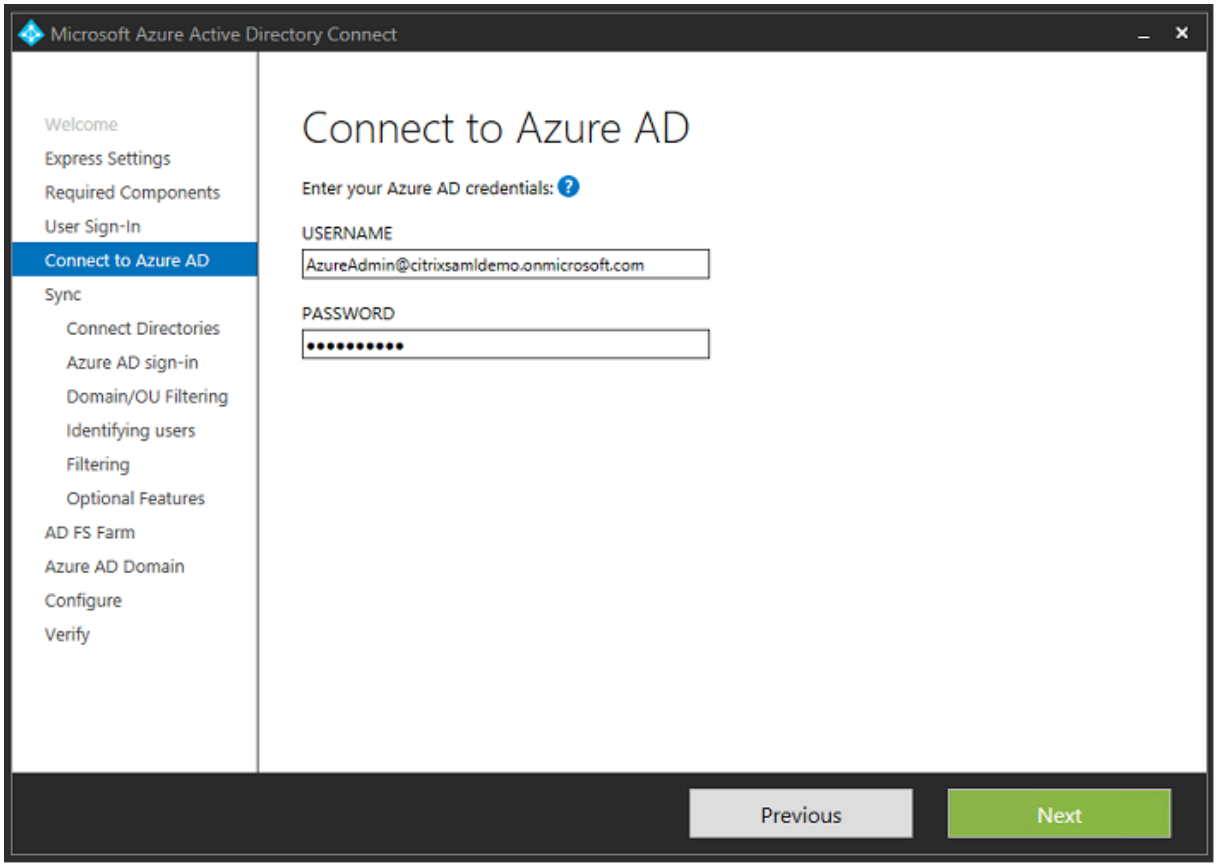
L'étape 2 de l'interface de configuration d'Azure AD redirige l'utilisateur vers la page de téléchargement Microsoft d'Azure AD Connect. Installez ce composant sur la VM ADFS. Utilisez **Installation personnalisée**, plutôt que **Configuration rapide** afin que les options ADFS soient disponibles.



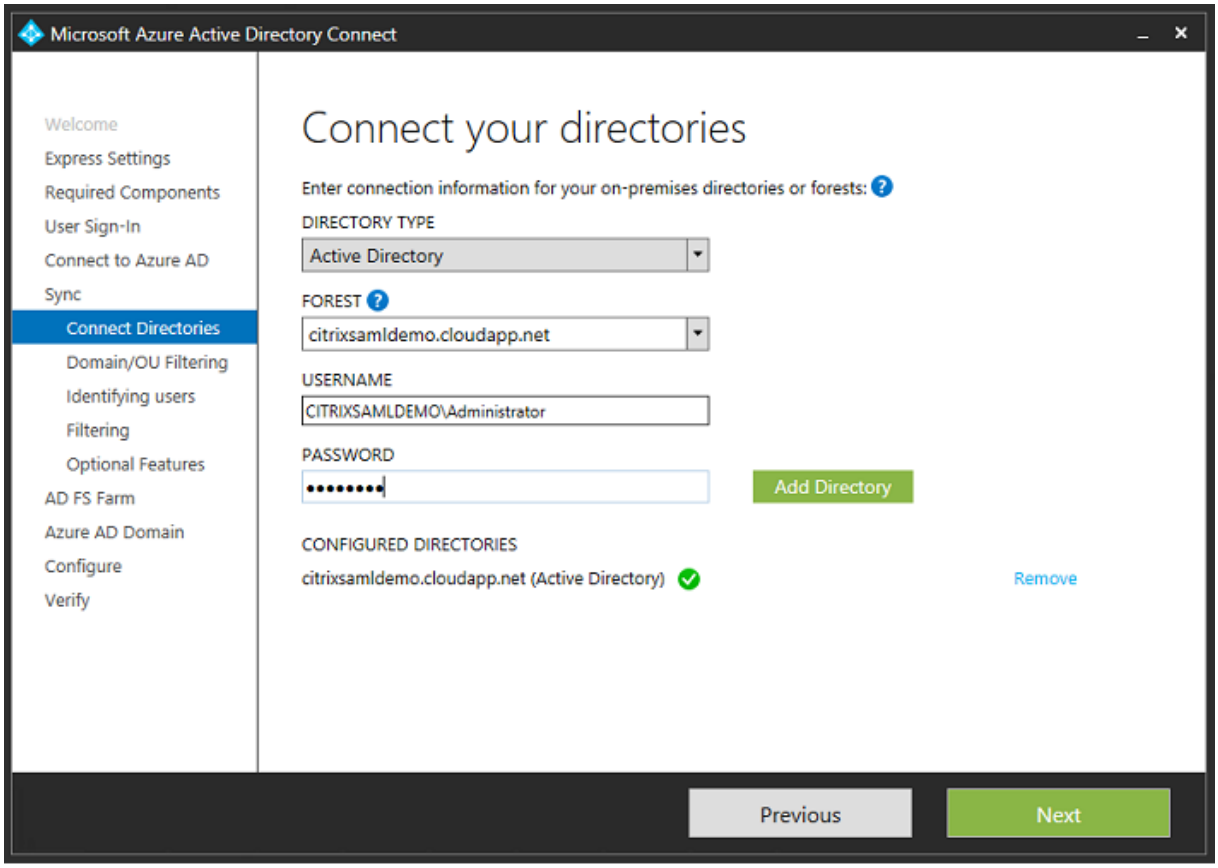
Sélectionnez l'option d'authentification unique **Fédération avec AD FS**.



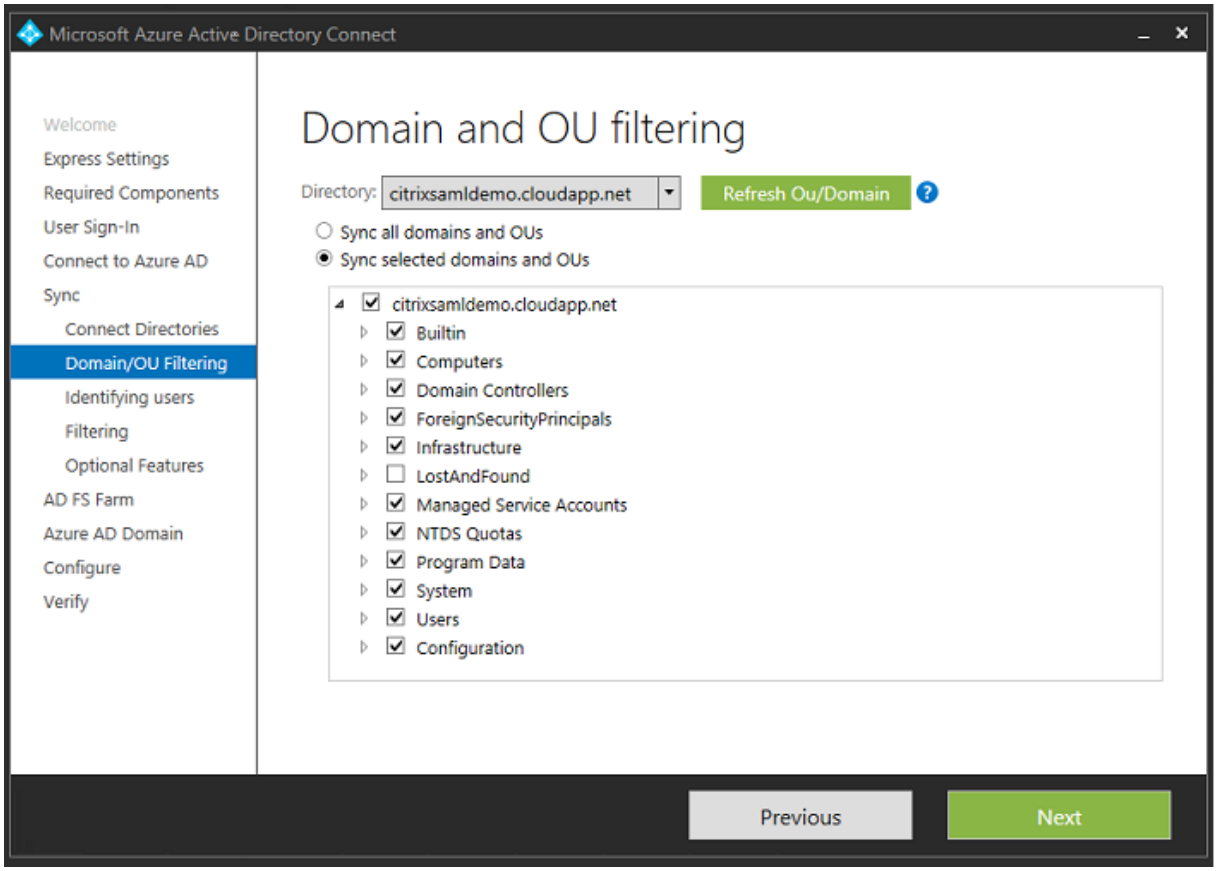
Connectez-vous à Azure avec le compte administrateur que vous avez créé précédemment.



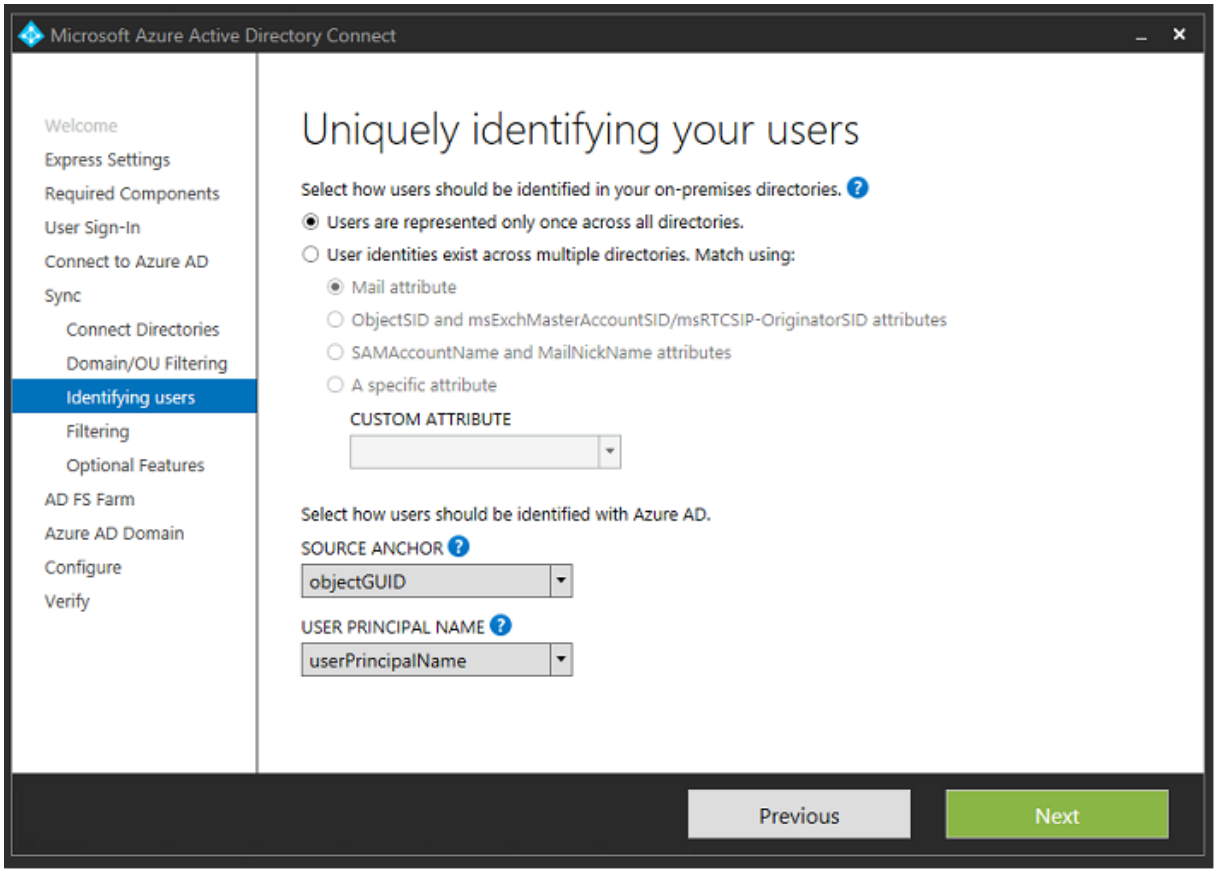
Sélectionnez la forêt AD interne.



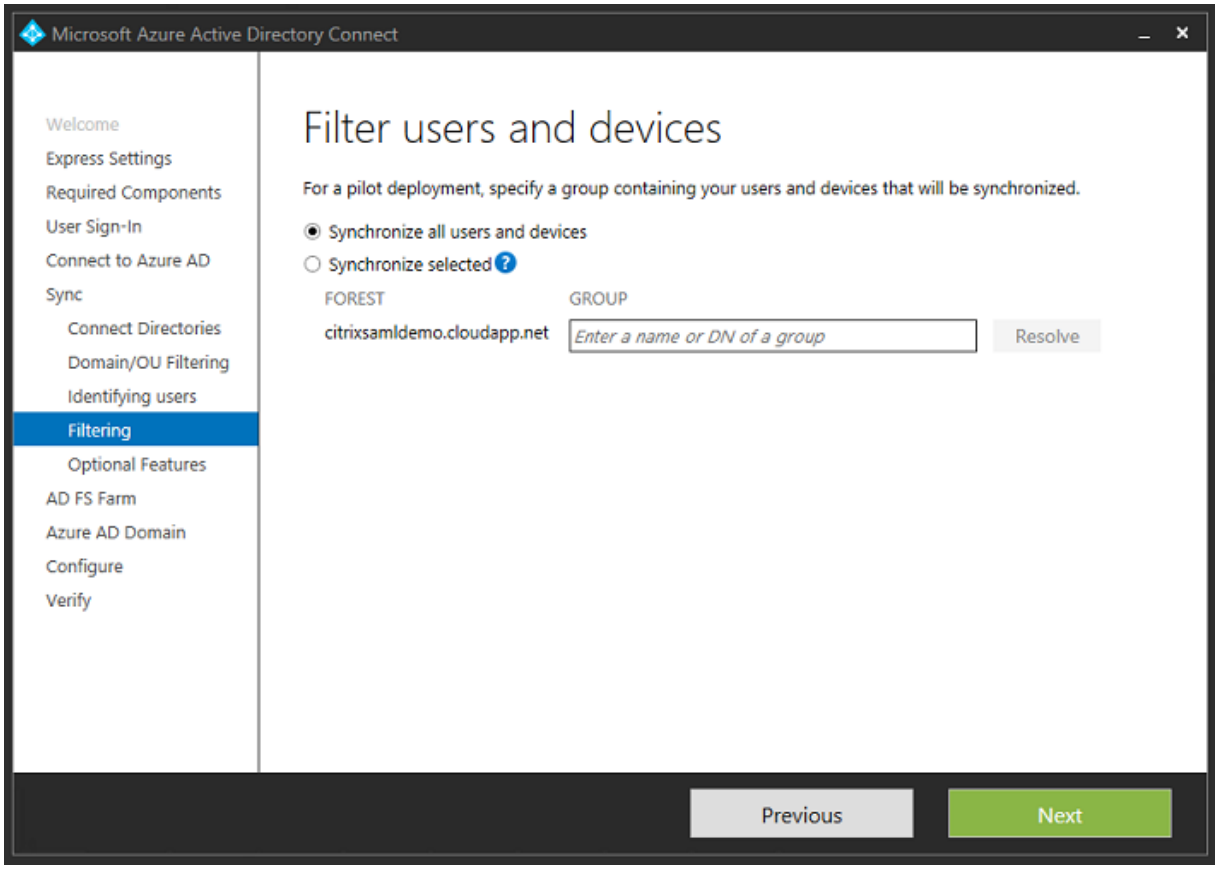
Synchronisez tous les anciens objets Active Directory avec Azure AD.



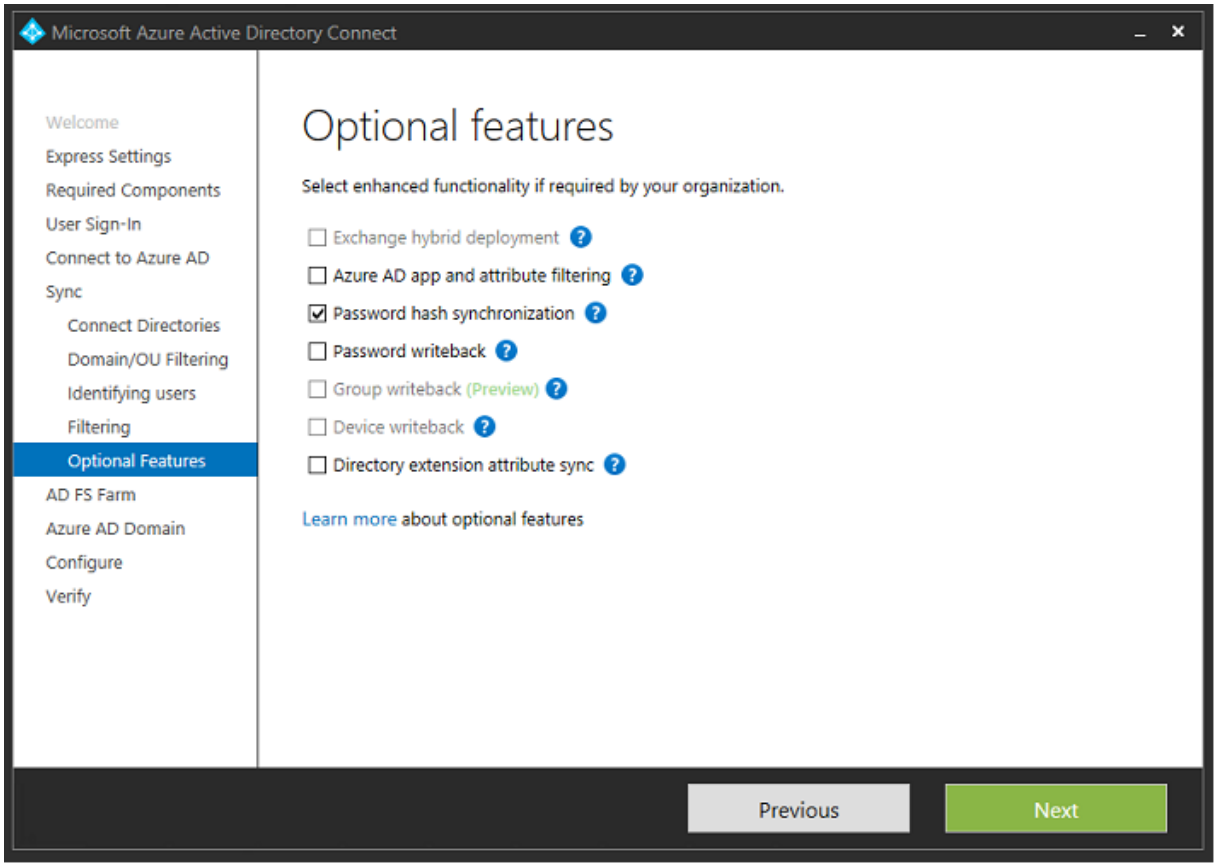
Si la structure de répertoire est simple, les noms d'utilisateur sont suffisamment uniques pour identifier un utilisateur qui ouvre une session.



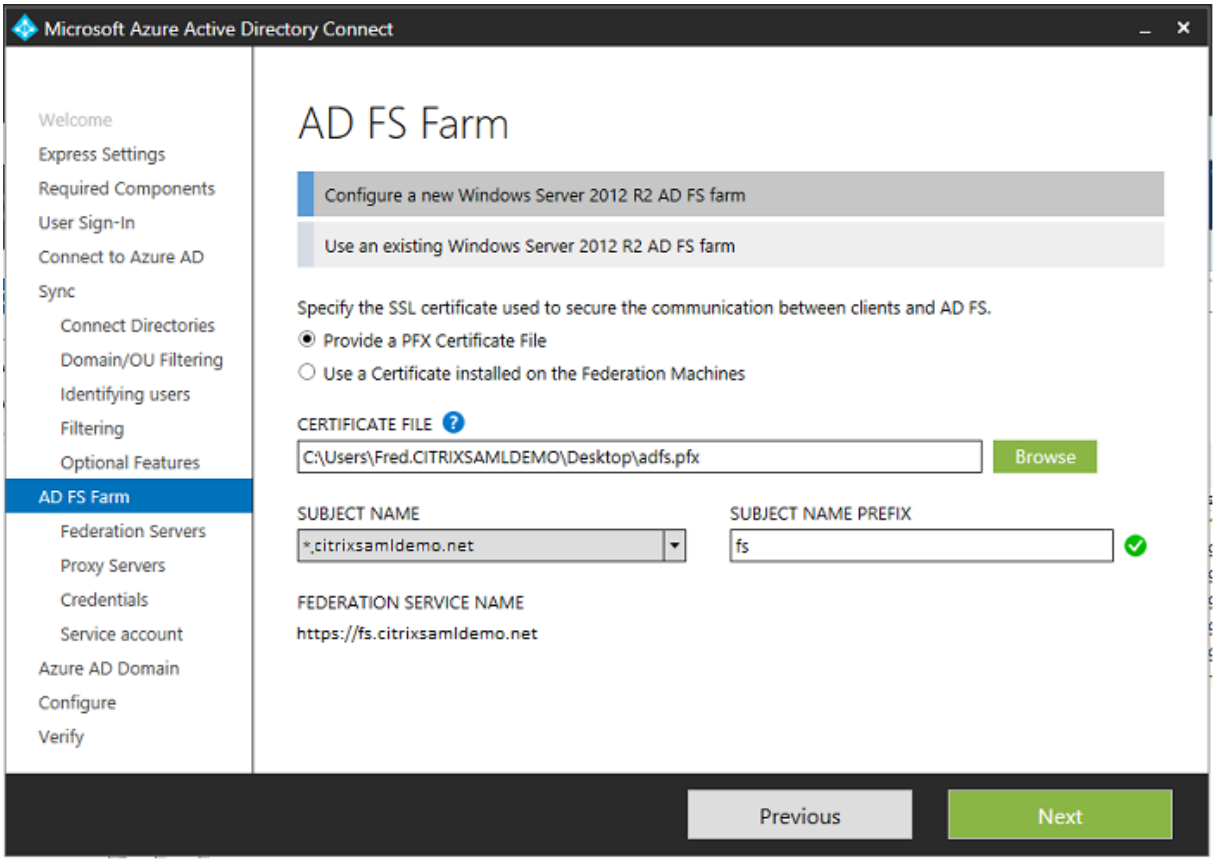
Acceptez les options de filtrage par défaut, ou limitez les utilisateurs et machines à un ensemble de groupes particulier.



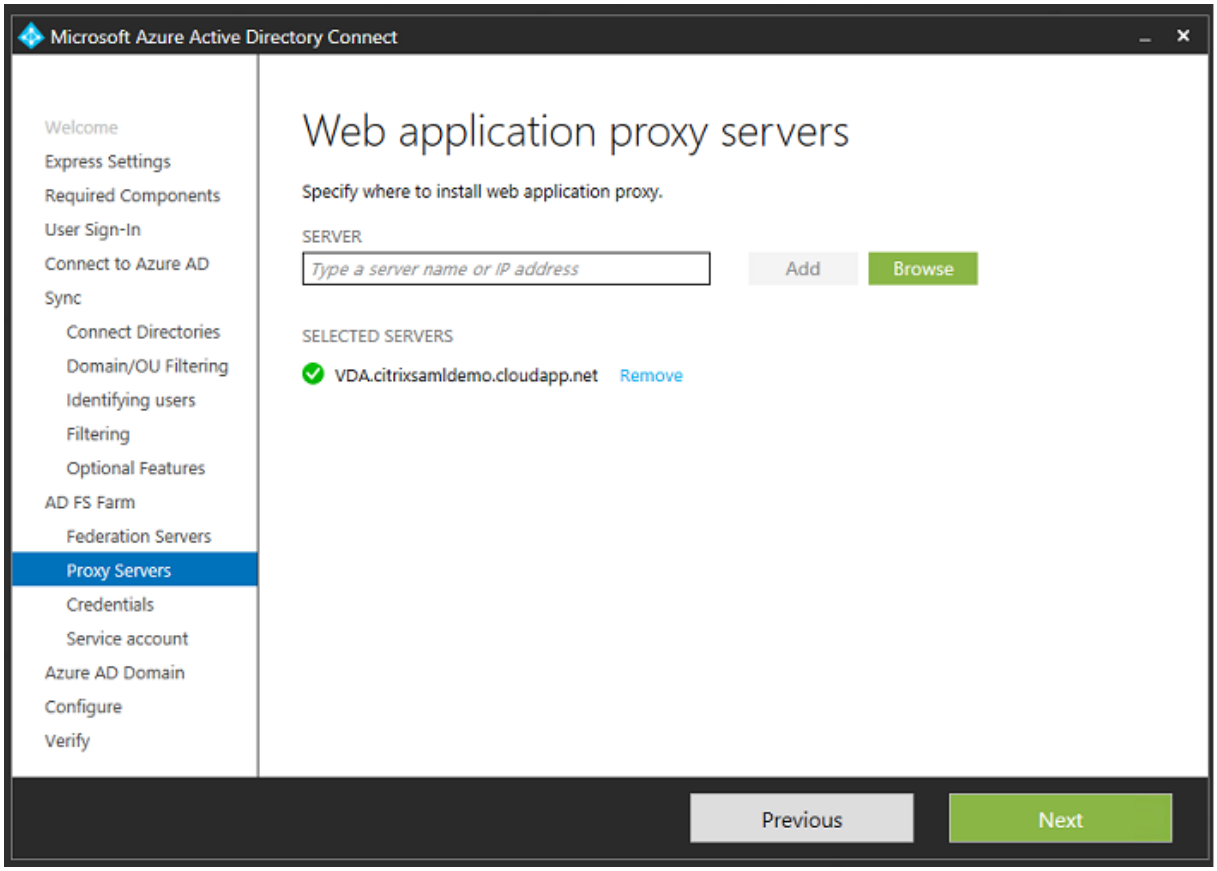
Si vous le souhaitez, vous pouvez synchroniser les mots de passe Azure AD avec Active Directory. Ceci n'est généralement pas nécessaire pour l'authentification ADFS.



Sélectionnez le fichier .pfx de certificat à utiliser dans ADFS, en spécifiant fs.citrixsamldemo.net en tant que nom DNS.

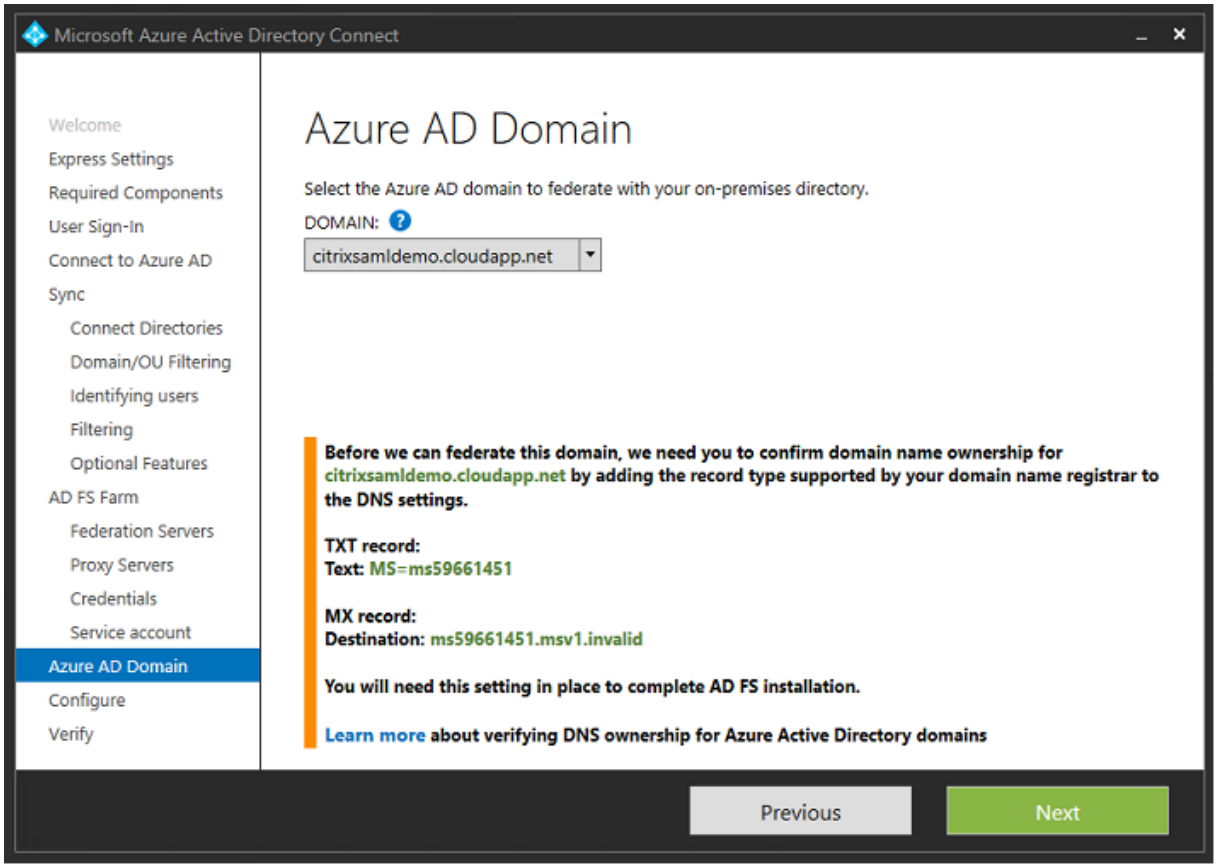


Lorsque vous êtes invité à sélectionner un serveur proxy, entrez l'adresse du serveur wap.citrixsamldemo.net. Vous devrez peut-être exécuter l'applet de commande **Enable-PSRemoting –Force** en tant qu'administrateur sur le serveur proxy d'application Web, de façon à ce que Azure AD Connect puisse le configurer.

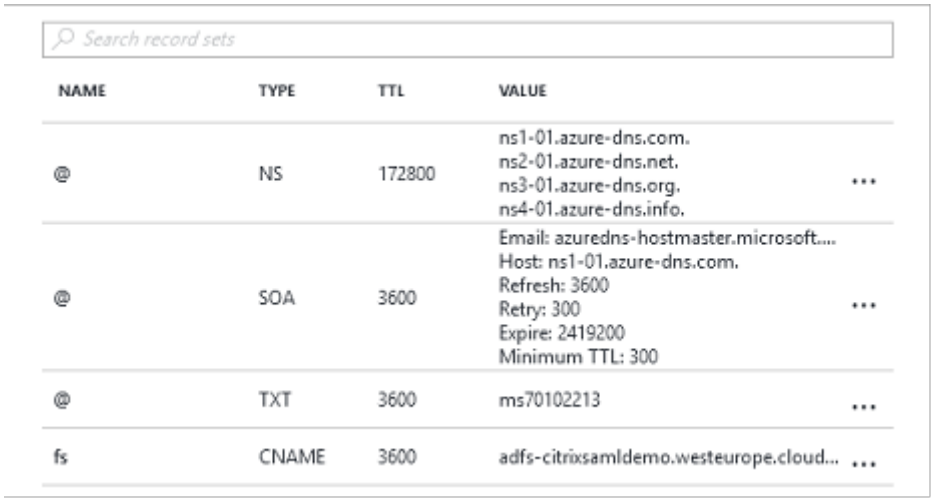


Remarque : si cette étape échoue en raison de problèmes de confiance avec PowerShell à distance, essayez de joindre le serveur proxy d'application Web au domaine.

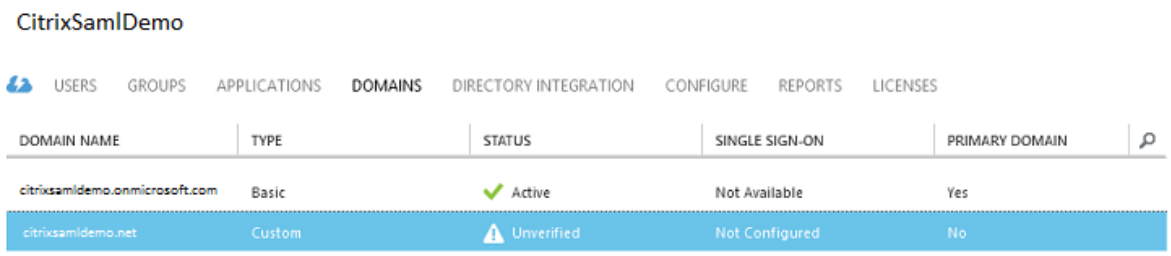
Pour les étapes restantes de l'assistant, utilisez les mots de passe de l'administrateur et créez un compte de service pour ADFS. Azure AD Connect vous invitera alors à valider l'appartenance de la zone DNS.



Ajoutez les enregistrements TXT et MX aux enregistrements d'adresses DNS dans Azure.

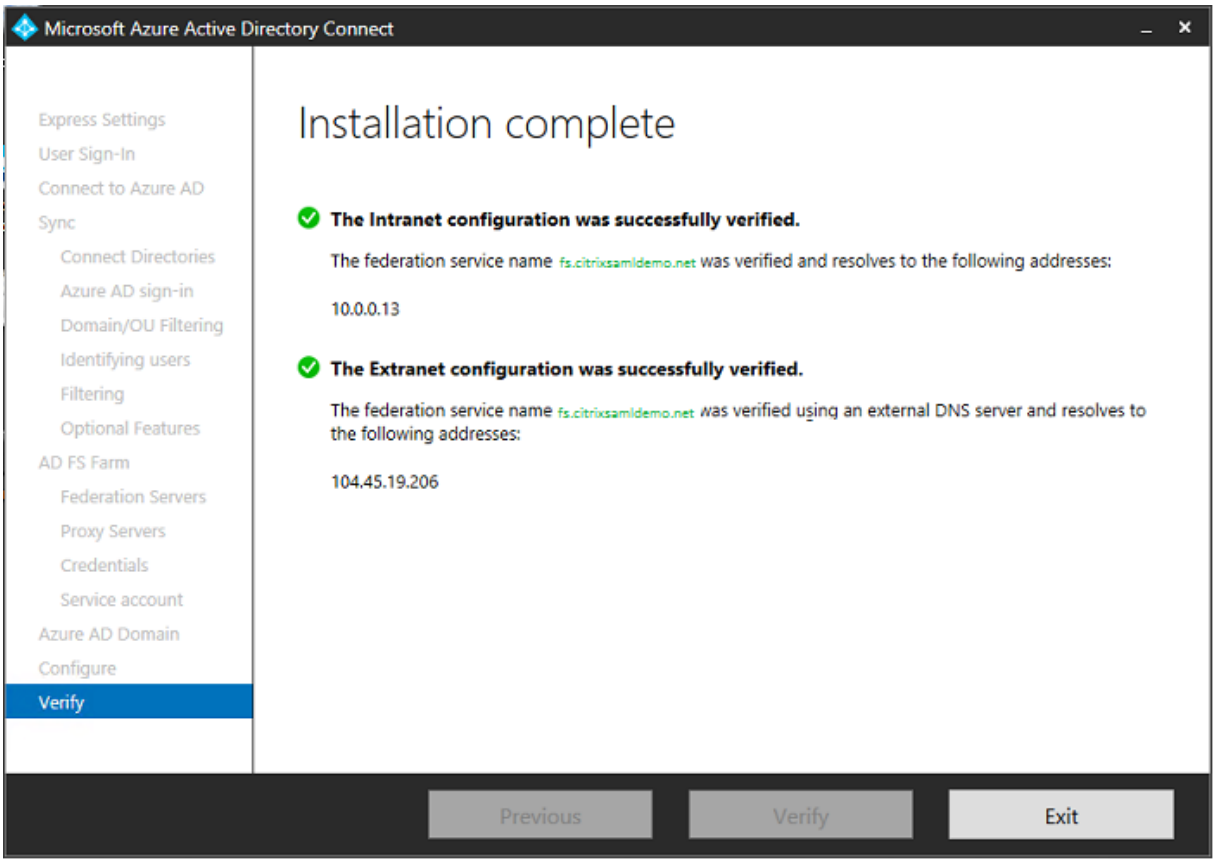


Cliquez sur **Vérifier** dans la console de gestion Azure.



Remarque : si cette étape échoue, vous pouvez vérifier le domaine avant d'exécuter Azure AD Connect.

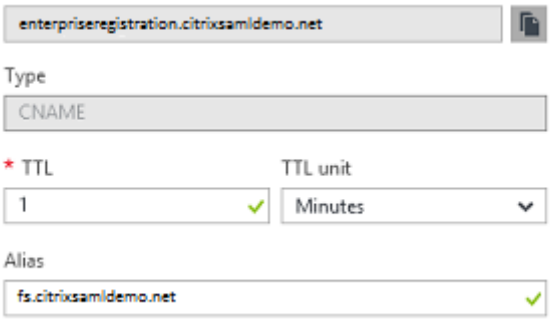
Lorsque l'installation est terminée, l'adresse externe fs.citrixsamldemo.net est contactée sur le port 443.



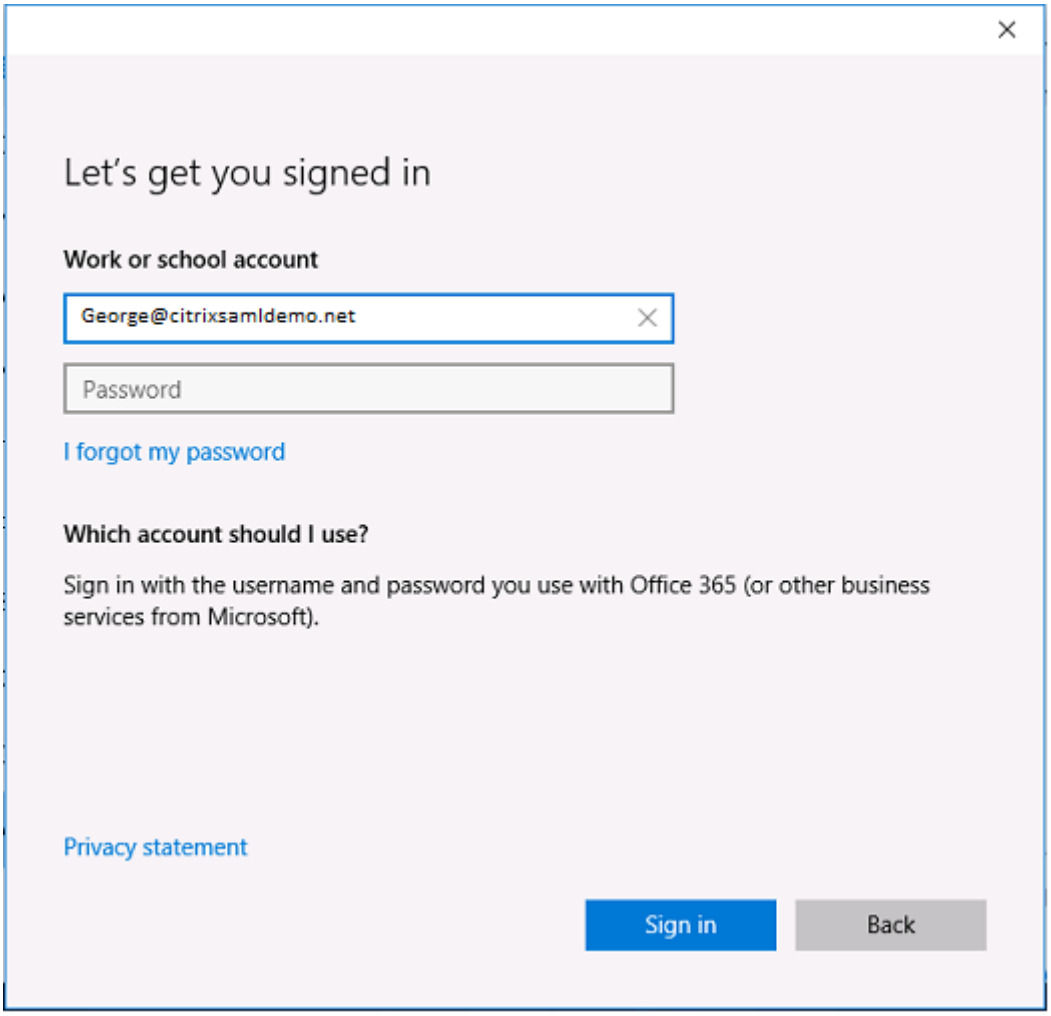
Activer Azure AD Join (Jonction à un domaine Azure AD)

Lorsqu'un utilisateur entre une adresse e-mail afin que Windows 10 puisse réaliser la jonction Azure AD, le suffixe DNS est utilisé pour construire un enregistrement DNS CNAME qui doit pointer vers ADFS : enterpriseregistration.<suffixeupn>.

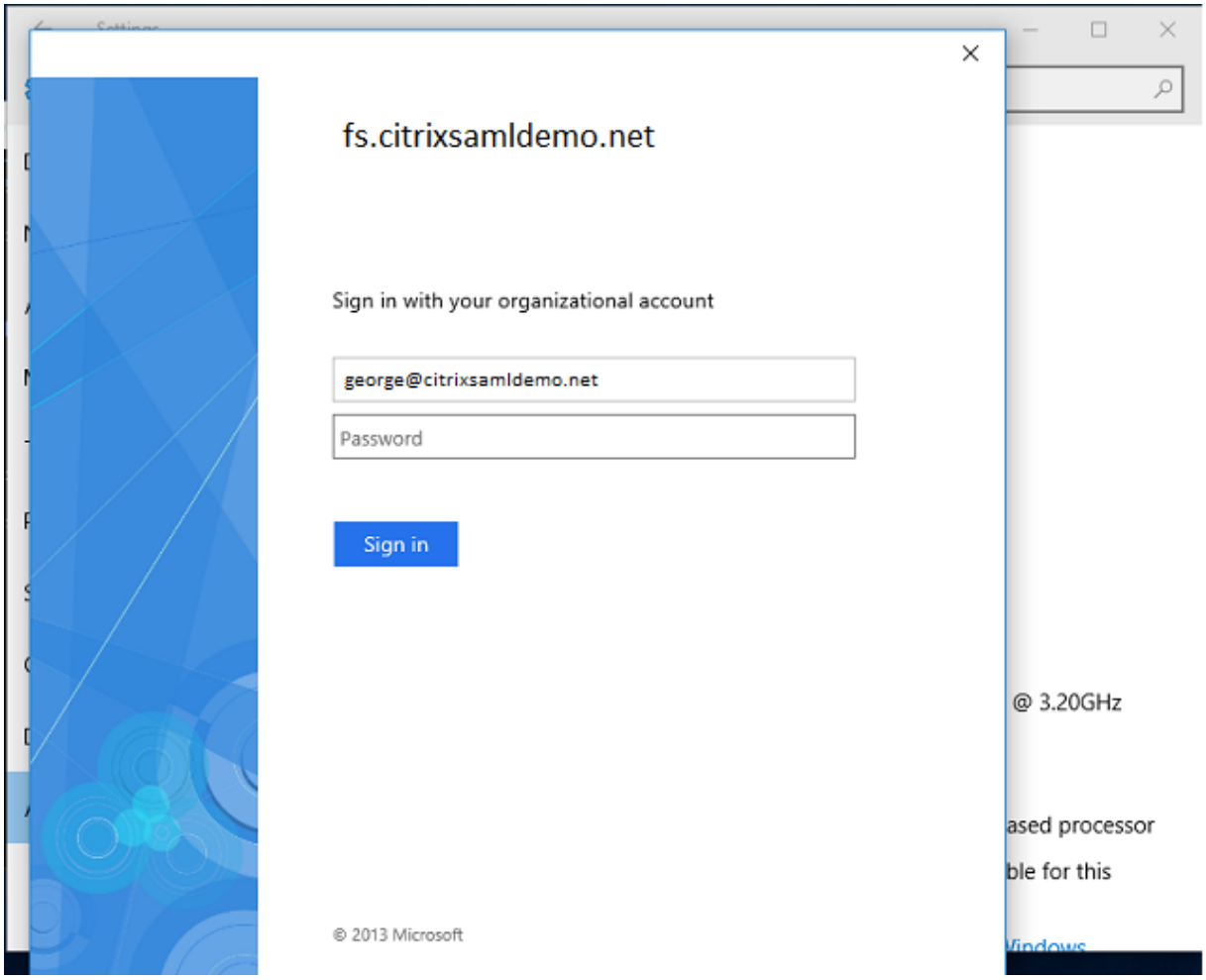
Dans cet exemple, il s'agit de fs.citrixsamldemo.net.

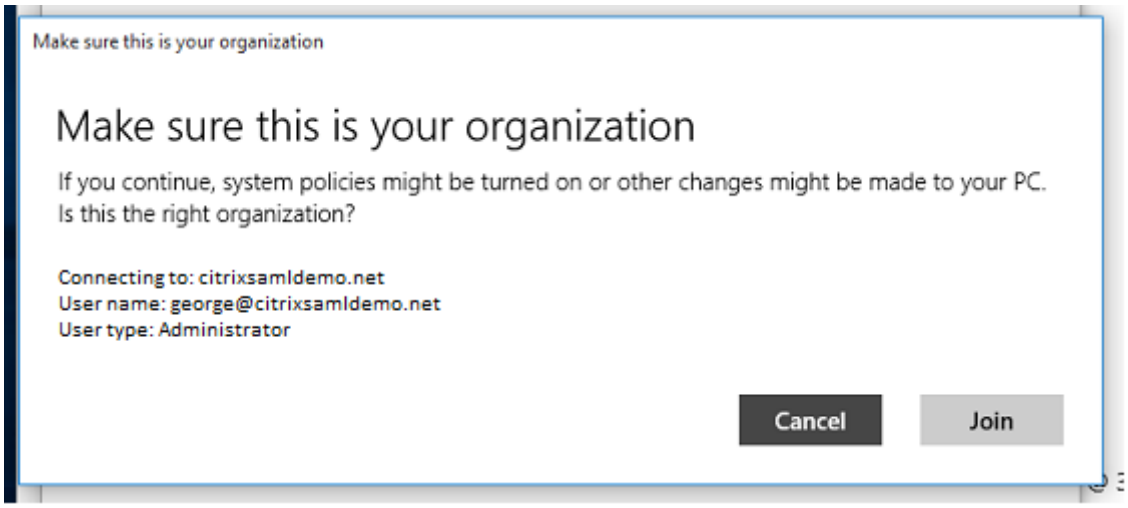


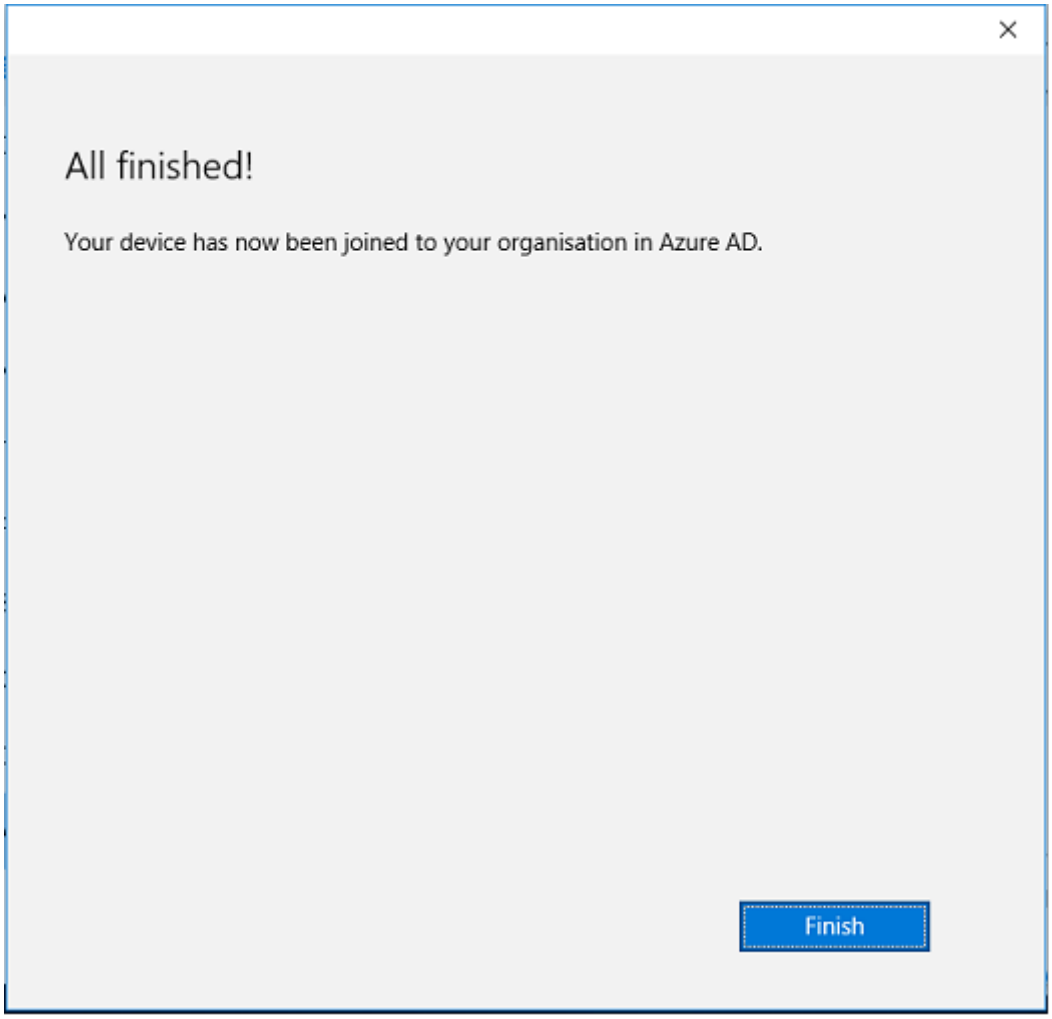
Si vous n'utilisez pas d'autorité de certification publique, assurez-vous que le certificat racine ADFS est installé sur l'ordinateur Windows 10 de façon à ce que Windows fasse confiance au serveur ADFS. Effectuez une jonction de domaine Azure AD à l'aide du compte utilisateur standard généré précédemment.



Veuillez noter que le nom UPN doit correspondre au nom UPN reconnu par le contrôleur de domaine ADFS.





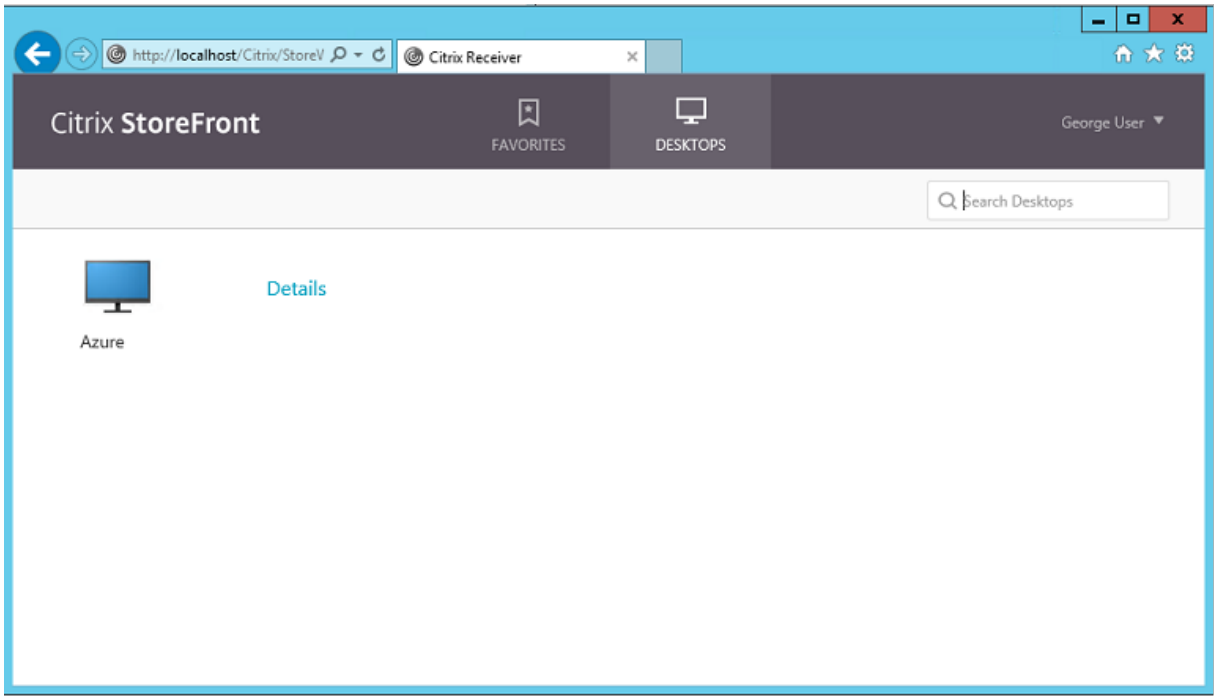


Vérifiez que la jonction Azure AD a réussi en redémarrant la machine et en ouvrant une session à l'aide de l'adresse e-mail de l'utilisateur. Une fois connecté, lancez Microsoft Edge et connectez-vous à https://myapps.microsoft.com. Le site Web doit utiliser l'authentification unique automatiquement.

Installer XenApp ou XenDesktop

Vous pouvez installer le Delivery Controller et des machines virtuelles VDA dans Azure directement depuis l'ISO XenApp ou XenDesktop de la manière habituelle.

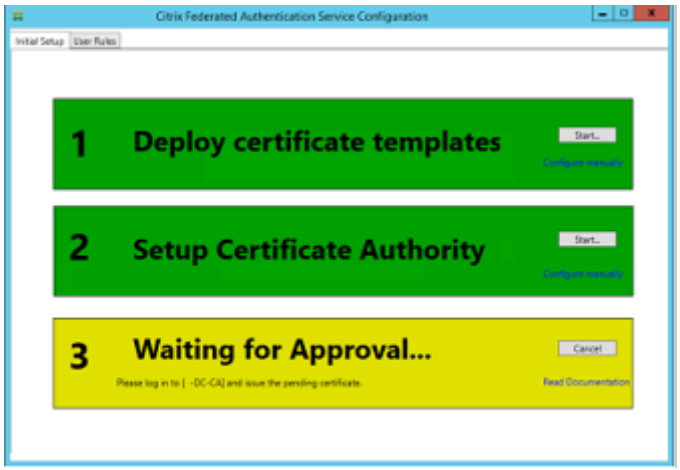
Dans cet exemple, StoreFront est installé sur le même serveur que le Delivery Controller. Le VDA est installé en tant que travailleur RDS Windows 2012 R2 autonome, sans intégration avec Machine Creation Services (mais cela peut être configuré). Vérifiez que l'utilisateur George@citrixsamldemo.net peut s'authentifier avec un mot de passe avant de continuer.

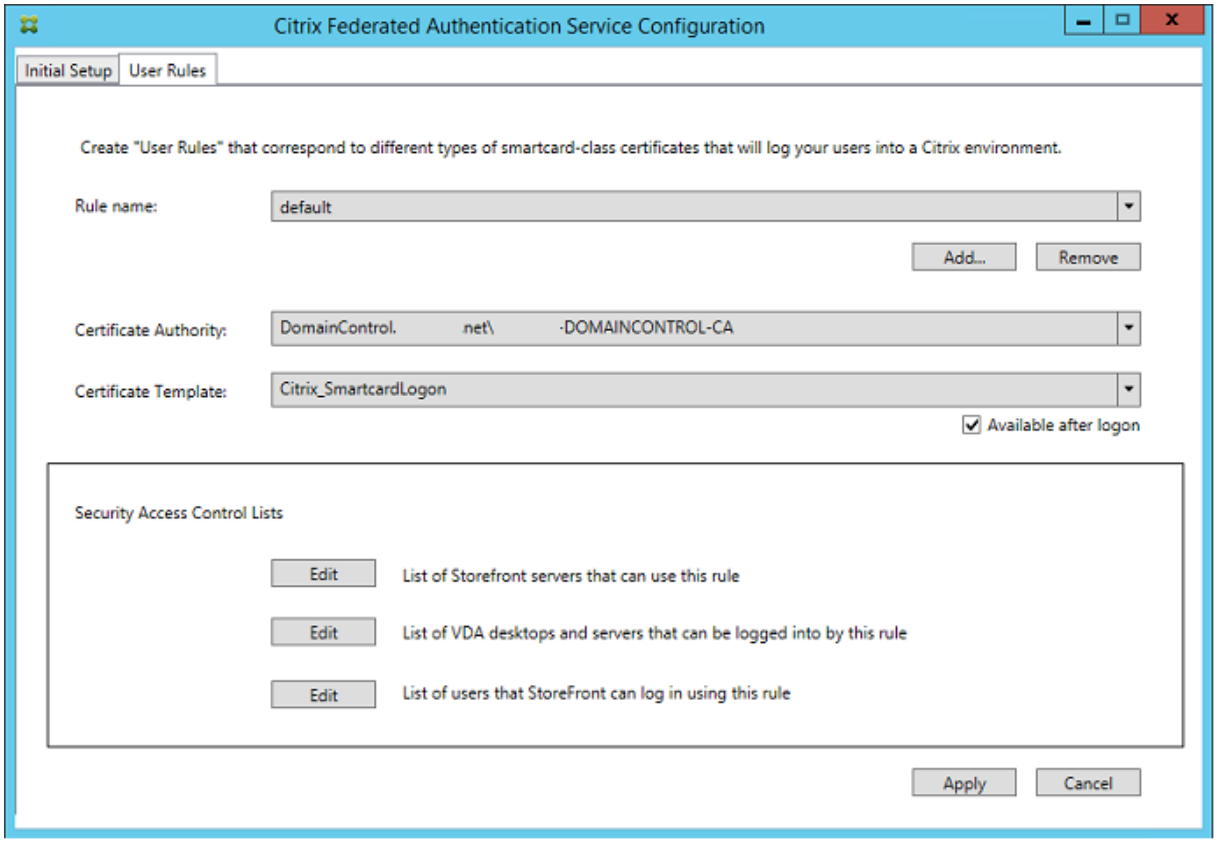


Exécutez l'applet de commande **Set-BrokerSite –TrustRequestsSentToTheXmlServicePort $true** sur le Controller pour permettre à StoreFront de s'authentifier sans les informations d'identification de l'utilisateur.

Installer le Service d'authentification fédérée

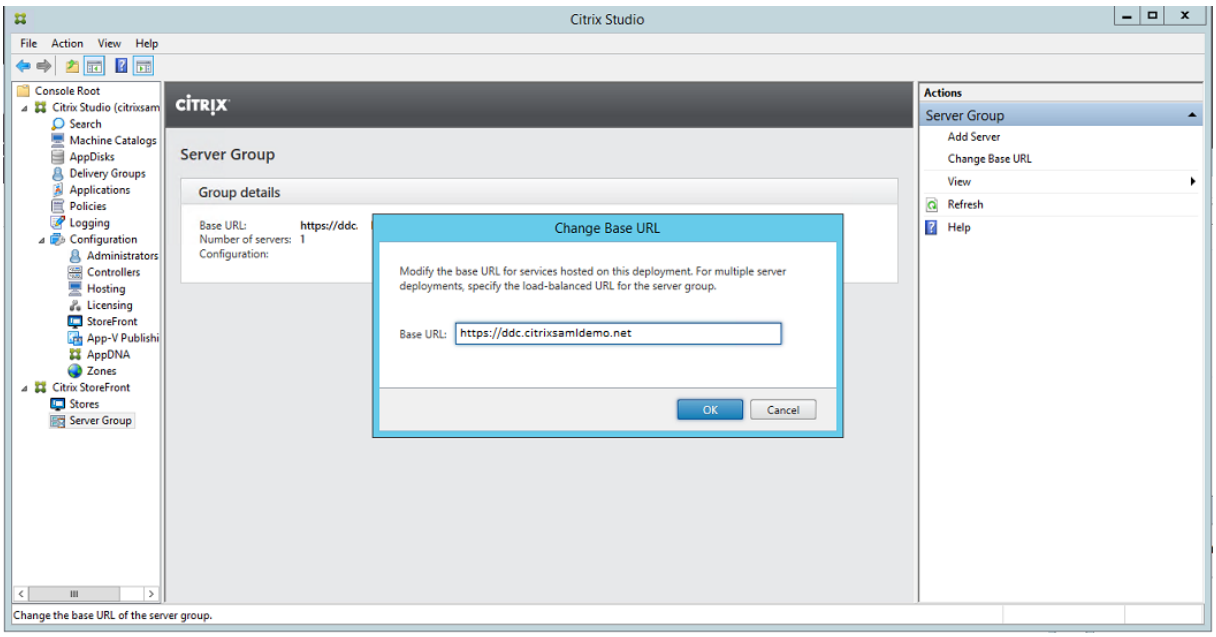
Installez le composant Service d'authentification fédérée (FAS) sur le serveur ADFS et configurez une règle pour faire en sorte que le Controller agisse en tant que StoreFront approuvé.



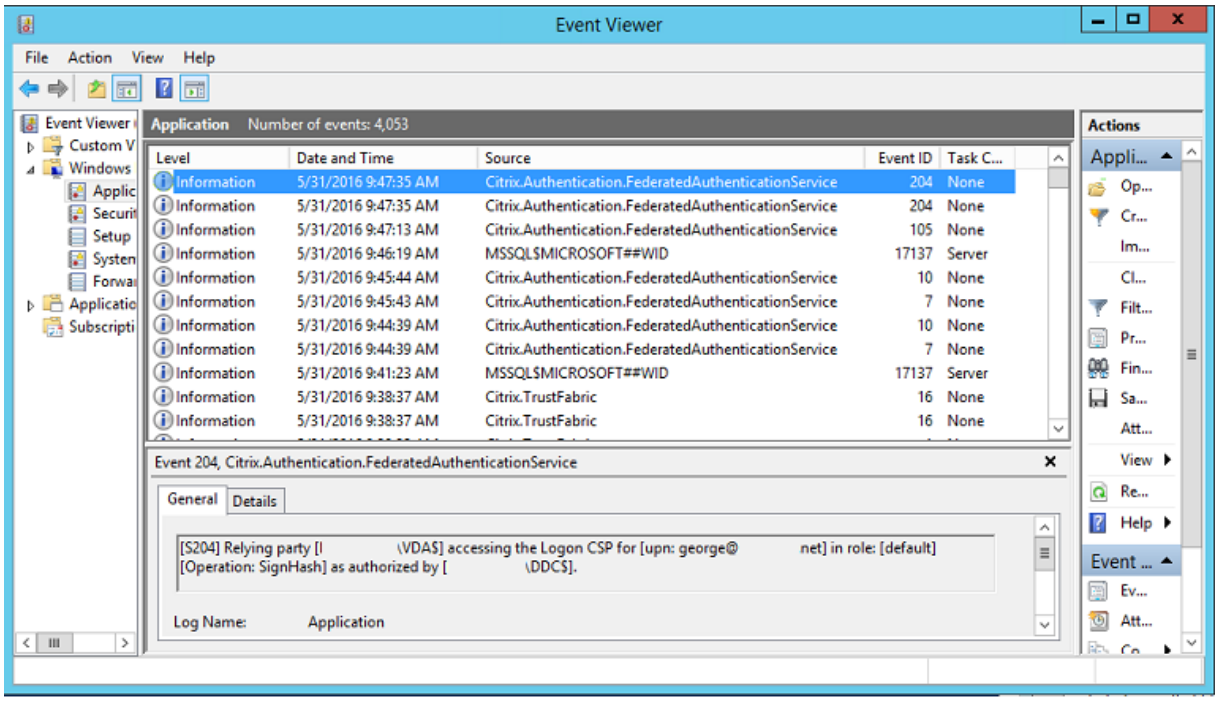


Configurer StoreFront

Demandez un certificat d'ordinateur pour le Delivery Controller, et configurez IIS et StoreFront pour utiliser HTTPS en définissant une liaison IIS pour le port 443 et en modifiant l'adresse de base de StoreFront sur https:.

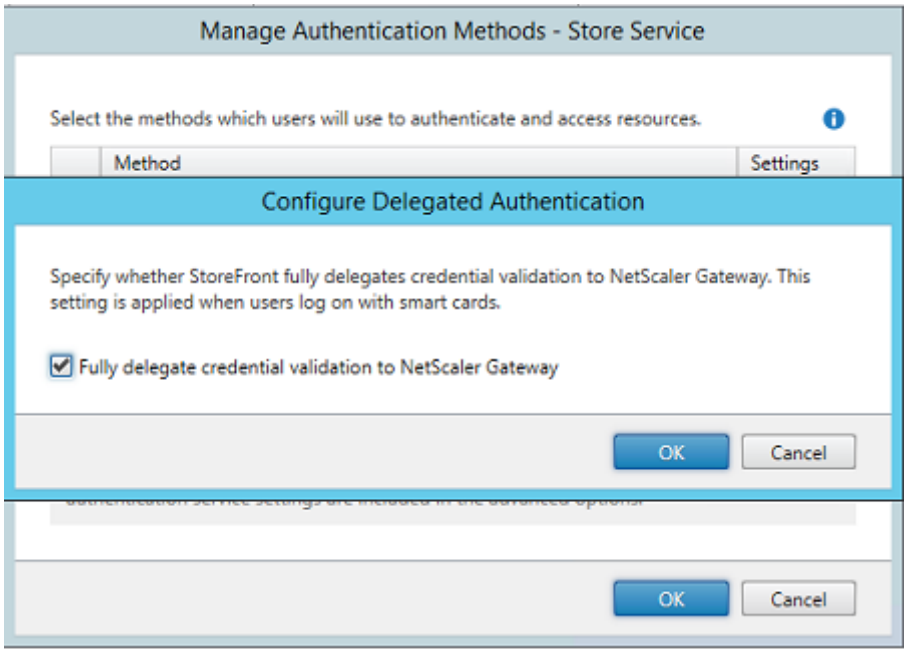


Configurez StoreFront pour utiliser le serveur (FAS) (utilisez le script PowerShell dans l'article Service d'authentification fédérée) et effectuez des tests en interne dans Azure, en vous assurant que l'ouverture de session utilise le FAS en vérifiant l'observateur d'événements sur le serveur FAS.

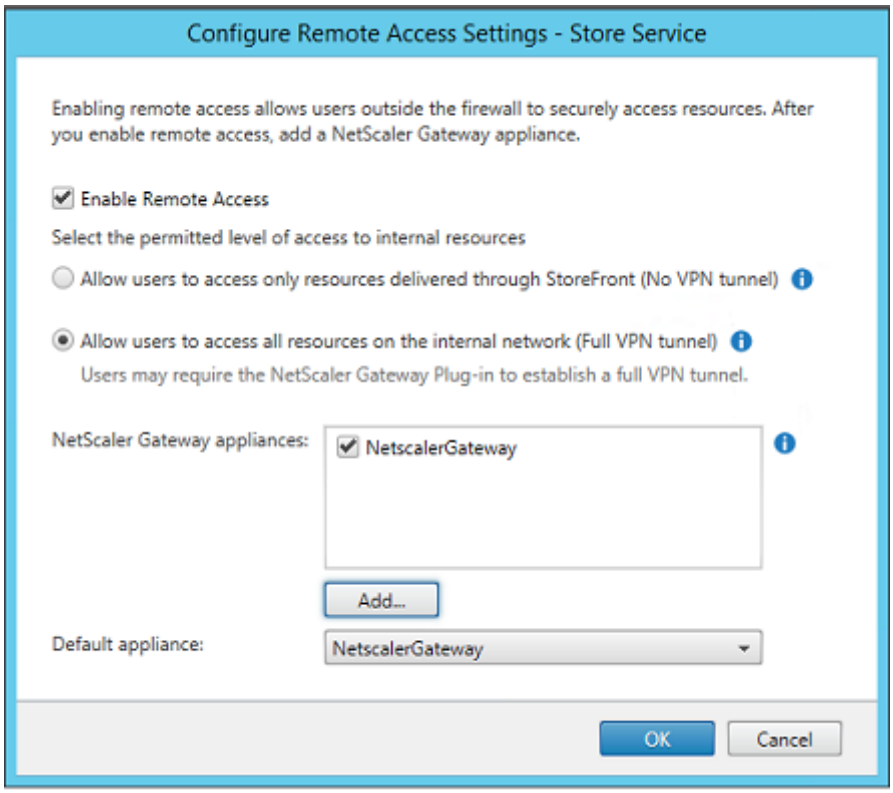


Configurer StoreFront pour utiliser NetScaler

À l'aide de l'interface **Gérer les méthodes d'authentification** de la console de gestion StoreFront, configurez StoreFront de manière à ce qu'il utilise NetScaler pour l'authentification.

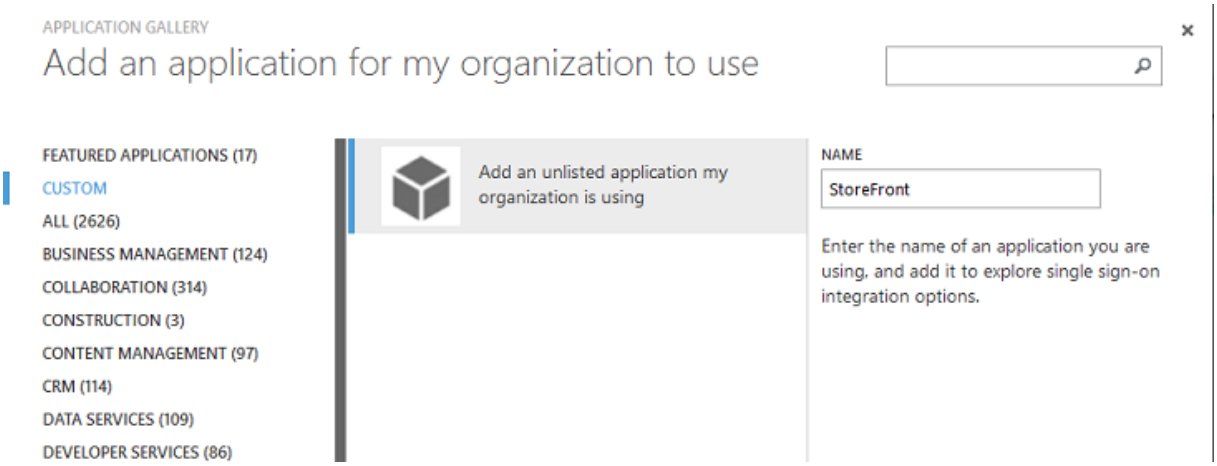


Pour intégrer les options d'authentification NetScaler, configurez une STA (Secure Ticket Authority) et configurez l'adresse NetScaler Gateway.



Configurer une nouvelle application Azure AD pour le Single Sign-On sur StoreFront

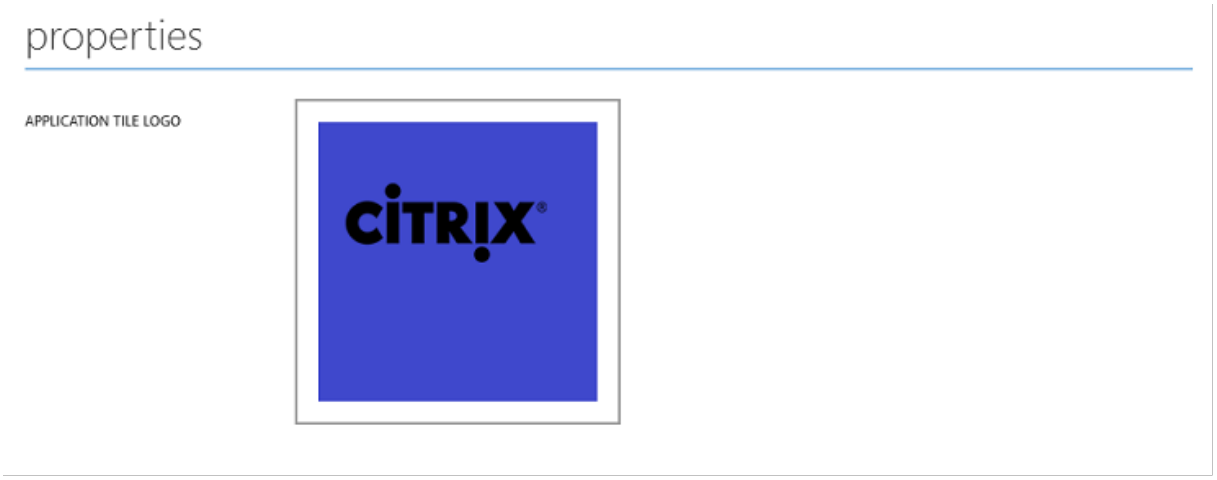
Cette section utilise les fonctionnalités d'authentification unique d'Azure AD SAML 2.0, qui requièrent un abonnement Azure Active Directory Premium. Dans l'outil de gestion Azure AD, sélectionnez **Nouvelle application** et **Ajouter une application à partir de la galerie**.



Sélectionnez **PERSONNALISER > Ajouter une application non répertoriée que mon organisation utilise** pour créer une nouvelle application personnalisée pour vos utilisateurs.

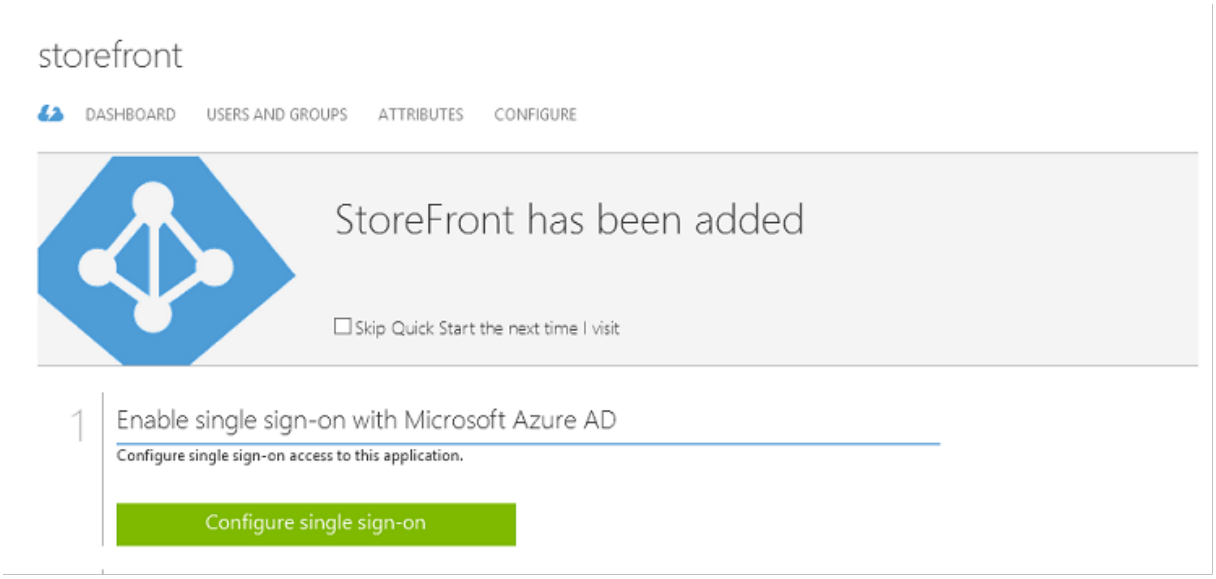
Configurer une icône

Créez une image de 215 x 215 pixels et chargez-la sur la page CONFIGURER pour l'utiliser comme icône pour l'application.

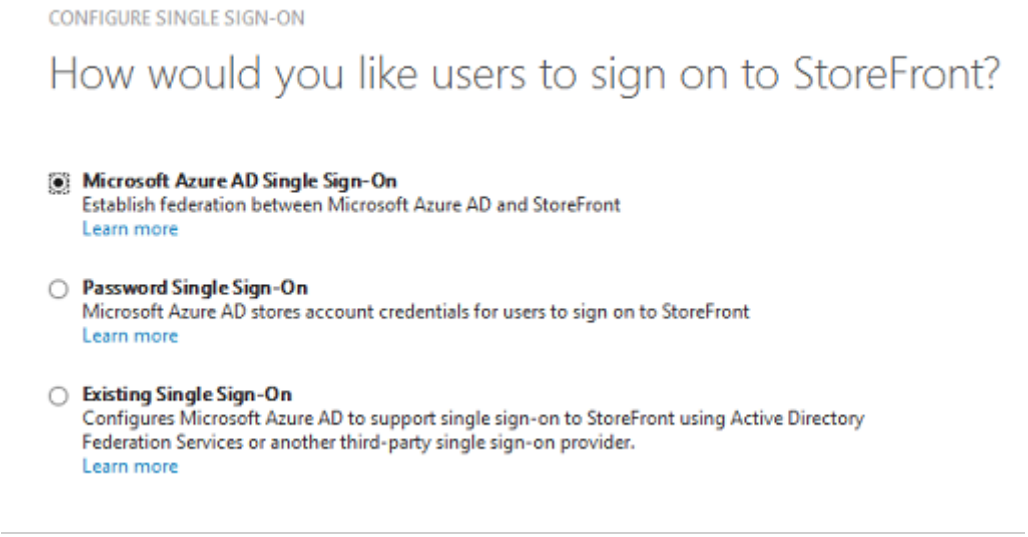


Configurer l'authentification SAML

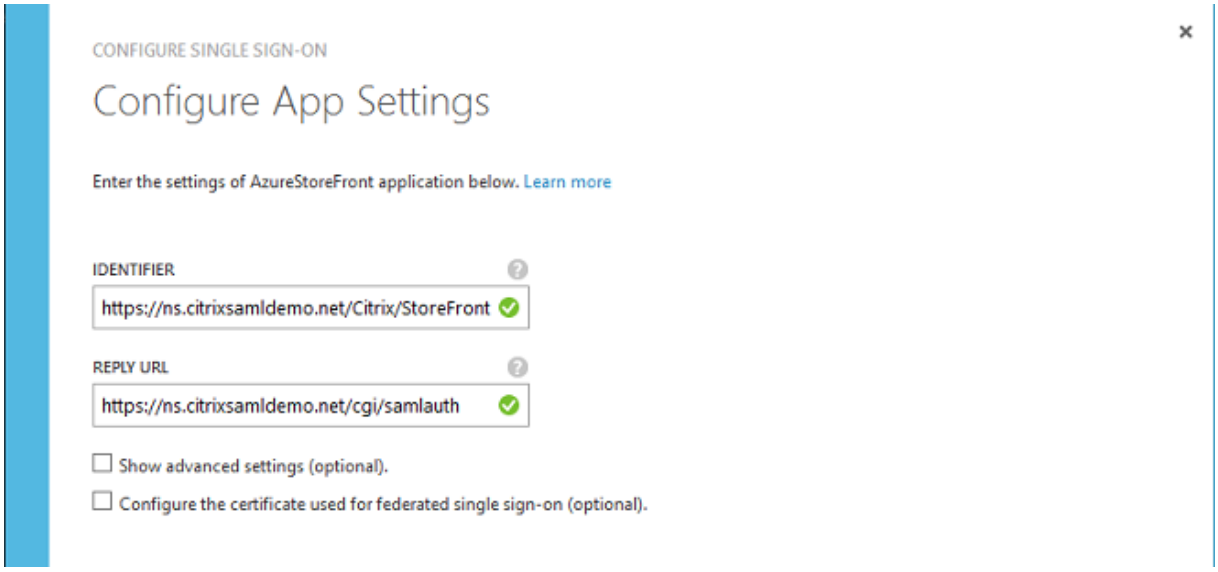
Retournez sur la page de tableau de bord de l'application et sélectionnez **Configurer l'authentification unique**.



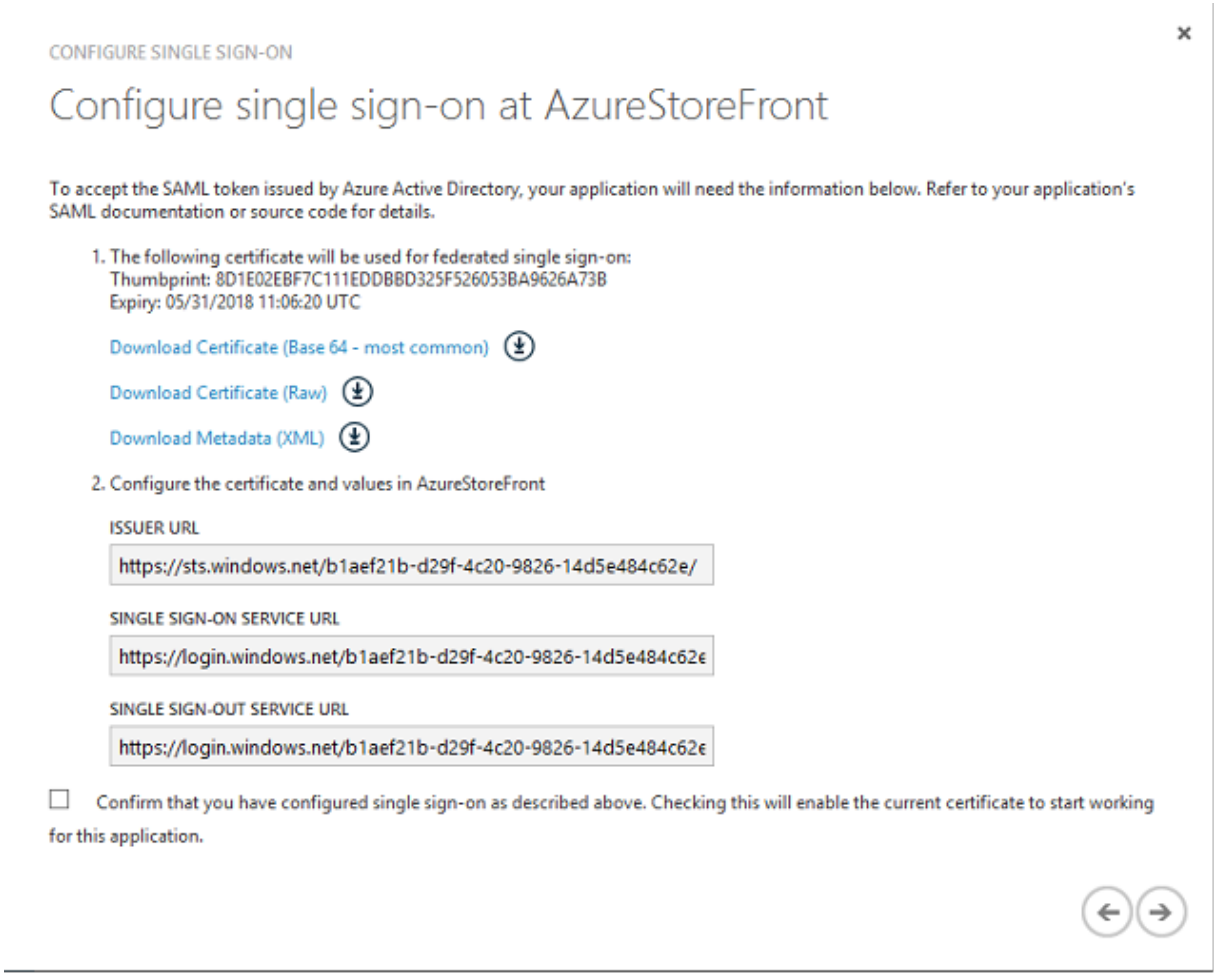
Ce déploiement utilise l'authentification SAML 2.0, qui correspond à **Authentification unique avec Microsoft Azure AD**.



L'**identificateur** peut être une chaîne arbitraire (doit correspondre à la configuration fournie à NetScaler) ; dans cet exemple, l'**URL de réponse** est /cgi/samlauth sur le serveur NetScaler.



La page suivante contient des informations qui sont utilisées pour configurer NetScaler en tant que partie de confiance pour Azure AD.

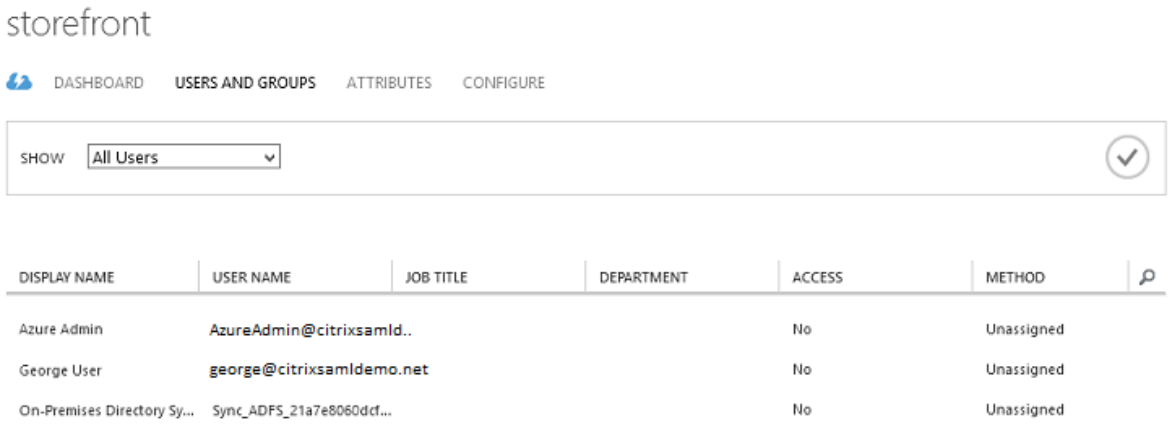


Téléchargez le certificat de signature approuvé base 64 et copiez les URL de connexion et de décon-

nexion. Collez ces dernières dans les écrans de configuration de NetScaler qui suivent.

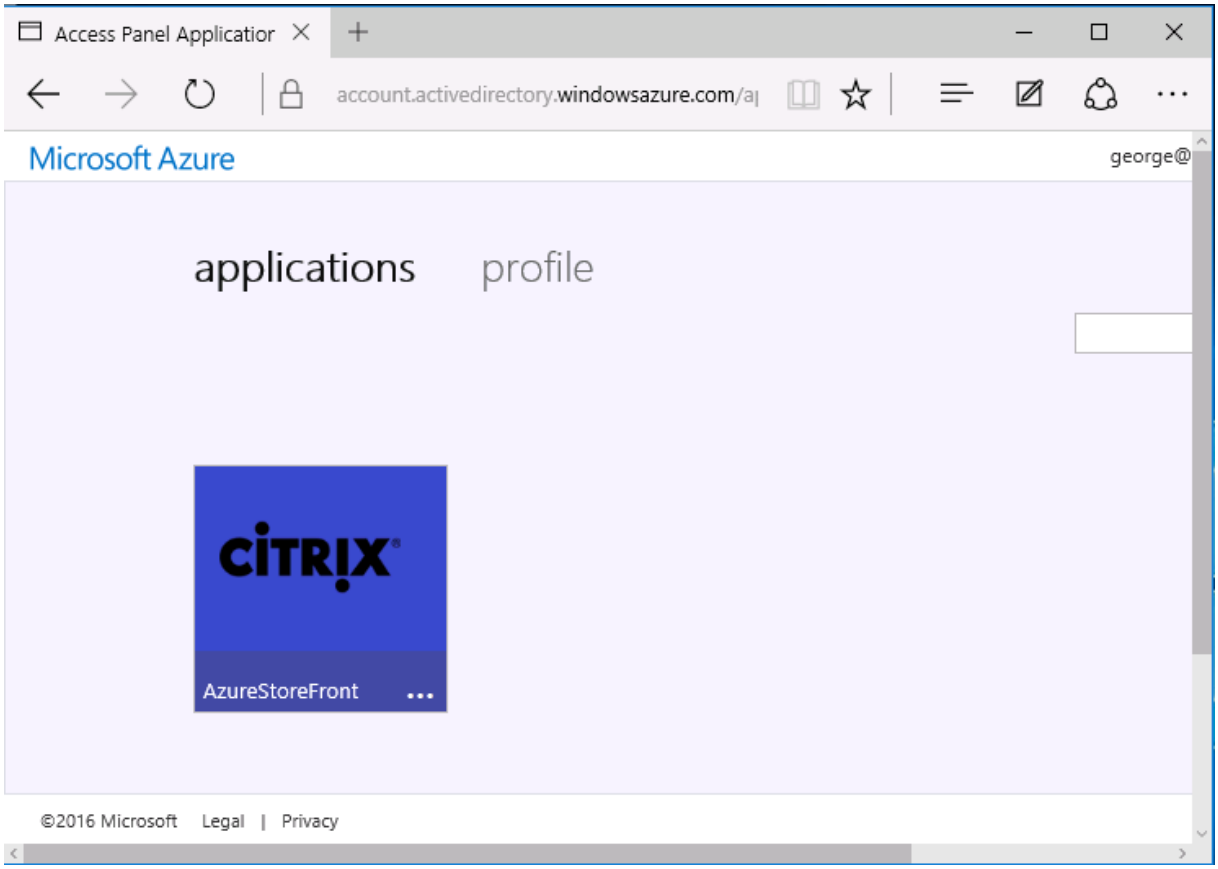
Attribuer l'application aux utilisateurs

La dernière étape consiste à activer l'application afin qu'elle apparaisse sur la page de contrôle "myapps.microsoft.com" des utilisateurs. Cette opération est réalisée sur la page UTILISATEURS ET GROUPES. Attribuez l'accès aux comptes d'utilisateurs de domaine synchronisés par Azure AD Connect. D'autres comptes peuvent également être utilisés, mais ils doivent être explicitement mappés car ils ne sont pas conformes au format <utilisateur>@<domaine>.



Page MyApps

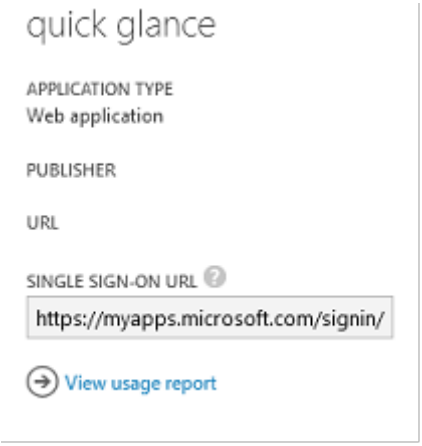
Lorsque l'application a été configurée, elle s'affiche dans les listes d'applications Azure des utilisateurs lorsqu'ils visitent https://myapps.microsoft.com.



Lorsqu'il est joint à Azure AD, Windows Azure 10 prend en charge l'authentification unique aux applications Azure pour l'utilisateur qui ouvre une session. Le fait de cliquer sur l'icône dirige le navigateur vers la page Web SAML cgi/samlauth qui a été configurée précédemment.

URL d'authentification unique

Retournez à l'application dans le tableau de bord Azure AD. Une adresse URL d'authentification unique est maintenant disponible pour l'application. Cette adresse URL est utilisée pour fournir des liens de navigateur Web ou pour créer des raccourcis du menu Démarrer qui dirigent les utilisateurs directement dans StoreFront.



Collez cette adresse URL dans un navigateur Web pour vous assurer que vous êtes redirigé par Azure AD sur la page Web NetScaler cgi/samlauth configurée précédemment. Ceci fonctionne uniquement pour les utilisateurs qui ont été attribués, et fournira l'authentification unique uniquement aux sessions Windows 10 jointes à Azure AD. (Les autres utilisateurs seront invités à entrer des informations d'identification Azure AD).

Installer et configurer NetScaler Gateway

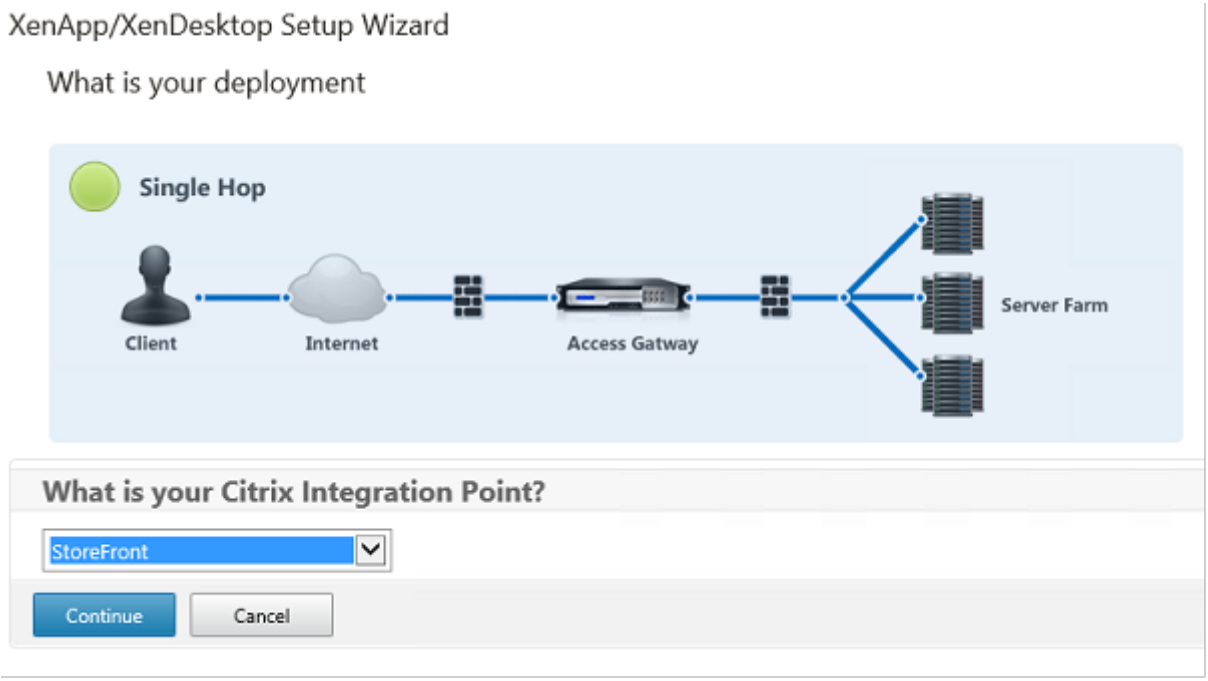
Pour accéder à distance au déploiement, cet exemple utilise une VM distincte exécutant NetScaler. Cela peut être acheté sur le Azure Store. Cet exemple utilise la version « BYOL » (avec apport de sa propre licence) de NetScaler 11.0.

Ouvrez une session sur la VM NetScaler en pointant un navigateur Web sur l'adresse IP interne et en entrant les informations d'identification spécifiées lorsque l'utilisateur s'est authentifié. Notez que vous devez modifier le mot de passe de l'utilisateur nsroot dans la VM Azure AD.

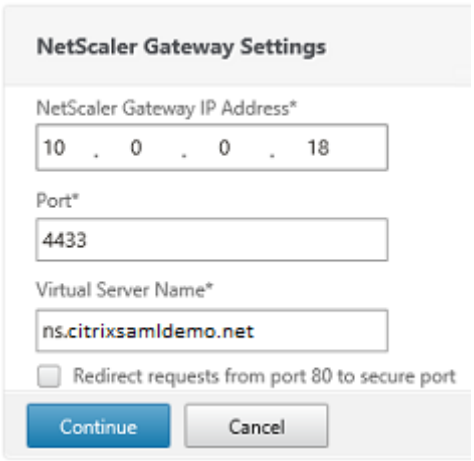
Ajoutez des licences en sélectionnant **redémarrer** après l'ajout de chaque fichier de licences, puis pointez la résolution DNS vers le contrôleur de domaine Microsoft.

Exécuter l'assistant d'installation XenApp et XenDesktop

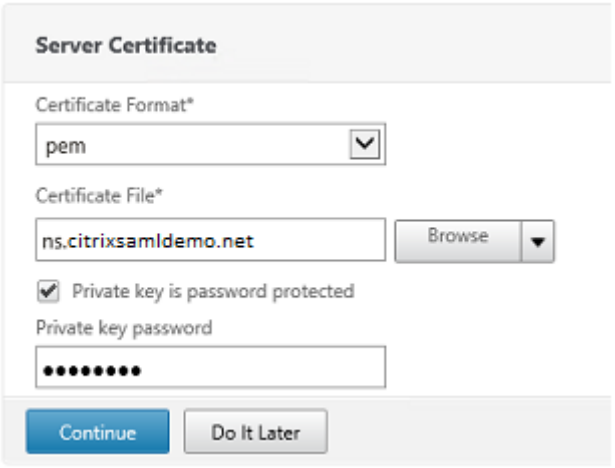
Cet exemple démarre en configurant une intégration StoreFront simple sans SAML. Une fois que le déploiement est opérationnel, il ajoute une stratégie d'ouverture de session SAML.



Sélectionnez les paramètres NetScaler StoreFront standard. À des fins d'utilisation dans Microsoft Azure, cet exemple configure le port 4433, plutôt que le port 443. Vous pouvez également transférer le port ou remapper le site Web d'administration de NetScaler.

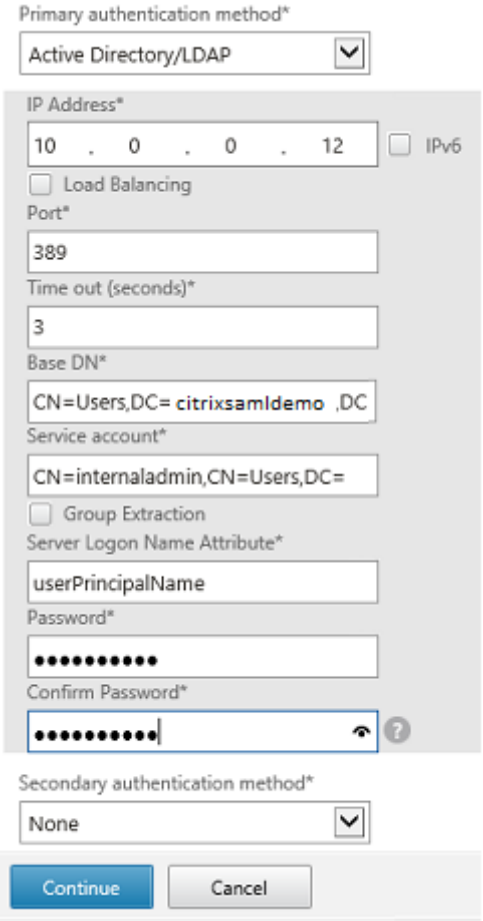


À des fins de simplicité, l'exemple charge un certificat de serveur existant et la clé privée stockée dans un fichier.



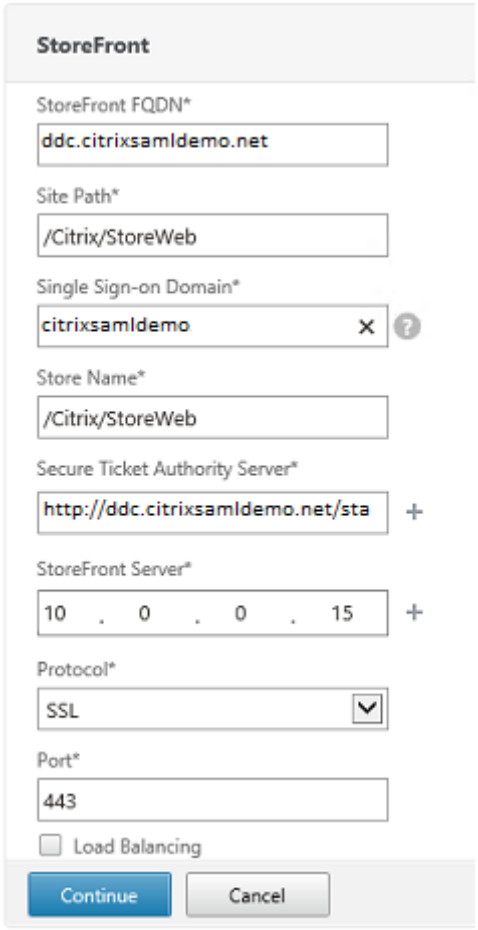
Configurer le contrôleur de domaine pour la gestion de comptes AD

Le contrôleur de domaine sera utilisé pour la résolution de compte, il convient donc d'ajouter son adresse IP dans la méthode d'authentification principale. Notez les formats attendus dans chaque champ de la boîte de dialogue.



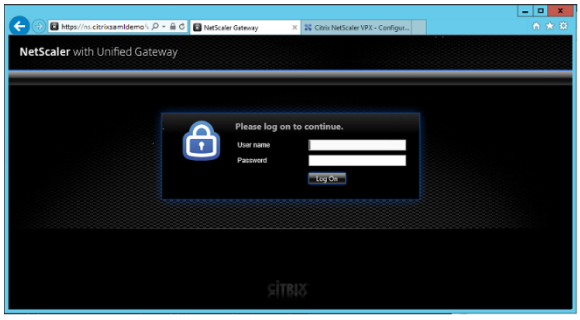
Configurer l'adresse de StoreFront

Dans cet exemple, StoreFront a été configuré avec HTTPS, vous devez donc sélectionner les options du protocole SSL.



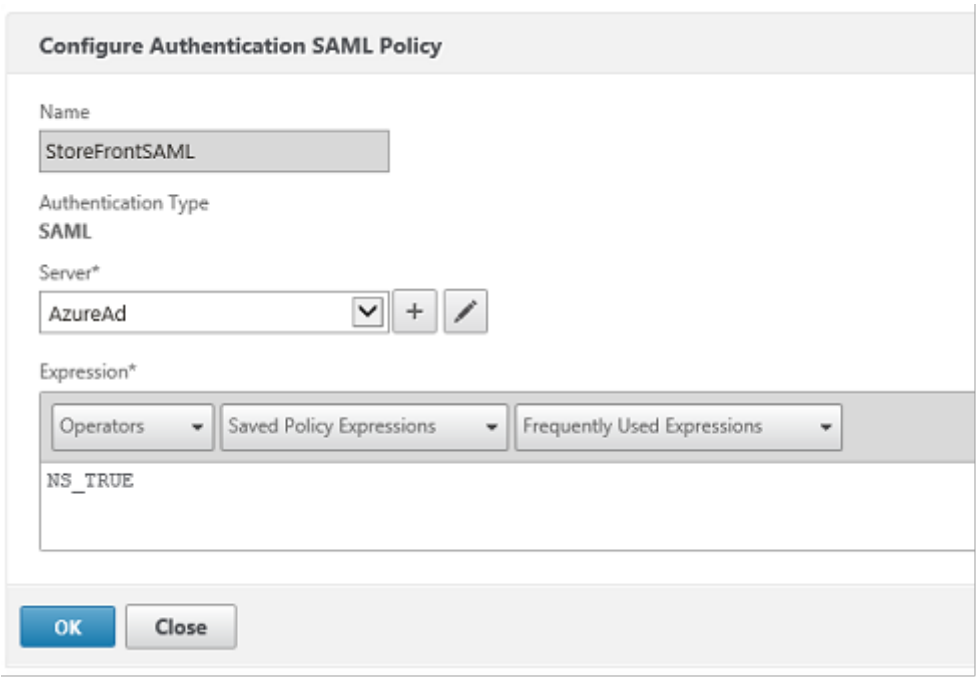
Vérifier le déploiement NetScaler

Connectez-vous à NetScaler et vérifiez le succès de l'authentification et du lancement avec le nom d'utilisateur et mot de passe.

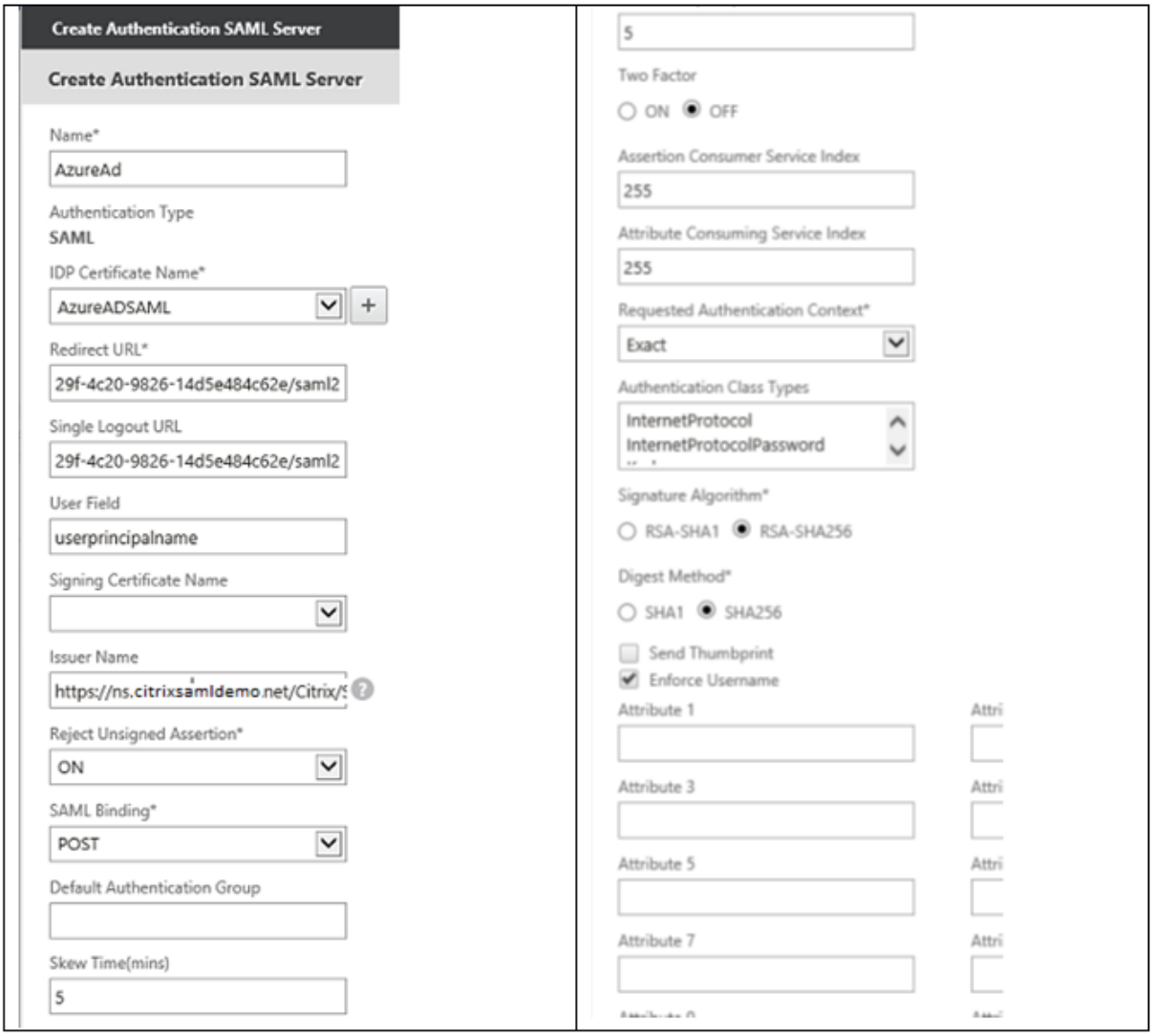


Activer la prise en charge de l'authentification SAML NetScaler

L'utilisation de SAML avec StoreFront est similaire à l'utilisation de SAML avec d'autres sites Web. Ajoutez une nouvelle stratégie SAML avec une expression **NS_TRUE**.



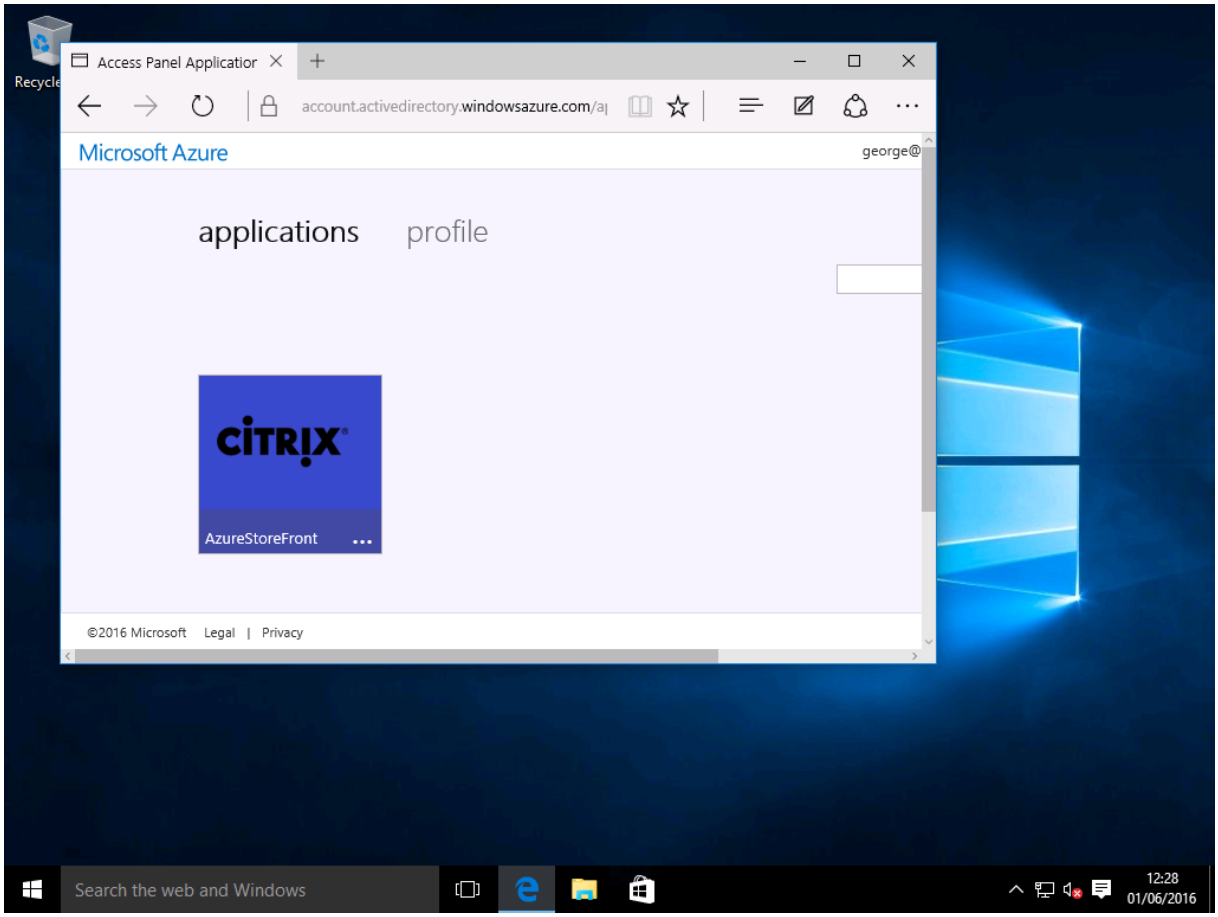
Configurez le nouveau serveur IdP SAML à l'aide des informations obtenues précédemment depuis Azure AD.



Vérifier le système de bout en bout

Ouvrez une session sur un bureau Windows 10 joint à Azure AD à l'aide d'un compte enregistré dans Azure AD. Lancez Microsoft Edge et connectez-vous à : https://myapps.microsoft.com.

Le navigateur Web devrait afficher les applications Azure AD de l'utilisateur.



Vérifiez qu'un clic sur l'icône vous redirige vers un serveur StoreFront authentifié.

De même, vérifiez que les connexions directes utilisant l'URL d'authentification unique et qu'une connexion directe au site NetScaler vous redirigent vers Microsoft Azure et vice versa.

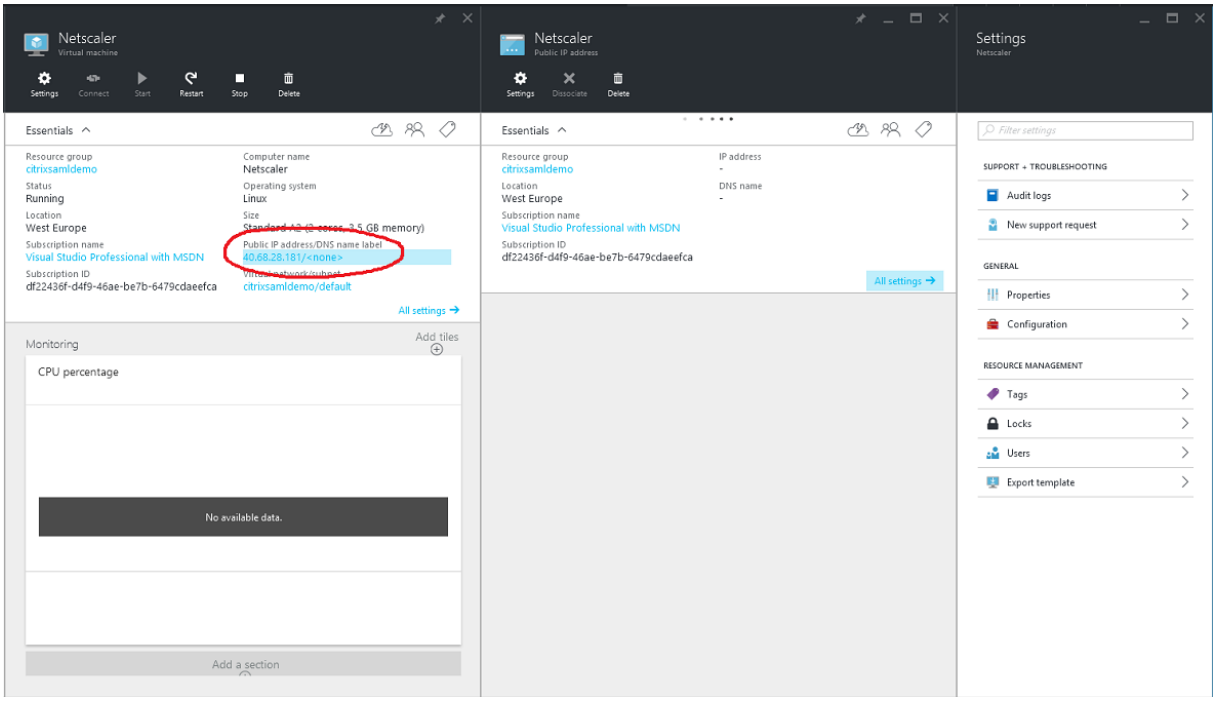
Enfin, vérifiez que les machines non jointes à Azure AD fonctionnent également avec les mêmes URL (bien qu'une authentification unique explicite à Azure AD sera utilisée pour la première connexion).

Annexe

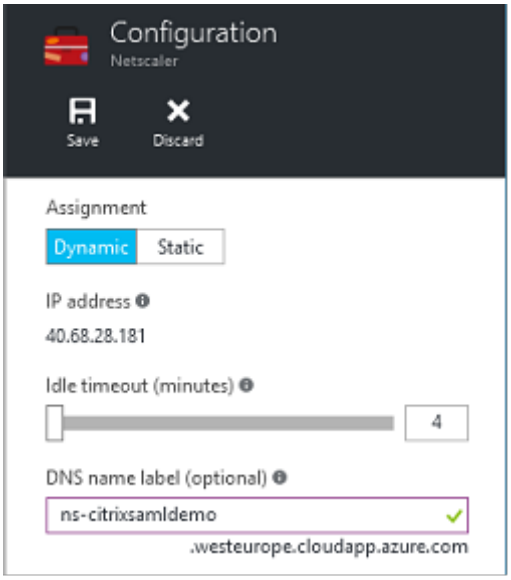
Plusieurs options standard doivent être configurées lors de la création d'une VM dans Azure.

Fournir une adresse IP publique et une adresse DNS

Azure attribue à toutes les VM une adresse IP sur le sous-réseau interne (10.*.*.* dans cet exemple). Par défaut, une adresse IP publique est également fournie et cette dernière peut être référencée par un nom DNS mis à jour de manière dynamique.



Dans **Configuration**, sélectionnez **Public IP address/DNS name label**. Choisissez une adresse DNS publique pour la VM. Elle peut être utilisée pour les références CNAME dans d'autres fichiers de zone DNS, pour s'assurer que tous les enregistrements DNS pointent toujours vers la VM, même si l'adresse IP est réallouée.

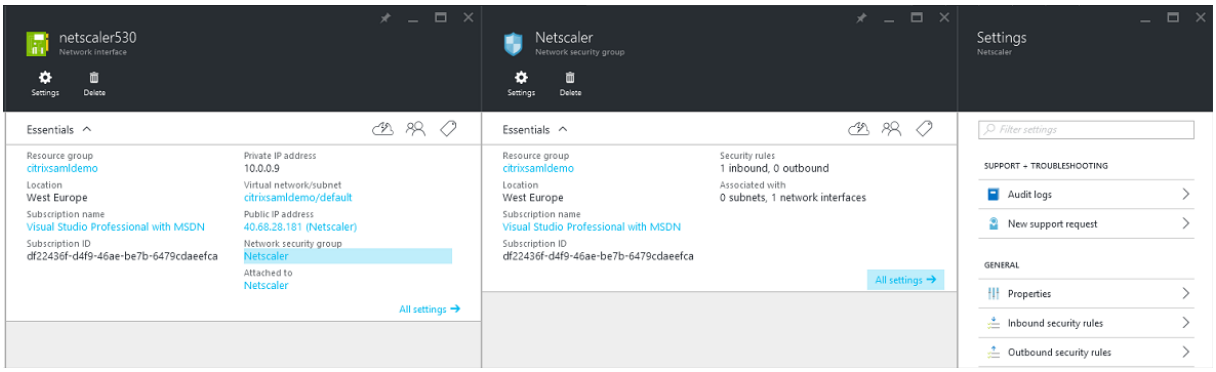


Configurer des règles de pare-feu (groupe de sécurité)

Chaque VM dans un cloud contient un ensemble de règles de pare-feu appliquées automatiquement, connues sous le nom de groupe de sécurité. Le groupe de sécurité contrôle le trafic transféré depuis

l'adresse publique vers l'adresse IP privée. Par défaut, Azure permet à RDP d'être transféré à toutes les VM. Les serveurs NetScaler et ADFS doivent également transférer le trafic TLS (443).

Ouvrez **Network Interfaces** pour une VM et cliquez sur **Network Security Group**. Configurez l'option **Inbound security rules** pour autoriser le trafic réseau approprié.



Informations connexes

- L'article Service d'authentification fédérée est le document de référence principal pour obtenir des informations sur l'installation et la configuration du FAS.
- Les déploiements FAS courants sont décrits dans l'article Vue d'ensemble des architectures du Service d'authentification fédérée.
- Des informations pratiques sont disponibles dans l'article Configuration et gestion du Service d'authentification fédérée.

Guide pratique sur le Service d'authentification fédérée : configuration et gestion

November 8, 2018

Les articles suivants fournissent des informations de configuration et de gestion avancées pour le Service d'authentification fédérée (FAS) :

- Protection de clé privée
- Configuration de l'autorité de certification
- Gestion du réseau et de la sécurité
- Résoudre les problèmes d'ouverture de session Windows
- Fichiers d'aide de l'applet de commande du SDK PowerShell

Informations connexes :

- L'article Service d'authentification fédérée est le document de référence principal pour obtenir des informations sur l'installation et la configuration du FAS.

- L'article Vue d'ensemble des architectures du Service d'authentification fédérée propose un résumé des principales architectures FAS, ainsi que des liens vers d'autres articles sur les architectures plus complexes.

Configuration de l'autorité de certification du Service d'authentification fédérée

January 23, 2019

Cet article décrit la configuration avancée du Service d'authentification fédérée Citrix (FAS) pour l'intégration avec les serveurs d'autorité de certification (CA) qui ne sont pas pris en charge par la console de gestion FAS. Les instructions utilisent les API PowerShell fournies par FAS. Vous devez disposer de connaissances de base sur PowerShell avant d'exécuter les instructions de cet article.

Définir plusieurs serveurs d'autorité de certification à utiliser dans FAS

Cette section décrit comment configurer un serveur FAS unique pour qu'il utilise plusieurs serveurs d'autorité de certification pour émettre des certificats. Cela permet l'équilibrage de charge et le basculement des serveurs d'autorité de certification.

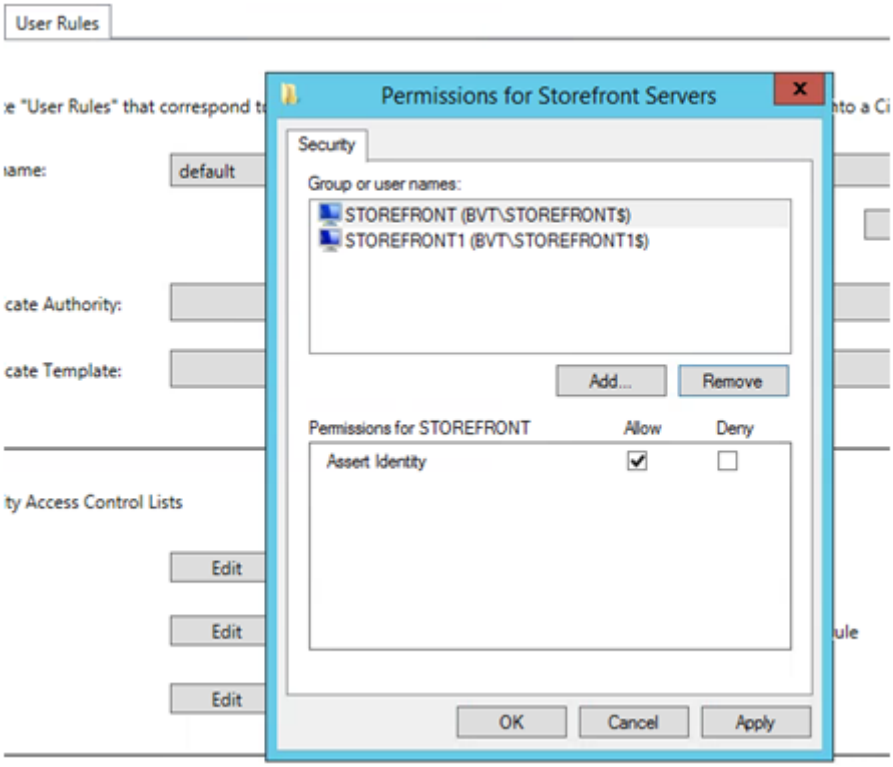
Étape 1 : Découvrir combien de serveurs d'autorité de certification FAS peut localiser

Utilisez l'applet de commande Get-FASMsCertificateAuthority pour déterminer les serveurs d'autorité de certification auxquels FAS peut se connecter. Dans l'exemple suivant, FAS peut se connecter à trois serveurs d'autorité de certification.

```
PS > Add-PSSnapin Citrix*
PS > Get-FASMsCertificateAuthority

Address                                IsDefault PublishedTemplates
-------                                --------- ------------------
DC1.bvt.local\bvt-DC1-CA                   False {Citrix_SmartcardLogon, Citrix_Regis...
ca1.bvt.local\CA1.bvt.local                False {Citrix_SmartcardLogon, Citrix_Regis...
ca2.bvt.local\ca2.bvt.local                False {Citrix_SmartcardLogon, Citrix_Regis...
```

Étape 2 : Modifier la définition de certificat existante

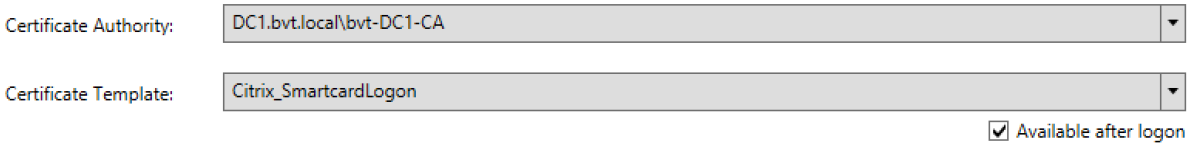
Citrix vous recommande de créer un rôle à l'aide de la console de gestion FAS, plutôt qu'à l'aide de PowerShell pour créer le rôle. Cela évite d'avoir à ajouter le SDL manuellement ultérieurement. Dans l'exemple suivant, un rôle appelé « default » est créé à l'aide de la règle d'accès configurée :



Pour ajouter plusieurs autorités de certification au champ d'autorité de certification (ce qui n'est pas pris en charge depuis la console d'administration dans cette version), vous devez configurer la définition de certificat. Tout d'abord, vous devez connaître le nom de la définition de certificat. Le nom ne peut pas être déterminé à partir de la console de gestion ; utilisez l'applet de commande Get-FASCertificateDefinition.

```
PS > Get-FASCertificateDefinition

Name                    : default_Definition
CertificateAuthorities  : {DC1.bvt.local\bvt-DC1-CA}
MsTemplate              : Citrix_SmartcardLogon
AuthorizationCertificate : 86ce221c-7599-43a3-9dbd-8e6a3c2be7b7
PolicyOids              : {}
InSession               : True
```

L'équivalent dans l'interface utilisateur est :



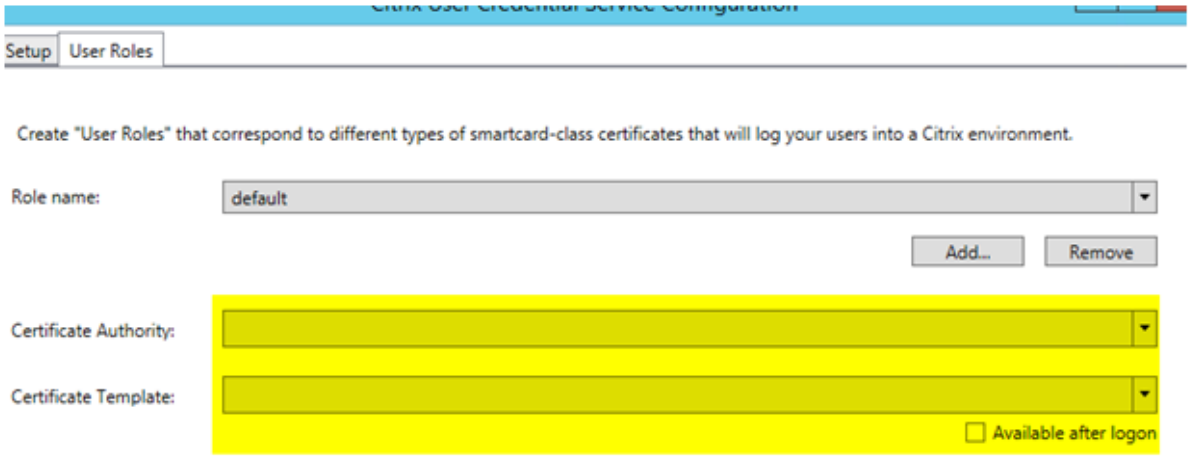
Une fois que vous avez le nom de la définition de certificat, modifiez la définition de certificat pour obtenir une liste de CertificateAuthorities, plutôt qu'un seul certificat :


```
PS > Set-FASCertificateDefinition -Name default_Definition -CertificateAuthorities @("DC1.bvt.
local\bvt-DC1-CA", "ca1.bvt.local\CA1.bvt.local", "ca2.bvt.local\ca2.bvt.local")
```

L'applet de commande Get-FASCertificateDefinition renvoie maintenant :

```
PS > Get-FASCertificateDefinition
Name                    : default_Definition
CertificateAuthorities  : {DC1.bvt.local\bvt-DC1-CA, ca1.bvt.local\CA1.bvt.local, ca2.bvt.local\ca2.bvt.local}
MsTemplate              : Citrix_SmartcardLogon
AuthorizationCertificate : 86ce221c-7599-43a3-9dbd-8e6a3c2be7b7
PolicyOids              : {}
InSession               : True
```

Remarque : votre console de gestion FAS ne sera pas opérationnelle après cette opération. Vous verrez un champ vide dans « Certificate Authority » et « Certificate Template » après le chargement :



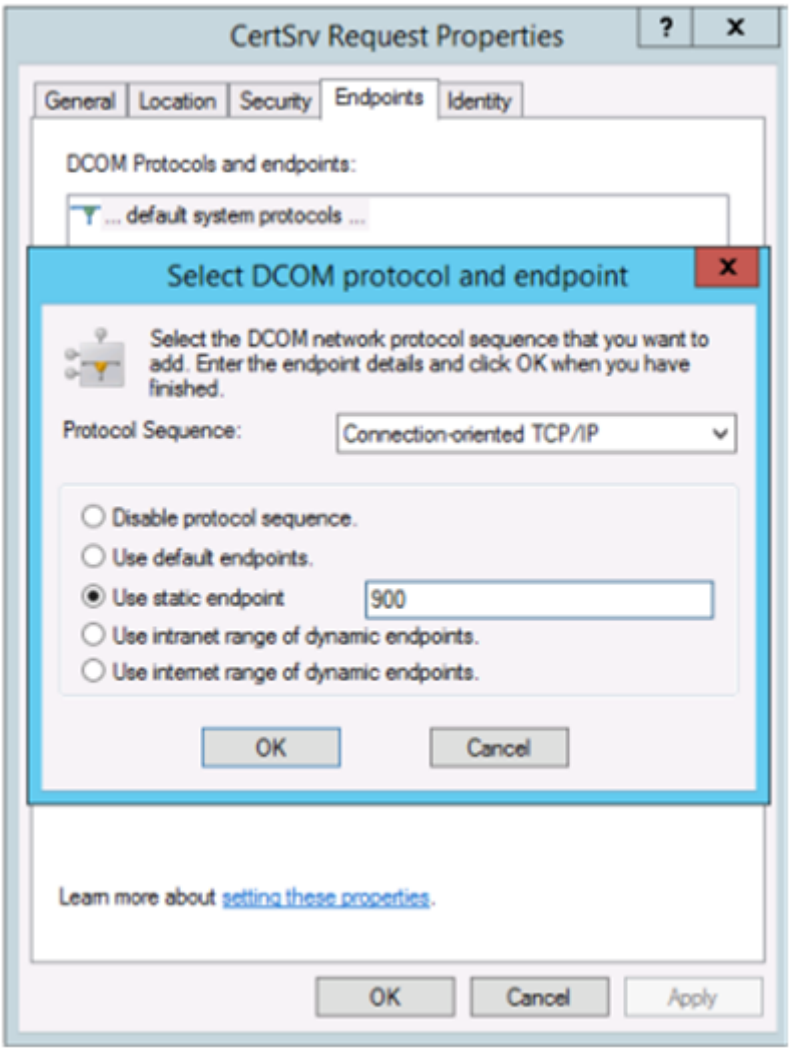
FAS fonctionne toujours. Si vous utilisez la console pour modifier la règle d'accès, il vous suffit de répéter l'étape 2 pour afficher toutes les autorités de certification.

Changements de comportement attendus

Une fois que vous avez configuré le serveur FAS avec de multiples serveurs d'autorité de certification, la génération de certificat utilisateur est distribuée entre tous les serveurs d'autorité de certification configurés. De plus, si l'un des serveurs d'autorité de certification configurés échoue, le serveur FAS bascule vers un autre serveur d'autorité de certification disponible.

Configurer l'autorité de certification Microsoft pour l'accès TCP

Par défaut, l'autorité de certification Microsoft utilise DCOM pour l'accès. Cela peut compliquer la mise en place d'un pare-feu de sécurité, par conséquent Microsoft permet le basculement vers un port TCP statique. Sur l'autorité de certification Microsoft, ouvrez le panneau de configuration de DCOM et modifiez les propriétés de l'application « CertSrv DCOM » :



Modifiez les points de terminaison (endpoints) pour sélectionner un point de terminaison statique et spécifiez un numéro de port TCP (900 dans l'illustration ci-dessus).

Redémarrez l'autorité de certification Microsoft et envoyez une demande de certificat. Si vous exécutez «netstat –a –n –b », vous verrez que certsvr écoute désormais le port 900 :

```
 TCP    0.0.0.0:636            dc:0                   LISTENING
[lsass.exe]
 TCP    0.0.0.0:900            dc:0                   LISTENING
[certsrv.exe]
 TCP    0.0.0.0:3268           dc:0                   LISTENING
[lsass.exe]
 TCP    0.0.0.0:3269           dc:0                   LISTENING
```

Il n'est pas nécessaire de configurer le serveur FAS (ou toute autre machine utilisant l'autorité de certification), car DCOM a une étape de négociation utilisant le port RPC. Lorsqu'un client doit utiliser DCOM, il se connecte au service DCOM RPC sur le serveur de certificats et demande l'accès à un serveur DCOM particulier. Cela déclenche l'ouverture du port 900 et le serveur DCOM indique au serveur FAS

comment se connecter.

Pré-générer les certificats utilisateur

La durée d'ouverture de session pour les utilisateurs peut nettement s'améliorer lorsque les certificats utilisateur sont pré-générés dans le serveur FAS. Les sections suivantes décrivent comment y procéder, pour un ou plusieurs serveurs FAS.

Obtenir une liste d'utilisateurs Active Directory

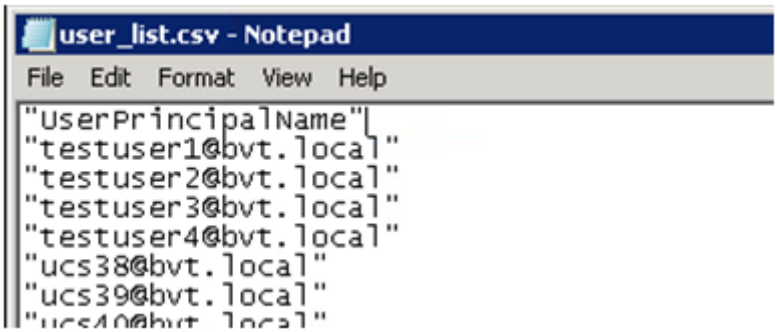
Vous pouvez améliorer la génération de certificat en interrogeant AD et en stockant la liste des utilisateurs dans un fichier (par exemple, un fichier .csv), comme illustré dans l'exemple suivant.

```
Import-Module ActiveDirectory

$searchbase = "cn=users,dc=bvt,dc=local" # AD User Base to Look for Users, leave it blank to search all
$filename = "user_list.csv" # Filename to save

if ($searchbase –ne "") {
   Get-ADUser -Filter {(UserPrincipalName -ne "null") -and (Enabled -eq "true")} -SearchBase $searchbase -Properties
UserPrincipalName |Select UserPrincipalName | Export-Csv -NoTypeInformation -Encoding utf8 -delimiter ","
$filename
} else {
   Get-ADUser -Filter {(UserPrincipalName -ne "null") -and (Enabled -eq "true")}  -Properties UserPrincipalName
|Select UserPrincipalName | Export-Csv -NoTypeInformation -Encoding utf8 -delimiter "," $filename
}
```

Get-ADUser est une applet de commande qui envoie une requête de liste d'utilisateurs. L'exemple ci-dessus contient un argument de filtre pour inclure uniquement les utilisateurs disposant d'un UserPrincipalName et avec un état de compte « activé ».

L'argument SearchBase spécifie la partie d'Active Directory dans laquelle rechercher des utilisateurs. Vous pouvez ignorer cette option si vous voulez inclure tous les utilisateurs présents dans Active Directory. **Remarque :** cette requête peut renvoyer un grand nombre d'utilisateurs.

Le fichier CSV ressemble à l'exemple ci-dessous :



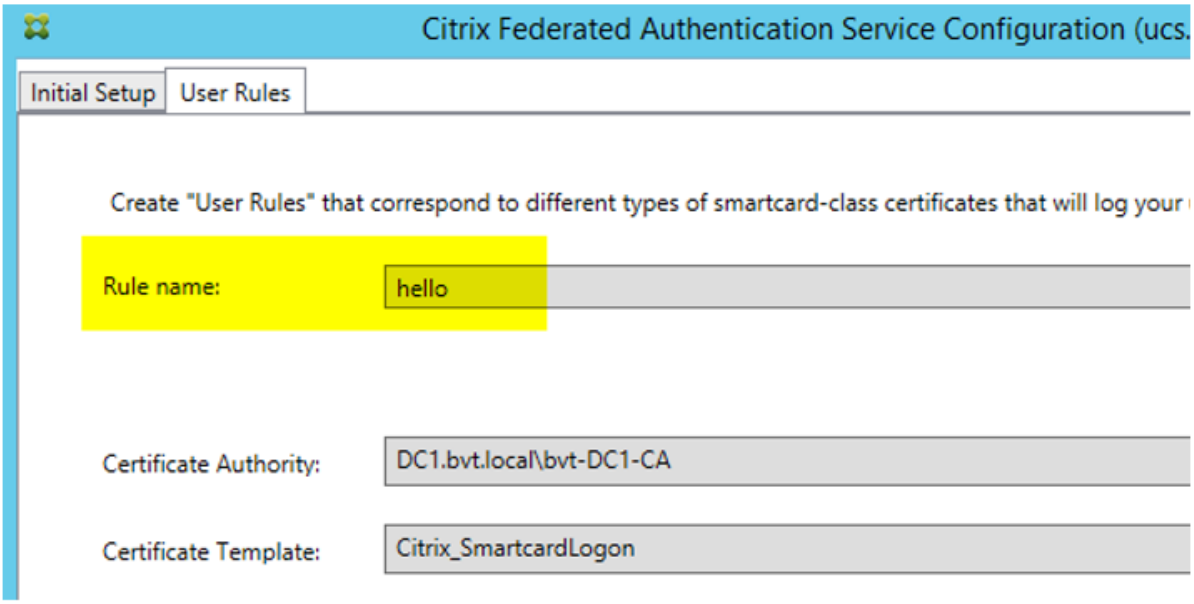
Serveur FAS

Le script PowerShell utilise la liste d'utilisateurs générée et crée une liste de certificats utilisateur.

```
Add-PSSnapin Citrix.A*

$csv = "user_list.csv"
$rule = "default" #rule/role in your admin console
$users = Import-Csv  -encoding utf8 $csv

foreach ( $user in $users )
{
  $server = Get-FASServerForUser -UserPrincipalNames $user.UserPrincipalName
  if ( $server.Server -ne $NULL ) {
     New-FASUserCertificate -Address $server.Server -UserPrincipalName $user.UserPrincipalName -
CertificateDefinition $rule"_Definition" -Rule $rule
  }
  if ( $server.Failover -ne $NULL ) {
     New-FASUserCertificate -Address $server.Failover -UserPrincipalName $user.UserPrincipalName -
CertificateDefinition $rule"_Definition" -Rule $rule
  }
}
```

Si vous disposez de plusieurs serveurs FAS, le certificat d'un utilisateur particulier est généré deux fois : une fois sur le serveur principal et une autre sur le serveur de basculement.

Le script ci-dessus inclut une règle « default ». Si votre règle porte un autre nom (par exemple, « hello »), il vous suffit de modifier la variable $rule dans le script.



Renouveler les certificats d'autorité d'inscription

Si plusieurs serveurs FAS sont utilisés, vous pouvez renouveler un certificat d'autorisation FAS sans affecter les utilisateurs connectés. **Remarque :** bien que vous puissiez également utiliser l'interface utilisateur pour annuler et renouveler l'autorisation FAS, cela a pour effet de réinitialiser les options de configuration FAS.

Effectuez la procédure suivante dans l'ordre indiqué :

1. Créer un nouveau certificat d'autorisation :

```
'New-FasAuthorizationCertificate'
```

2. Noter le GUID du nouveau certificat d'autorisation, renvoyé par :

```
'Get-FasAuthorizationCertificate'
```

3. Placer le serveur FAS en mode de maintenance :

```
'Set-FasServer  -Address \<FAS server\> -MaintenanceMode $true'
```

4. Changer le nouveau certificat d'autorisation :

```
'Set-FasCertificateDefinition  -AuthorizationCertificate \<GUID\>'
```

5. Retirer le serveur FAS du mode de maintenance :

```
'Set-FasServer  -Address \<FAS server\> -MaintenanceMode $false'
```

6. Supprimer l'ancien certificat d'autorisation :

```
'Remove-FasAuthorizationCertificate'
```

Informations connexes

- L'article Service d'authentification fédérée est le document de référence principal pour obtenir des informations sur l'installation et la configuration du FAS.
- Les déploiements FAS courants sont décrits dans l'article Vue d'ensemble des architectures du Service d'authentification fédérée.
- D'autres informations pratiques sont disponibles dans l'article Configuration et gestion du service d'authentification fédérée.

Protection des clés privées du service d'authentification fédérée

February 28, 2019

Introduction

Les clés privées sont stockées par le biais du compte de service réseau et marquées comme non-exportables par défaut.

Il existe deux types de clés privées:

- La clé privée associée au certificat de l'autorité d'inscription (RA), à partir du modèle de certificat Citrix_RegistrationAuthority.
- Les clés privées associées aux certificats utilisateur, à partir du modèle de certificat Citrix_SmartcardLogon.

Il existe en fait deux certificats d'autorité d'inscription : Citrix_RegistrationAuthority_ManualAuthorization (valide pendant 24 heures par défaut) et Citrix_RegistrationAuthority (valide pendant deux ans par défaut).

Lors de l'étape 3 de la configuration initiale dans la console de gestion FAS, lorsque l'administrateur clique sur « Autoriser », le serveur FAS génère une paire de clés et envoie une demande de signature de certificat (CSR) à l'autorité de certification pour le certificat Citrix_RegistrationAuthority_ManualAuthorization. Il s'agit d'un certificat temporaire, valide pendant 24 heures par défaut. L'autorité de certification n'émet pas automatiquement ce certificat ; son émission doit être manuellement autorisée sur l'autorité de certification par un administrateur. Une fois que le certificat a été généré sur le FAS serveur, FAS utilise le certificat Citrix_RegistrationAuthority_ManualAuthorization pour obtenir automatiquement le certificat Citrix_RegistrationAuthority (valide pendant deux ans par défaut). Le serveur FAS supprime le certificat et la clé pour Citrix_RegistrationAuthority_ManualAuthorization dès qu'il obtient le certificat Citrix_RegistrationAuthority.

La clé privée associée au certificat RA est particulièrement sensible car la stratégie de certificat RA permet à toute personne qui dispose de la clé privée d'émettre des demandes de certificat pour le groupe d'utilisateurs configuré dans le modèle. En conséquence, toute personne qui contrôle cette clé peut se connecter à l'environnement en tant qu'utilisateur du groupe.

Vous pouvez configurer le serveur FAS pour protéger les clés privées selon les besoins de sécurité de votre organisation, à l'aide de l'une des configurations suivantes :

- Microsoft Enhanced RSA and AES Cryptographic Provider ou Microsoft Software Key Storage Provider pour le certificat RA et les clés privées des certificats utilisateur.
- Microsoft Platform Key Storage Provider avec une puce Trusted Platform Module (TPM) pour la clé privée du certificat RA et Microsoft Enhanced RSA and AES Cryptographic Provider ou Microsoft Software Key Storage Provider pour les clés privées des certificats utilisateur.

- Un fournisseur de service cryptographique ou un fournisseur de stockage de clés de module de sécurité matérielle (HSM) avec le périphérique HSM pour le certificat RA et les clés privées des certificats utilisateur.

Paramètres de configuration des clés privées

Configurez FAS pour utiliser l'une des trois options. Utilisez un éditeur de texte pour modifier le fichier Citrix.Authentication.FederatedAuthenticationService.exe.config. L'emplacement par défaut du fichier est le dossier Program Files\Citrix\Federated Authentication Service sur le serveur FAS.

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <!-- This option switch between CAPI API  (true) and CNG API (false) Cryptographic Providers  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp" value="false"/>

    <!-- Specify the Cryptographic Service Provider (CSP) / Key Storage Provider (KSP) Name.  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="Microsoft Software Key Storage Provider"/ -->

    <!-- Specify the Cryptographic Service Provider Type (only for CSP - not KSP).  For example: PROV_RSA_AES is 24  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType" value="24"/ -->

    <!-- Specify Private Key protection [NoProtection|GenerateNonExportableKey|GenerateTPMProtectedKey] -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection" value="GenerateNonExportableKey"/>

    <!-- Specify RSA Key length -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength" value="2048"/>

    <!-- Logging: Event log Verbosity (0 Disabled, 1 Errors, 2 Warnings, 3 Informational) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.LogLevel" value="3" / -->

    <!-- Logging: Event IDs to not log (comma separated) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.Supress" value="" / -->

    <!-- Logging: Disable Key Management logs -->
    <!-- add key="Citrix.TrustFabric.Logging.SystemLog" value=""/ -->
  </appSettings>
<startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/></startup></configuration>
```

Le FAS lit le fichier de configuration uniquement lorsque le service démarre. Si des valeurs sont modifiées, le FAS doit être redémarré avant qu'il reflète les nouveaux paramètres.

Définissez les valeurs appropriées dans le fichier Citrix.Authentication.FederatedAuthenticationService.exe.config comme suit :

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderLegacyCsp** (basculement entre API CAPI et CNG)

Valeur	Commentaires
vrai	Utiliser les API CAPI
false (valeur par défaut)	Utiliser les API CNG

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderName** (nom du fournisseur à utiliser)

Valeur	Commentaires
Microsoft Enhanced RSA and Cryptographic Provider	Fournisseur CAPI par défaut
Fournisseur de stockage des clés de logiciel Microsoft	Fournisseur CNG par défaut
Fournisseur de stockage des clés de plateforme Microsoft	Fournisseur TPM par défaut Veuillez noter que TPM n'est pas recommandé pour les clés utilisateur. Utilisez TPM uniquement pour la clé RA. Si vous prévoyez d'exécuter votre serveur FAS dans un environnement virtualisé, demandez à votre fournisseur d'hyperviseur et de puce TPM si la virtualisation est prise en charge.
HSM_Vendor CSP/Fournisseur de stockage de clés	Fourni par le fournisseur HSM. La valeur diffère d'un fournisseur à l'autre. Si vous prévoyez d'exécuter votre serveur FAS dans un environnement virtualisé, demandez à votre fournisseur HSM si la virtualisation est prise en charge.

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderType** (requis uniquement avec API CAPI)

Valeur	Commentaires
24	Valeur par défaut. Fait référence à la propriété Microsoft KeyContainerPermissionAccessEntry.ProviderType PROV_RSA_AES 24. Doit être toujours 24, sauf si vous utilisez un HSM avec CAPI et que le fournisseur HSM en décide autrement.

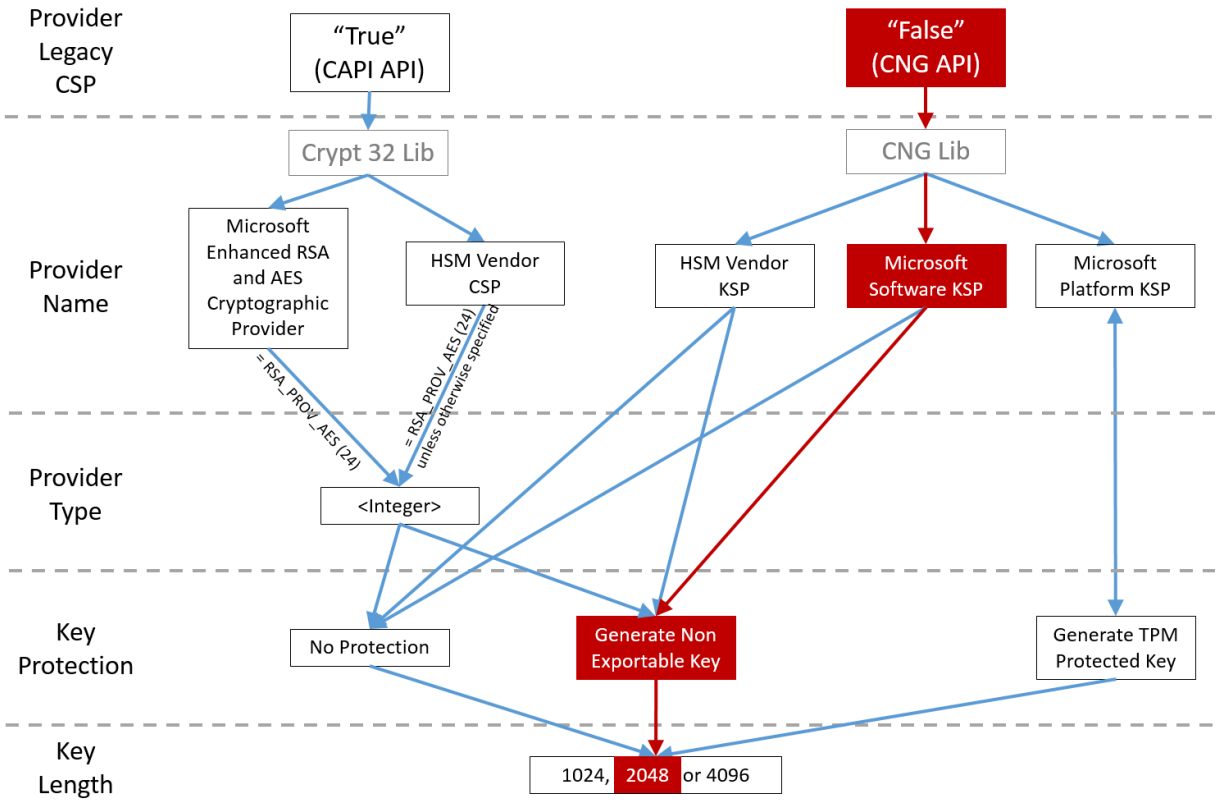
Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**KeyProtection** (lorsque FAS doit effectuer une opération de clé privée, il utilise la valeur spécifiée ici) Contrôle l'indicateur « exportable » des clés privées. Permet l'utilisation de stockage de clé TPM, s'il est pris en charge par le matériel.

Valeur	Commentaires
NoProtection	La clé privée peut être exportée.
GenerateNonExportableKey	Valeur par défaut. La clé privée ne peut pas être exportée.
GenerateTPMProtectedKey	La clé privée sera gérée à l'aide de TPM. La clé privée est stockée via le nom de fournisseur que vous avez spécifié dans NomFournisseur (par exemple, Microsoft Platform Key Storage Provider).

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**KeyLength** (spécifiez la taille de la clé privée en bits)

Valeur	Commentaires
2048	Default. 1024 ou 4096 peut également être utilisé.

Les paramètres du fichier de configuration sont représentés sous forme de graphiques comme suit (les valeurs par défaut d'installation apparaissent en rouge) :



Exemples de scénario de configuration

Exemple 1

Cet exemple concerne la clé privée du certificat RA et les clés privées des certificats utilisateur à l'aide de Microsoft Software Key Storage Provider

Il s'agit de la configuration post-installation par défaut. Aucune configuration de clé privée supplémentaire n'est requise.

Exemple 2

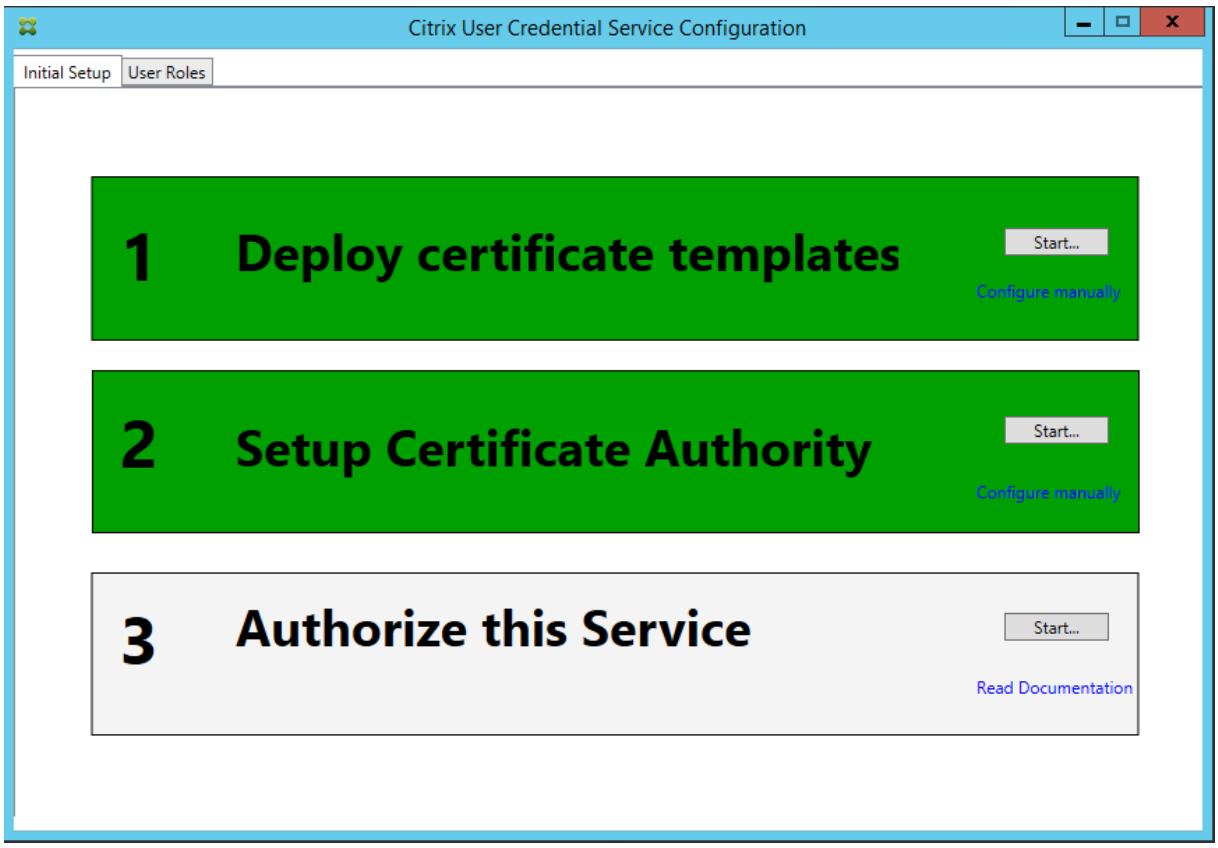
Cet exemple illustre la clé privée de certificat RA stockée dans la puce TPM matérielle de la carte mère du serveur FAS via Microsoft Platform Key Storage Provider et les clés privées des certificats utilisateur stockées à l'aide de Microsoft Software Key Storage Provider.

Ce scénario part du principe que la puce TPM sur la carte mère de votre serveur FAS a été activée dans le BIOS selon la documentation du fabricant de la puce TPM et initialisée dans Windows ; consultez la section https://technet.microsoft.com/en-gb/library/cc749022(v=ws.10).aspx.

Utilisation de PowerShell (recommandé)

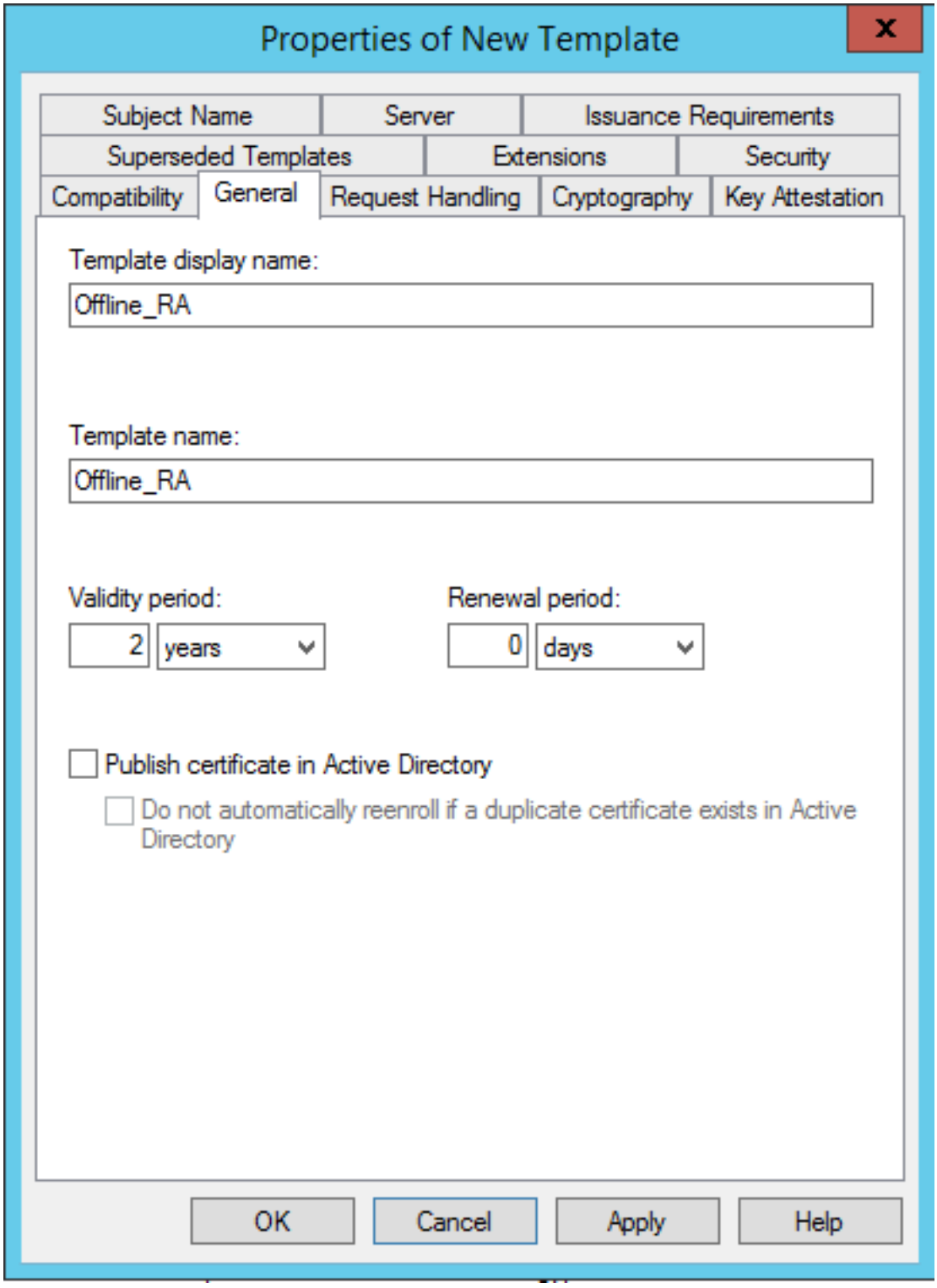
Le certificat RA peut être demandé en mode déconnecté à l'aide de PowerShell. Cette option est recommandée pour les entreprises qui ne souhaitent pas que l'autorité de certification émette un certificat RA via une demande de signature de certificat en ligne. Une demande de signature de certificat RA en mode déconnecté ne peut pas être effectuée à l'aide de la console de gestion FAS.

Étape 1 : lors de la configuration initiale du FAS à l'aide de la console de gestion, effectuez uniquement les deux premières étapes : « Déployer les modèles de certificat » et « Configurer l'autorité de certification ».



Étape 2 : sur le serveur d'autorité de certification, ajoutez le composant logiciel enfichable MMC des modèles de certificat. Cliquez avec le bouton droit sur le modèle **Citrix_RegistrationAuthority_ManualAuthoriza** et sélectionnez **Dupliquer le modèle**.

Sélectionnez l'onglet **Général**. Modifiez le nom et la période de validité. Dans cet exemple, le nom est Offline_RA et la période de validité est de 2 ans :



Étape 3 : sur le serveur d'autorité de certification, ajoutez le composant logiciel enfichable MMC d'autorité de certification. Cliquez avec le bouton droit sur **Modèles de certificats**. Sélectionnez **Nouveau**, puis cliquez sur **Modèle de certificat à délivrer**. Choisissez le modèle que vous venez de créer.

Étape 4 : chargez les applets de commande PowerShell suivantes sur le serveur FAS :

Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1

Étape 5 : générez la paire de clés RSA dans la puce TPM du serveur FAS et créez la CSR en entrant l'applet de commande PowerShell suivante sur le FAS serveur. **Remarque** : certaines puces TPM limitent la longueur de clé. La valeur par défaut est une longueur de 2048 bits. Veillez à spécifier une longueur de clé prise en charge par votre matériel.

New-FasAuthorizationCertificateRequest -UseTPM $true -address <nom de domaine complet du serveur FAS>

Par exemple :

New-FasAuthorizationCertificateRequest -UseTPM $true -address fashsm.auth.net

Les éléments suivants sont affichés :

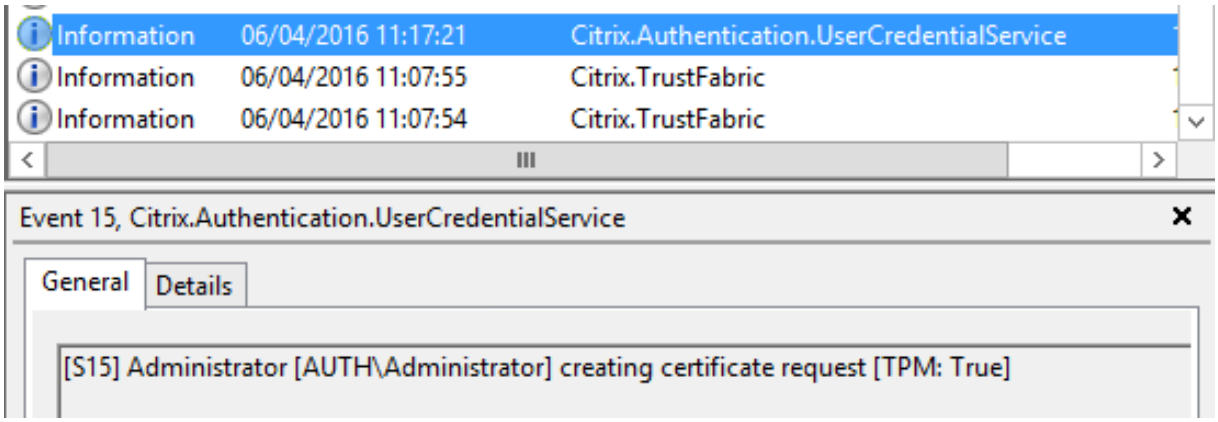
```
PS C:\Users\Administrator.AUTH> New-UcsAuthorizationCertificateRequest -UseTPM $true -address ucshsm.auth.local


Id                  : 5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39
Address             : [Offline CSR]
TrustArea           :
CertificateRequest  : -----BEGIN CERTIFICATE REQUEST-----
                      MIICaDCCAVACAQIwIzEhMB8GCgmSJomT8ixkARkWEUNpdHJpeFRydXNORmFicmljMIIBIjANBgkq
                      hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwAtwoCLXJuJ3yIscT8Y5v/7zuYqBhbHkhZV3wTNfRO XW
                      lhCMwi7X4YpTE7CbJtgiFY/9SEBa9StGeTVpeJi66gKoZCdxydc2BwX6JNZrLi9hAflbInFPgrz+
                      vbG3YjKuKtK35JpGqYWjUEDzKiQFaob3Dkh/pwP3V7OcEYthxB8CfbaM9MHOEFbepoSYOCAfunXW
                      snwIbXD91c/fGyN/3f94P4fbNrjEIOHc+4Dy/WsPgPRgcq9XBwRjzpGj0g0WRoJS9g22DY5PwD77
                      7f7vZvoQkRy5N XXXATJ+xxYEPLp9JuJaE1WXrTJG+XP3SnG/oCCPit7iUIIc9FjGa3qTUQIDAQAB
                      oAAwDQYJKoZIhvcNAQENBQADggEBAIJV8jR9XWH1vztpjxPeJzAVOsrLpOsCfNdvYn9u+I7J8Gsr
                      4tuLjuQ+An4Y2Rw7b6pZxEICV8rqd5Gy+wtPnUZoAf6eLg1Vht2RVfb6d7Ns6+Mc+F5bFegLHs8c
                      YlITNOtmcHFKt4Loz5O5E+tQw39MProEj3p7GwF7HrGY+QSbFD38rbL19Z5cfNYYqMbsgyMgdR8F
                      3SmagQjN3C8lyqT8z1iF4l32xlmQrP/4XQvr1F+TO15PM5Fxjj6PEKWopWTYZXGzSC1ufxevcO1K
                      +tTH9tQYJM6xw3+6TIcfuWOjrd8KJjTdC5SMu7LJuIajTNZ5Z+1eM61TATO3XG/AB7o=
                      -----END CERTIFICATE REQUEST-----
Status              : WaitingForApproval


PS C:\Users\Administrator.AUTH> _
```

Remarques :

- L'ID GUID (dans cet exemple, « 5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39 ») est requis dans une étape suivante.
- Considérez cette applet de commande PowerShell comme un « remplacement » à usage unique, utilisé pour générer la clé privée pour le certificat RA.
- Lors de l'exécution de cette applet de commande, les valeurs qui sont lues à partir du fichier de configuration lorsque le service FAS démarre sont vérifiées pour déterminer la longueur de clé à utiliser (la valeur par défaut est de 2048).
- Étant donné que -UseTPM est défini sur $true dans cette opération manuelle de clé privée de certificat RA initiée par PowerShell, le système ignore les valeurs du fichier qui ne correspondent pas aux paramètres requis pour utiliser une puce TPM.
- L'exécution de cette applet de commande ne modifie pas les paramètres du fichier de configuration.
- Durant les opérations automatiques de clé privée de certificat utilisateur initiées par FAS, les valeurs qui ont été lues à partir du fichier lorsque le service FAS a démarré seront utilisées.
- Il est également possible de définir la valeur KeyProtection dans le fichier de configuration sur

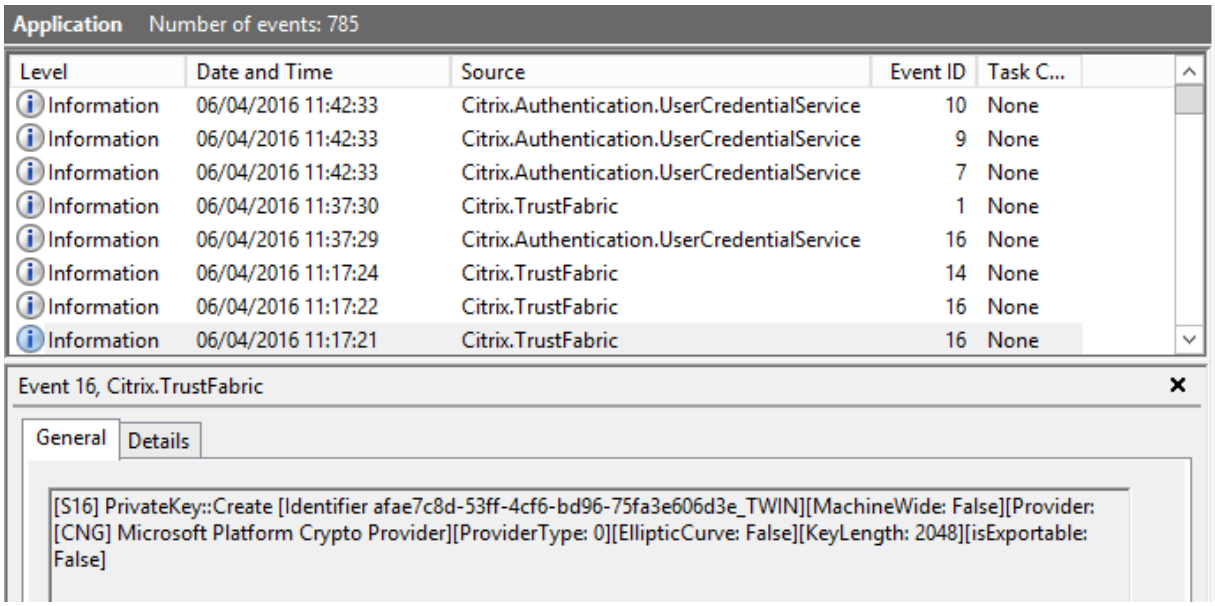
GenerateTPMProtectedKey lorsque le serveur FAS émet des certificats utilisateur pour générer des clés privées de certificat utilisateur protégées par la puce TPM.

Pour vérifier que la puce TPM a été utilisée pour générer la paire de clés, consultez le journal d'application dans l'observateur d'événements de Windows sur le serveur FAS, à l'heure où la paire de clés a été générée.



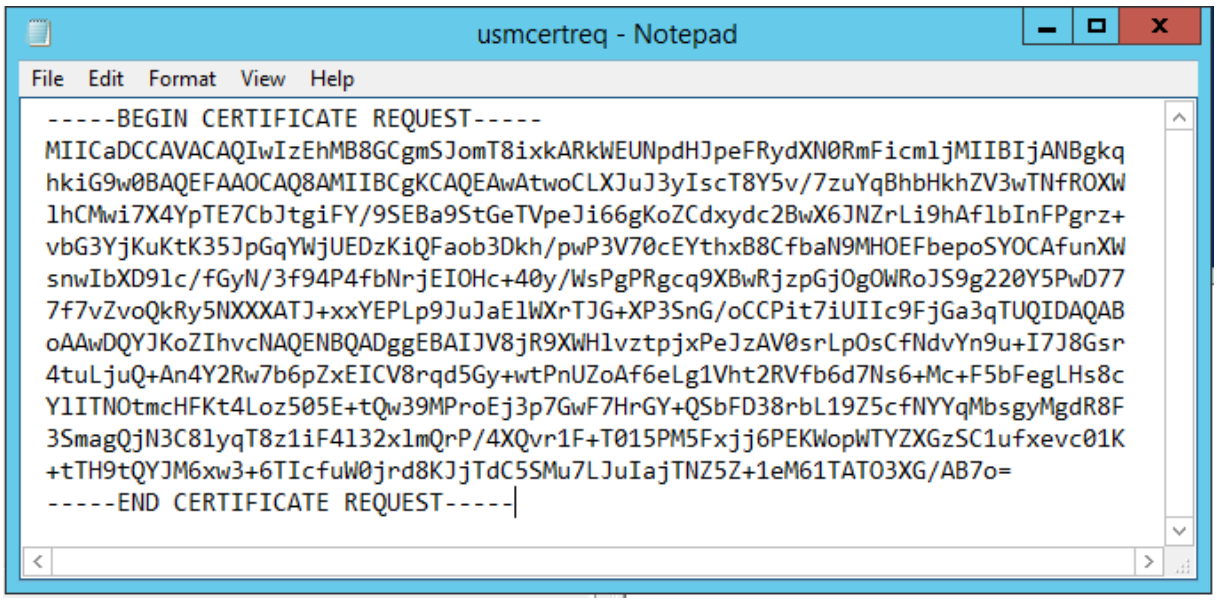
Notez : "[TPM: True]"

Suivi de :



Notez « Provider: [CNG] Microsoft Platform Crypto Provider »

Étape 6 : copiez la section de requête de certificat dans un éditeur de texte et enregistrez-la sur disque en tant que fichier texte.



Étape 7 : envoyez la demande de signature de certificat à l'autorité de certification (CA) en tapant les commandes suivantes dans PowerShell sur le serveur FAS :

certreq -submit -attrib "certificatetemplate:<modèle de certificat de l'étape 2>" <fichier de demande de certificat de l'étape 6>

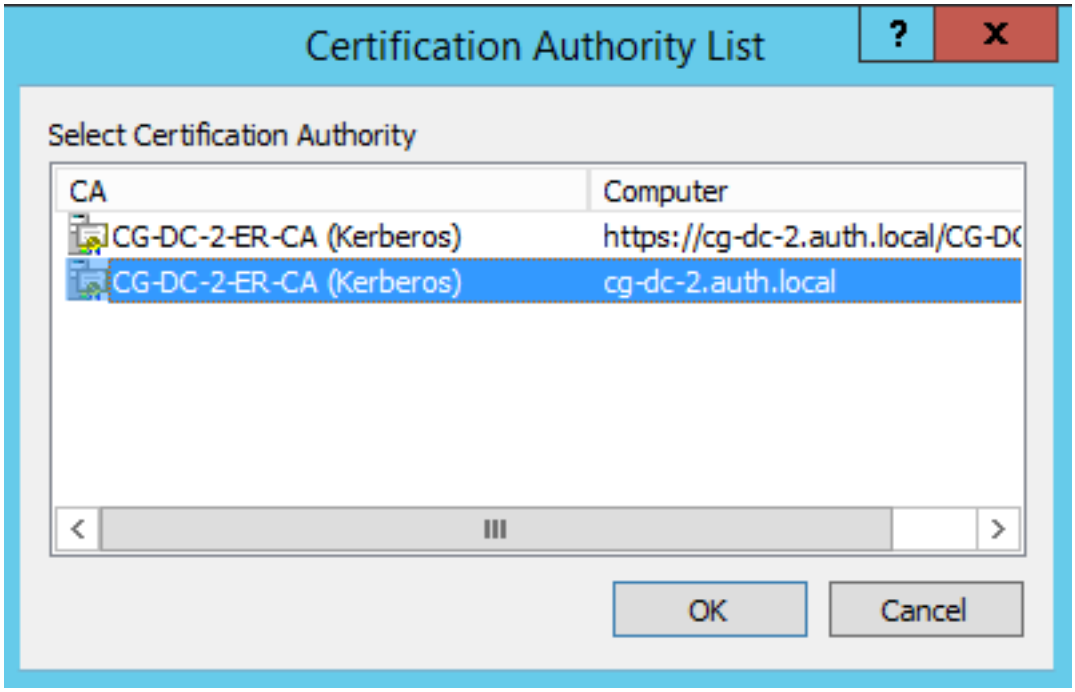
Par exemple :

certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Desktop\usmcertreq.txt

Les éléments suivants sont affichés :

```
PS C:\Users\Administrator.AUTH> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Des
ktop\usmcertreq.txt
Active Directory Enrollment Policy
  {4F7616DE-DB0C-4D21-A4FD-2E29502177C2}
  ldap:
```

À ce stade, une fenêtre contenant une liste d'autorités de certification peut s'afficher. Dans cet exemple, les inscriptions http (haut) et DCOM (bas) sont activées toutes les deux pour l'autorité de certification. Sélectionnez l'option DCOM, si elle est disponible :

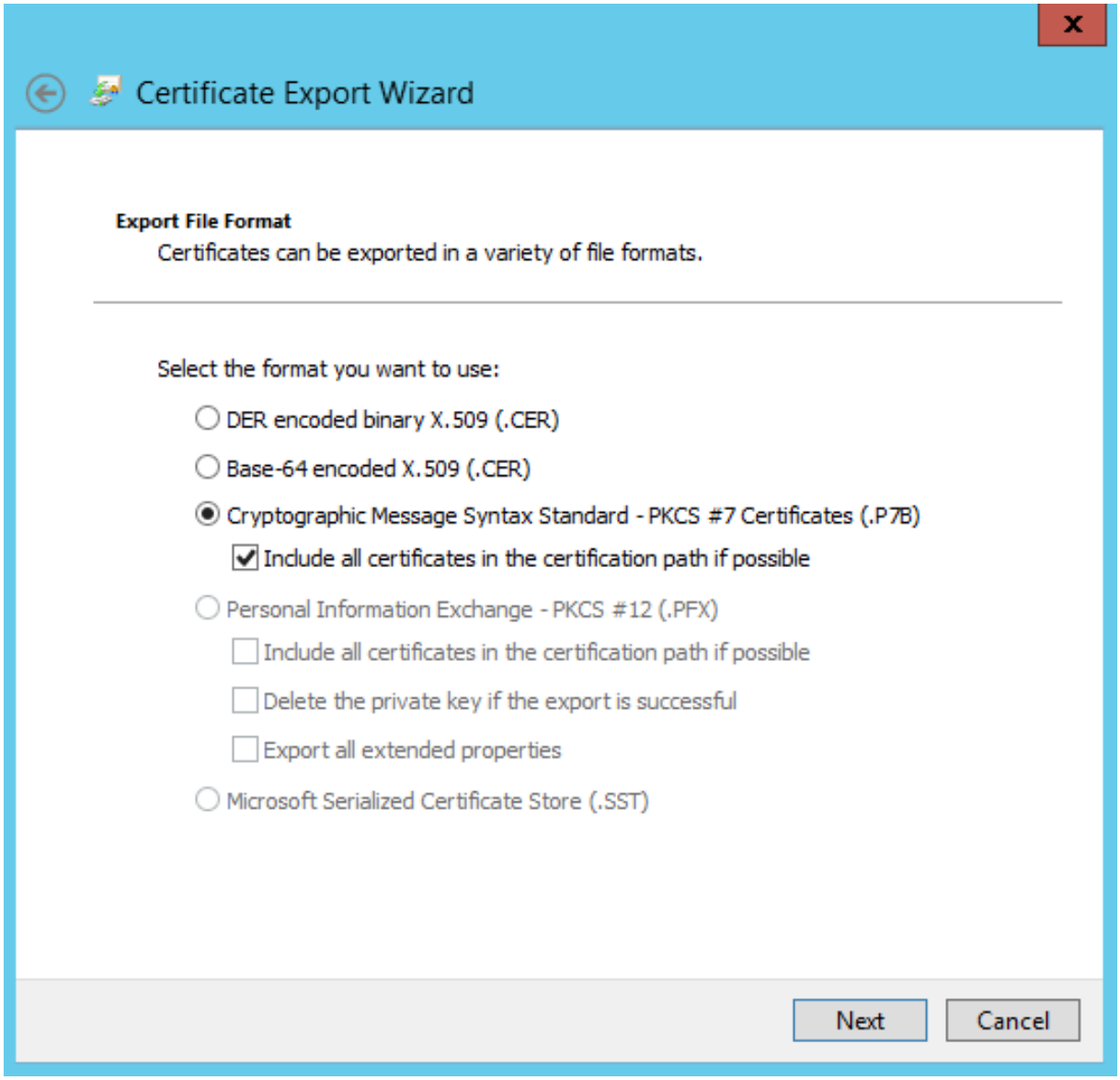


Après que l'autorité de certification (CA) a été spécifiée, PowerShell affiche la RequestID :

```
PS C:\Users\Administrator.AUTH> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Des
ktop\usmcertreq.txt
Active Directory Enrollment Policy
  {4F7616DE-DB0C-4D21-A4FD-2E29502177C2}
  ldap:
RequestId: 106
RequestId: "106"
Certificate request is pending: Taken Under Submission (0)
PS C:\Users\Administrator.AUTH>
```

Étape 8 : sur le serveur de l'autorité de certification (CA), dans le composant logiciel enfichable MMC CA, cliquez sur **Demandes en attente**. Notez l'ID de la demande, RequestID. Puis cliquez avec le bouton droit sur la demande et choisissez **Délivrer**.

Étape 9: sélectionnez le nœud **Certificats délivrés**. Recherchez le certificat qui vient d'être émis (l'ID de demande doit correspondre). Cliquez deux fois pour ouvrir le certificat. Sélectionnez la page de l'onglet **Détails**. Cliquez sur **Copier dans un fichier**. L'Assistant d'exportation de certificat s'ouvre. Cliquez sur **Suivant**. Choisissez les options suivantes pour le format de fichier :



Le format doit être **Standard de syntaxe de message cryptographique – Certificate PKCS #7 (.P7B)** et **Inclure tous les certificats dans le chemin d'accès de certification, si possible** doit être sélectionné.

Étape 10 : copiez le fichier de certificat exporté sur le serveur FAS.

Étape 11 : importez le certificat RA dans le registre du serveur FAS en entrant l'applet de commande PowerShell suivante sur le serveur FAS :

```
Import-FasAuthorizationCertificateResponse -address <FQDN of FAS server> -Id <ID
GUID from step 5> -Pkcs7CertificateFile <Certificate file from step 10>
```

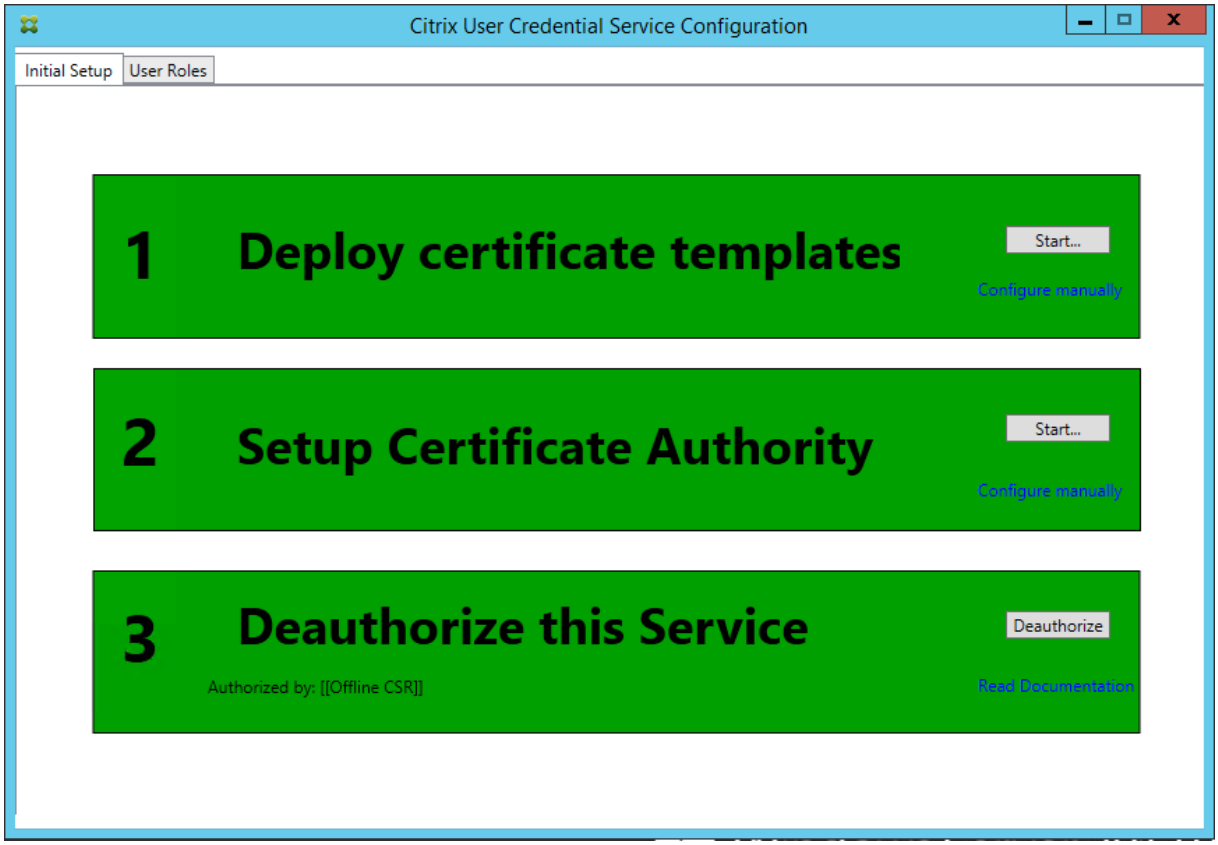
Par exemple :


```
Import-FasAuthorizationCertificateResponse -address fashsm.auth.net -Id 5ac3d8bd-
b484-4ebe-abf8-4b2cfd62ca39 -Pkcs7CertificateFile
C:\Users\Administrator.AUTH\Desktop\TPM_FAS_Cert.p7b
```

Les éléments suivants sont affichés :

```
PS C:\Users\Administrator.AUTH> Import-UcsAuthorizationCertificateResponse -address ucshsm.auth.local -Id 5ac3d8bd-b484-
4ebe-abf8-4b2cfd62ca39 -Pkcs7CertificateFile C:\Users\Administrator.AUTH\Desktop\TPM_UCS_Cert.p7b


Id                  : 5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39
Address             : [Offline CSR]
TrustArea           : a5c27fcc-1dd7-4c2b-8963-16ec31102Dfc
CertificateRequest :
Status              : Ok
```

Étape 12 : fermez la console de gestion FAS, puis redémarrez-la.



Vous remarquerez que l'étape « Authorize this Service » est indiquée en vert, et affiche maintenant « Deauthorize this Service ». L'entrée en-dessous indique « Authorized by: Offline CSR »

Étape 13 : sélectionnez l'onglet User **Roles** dans la console de gestion FAS et modifiez les paramètres décrits dans l'article FAS principal.

Remarque : annuler l'autorisation du FAS par le biais de la console de gestion supprime la règle de l'utilisateur.

Utilisation de la console de gestion FAS

La console de gestion ne peut pas effectuer de requête de signature de certificat en mode déconnecté ; son utilisation n'est donc pas recommandée si votre organisation ne permet pas les requêtes CSR en mode connecté pour les certificats RA.

Lorsque vous effectuez les étapes de configuration initiale du FAS, après le déploiement des modèles de certificat et la configuration de l'autorité de certification, mais avant d'autoriser le service (étape 3 dans la séquence de configuration) :

Étape 1 : modifiez le fichier de configuration en modifiant la ligne suivante comme suit :

```
<add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection"
value="GenerateTPMProtectedKey"/>
```

Le fichier doit maintenant s'afficher comme suit :

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <!-- This option switch between CAPI API  (true) and CNG API (false) Cryptographic Providers  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp" value="false"/>

    <!-- Specify the Cryptographic Service Provider (CSP) / Key Storage Provider (KSP) Name.  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="Microsoft Software Key Storage Provider"/ -->

    <!-- Specify the Cryptographic Service Provider Type (only for CSP - not KSP).  For example: PROV_RSA_AES is 24  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType" value="24"/ -->

    <!-- Specify Private Key protection [NoProtection|GenerateNonExportableKey|GenerateTPMProtectedKey] -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection" value="GenerateTPMProtectedKey"/>

    <!-- Specify RSA Key length -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength" value="2048"/>

    <!-- Logging: Event log Verbosity (0 Disabled, 1 Errors, 2 Warnings, 3 Informational) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.LogLevel" value="3" / -->

    <!-- Logging: Event IDs to not log (comma separated) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.Supress" value="" / -->

    <!-- Logging: Disable Key Management logs -->
    <!-- add key="Citrix.TrustFabric.Logging.SystemLog" value=""/ -->
  </appSettings>
<startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/></startup></configuration>
```

Certaines puces TPM limitent la longueur de clé. La valeur par défaut est une longueur de 2048 bits. Veillez à spécifier une longueur de clé prise en charge par votre matériel.

Étape 2 : autorisez le service.

Étape 3 : émettez manuellement la requête de certificat en attente depuis le serveur de l'autorité de certification. Une fois que le certificat RA a été obtenu, l'étape 3 dans la séquence d'installation de la console de gestion doit être indiquée en vert. À ce stade, la clé privée du certificat RA est générée dans la puce TPM. Le certificat sera valide pendant 2 ans par défaut.

Étape 4 : modifiez le fichier de configuration comme suit :

```
<add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection"
value="GenerateNonExportableKey"/>
```


Remarque : bien que FAS puisse générer des certificats utilisateur avec des clés protégées TPM, le matériel TPM peut être trop lent pour les déploiements de grande envergure.

Étape 5 : redémarrez le Service d'authentification fédérée Citrix. Cela oblige le service à relire le fichier de configuration et à refléter les valeurs modifiées. Les opérations de clé privée automatiques suivantes affecteront les clés de certificat utilisateur ; ces opérations ne stockeront pas les clés privées dans la puce TPM, mais utiliseront Microsoft Software Key Storage Provider.

Étape 6 : sélectionnez l'onglet User Roles dans la console de gestion FAS et modifiez les paramètres décrits dans l'article FAS principal.

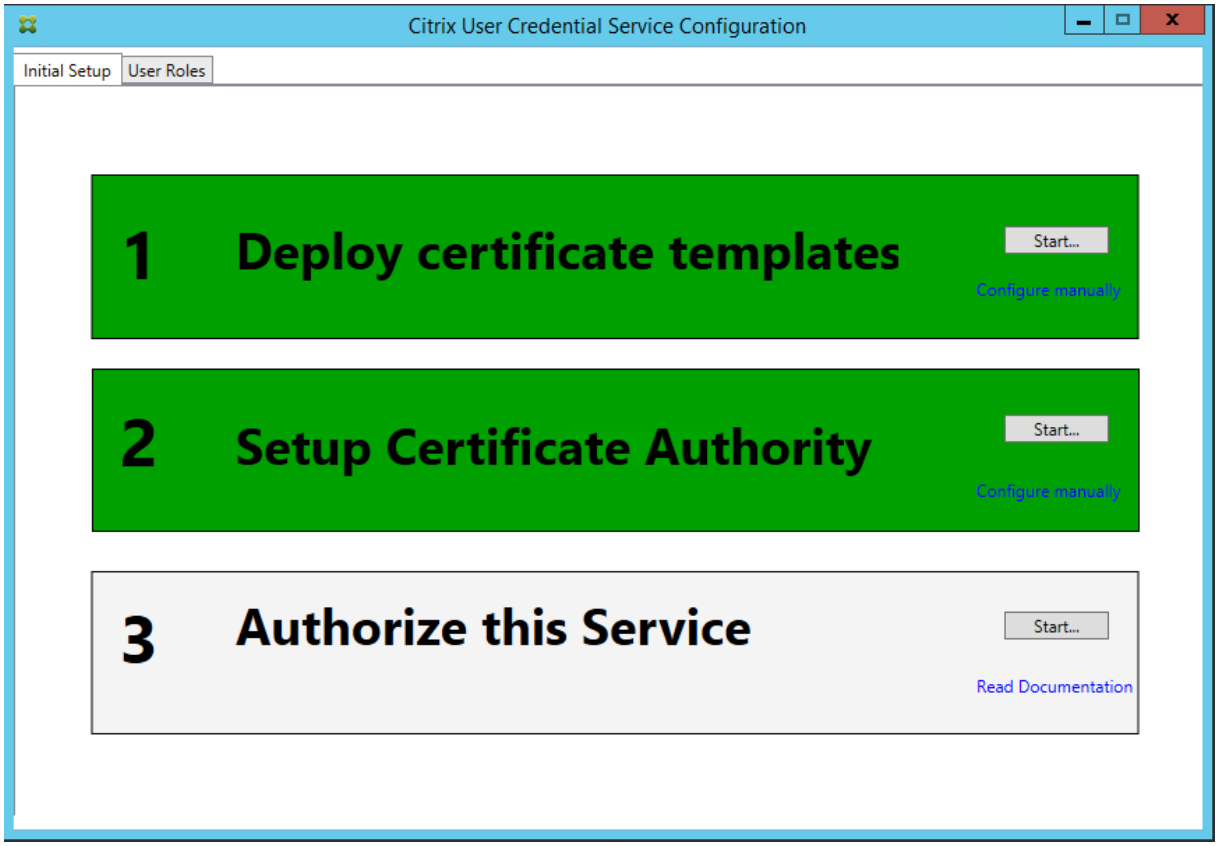
Remarque : annuler l'autorisation du FAS par le biais de la console de gestion supprime la règle de l'utilisateur.

Exemple 3

Cet exemple illustre une clé privée de certificat RA et les clés privées de certificats utilisateur stockées dans un HSM. Cet exemple suppose un HSM configuré. Votre HSM aura un nom de fournisseur, par exemple « HSM_Vendor's Key Storage Provider ».

Si vous prévoyez d'exécuter votre serveur FAS dans un environnement virtualisé, demandez à votre fournisseur HSM si l'hyperviseur est pris en charge.

Étape 1 – Lors de la configuration initiale du FAS à l'aide de la console de gestion, effectuez uniquement les deux premières étapes : « Déployer les modèles de certificat » et « Configurer l'autorité de certification ».



Étape 2 : consultez la documentation de votre fournisseur HSM pour déterminer ce que doit être la valeur ProviderName de votre HSM. Si votre HSM utilise CAPI, le fournisseur peut être désigné dans la documentation comme fournisseur de service cryptographique (CSP). Si votre HSM utilise CNG, le fournisseur peut être désigné comme Key Storage Provider (KSP).

Étape 3 : modifiez le fichier de configuration comme suit :

```
<add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName"
value="HSM_Vendor's Key Storage Provider"/>
```

Le fichier doit maintenant s'afficher comme suit :


```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <!-- This option switch between CAPI API  (true) and CNG API (false) Cryptographic Providers  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp" value="false"/>

    <!-- Specify the Cryptographic Service Provider (CSP) / Key Storage Provider (KSP) Name.  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="HSM_Vendor's Key Storage Provider"/>

    <!-- Specify the Cryptographic Service Provider Type (only for CSP - not KSP).  For example: PROV_RSA_AES is 24  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType" value="24"/ -->

    <!-- Specify Private Key protection [NoProtection|GenerateNonExportableKey|GenerateTPMProtectedKey] -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection" value="GenerateNonExportableKey"/>

    <!-- Specify RSA Key length -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength" value="2048"/>

    <!-- Logging: Event log Verbosity (0 Disabled, 1 Errors, 2 Warnings, 3 Informational) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.LogLevel" value="3" / -->

    <!-- Logging: Event IDs to not log (comma separated) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.Supress" value="" / -->

    <!-- Logging: Disable Key Management logs -->
    <!-- add key="Citrix.TrustFabric.Logging.SystemLog" value=""/ -->
  </appSettings>
<startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/></startup></configuration>
```

Ce scénario part du principe que votre HSM utilise CNG de sorte que la valeur ProviderLegacyCsp est définie sur false. Si votre HSM utilise CAPI, la valeur ProviderLegacyCsp devrait être définie sur true. Consultez la documentation de votre fournisseur HSM pour déterminer si votre HSM utilise CAPI ou CNG. De plus, consultez la documentation de votre fournisseur HSM sur les longueurs de clé prises en charge pour la génération de clé asymétrique RSA. Dans cet exemple, la longueur de clé est définie sur la valeur par défaut de 2048 bits. Assurez-vous que la longueur de clé que vous avez spécifiée est prise en charge par votre matériel.

Étape 4: redémarrez le Service d'authentification fédérée Citrix pour lire les valeurs à partir du fichier de configuration.

Étape 5 : générez la paire de clés RSA dans le HSM et créez la demande de signature de certificat en cliquant sur **Autoriser** dans l'onglet Initial Setup de la console de gestion FAS.

Étape 6 : pour vérifier que la paire de clés a été générée dans le HSM, vérifiez les entrées d'application dans le journal d'événements Windows :

```
[S16] PrivateKey::Create [Identifier e1608812-6693-4c54-a937-91a2e27df75b_TWIN][MachineWide: False][Provider: [CNG] HSM_Vendor's Key Storage Provider][ProviderType: 0][EllipticCurve: False][KeyLength: 2048][isExportable: False]
```

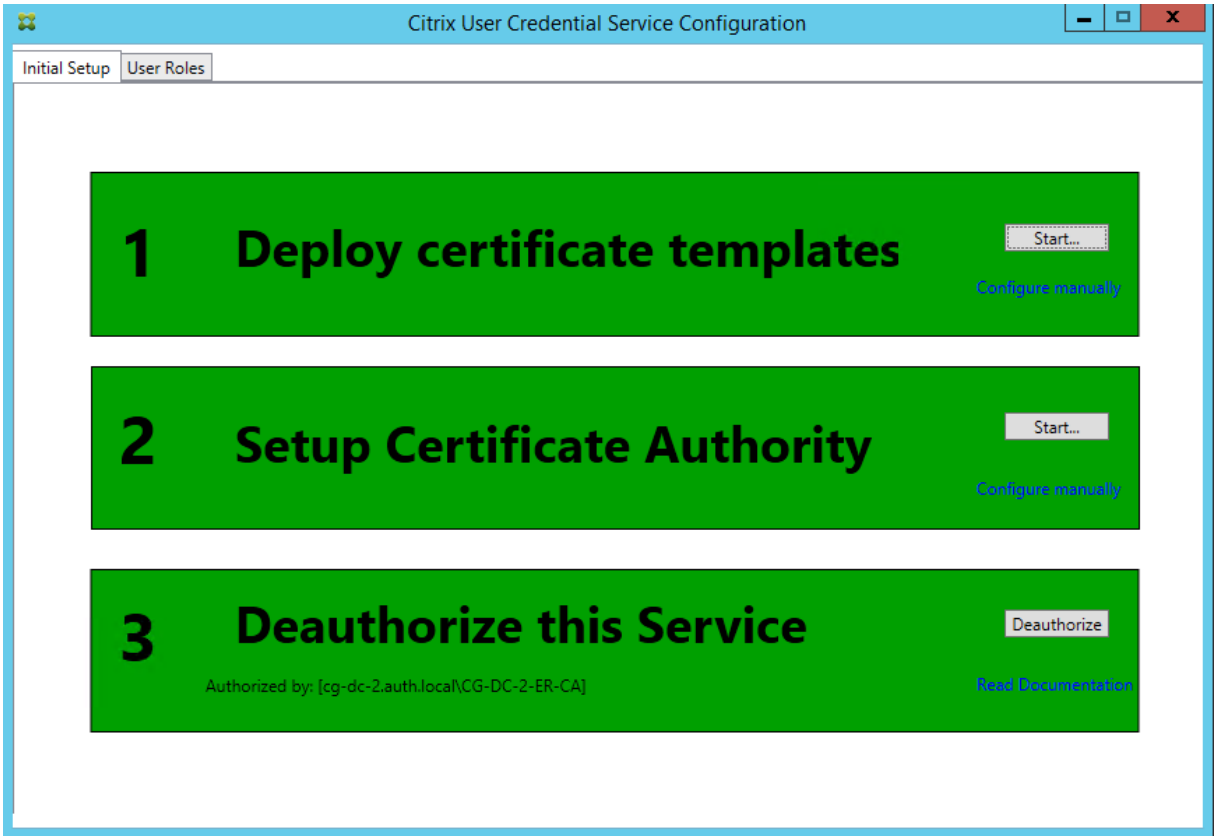
Remarque : [Provider: [CNG] HSM_Vendor's Key Storage Provider]

Étape 7 : sur le serveur de l'autorité de certification (CA), dans la MMC CA, sélectionnez le nœud **Demandes en attente**.

Request ID	Binary Request	Request Status Code	Request Disposition Message	Request Submission Date	Requester Name	Request Country/Region
107	-----BEGIN NE...	The operation compl...	Taken Under Submission	07/04/2016 14:04	AUTH\UCSHSM$	

Cliquez avec le bouton droit sur la demande et choisissez **Délivrer**.

Vous remarquerez que l'étape « Authorize this Service » est indiquée en vert, et affiche maintenant « Deauthorize this Service ». L'entrée en-dessous indique « Authorized by: [<Nom CA>] »



Étape 8 : sélectionnez l'onglet **User Roles** dans la console de gestion FAS et modifiez les paramètres décrits dans l'article FAS principal.

Remarque : annuler l'autorisation du FAS par le biais de la console de gestion supprime la règle de l'utilisateur.

Stockage de certificats FAS

FAS n'utilise pas le magasin de certificats Microsoft sur le serveur FAS pour stocker ses certificats. Il utilise le registre.

Remarque : lorsque vous utilisez un HSM pour stocker des clés privées, les conteneurs HSM sont identifiés par un GUID. Le GUID pour la clé privée dans le HSM correspond au GUID du certificat équivalent dans le registre.

Pour déterminer le GUID du certificat RA, entrez les applets de commande PowerShell suivantes sur le serveur FAS :

Add-pssnapin Citrix.a*

Get-FasAuthorizationCertificate –address <nom de domaine complet du serveur FAS>

Par exemple :

Get-FasAuthorizationCertificate –address cg-fas-2.auth.net

```
PS C:\Users\Administrator.AUTH> Get-UcsAuthorizationCertificate -address cg-ucs-2.auth.local


Id                : a3958424-b8c3-4cac-ba0d-7eb3ce24591c
Address           : cg-dc-2.auth.local\CG-DC-2-ER-CA
TrustArea         : 3df77088-00e0-4dca-a47a-28060dc16986
CertificateRequest :
Status            : MaintenanceDue

Id                : fcb185f9-5069-4e34-8625-a333ac126535
Address           : [Offline CSR]
TrustArea         :
CertificateRequest : -----BEGIN CERTIFICATE REQUEST-----
                     MIICaDCCAVACAQIwIzEhMB8GCgm5JomT8ixkARkWEUNpdHJpeFRydXN0RmFicmljMIIBIjANBgkq
                     hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxyNzaiWX8DhUnOZMS2YVSDhr36AV5BGeIYOGVCFKvZPe
                     Rmm/xOVM6cNKsLbew3dYlbo+vdgWg86DFRVxTORholV86iazDZyOiYGgxe9/s8YZzCspVWN1nB1
                     zXOUJfo1qo9UsmImYr7MR/dhGAtkfsFUoPcd2+zcezmgOfq/4vmCIuerwqzRR5T/p4og7+IjR1se
                     ECz/CbXROOuiDhW+VWbjcsgklcavzvC/jR33F9dZSXNgKRiGHgfd/lBb3elZKA4OOoi90u64Q916
                     3ba9BnihqxIgvwWILOmyUfiJmCgbhLJV4TPBopOdKz/axZEIO5p5XYVjCcpXqhqL7Ppn1wIDAQAB
                     oAAwDQYJKoZIhvcNAQENBQADggEBAJhdvw6yrLGBMtAgo3oPL6o8/at+IqHjHKqgcJNJO/MU7/7X
                     bZB46drLPFzpzF88DkmfoCEgOxlbzFX9waaiFs9CHC/AcEzblN925y1gqljsfC3l5TCKBAeLFoMl
                     PSEkfYMQUOSBYCuLlkFn1LXLSeQ3qJTzSvptYROawFmUMQLffwLSR1vOuS8DJSrpASrwdXJk3TOa
                     Glo/xJo/NRMOwMH+AvGbBsgp3l+jnDjXED5RudqARfgVgcW714JP+XIeFrE1TZmUL2skNIXEPNHC
                     H8eAHdYD26caFigydfefbjx4fbaJDFHJs5+1tnrTZ9knCrawhUiIyOMLGZOOaiER+z8=
                     -----END CERTIFICATE REQUEST-----
Status            : WaitingForApproval
```

Pour obtenir une liste de certificats utilisateur, entrez :

Get-FasUserCertificate –address <nom de domaine complet du serveur FAS>

Par exemple :

Get-FasUserCertificate –address cg-fas-2.auth.net

```
PS C:\Users\Administrator.AUTH> Get-UcsUserCertificate -address cg-ucs-2.auth.local


ThumbPrint            : 7BA22879F40EE92125A2F96E7DD2D52C73820459
UserPrincipalName     : walter@adfs.ext
Role                  : default
CertificateDefinition : default_Definition
ExpiryDate            : 05/04/2016 12:02:13
```

Informations connexes

- L'article Service d'authentification fédérée est le document de référence principal pour obtenir des informations sur l'installation et la configuration du FAS.
- Les déploiements FAS courants sont décrits dans l'article Vue d'ensemble des architectures du Service d'authentification fédérée.
- D'autres informations pratiques sont disponibles dans l'article Configuration et gestion du service d'authentification fédérée.

Configuration du réseau et de la sécurité du Service d'authentification fédérée

January 23, 2019

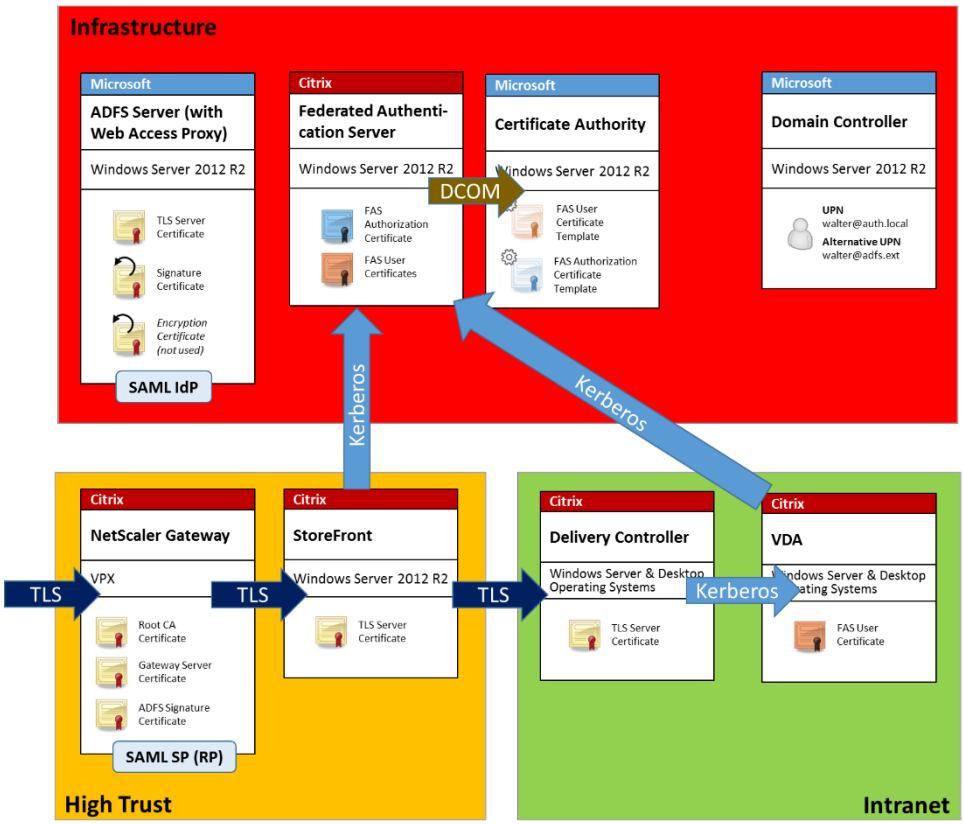
Le Service d'authentification fédérée de Citrix (FAS) est étroitement intégré à Microsoft Active Directory et à l'autorité de certification Microsoft (CA). Il est essentiel de vous assurer que le système est géré et sécurisé de manière appropriée, en développant une stratégie de sécurité comme vous le feriez pour un contrôleur de domaine ou toute autre infrastructure critique.

Ce document présente les problèmes de sécurité à prendre en compte lorsque vous déployez FAS. Il offre également une vue d'ensemble des fonctionnalités qui peuvent vous aider à sécuriser votre infrastructure.

Architecture réseau

Le diagramme suivant illustre les composants principaux et les limites de sécurité utilisés dans un déploiement FAS.

Le serveur FAS doit être considéré comme faisant partie de l'infrastructure de sécurité, tout comme l'autorité de certification et le contrôleur de domaine. Dans un environnement fédéré, Citrix NetScaler et Citrix StoreFront sont des composants approuvés pour authentifier les utilisateurs ; les autres composants de XenApp et XenDesktop ne sont pas affectés par l'introduction du service FAS.



Sécurité du réseau et pare-feu

Les communications entre les composants NetScaler, StoreFront et Delivery Controller doivent être protégées par TLS sur le port 443. Le serveur StoreFront se charge uniquement des connexions sortantes, et NetScaler Gateway doit uniquement accepter les connexions via Internet utilisant HTTPS sur le port 443.

Le serveur StoreFront contacte le serveur FAS sur le port 80 à l'aide de l'authentification mutuelle Kerberos. L'authentification utilise l'identité Kerberos HOST/fqdn du serveur FAS, et l'identité du compte de machine Kerberos du serveur StoreFront. Ceci génère un « handle d'informations d'identification » à usage unique requis par le Citrix Virtual Delivery Agent (VDA) pour connecter l'utilisateur.

Lorsqu'une session HDX est connectée au VDA, le VDA contacte également le serveur FAS sur le port 80. L'authentification utilise l'identité Kerberos HOST/fqdn du serveur FAS, et l'identité de la machine Kerberos du VDA. En outre, le VDA doit fournir le « handle d'informations d'identification » pour accéder au certificat et à la clé privée.

L'autorité de certification Microsoft accepte les communications à l'aide du DCOM authentifié auprès de Kerberos, qui peut être configuré pour utiliser un port TCP fixe. L'autorité de certification requiert également que le serveur FAS fournisse un paquet CMC signé par un certificat d'agent d'inscription approuvé.

Serveur	Ports du pare-feu
Service d'authentification fédérée	[entrant] Kerberos via HTTP depuis StoreFront et VDA, [sortant] DCOM vers autorité de certification Microsoft
NetScaler	[entrant] HTTPS depuis les machines clientes, [entrant/sortant] HTTPS depuis/vers un serveur StoreFront, [sortant] HDX vers VDA
StoreFront	[entrant] HTTPS depuis NetScaler, [sortant] HTTPS vers Delivery Controller, [sortant] HTTP Kerberos vers FAS
Delivery Controller	[entrant] HTTPS depuis un serveur StoreFront, [entrant/sortant] Kerberos via HTTP depuis des VDA
VDA	[entrant/sortant] Kerberos via HTTP depuis Delivery Controller, [entrant] HDX depuis NetScaler Gateway, [sortant] Kerberos HTTP vers FAS
Autorité de certification Microsoft	[entrant] DCOM et signé depuis FAS

Responsabilités en matière d'administration

L'administration de l'environnement peut être divisée dans les groupes suivants :

Name	Responsabilité
Administrateur d'entreprise	Installer et sécuriser les modèles de certificat dans la forêt
Administrateur de domaine	Configurer les paramètres de stratégie de groupe
Administrateur d'autorité de certification	Configurer l'autorité de certification
Administrateur FAS	Installer et configurer le serveur FAS
Administrateur StoreFront/Netscaler	Configurer l'authentification utilisateur
Administrateur XenDesktop	Configurer les VDA et les Controller

Chaque administrateur contrôle différents aspects du modèle de sécurité, ce qui assure une protec-

tion approfondie du système.

Paramètres de stratégie de groupe

Les machines FAS approuvées sont identifiées par une table de recherche « numéro d'index -> FQDN » configurée via la stratégie de groupe. Lors de la communication avec un serveur FAS, les clients vérifient l'identité Kerberos HOST\<fqdn> du serveur FAS. Tous les serveurs qui accèdent au serveur FAS doivent posséder les mêmes configurations de nom domaine complet (FQDN) pour le même index ; dans le cas contraire, il est possible que StoreFront et les VDA contactent des serveurs FAS différents.

Pour éviter toute erreur de configuration, Citrix recommande d'appliquer une seule stratégie à toutes les machines dans l'environnement. Soyez prudent lors de la modification de la liste des serveurs FAS, plus particulièrement lors de la suppression ou de la réorganisation d'entrées.

Le contrôle de cet objet de stratégie de groupe doit être limité aux administrateurs FAS (et/ou aux administrateurs de domaine) qui installent et désactivent des serveurs FAS. Prenez soin de ne pas réutiliser le nom de domaine complet (FQDN) d'une machine peu de temps après avoir désactivé un serveur FAS.

Modèles de certificats

Si vous ne souhaitez pas utiliser le modèle de certificat Citrix_SmartcardLogon fourni avec FAS, vous pouvez modifier une copie. Les modifications suivantes sont prises en charge.

Renommer un modèle de certificat

Si vous souhaitez renommer Citrix_SmartcardLogon pour qu'il corresponde aux conventions de nom de modèle de votre entreprise, vous devez :

- Créer une copie du modèle de certificat et le renommer pour qu'il corresponde aux conventions de nom de modèle de votre entreprise.
- Utiliser les commandes PowerShell FAS pour administrer FAS, plutôt que l'interface utilisateur d'administration. (L'interface utilisateur d'administration est conçue uniquement pour une utilisation avec les noms de modèle par défaut Citrix).
  - Utiliser le composant logiciel enfichable pour modèles de certificats MMC de Microsoft ou la commande Publish-FasMsTemplate pour publier votre modèle et
  - utiliser la commande New-FasCertificateDefinition pour configurer les FAS avec le nom de votre modèle.

Modifier les propriétés générales

Vous pouvez modifier la période de validité dans le modèle de certificat.

Ne modifiez pas la période de renouvellement. FAS ignore ce paramètre dans le modèle de certificat. FAS renouvelle automatiquement le certificat au cours de sa période de validité.

Modifier les propriétés de traitement de demande

Ne modifiez pas ces propriétés. FAS ignore ces paramètres dans le modèle de certificat. FAS désélectionne toujours **Autoriser l'exportation de la clé privée** et **Renouveler avec la même clé**.

Modifier les propriétés de cryptographie

Ne modifiez pas ces propriétés. FAS ignore ces paramètres dans le modèle de certificat.

Consultez Protection des clés privées du service d'authentification fédérée pour connaître les paramètres équivalents fournis par FAS.

Modifier les propriétés d'attestation de clé

Ne modifiez pas ces propriétés. FAS ne gère pas l'attestation de clé.

Modifier les propriétés de modèles obsolètes

Ne modifiez pas ces propriétés. FAS ne gère pas les modèles obsolètes.

Modifier les propriétés d'extensions

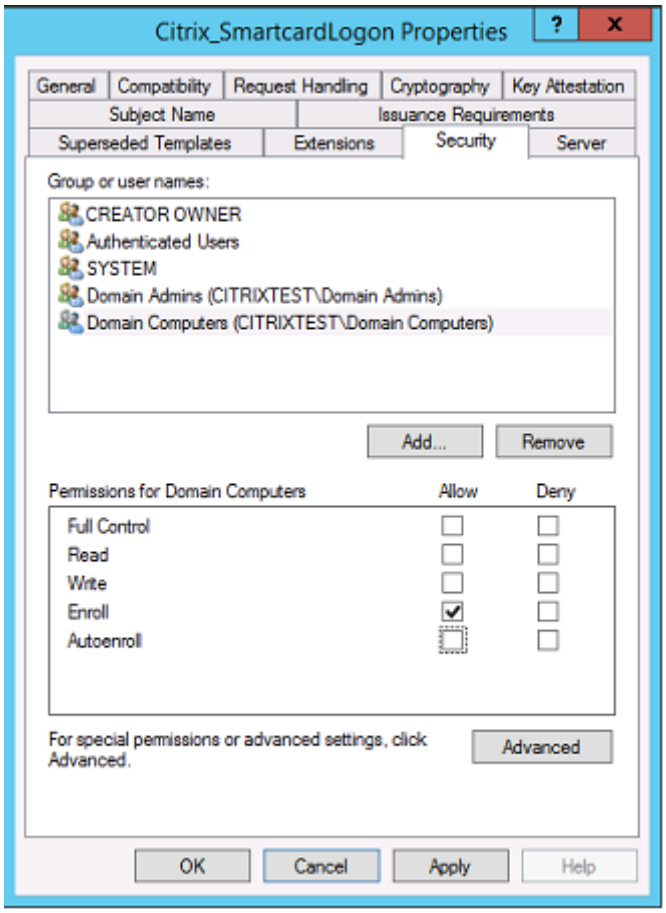
Vous pouvez modifier ces paramètres en fonction de la stratégie de votre organisation.

Remarque : des paramètres d'extension inappropriés peuvent entraîner des problèmes de sécurité ou aboutir à des certificats inutilisables.

Modifier les propriétés de sécurité

Citrix recommande de modifier ces paramètres pour accorder l'autorisation **Inscription** pour les comptes d'ordinateur des serveurs FAS uniquement. Comme pour les autres services, accordez également l'autorisation **Contrôle total**pour le système. Aucune autre autorisation n'est nécessaire. Vous

souhaiterez peut-être accorder d'autres autorisations, par exemple permettre aux administrateurs de FAS d'afficher un modèle modifié à des fins de dépannage.



Modifier les propriétés de nom du sujet

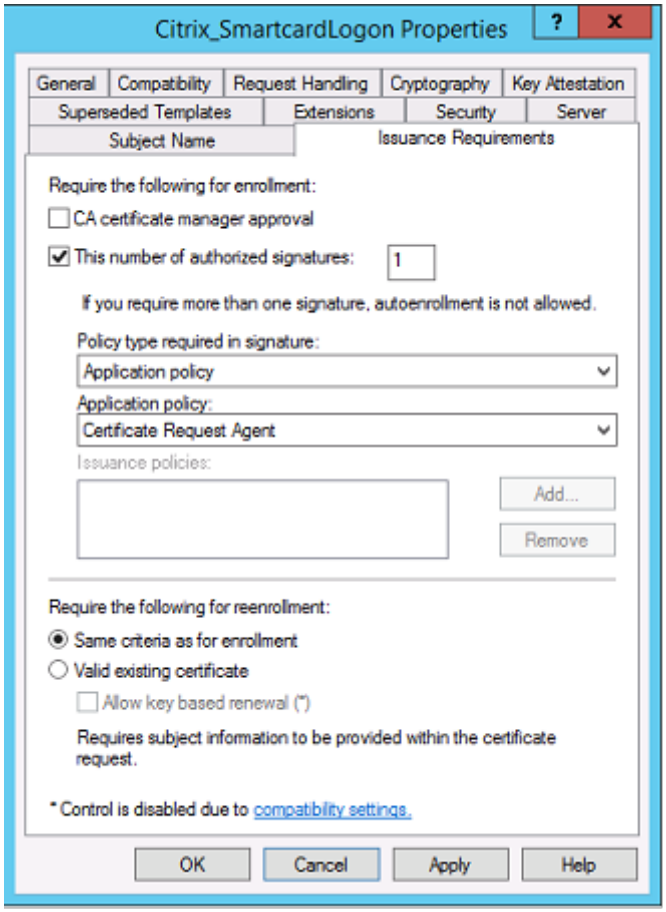
Vous pouvez modifier ces paramètres en fonction de la stratégie de votre organisation, si nécessaire.

Modifier les propriétés de serveur

Citrix ne le recommande pas, mais vous pouvez modifier ces paramètres en fonction de la stratégie de votre organisation, si nécessaire.

Modifier les propriétés de conditions d'émission

Ne modifiez pas ces paramètres. Ces paramètres doivent être comme indiqué :



Modifier les propriétés de compatibilité

Vous pouvez modifier ces paramètres. Le paramètre doit être au moins **Windows Server 2003 CAs** (version de schéma 2). Toutefois, FAS prend en charge uniquement Windows Server 2008 et les autorités de certification ultérieures. Comme expliqué ci-dessus, FAS ignore également les paramètres supplémentaires disponibles si **Windows Server 2008 CAs** (version de schéma 3) ou **Windows Server 2012 CAs** est sélectionné (version de schéma 4).

Administration de l'autorité de certification

L'administrateur de l'autorité de certification est responsable de la configuration du serveur d'autorité de certification et de l'émission de la clé privée de certificat qu'il utilise.

Publication de modèles

Pour qu'une autorité de certification puisse émettre des certificats basés sur un modèle fourni par l'administrateur de l'entreprise, l'administrateur de l'autorité de certification doit choisir de publier

ce modèle.

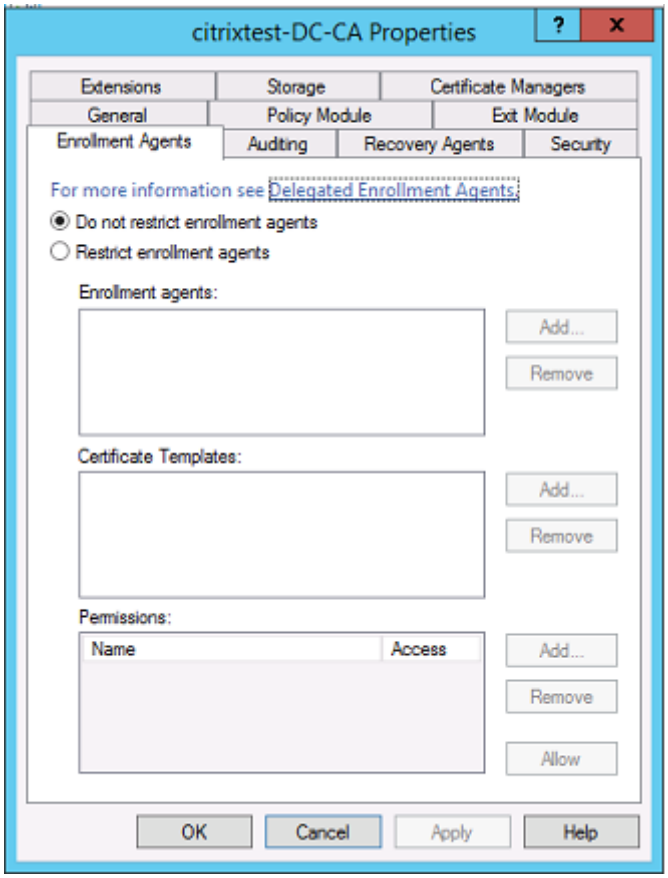
Une simple pratique de sécurité consiste à publier uniquement les modèles de certificat RA lorsque les serveurs FAS sont installés, ou d'opter pour un processus d'émission hors connexion. Dans les deux cas, l'administrateur CA doit conserver un contrôle total sur l'autorisation des demandes de certificat RA, et disposer d'une stratégie pour autoriser les serveurs FAS.

Paramètres de pare-feu

En général, l'administrateur CA contrôlera également les paramètres de pare-feu réseau de l'autorité de certification, ce qui permet de contrôler les connexions entrantes. L'administrateur de l'autorité de certification peut configurer le protocole TCP de DCOM et des règles de pare-feu de manière à ce que seuls les serveurs FAS puissent demander des certificats.

Inscription restreinte

Par défaut, le détenteur d'un certificat RA peut émettre des certificats pour tous les utilisateurs, à l'aide d'un quelconque modèle de certificat autorisant l'accès. Ceci devrait être restreint à un groupe d'utilisateurs non privilégiés à l'aide de la propriété d'autorité de certification « Restreindre les agents d'inscription ».



Modules de stratégie et d'audit

Pour les déploiements avancés, des modules de sécurité personnalisés peuvent être utilisés pour assurer le suivi et interdire l'émission de certificats.

Administration du FAS

Le FAS possède plusieurs fonctions de sécurité.

Restreindre StoreFront, les utilisateurs et les VDA via une liste de contrôle d'accès

Au centre du modèle de sécurité du FAS figure le contrôle grâce auquel les comptes Kerberos peuvent accéder aux fonctionnalités :

Vecteur d'accès	Description
StoreFront [fournisseur d'identité]	Ces comptes Kerberos sont approuvés pour déclarer qu'un utilisateur a été correctement authentifié. Si l'un de ces comptes est compromis, des certificats peuvent être créés et utilisés pour les utilisateurs autorisés par la configuration du FAS.
VDA [partie de confiance]	Il s'agit des machines qui sont autorisées à accéder aux certificats et aux clés privées. Un handle d'informations d'identification récupéré par le fournisseur d'identité est également nécessaire, de façon à limiter les possibilités d'attaque du système par un compte VDA compromis dans ce groupe.
Utilisateurs	Contrôle les utilisateurs qui peuvent être certifiés par le fournisseur d'identité. Veuillez noter qu'il existe un chevauchement avec les options de configuration « Restreindre les agents d'inscription » de l'autorité de certification. En règle générale, il est conseillé d'inclure uniquement des comptes non privilégiés dans cette liste. Ceci empêche un compte StoreFront compromis de réaffecter des privilèges à un niveau administratif plus élevé. En particulier, les comptes d'administrateur de domaine ne doivent pas être autorisés par cette ACL.

Configurer des règles

Les règles sont utiles si plusieurs déploiements XenApp ou XenDesktop indépendants utilisent la même infrastructure de serveur FAS. Chaque règle dispose d'options de configuration distinctes ; en particulier, les ACL peuvent être configurées indépendamment.

Configurer l'autorité de certification et les modèles

Différents modèles de certificats et autorités de certification peuvent être configurés afin d'octroyer des droits d'accès différents. Des configurations avancées peuvent choisir d'utiliser plus ou moins de certificats puissants, en fonction de l'environnement. À titre d'exemple, les utilisateurs identifiés en tant que « externes » peuvent posséder un certificat avec moins de privilèges que les utilisateurs « internes ».

Certificats d'authentification et dans la session

L'administrateur FAS peut contrôler si le certificat utilisé pour l'authentification peut être utilisé dans la session de l'utilisateur. Par exemple, ceci peut être utilisé pour mettre uniquement à disposition des certificats « de signature » dans la session, afin de réserver le certificat « d'ouverture de session » plus puissant uniquement pour l'ouverture de session.

Protection de clé privée et longueur de clé

L'administrateur FAS peut configurer FAS afin de stocker les clés privées dans un module de sécurité matériel (HSM) ou un module de plateforme sécurisée (TPM). Citrix recommande de protéger au moins une clé privée de certificat RA en la stockant dans un TPM ; cette option est fournie dans le cadre du processus de demande de certificat « hors connexion ».

De même, les clés privées de certificat utilisateur peuvent être stockées dans un module TPM ou HSM. Toutes les clés doivent être générées en tant que « non exportables » et d'une longueur minimum de 2 048 bits.

Journaux d'événements

Le serveur FAS fournit des informations détaillées sur la configuration et des journaux d'événements, qui peuvent être utilisés pour l'audit et la détection des intrusions.

Accès administratif et outils d'administration

Le FAS comprend des fonctionnalités d'administration à distance (authentification mutuelle Kerberos) ainsi que des outils. Les membres du « groupe Administrateurs local » exercent un contrôle total sur la configuration du FAS. Cette liste doit être soigneusement tenue à jour.

Administrateurs XenApp, XenDesktop et VDA

En général, l'utilisation du FAS ne modifie pas le modèle de sécurité des administrateurs Delivery Controller et VDA, car le « handle d'informations d'identification » du FAS remplace simplement le « mot de passe Active Directory. » Les groupes d'administration Controller et VDA doivent contenir uniquement des utilisateurs approuvés. L'audit et les journaux d'événements doivent être tenus à jour.

Sécurité des serveurs Windows

Tous les correctifs doivent avoir été installés sur tous les serveurs, de même que des pare-feu et des logiciels antivirus. Les serveurs d'infrastructure critiques à la sécurité doivent être conservés dans un endroit sécurisé, et un soin tout particulier doit être apporté au cryptage du disque et aux options de maintenance des machines virtuelles.

L'audit et les journaux d'événements doivent être stockés de manière sécurisée sur une machine distante.

L'accès RDP doit être limité aux administrateurs autorisés. Dans la mesure du possible, les comptes utilisateur doivent demander une ouverture de session par carte à puce, plus particulièrement pour les comptes d'administrateur de domaine et d'autorité de certification.

Informations connexes

- L'article Service d'authentification fédérée est le document de référence principal pour obtenir des informations sur l'installation et la configuration du FAS.
- Les architectures FAS sont présentées dans l'article Vue d'ensemble des architectures du Service d'authentification fédérée.
- D'autres informations pratiques sont disponibles dans l'article Configuration et gestion du service d'authentification fédérée.

Service d'authentification fédérée - Résoudre les problèmes d'ouverture de session Windows

January 23, 2019

Cet article décrit les journaux et les messages d'erreur Windows lorsqu'un utilisateur ouvre une session à l'aide de certificats et/ou de cartes à puce. Ces journaux fournissent des informations que vous pouvez utiliser pour résoudre les échecs d'authentification.

Certificats et infrastructure de clé publique

Windows Active Directory propose plusieurs magasins de certificats qui gèrent les certificats pour les utilisateurs qui ouvrent une session.

- **Magasin de certificats NTAuth :** pour s'authentifier auprès de Windows, l'autorité de certification émettant les certificats utilisateur (aucune chaîne n'est prise en charge) doit être placée dans le magasin NTAuth. Pour afficher ces certificats, depuis le programme certutil, entrez : certutil –viewstore –enterprise NTAuth.
- **Magasins de certificats racine et intermédiaires :** en règle générale, les systèmes d'ouverture de session par certificat peuvent fournir un seul certificat. Donc, si une chaîne est utilisée, le magasin de certificats intermédiaires sur toutes les machines doit inclure ces certificats. Le certificat racine doit être dans le magasin racine de confiance et l'avant-dernier certificat doit être dans le magasin NTAuth.
- **Extensions de certificat d'ouverture de session et stratégie de groupe :** Windows peut être configuré pour appliquer la vérification des EKU et d'autres stratégies de certificat. Reportez-vous à la documentation Microsoft : https://technet.microsoft.com/en-us/library/ff404287%28v=ws.10%29.aspx.

Stratégie du Registre	Description
AllowCertificatesWithNoEKU	Lorsqu'elle est désactivée, les certificats doivent inclure l'Utilisation améliorée de la clé (EKU) pour l'ouverture de session avec carte à puce.
AllowSignatureOnlyKeys	Par défaut, Windows filtre les clés privées de certificats qui ne permettent pas le décryptage RSA. Cette option remplace ce filtre.
AllowTimeInvalidCertificates	Par défaut, Windows filtre les certificats expirés. Cette option remplace ce filtre.
EnumerateECCCerts	Active l'authentification à courbe elliptique.
X509HintsNeeded	Si un certificat ne contient pas de nom d'utilisateur principal (UPN) unique, ou s'il peut être ambigu, cette option permet aux utilisateurs de spécifier manuellement leur compte d'ouverture de session Windows.
UseCachedCRLOnlyAnd, IgnoreRevocationUnknownErrors	Désactive la vérification de la révocation des certificats (généralement définie sur le contrôleur de domaine).

- **Certificats du contrôleur de domaine :** pour authentifier les connexions Kerberos, tous les serveurs doivent avoir des certificats « Contrôleur de domaine » appropriés. Ils peuvent être demandés depuis le menu du composant logiciel enfichable MMC « Local Computer Certificate Personal Store » (magasin personnel de certificats de l'ordinateur local).

Nom UPN et mappage de certificat

Il est recommandé que les certificats utilisateur incluent un nom d'utilisateur principal (UPN) unique dans l'extension Nom de sujet alternatif.

Noms UPN dans Active Directory

Par défaut, chaque utilisateur d'Active Directory est associé à un UPN implicite, basé sur le modèle <NomUtilisateur_sam>@<NetBios_domaine> et <NomUtilisateur_sam>@<FQDN_domaine>. Les domaines disponibles et les noms de domaine complets sont inclus dans l'entrée RootDSE de la forêt. Veuillez noter qu'un seul domaine peut disposer de plusieurs noms de domaine complets enregistrés dans RootDSE.

En outre, chaque utilisateur d'Active Directory a un nom UPN explicite et des altUserPrincipalNames. Ce sont des entrées LDAP qui spécifient le nom d'utilisateur principal (UPN) pour l'utilisateur.

Lors d'une recherche d'utilisateurs par UPN, Windows recherche d'abord dans le domaine courant (en fonction de l'identité du processus de recherche de l'UPN) les UPN explicites, puis les UPN alternatifs. S'il n'existe pas de correspondance, il recherche l'UPN implicite, qui peut se résoudre sur différents domaines de la forêt.

Service de mappage de certificat

Si un certificat ne contient pas d'UPN explicite, Active Directory peut stocker un certificat public exact pour chaque utilisation dans un attribut « x509certificate ». Pour résoudre un tel certificat pour un utilisateur, un ordinateur peut interroger cet attribut directement (par défaut, dans un seul domaine).

L'utilisateur peut spécifier un compte d'utilisateur qui accélère la recherche et permet également à cette fonctionnalité d'être utilisée dans un environnement inter-domaines.

S'il existe plusieurs domaines dans la forêt et que l'utilisateur ne spécifie pas explicitement un domaine, Active Directory rootDSE spécifie l'emplacement du service de mappage de certificat. Il est généralement situé sur une machine de catalogue global et bénéficie d'une vue en cache de tous les attributs x509certificate de la forêt. Cet ordinateur peut être utilisé pour rechercher efficacement un compte utilisateur dans tout domaine, en se basant uniquement sur le certificat.

Sélection du contrôleur de domaine d'ouverture de session

Lorsqu'un environnement contient plusieurs contrôleurs de domaine, il est utile de voir et de restreindre le contrôleur de domaine qui est utilisé pour l'authentification, de façon à ce que les journaux puissent être activés et récupérés.

Contrôler la sélection du contrôleur de domaine

Pour forcer Windows à utiliser un contrôleur de domaine Windows spécifique pour l'ouverture de session, vous pouvez explicitement définir la liste des contrôleurs de domaine qu'une machine Windows utilise en configurant le fichier lmhosts : \Windows\System32\drivers\etc\lmhosts.

Il existe généralement un exemple de fichier nommé « lmhosts.sam » dans cet emplacement. Il vous suffit d'inclure une ligne :

1.2.3.4 dcnetbiosname #PRE #DOM:mondomaine

Où « 1.2.3.4 » est l'adresse IP du contrôleur de domaine nommé « dcnetbiosname » dans le domaine « mondomaine ».

Après un redémarrage, la machine Windows utilise ces informations pour ouvrir une session sur mondomaine. Notez que cette configuration doit être rétablie lors d'un débogage.

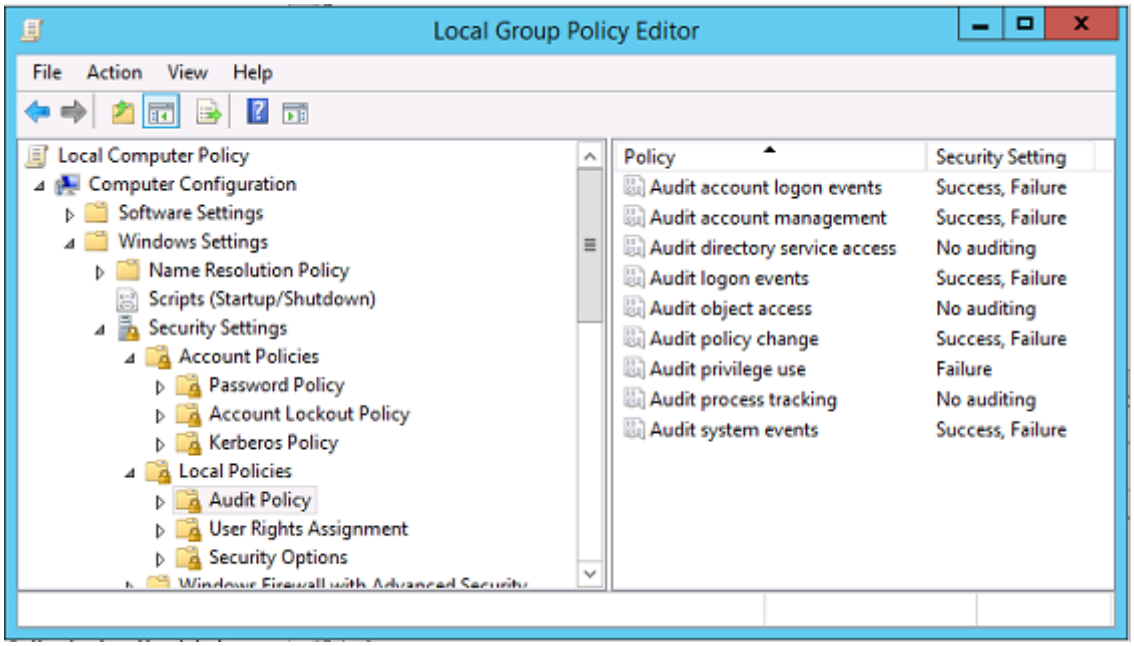
Identifier le contrôleur de domaine utilisé

À l'ouverture de session, Windows définit une variable d'environnement MSDOS avec le contrôleur de domaine qui a ouvert la session de l'utilisateur. Pour la voir, démarrez l'invite de commande avec la commande : **echo %LOGONSERVER%**.

Les journaux liés à l'authentification sont stockés sur l'ordinateur renvoyé par cette commande.

Activer les événements d'audit de compte

Par défaut, les contrôleurs de domaine Windows n'activent pas les journaux d'audit de compte complets. Ce réglage peut être contrôlé par le biais des stratégies d'audit dans les paramètres de sécurité dans l'éditeur de stratégie de groupe. Une fois qu'ils sont activés, le contrôleur de domaine génère des informations supplémentaires dans le journal d'événements de sécurité.



Journaux de validation de certificat

Vérifier la validité du certificat

Si un certificat de carte à puce est exporté en tant que certificat DER (sans clé privée), vous pouvez le valider avec la commande : certutil –verify user.cer

Activer la journalisation CAPI

Sur le contrôleur de domaine et les machines utilisateur, ouvrez l'observateur d'événements et activez la journalisation pour Microsoft/Windows/CAPI2/Operational Logs.

Vous pouvez contrôler la journalisation CAPI avec les clés de registre dans : CurrentControlSet\Services\crypt32.

Valeur	Description
DiagLevel (DWORD)	Niveau de détail (0 à 5)
DiagMatchAnyMask (QUADWORD)	Filtre d'événements (utiliser 0xffffff pour tout)
DiagProcessName (MULTI_SZ)	Filtre par nom du processus (par exemple, LSASS.exe)

Journaux CAPI

Message	Description
Build Chain	CertGetCertificateChain appelé par LSA (comprend résultat)
Verify Revocation	CertVerifyRevocation appelé par LSA (comprend résultat)
X509 Objects	En mode détaillé, les certificats et les listes de révocation de certificats (CRL) sont placés dans AppData\LocalLow\Microsoft\X509Objects
Verify Chain Policy	CertVerifyChainPolicy appelé par LSA (comprend paramètres)

Messages d'erreur

Code d'erreur	Description
Certificat non approuvé	Le certificat de carte à puce n'a pas pu être créé à l'aide de certificats contenus dans les magasins de certificats racine approuvés et intermédiaires de l'ordinateur.
Erreur de vérification de la révocation de certificats	La liste de révocation de certificats pour la carte à puce n'a pas pu être téléchargée à partir de l'adresse spécifiée par le point de distribution de la liste de révocation de certificat. Si la vérification de la révocation des certificats est obligatoire, l'ouverture de session échoue. Consultez la section Certificats et infrastructure de clé publique.
Erreurs d'utilisation de certificat	Le certificat n'est pas approprié pour l'ouverture de session. Par exemple, il peut s'agir d'un certificat de serveur ou d'un certificat de signature.

Journaux Kerberos

Pour activer la journalisation Kerberos, sur le contrôleur de domaine et la machine utilisateur, créez les valeurs de registre suivantes :

Ruche	Nom de la valeur	Valeur [DWORD]
CurrentControlSet\Control\Lsa	LogLevel	0x1
CurrentControlSet\Control\Lsa\Kerberos\Parameters	KerbDebugLevel	0xffffffff
CurrentControlSet\Services\Kd	KdcDebugLevel	0x1
CurrentControlSet\Services\Kdc	KdcExtraLogLevel	0x1f

La journalisation Kerberos est écrite dans le journal d'événements système.

- Les messages tels que « certificat non approuvé » (untrusted certificate) devraient être faciles à diagnostiquer.
- Deux codes d'erreur sont des messages d'informations et peuvent être ignorés :
  - KDC_ERR_PREAUTH_REQUIRED (utilisé pour la rétrocompatibilité avec les contrôleurs de domaine plus anciens)
  - Erreur inconnue 0x4b

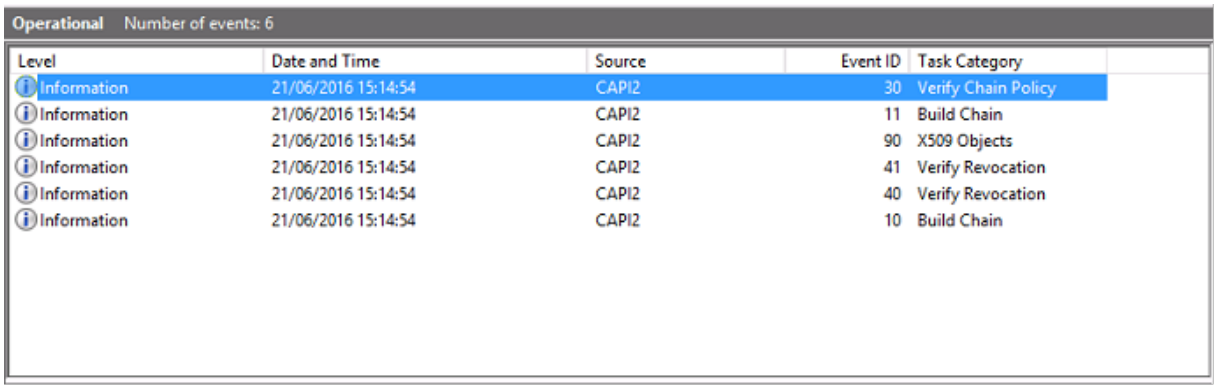
Messages des journaux d'événements

Cette section décrit les entrées de journal attendues sur le contrôleur de domaine et la station de travail lorsque l'utilisateur ouvre une session avec un certificat.

- Journal CAPI2 du contrôleur de domaine
- Journaux de sécurité du contrôleur de domaine
- Journal de sécurité VDA
- Journal CAPI VDA
- Journal système VDA

Journal CAPI2 du contrôleur de domaine

Lors d'une ouverture de session, le contrôleur de domaine valide le certificat de l'appelant, produisant une séquence d'entrées de journal comme illustré ci-dessous.



Operational Number of events: 6

Level	Date and Time	Source	Event ID	Task Category
Information	21/06/2016 15:14:54	CAPI2	30	Verify Chain Policy
Information	21/06/2016 15:14:54	CAPI2	11	Build Chain
Information	21/06/2016 15:14:54	CAPI2	90	X509 Objects
Information	21/06/2016 15:14:54	CAPI2	41	Verify Revocation
Information	21/06/2016 15:14:54	CAPI2	40	Verify Revocation
Information	21/06/2016 15:14:54	CAPI2	10	Build Chain

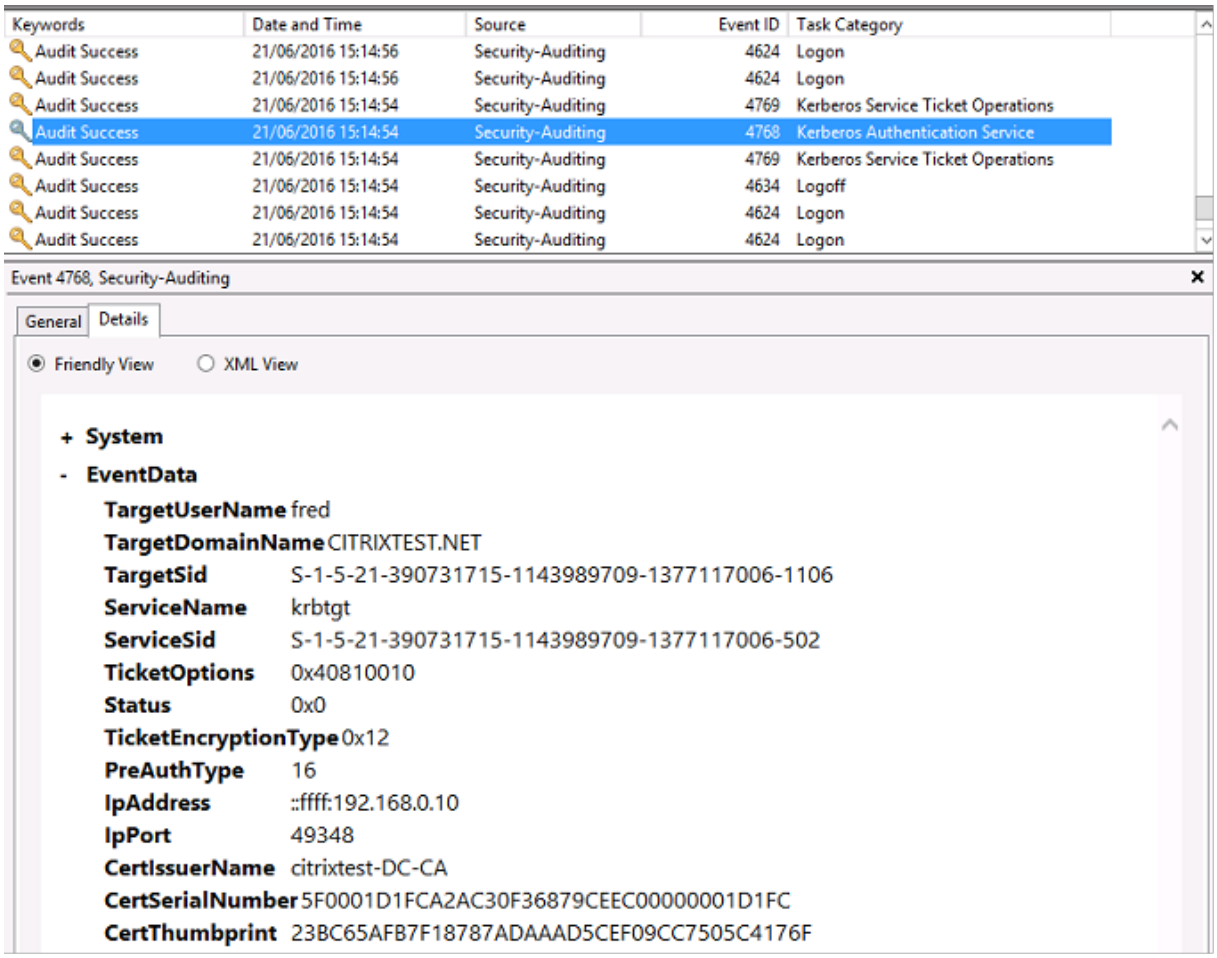
Le dernier message du journal d'événements indique que lsass.exe sur le contrôleur de domaine construit une chaîne en fonction du certificat fourni par le VDA et vérifie sa validité (y compris la révocation). Le résultat est « ERROR_SUCCESS ».

- **CertVerifyCertificateChainPolicy**
  - **Policy**
    - [**type**] CERT_CHAIN_POLICY_NT_AUTH
    - [**constant**] 6
  - **Certificate**
    - [**fileRef**] 23BC65AFB7F18787ADAAAD5CEF09CC7505C4176F.cer
    - [**subjectName**] fred
  - **CertificateChain**
    - [**chainRef**] {FF03F79B-52F8-4C93-877A-5DFFE40B9574}
  - **Flags**
    - [**value**] 0
  - **Status**
    - [**chainIndex**] -1
    - [**elementIndex**] -1
  - **EventAuxInfo**
    - [**ProcessName**] lsass.exe
  - **CorrelationAuxInfo**
    - [**TaskId**] {F5E7FD3F-628F-4C76-9B1C-49FED786318F}
    - [**SeqNumber**] 1
  - **Result**
    - [**value**] 0

Journal de sécurité du contrôleur de domaine

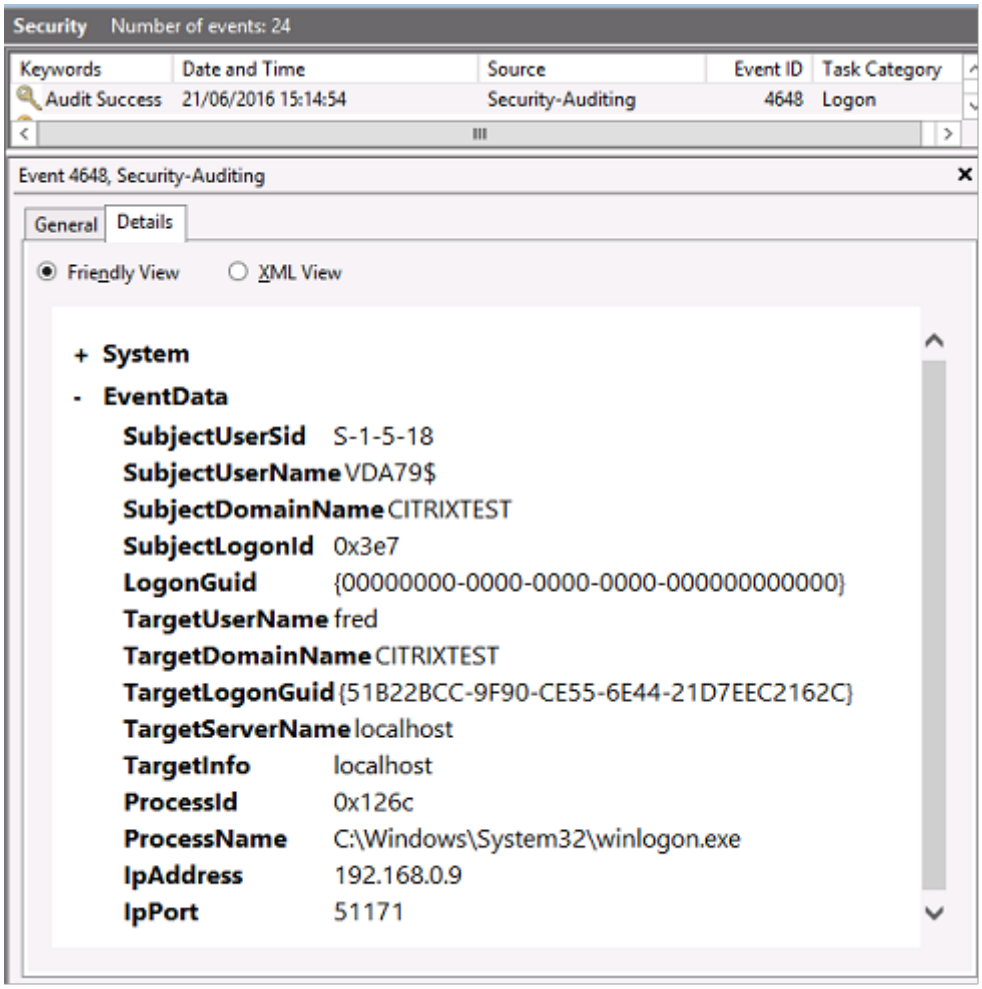
Le contrôleur de domaine présente une séquence des événements d'ouverture de session, l'événement clé étant 4768, dans lequel le certificat est utilisé pour émettre le ticket Kerberos Ticket Granting (krbtgt).

Les messages précédents indiquent que le compte de machine du serveur s'authentifie auprès du contrôleur de domaine. Les messages suivants indiquent le compte d'utilisateur appartenant au nouveau krbtgt utilisé pour s'authentifier auprès du contrôleur de domaine.



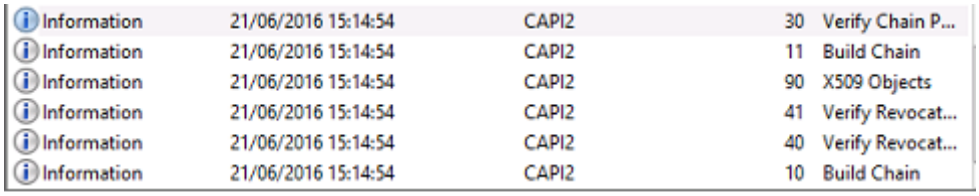
Journal de sécurité VDA

Le journal d'audit de sécurité VDA correspondant à l'événement d'ouverture de session est l'entrée avec l'ID 4648, provenant de winlogon.exe.



Journal CAPI VDA

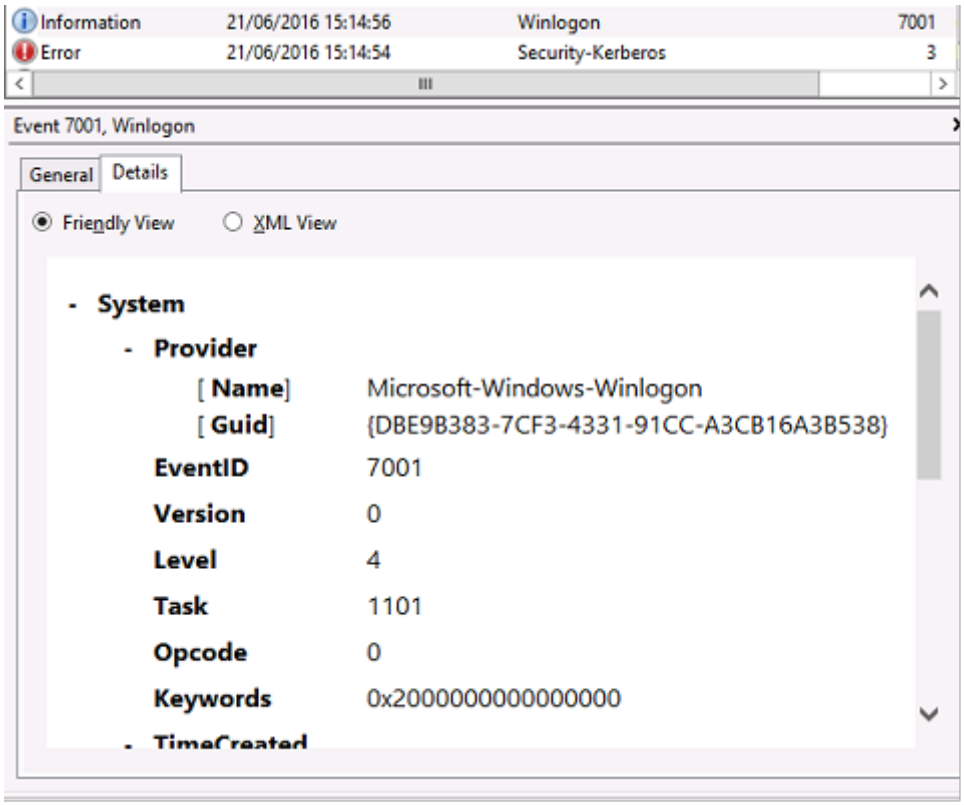
Cet exemple de journal CAPI VDA présente une séquence de création de chaîne et de vérification depuis lsass.exe, validant le certificat du contrôleur de domaine (dc.citrixtest.net).



- **UserData**
  - **CertVerifyCertificateChainPolicy**
    - **Policy**
      - [**type**] CERT_CHAIN_POLICY_NT_AUTH
      - [**constant**] 6
    - **Certificate**
      - [**fileRef**] 813C6D12E1E1800E61B8DB071E186EB912B7
      - [**subjectName**] dc.citrixtest.net
    - **CertificateChain**
      - [**chainRef**] {84E0B3D1-A4D4-4AC7-BA99-5291415B343
    - **Flags**
      - [**value**] 0
    - **Status**
      - [**chainIndex**] -1

Journal système VDA

Lorsque l'ouverture de session Kerberos est activée, le journal système affiche l'erreur KDC_ERR_PREAUTH_REQUI
(qui peut être ignorée) et une entrée de Winlogon, indiquant que l'ouverture de session Kerberos a
réussi.



Messages d'erreur de l'utilisateur final

Cette section dresse la liste des messages d'erreur courants s'affichant sur la page d'ouverture de session Windows.

Message d'erreur affiché	Description et référence
Nom d'utilisateur ou mot de passe non valide	L'ordinateur détecte que vous disposez d'un certificat et d'une clé privée valides, mais le contrôleur de domaine Kerberos a rejeté la connexion. Consultez la section *Journaux Kerberos* de cet article.
Le système n'a pas pu vous connecter. Impossible de vérifier les informations d'identification.	Le contrôleur de domaine ne peut pas être contacté, ou les certificats appropriés ne sont pas installés sur le contrôleur de domaine.
La requête n'est pas prise en charge.	Réinscrivez les certificats « Contrôleur de domaine » et « Authentification du contrôleur de domaine » sur le contrôleur de domaine, comme décrit dans la section CTX206156. Cette réinscription est recommandée, même lorsque les certificats existants semblent valides.
Le système n'a pas pu vous connecter. Le certificat de carte à puce utilisé pour l'authentification n'est pas approuvé.	Les certificats racine et intermédiaire ne sont pas installés sur l'ordinateur local. Consultez l'article CTX206156 pour obtenir des instructions sur l'installation de certificats de carte à puce sur des ordinateurs n'appartenant pas à un domaine. Voir également *Certificats et infrastructure de clé publique* dans cet article.
Vous ne pouvez pas ouvrir de session car l'ouverture de session par carte à puce n'est pas prise en charge par votre compte.	Un compte utilisateur de groupe de travail n'a pas été complètement configuré pour l'ouverture de session par carte à puce.
La clé requise n'existe pas	Un certificat fait référence à une clé privée qui n'est pas accessible. Cela peut se produire lorsqu'une carte PIV n'est pas correctement configurée et que le fichier CCC ou CHUID est manquant.
Une erreur s'est produite lors de la tentative d'utilisation de la carte à puce	Le middleware de carte à puce n'a pas été correctement installé. Voir CTX206156 pour des instructions d'installation de carte à puce.

Message d'erreur affiché	Description et référence
Insérez une carte à puce.	Le lecteur ou la carte à puce n'a pas été détecté. Si la carte à puce est insérée, ce message indique un problème de matériel ou de middleware. Voir CTX206156 pour des instructions d'installation de carte à puce.
Le code PIN est incorrect	La carte à puce a rejeté un code PIN entré par l'utilisateur.
Aucun certificat de carte à puce valide n'a été trouvé.	Les extensions du certificat peuvent ne pas être correctement configurées, ou la clé RSA est trop courte (<2 048 bits). Consultez la section CTX206901 pour de plus amples informations sur la génération de certificats de carte à puce valides.
La carte à puce est bloquée	Une carte à puce a été verrouillée (par exemple, la saisie d'un code PIN incorrect plusieurs fois). Un administrateur peut avoir accès au code de déverrouillage du code PIN (puk) pour la carte et peut réinitialiser le code PIN de l'utilisateur à l'aide d'un outil du fournisseur de carte à puce. Si le code puk n'est pas disponible ou verrouillé, la carte doit être réinitialisée sur ses paramètres d'usine.
Demande incorrecte	Une clé privée de carte à puce ne prend pas en charge la cryptographie requise par le contrôleur de domaine. Par exemple, le contrôleur de domaine peut avoir demandé un « décryptage de clé privée », mais la carte à puce ne prend en charge que la signature. Ceci indique habituellement que les extensions sur le certificat ne sont pas définies correctement, ou que la clé RSA est trop courte (<2 048 bits). Consultez la section CTX206901 pour de plus amples informations sur la génération de certificats de carte à puce valides.

Informations connexes

- Configuration d'un domaine pour l'ouverture de session par carte à puce : https://support.citrix.com/article/CTX206156
- Stratégies d'ouverture de session par carte à puce : https://technet.microsoft.com/en-us/library/ff404287%28v=ws.10%29.aspx
- Activation de la journalisation CAPI : https://social.technet.microsoft.com/wiki/contents/articles/242.troubleshooting-pki-problems-on-windows.aspx
- Activation de la journalisation Kerberos : https://support.microsoft.com/en-us/kb/262177
- Recommandations pour l'activation de l'ouverture de session par carte à puce avec des autorités de certification tierces : https://support.microsoft.com/en-us/kb/281245

Applets de commande PowerShell du Service d'authentification fédérée

November 8, 2018

Vous pouvez utiliser la console d'administration Service d'authentification fédérée pour les déploiements simples, toutefois l'interface PowerShell offre des options plus avancées. Si vous prévoyez d'utiliser des options qui ne sont pas disponibles dans la console, Citrix recommande d'utiliser uniquement PowerShell pour la configuration.

La commande suivante ajoute les applets de commande PowerShell du FAS :

```
1 Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1
```

Dans une fenêtre PowerShell, vous pouvez utiliser Get-Help <*nom cmdlet*> pour afficher l'aide de l'applet de commande.

Le lien vers le fichier zip ci-dessous contient des fichiers d'aide pour toutes les applets de commande du SDK PowerShell du FAS. Pour l'utiliser, cliquez sur le lien pour télécharger le fichier zip. Extrayez ensuite le contenu du fichier sur un dossier local. Le fichier index.html répertorie toutes les applets de commande, avec des liens vers les fichiers d'aide d'applet de commande individuels.

Fichiers d'aide de l'applet de commande du PowerShell du Service d'authentification fédérée

Graphiques

November 8, 2018

Les graphiques Citrix HDX comprennent un ensemble complet de technologies de codage et d'accélération graphique qui optimise la mise à disposition des applications riches en graphiques à partir de XenApp et XenDesktop. Les technologies graphiques fournissent la même expérience

qu'avec un bureau physique lors de l'utilisation à distance d'applications virtuelles qui sont riches en graphiques.

Vous pouvez utiliser une solution logicielle ou matérielle pour la restitution des graphiques. La restitution logicielle requiert une bibliothèque tierce appelée logiciel de rastérisation. Par exemple, Windows inclut le module de rastérisation WARP pour les graphiques DirectX. Vous pouvez souhaiter utiliser un autre outil de restitution logicielle (par exemple, l'
accélération logicielle OpenGL). Le rendu matériel (accélération matérielle) nécessite un processeur graphique (GPU).

Les graphiques HDX proposent une configuration de codage par défaut qui est optimisée pour les cas d'utilisation les plus courants. Les administrateurs informatiques peuvent également utiliser des stratégies Citrix pour configurer divers paramètres liés aux graphiques afin de répondre aux différents besoins et proposer l'expérience utilisateur recherchée.

ThinWire

Thinwire est la technologie de communication à distance d'écran par défaut de Citrix utilisée dans XenApp et XenDesktop.

La technologie de communication à distance d'écran permet aux graphiques générés sur une machine d'être transmis, généralement via un réseau, vers une autre machine. Les graphiques sont créés par l'utilisateur, à l'aide de frappes clavier ou d'actions de souris par exemple.

HDX 3D Pro

Les fonctions HDX 3D Pro dans XenApp et XenDesktop vous permettent de mettre à disposition des bureaux et applications qui fonctionnent mieux avec un processeur graphique pour l'accélération matérielle. Ces applications incluent les applications graphiques 3D professionnelles basées sur OpenGL et DirectX. Le VDA standard prend uniquement en charge l'accélération GPU de DirectX.

Accélération GPU pour OS de bureau Windows

Avec HDX 3D Pro, vous pouvez mettre à disposition des applications au graphisme intensif dans le cadre des applications ou bureaux hébergés sur des machines avec OS de bureau. HDX 3D Pro prend en charge les ordinateurs hôtes physiques, (y compris les bureaux, les lames et les stations de travail en rack) et les technologies de virtualisation GPU Passthrough et GPU offertes par les hyperviseurs XenServer, vSphere et Hyper-V (Passthrough uniquement).

À l'aide de la fonctionnalité GPU Passthrough, vous pouvez créer des VM bénéficiant d'un accès exclusif à du matériel de traitement graphique dédié. Vous pouvez installer plusieurs processeurs graphiques sur l'hyperviseur et affecter individuellement des VM à chacun de ces processeurs graphiques.

À l'aide de la virtualisation GPU, plusieurs machines virtuelles peuvent accéder directement à la puissance de traitement graphique d'un processeur graphique physique unique.

Accélération GPU pour OS de serveur Windows

HDX 3D Pro permet aux applications exigeantes en ressources graphiques exécutées dans de sessions d'OS de serveur Windows d'être restituées sur le processeur graphique du serveur (GPU). En déplaçant la restitution OpenGL, DirectX, Direct3D et Windows Presentation Foundation (WPF) sur le processeur graphique du serveur, l'unité centrale du serveur n'est pas ralentie par la restitution des graphiques. Par ailleurs, le serveur est capable de traiter davantage de graphiques car la charge est partagée entre le processeur graphique et l'unité centrale.

Framehawk

Framehawk est une technologie de communication à distance d'écran pour les travailleurs mobiles via des connexions sans fil haut débit (réseaux cellulaires Wi-Fi et 4G/LTE). Framehawk aide à résoudre les problèmes d'interférence spectrale et de propagation à trajets multiples, proposant une expérience fluide et interactive aux utilisateurs d'applications et de bureaux virtuels.

Accélérateur logiciel OpenGL

L'accélérateur logiciel OpenGL est un logiciel de rastérisation pour des applications OpenGL comme ArcGIS, Google Earth, Nehe, Maya, Fusion, Voxler, CAD et CAM. Dans certains cas, l'accélérateur logiciel OpenGL peut éliminer le besoin d'utiliser des cartes graphiques pour offrir une expérience utilisateur optimale avec des applications OpenGL.

Informations connexes

- ThinWire
- HDX 3D Pro
- Accélération GPU pour OS de bureau Windows
- Accélération GPU pour OS de serveur Windows
- Framehawk
- Accélérateur logiciel OpenGL

Framehawk

January 23, 2019

Framehawk est une technologie de communication à distance d'écran pour les travailleurs mobiles via des connexions sans fil haut débit (réseaux cellulaires Wi-Fi et 4G/LTE). Framehawk aide à résoudre les problèmes d'interférence spectrale et de propagation à trajets multiples, proposant une expérience fluide et interactive aux utilisateurs d'applications et de bureaux virtuels. Framehawk peut être une solution idéale pour les utilisateurs sur connexions réseau longue distance à haut débit (à latence élevée) où une petite quantité de perte de paquets peut dégrader l'expérience de l'utilisateur. Nous

vous suggérons d'utiliser le transport adaptatif pour ce scénario ; pour plus d'informations, consultez la section Transport adaptatif.

Vous pouvez utiliser les modèles de stratégie Citrix pour mettre en œuvre Framehawk pour un ensemble d'utilisateurs et de scénarios d'accès de manière appropriée pour votre organisation. Framehawk cible les configurations à écran unique telles que les ordinateurs portables et les tablettes. Utilisez Framehawk lorsque l'importance de performances interactives en temps réel justifie les coûts supplémentaires en ressources serveur et le besoin d'une connexion haut débit.

Comment Framehawk assure une expérience utilisateur fluide

Imaginez Framehawk comme une implémentation logicielle de l'œil humain, observant ce qui se trouve dans le tampon de trame et identifiant les différents types de contenu sur l'écran. Qu'est-ce qui est important pour l'utilisateur ? Pour les zones de l'écran qui changent rapidement, comme les vidéos ou les graphiques animés, il n'est pas très important pour l'œil humain que quelques pixels se perdent, car ils sont rapidement remplacés par de nouvelles données.

Toutefois, pour les zones statiques de l'écran, telles que les icônes dans la barre d'outils ou la zone de notification ou un texte qui s'affiche après défilement par l'utilisateur pour atteindre son point de lecture, l'œil humain est très exigeant. Un utilisateur attend une perfection au pixel près. À l'inverse des protocoles qui recherchent la **précision technique**, Framehawk vise à s'adapter à l'être humain utilisant la technologie.

Framehawk comprend un amplificateur de signal (QoS) nouvelle génération ainsi qu'une carte thermique temporelle pour une identification plus précise et plus efficace des charges de travail. Il utilise des transformations autonomiques à réparation spontanée en plus de la compression de données, et évite la retransmission des données pour maintenir une réponse rapide aux clics, la linéarité et une cadence régulière. Sur une connexion réseau avec perte, Framehawk peut masquer la perte avec une interpolation, permettant à l'utilisateur de continuer à percevoir une bonne qualité d'image tout en bénéficiant d'une expérience plus fluide. En outre, les algorithmes Framehawk peuvent faire la distinction entre les différents types de perte de paquets. Par exemple, perte aléatoire (envoi de données supplémentaires pour compenser) ou perte avec congestion (arrêt de l'envoi de données, car le canal est déjà saturé).

Le moteur Framehawk Intent Engine dans Citrix Receiver fait la distinction entre le défilement vers le haut ou vers le bas, le zoom, le déplacement vers la gauche ou vers la droite, la lecture, la saisie et autres actions courantes. Le moteur gère également les communications vers le Virtual Delivery Agent (VDA) à l'aide d'un dictionnaire partagé. Si l'utilisateur lit un texte, la qualité visuelle du texte doit être excellente. Si l'utilisateur fait défiler l'écran, le mouvement doit être rapide et fluide. Par ailleurs, il doit pouvoir être interrompu, de façon à ce que l'utilisateur puisse constamment contrôler l'interaction avec l'application ou le bureau.

En mesurant la cadence sur la connexion réseau (**engrenage**, par analogie avec la tension d'une chaîne de vélo), la logique de Framehawk réagit plus rapidement, offrant une expérience supérieure sur des connexions à latence élevée. Ce système d'engrenage unique et breveté offre un retour permanent sur les conditions du réseau, ce qui permet à Framehawk de réagir immédiatement aux changements de bande passante, à la latence et à la perte de données.

Considérations relatives à la conception avec Thinwire et Framehawk

Bien que Thinwire soit leader du secteur en termes d'efficacité de bande passante et soit adapté à un large éventail de scénarios d'accès et de conditions de réseau, il utilise TCP pour des communications de données fiables. Par conséquent, il doit retransmettre les données en cas de réseau avec perte ou saturé, entraînant un décalage pour l'utilisateur. Thinwire sur une couche Enlightened Data Transport (EDT) est disponible ; cette solution résout les limitations de TCP sur des connexions réseau à latence élevée.

Framehawk utilise une couche de transport de données fondée sur UDP. UDP ne représente qu'une petite partie de la façon dont Framehawk traite les problèmes de perte, comme vous pouvez le voir en comparant les performances de Framehawk avec d'autres protocoles basés sur UDP. UDP joue un rôle fondamental pour les techniques centrées sur l'être humain qui distinguent Framehawk du reste.

Quelle quantité de bande passante est requise par Framehawk ?

Une connexion sans fil haut débit repose sur plusieurs facteurs, y compris le nombre d'utilisateurs qui partagent la connexion, la qualité de la connexion et les applications en cours d'utilisation. Pour des performances optimales, Citrix suggère une configuration de base de 4 ou 5 Mbits/s ainsi que 150 Kbits/s par utilisateur.

Pour Thinwire, nous recommandons une bande passante de 1,5 Mbits/s ainsi que 150 Kbits/s par utilisateur. Pour plus d'informations, veuillez consulter le blog sur la bande passante XenApp et XenDesktop. Avec une perte de paquets de 3 %, vous remarquerez que Thinwire requiert beaucoup plus de bande passante que Framehawk pour garantir une expérience utilisateur positive.

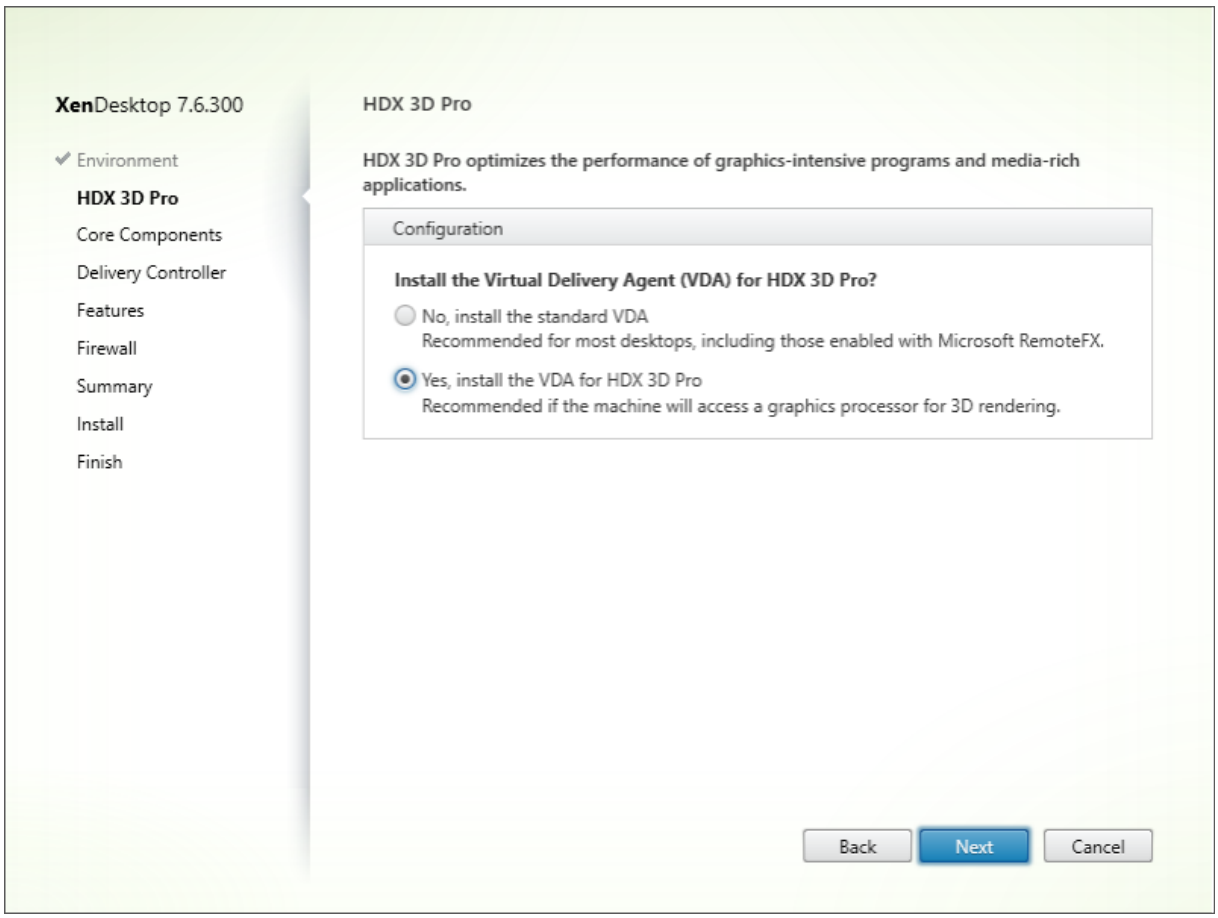
Thinwire reste le canal de communication à distance d'écran principal dans le protocole ICA. Framehawk est désactivé par défaut. Citrix recommande de l'activer pour répondre aux scénarios d'accès sans fil haut débit dans votre organisation. N'oubliez pas que Framehawk requiert beaucoup plus de ressources serveur (UC et mémoire) que Thinwire.

Framehawk et HDX 3D Pro

Framehawk prend en charge tous les cas d'utilisation de HDX 3D Pro, pour XenApp (OS de serveur) et XenDesktop (OS de bureau). Il a été validé dans des environnements client avec 400-500 ms de latence et 1-2 % de perte de paquets, offrant par conséquent une bonne interactivité avec des applications de

modélisation 3D standard telles que AutoCAD, Siemens NX et autres. Cette prise en charge améliore la capacité d'afficher et de manipuler des modèles CAD de grande taille en déplacement ou en cas de travail délocalisé ou de conditions de réseau insatisfaisantes. (Les organisations devant mettre à disposition des applications 3D sur des connexions réseau longue distance sont encouragées à utiliser le transport adaptatif. Pour plus d'informations, consultez la section Transport adaptatif.

L'activation de cette fonctionnalité ne nécessite pas de tâches de configuration supplémentaires. Lors de l'installation du VDA, sélectionnez l'option 3DPro au début de l'installation :



Avec cette sélection, HDX utilise le pilote vidéo du fournisseur de GPU plutôt que le pilote vidéo Citrix. Il se règle par défaut sur l'encodage H.264 plein écran via Thinwire plutôt que sur l'affichage adaptatif par défaut habituel avec encodage H.264 sélectif.

Configuration requise et considérations

Framehawk requiert au minimum VDA 7.6.300 et Gestion de stratégie de groupe 7.6.300.

Le point de terminaison doit disposer au minimum de Citrix Receiver pour Windows 4.3.100 ou Citrix Receiver pour iOS 6.0.1.

Par défaut, Framehawk utilise un port UDP bidirectionnel (3224-3324) pour échanger des données de canal d'affichage Framehawk à l'aide de Citrix Receiver. La plage peut être personnalisée dans un paramètre de stratégie appelé **Plage de ports du canal d'affichage Framehawk**. Chaque connexion simultanée entre le client et le bureau virtuel requiert un port unique. Dans les environnements de système d'exploitation multi-utilisateurs, tels que les serveurs XenApp, définissez suffisamment de ports pour prendre en charge le nombre maximal de sessions utilisateur simultanées. Pour un système d'exploitation à utilisateur unique, tels que les bureaux VDI, il suffit de définir un port UDP unique. Framehawk tente d'abord d'utiliser le premier port défini et progresse jusqu'au dernier port spécifié dans la plage. Ce comportement s'applique à la fois à la communication via NetScaler Gateway et aux connexions internes directes vers le serveur StoreFront.

Pour l'accès à distance, NetScaler Gateway doit être déployé. Par défaut, NetScaler utilise le port UDP 443 pour les communications cryptées entre les Citrix Receiver du client et Gateway. Ce port doit être ouvert sur les pare-feu externes pour permettre les communications sécurisées dans les deux sens. La fonctionnalité est appelée Datagram Transport Security (DTLS).

> **Remarque :**
>
> Les connexions Framehawk/DTLS ne sont pas prises en charge sur les boîtiers FIPS.

Les connexions Framehawk chiffrées sont prises en charge, depuis NetScaler Gateway version 11.0.62 et NetScaler Unified Gateway version 11.0.64.34 ou version ultérieure.

NetScaler High Availability (HA) est pris en charge depuis XenApp et XenDesktop 7.12.

Tenez compte des recommandations suivantes avant la mise en place de Framehawk :

- Contactez votre administrateur de sécurité pour vérifier que les ports UDP définis pour Framehawk sont bien ouverts sur le pare-feu. Le processus d'installation ne configure pas automatiquement le pare-feu.
- NetScaler Gateway peut être installé dans la DMZ, entouré de pare-feu du côté externe ainsi que du côté interne. S'assurer que le port UDP 443 est ouvert sur le pare-feu externe Assurez-vous que les ports UDP 3224-3324 sont ouverts sur le pare-feu interne si votre environnement utilise les plages de port par défaut.

Configuration

> **Attention :**
>
> Citrix vous recommande d'activer Framehawk uniquement pour les utilisateurs qui sont susceptibles de rencontrer une perte importante de paquets. Nous vous recommandons de ne pas activer Framehawk en tant que stratégie universelle pour tous les objets du site.

Framehawk est désactivé par défaut. Lorsque cette option est activée, le serveur tente d'utiliser Framehawk pour les graphiques et la saisie. Si les conditions requises ne sont pas réunies pour

quelque raison que ce soit, la connexion est établie à l'aide du mode par défaut (Thinwire).

Les paramètres de stratégie suivants affectent Framehawk :

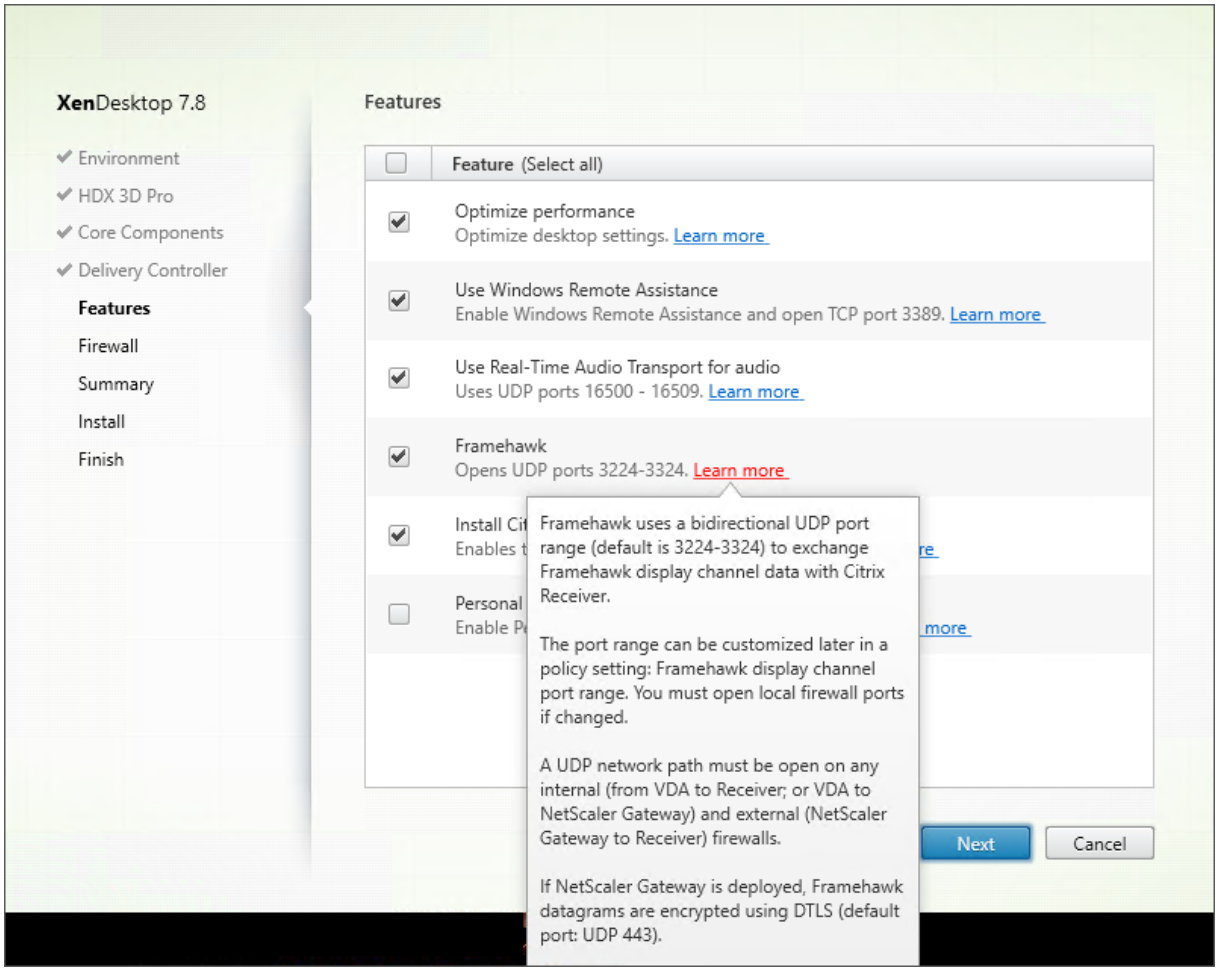
- Canal d'affichage Framehawk : active ou désactive la fonctionnalité.
- Plage de ports du canal d'affichage Framehawk : spécifie la plage de numéros de port UDP (le numéro de port le plus bas vers le plus élevé) que le VDA peut utiliser pour échanger les données de canal d'affichage Framehawk avec la machine utilisateur. Le VDA tente d'utiliser chaque port, en commençant par le numéro de port le plus bas et en remontant pour chaque tentative. Le port gère le trafic entrant et sortant.

Ouverture de ports pour le canal d'affichage Framehawk

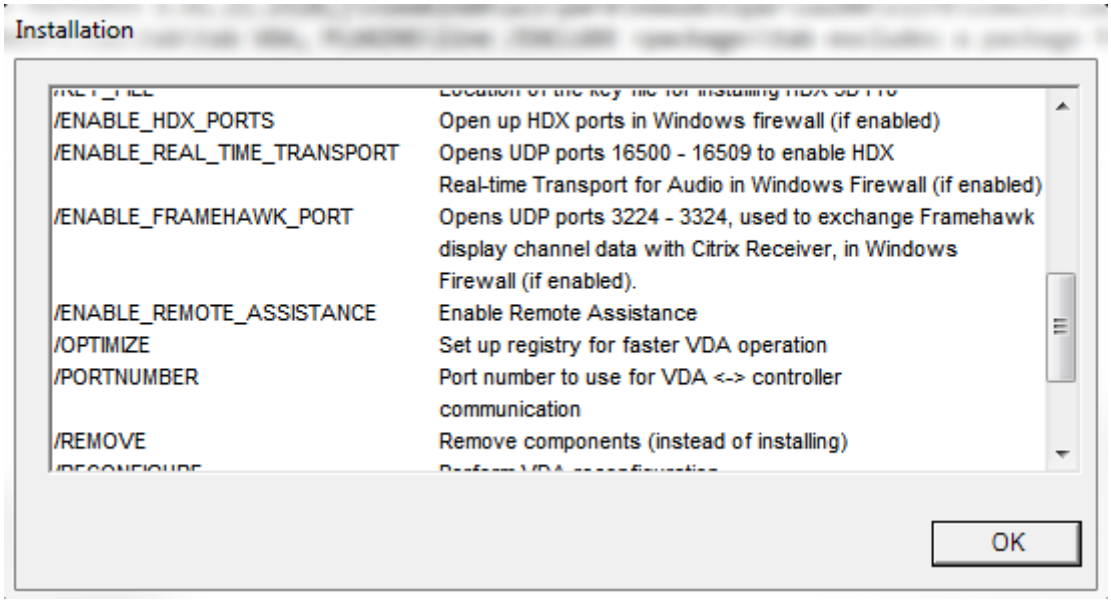
Dans XenApp et XenDesktop 7.8, vous pouvez choisir de reconfigurer le pare-feu lors de l'étape **Fonctionnalités** du programme d'installation du VDA. Cette case à cocher ouvre les ports UDP 3224-3324 sur le pare-feu Windows, si elle est sélectionnée. La configuration manuelle des pare-feux est requise dans certaines circonstances :

- pour les pare-feux de réseau
  ou
- si la plage de ports par défaut est personnalisée.

Pour ouvrir ces ports UDP, sélectionnez la case à cocher **Framehawk** :

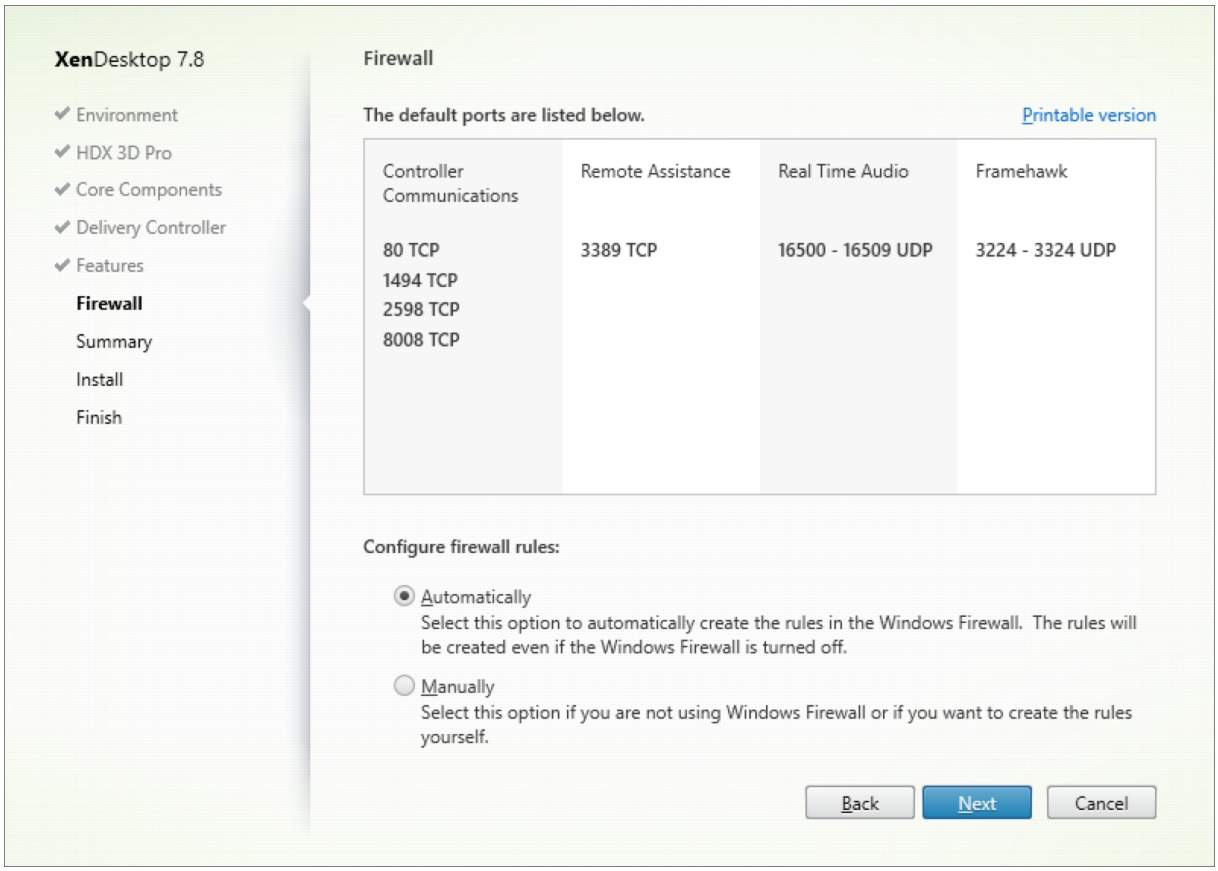


Vous pouvez également utiliser la ligne de commande pour ouvrir les ports UDP pour Framehawk à l'aide de **/ENABLE_FRAMEHAWK_PORT** :

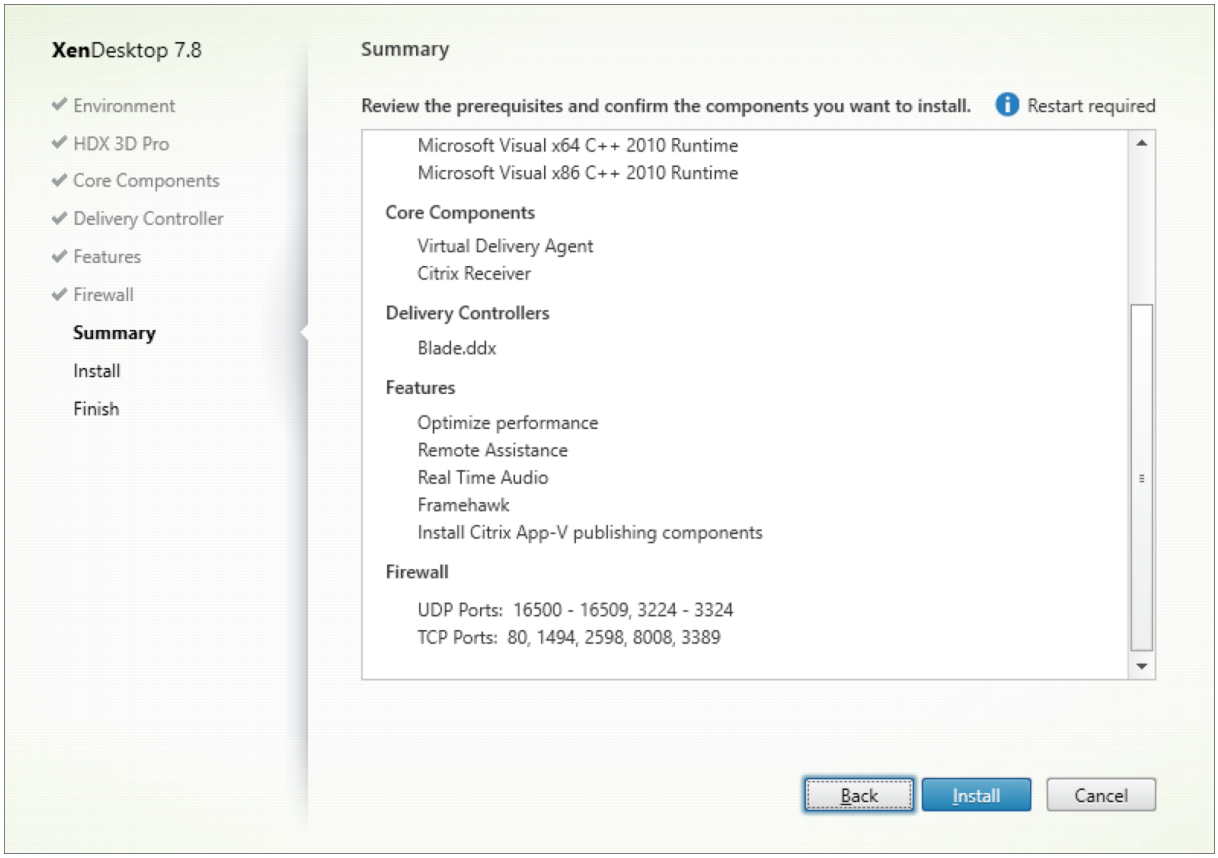


Vérification des attributions de port UDP Framehawk

Lors de l'installation, vous pouvez vérifier les ports UDP attribués à Framehawk dans l'écran **Pare-feu** :



L'écran **Résumé** indique si la fonctionnalité de Framehawk est activée :



Prise en charge de NetScaler Gateway pour Framehawk

Le trafic Framehawk crypté est pris en charge sur NetScaler Gateway 11.0.62.10 ou version ultérieure, et NetScaler Unified Gateway 11.0.64.34 ou version ultérieure.

- NetScaler Gateway fait référence à l'architecture de déploiement dans laquelle le VPN vServer de passerelle est directement accessible depuis la machine cliente. Une adresse IP publique est attribuée au VPN vServer et l'utilisateur se connecte directement à cette adresse IP.
- NetScaler avec Unified Gateway fait référence au déploiement dans lequel le VPN vServer de passerelle est lié en tant que cible au vServer de basculement du contenu (CS). Dans ce déploiement, CS vServer dispose de l'adresse de protocole Internet public et le VPN vServer de passerelle dispose d'une adresse de protocole Internet fictive.

Pour activer la prise en charge de Framehawk sur NetScaler Gateway, le paramètre DTLS au niveau du vServer VPN de passerelle doit être activé. Une fois que ce paramètre est activé et que les composants sur XenApp ou XenDesktop sont mis à jour correctement, le trafic audio, vidéo et interactif Framehawk est crypté entre le VPN vServer de passerelle et la machine utilisateur.

NetScaler Gateway, Unified Gateway et NetScaler Gateway + équilibrage de charge de serveur global sont pris en charge avec Framehawk.

Les scénarios suivants ne sont pas pris en charge avec Framehawk :

- HDX Insight
- NetScaler Gateway en mode IPv6
- NetScaler Gateway Double Hop
- NetScaler Gateway avec la configuration en cluster

Scénario	Prise en charge de Framehawk
NetScaler Gateway	Oui
NetScaler + équilibrage de charge de serveur global	Oui
NetScaler avec Unified Gateway	Oui. **Remarque :** Unified Gateway version 11.0.64.34 et supérieure est prise en charge.
HDX Insight	Non
NetScaler Gateway en mode IPv6	Non
NetScaler Gateway Double Hop	Non
Plusieurs Secure Ticket Authority sur NetScaler Gateway	Oui
NetScaler Gateway et haute disponibilité	Oui
NetScaler Gateway et la configuration en cluster	Non

Configuration de NetScaler pour la prise en charge de Framehawk

Pour activer la prise en charge de Framehawk sur NetScaler Gateway, activez le paramètre DTLS au niveau du *vServer* VPN de passerelle. Une fois que ce paramètre est activé et que les composants sur XenApp ou XenDesktop sont mis à jour correctement, le trafic audio, vidéo et interactif Framehawk est crypté entre le VPN vServer de passerelle et la machine utilisateur.

Cette configuration est nécessaire si vous activez le cryptage UDP sur NetScaler Gateway pour l'accès distant.

Lors de la configuration de NetScaler pour la prise en charge de Framehawk :

- S'assurer que le port UDP 443 est ouvert sur les pare-feu externes
- S'assurer que le port CGP (par défaut 2598) est ouvert sur les pare-feu externes
- Activer DTLS dans les paramètres pour le serveur virtuel VPN
- Annuler puis rétablir la liaison de la paire cert-clé SSL. Cette étape n'est pas obligatoire si vous utilisez NetScaler version 11.0.64.34 ou version ultérieure.

Pour configurer NetScaler Gateway pour la prise en charge de Framehawk :

1. Déployez et configurez NetScaler Gateway pour communiquer avec StoreFront et authentifier les utilisateurs pour XenApp et XenDesktop.
2. Dans l'onglet de configuration NetScaler, développez NetScaler Gateway et sélectionnez **Serveurs virtuels**.
3. Cliquez sur **Modifier** pour afficher les paramètres de base pour le serveur virtuel VPN ; vérifiez l'état du paramètre DTLS.
4. Cliquez sur **Plus** pour afficher d'autres options de configuration :
5. Sélectionnez **DTLS** pour assurer la sécurité des communications pour les protocoles UDP tels que Framehawk. Cliquez sur **OK**. La zone Paramètres de base du serveur virtuel VPN indique que l'indicateur DTLS est défini sur **True**.
6. Ouvrez de nouveau l'écran Server Certificate Binding et cliquez sur **+** pour lier la paire de clés de certificat.
7. Choisissez la paire de clés de certificat requise et cliquez sur **Select**.
8. Enregistrez les modifications apportées à la liaison du certificat du serveur.
9. Après l'enregistrement, la paire de clés de certificat s'affiche. Cliquez sur **Bind**.
10. Ignorez le message **No usable ciphers configured on the SSL vserver/service** s'il s'affiche.

Étapes pour les anciennes versions de NetScaler Gateway

Si vous utilisez une version de NetScaler Gateway antérieure à 11.0.64.34 :

1. Ouvrez de nouveau l'écran Server Certificate Binding et cliquez sur + pour lier la paire de clés de certificat.
2. Choisissez la paire de clés de certificat requise et cliquez sur **Select**.
3. Enregistrez les modifications apportées à la liaison du certificat du serveur.
4. Après l'enregistrement, la paire de clés de certificat s'affiche. Cliquez sur **Bind**.
5. Ignorez le message **No usable ciphers configured on the SSL vserver/service** s'il s'affiche.

Pour configurer Unified Gateway pour la prise en charge de Framehawk :

1. Assurez-vous que Unified Gateway est installé et correctement configuré. Pour de plus amples informations, reportez-vous à la section Unified Gateway sur le site de documentation des produits Citrix.
2. Activez le paramètre DTLS sur le *vServer VPN *qui est lié au *vServer* CS en tant que *vServer* cible.

Limitations

S'il existe des entrées DNS périmées pour le serveur virtuel NetScaler Gateway sur la machine cliente, le transport adaptatif et Framehawk peuvent revenir au transport TCP au lieu du transport UDP. En

cas de retour vers le transport TCP, purgez le cache DNS sur le client et reconnectez pour établir la session à l'aide du transport UDP.

Prise en charge d'autres produits VPN

NetScaler Gateway est le seul produit VPN SSL qui prend en charge le cryptage UDP requis par Framehawk. Si un autre VPN SSL ou une version incorrecte de NetScaler Gateway est utilisé(e), la stratégie Framehawk peut ne pas s'appliquer. Les produits VPN IPsec traditionnels prennent en charge Framehawk sans nécessiter de modifications.

Configurer Citrix Receiver pour iOS pour la prise en charge de Framehawk

Pour configurer les anciennes versions de Citrix Receiver pour iOS pour la prise en charge de Framehawk, vous devez manuellement modifier default.ica.

1. Sur le serveur StoreFront, accédez au répertoire App_Data de votre magasin dans c:\inetpub\wwwroot\.
2. Ouvrez le fichier default.ica et ajoutez la ligne suivante dans la section WFClient : Framehawk=On
3. Enregistrez les modifications.

Cette procédure permet aux sessions Framehawk d'être établies depuis un Citrix Receiver compatible sur des appareils iOS. Cette étape n'est pas nécessaire si vous utilisez Citrix Receiver pour Windows.

> **Remarque :**
>
> Lors de l'utilisation de Citrix Receiver pour iOS version 7.0 et versions ultérieures, vous n'avez pas à ajouter explicitement le paramètre **Framehawk=On** dans le fichier default.ica.

Contrôle de Framehawk

Vous pouvez contrôler l'utilisation et les performances de Framehawk depuis Citrix Director. La vue Détails du canal virtuel HDX contient des informations utiles pour la résolution des problèmes et le contrôle de Framehawk dans une session. Pour afficher les statistiques concernant Framehawk, sélectionnez **Graphiques - Framehawk**.

Si la connexion avec Framehawk est établie, vous voyez **Provider=VD3D** et **Connected=True** dans la page des détails. Il est normal que l'état du canal virtuel soit inactif car il surveille le canal de signalisation, qui est uniquement utilisé durant la négociation initiale. Cette page fournit également d'autres statistiques utiles relatives à la connexion.

Si vous rencontrez des problèmes, consultez le blog de résolution des problèmes Framehawk.

HDX 3D Pro

November 8, 2018

Les fonctions HDX 3D Pro de XenApp et XenDesktop vous permettent de mettre à disposition des bureaux et applications qui fonctionnent mieux avec un processeur graphique pour l'accélération matérielle. Ces applications incluent les applications graphiques 3D professionnelles basées sur OpenGL et DirectX. Le VDA standard prend uniquement en charge l'accélération GPU de DirectX. Pour plus d'informations sur le choix de la norme ou VDA HDX 3D Pro, consultez la section « Étape 5. Choisir si le mode HDX 3D Pro est activé » dans l'article Installer des VDA.

Tous les Citrix Receiver pris en charge peuvent être utilisés avec des graphiques 3D. Pour de meilleures performances avec les charges de travail 3D complexes, les moniteurs haute résolution, les configurations multi-moniteurs et les applications haute fréquence d'images, nous recommandons d'utiliser la dernière version de Citrix Receiver pour Windows et Citrix Receiver pour Linux. Pour obtenir des informations sur les versions prises en charge de Citrix Receiver, consultez la section Étapes clés du cycle de vie de Citrix Receiver.

Les applications professionnelles 3D exemples comprennent :

- les applications de conception, de fabrication et d'ingénierie assistées par ordinateur (CAD/-CAM/CAE) ;
- les logiciels GIS (Geographical Information System) ;
- PACS (Picture Archiving Communication System) pour l'imagerie médicale ;
- les applications utilisant les dernières versions OpenGL, DirectX, NVIDIA CUDA, OpenCL et WebGL ;
- les applications non graphiques consommant énormément de ressources informatiques qui utilisent des GPU NVIDIA CUDA (Compute Unified Device Architecture) pour le traitement en parallèle.

HDX 3D Pro offre la meilleure expérience utilisateur possible sur toute bande passante :

- Sur les connexions WAN : mettez à disposition une expérience utilisateur interactive sur des connexions WAN avec des bandes passantes de 1,5 Mbps seulement.
- Sur les connexions LAN : mettez à disposition une expérience utilisateur équivalente à celle d'un bureau local sur des connexions LAN.

  Vous pouvez remplacer les stations de travail complexes et coûteuses par des machines utilisateur beaucoup plus simples et transférer le traitement graphique vers le centre de données pour une gestion centralisée.

HDX 3D Pro offre une accélération GPU des machines avec OS Windows Desktop et des machines avec OS Windows Server. Pour de plus amples informations, consultez les sections Accélération GPU pour OS de bureau Windows et Accélération GPU pour OS de serveur Windows.

HDX 3D Pro est compatible avec les technologies de virtualisation GPU Passthrough et GPU offertes par les hyperviseurs suivants, ainsi que les machines bare metal :

- Citrix XenServer
  - GPU Passthrough avec NVIDIA GRID et Intel GVT-d
  - Virtualisation GPU avec NVIDIA GRID et Intel GVT-d
- Microsoft Hyper-V
  - GPU Passthrough (DDA) avec NVIDIA GRID et AMD
- VMware vSphere
  - GPU Passthrough (vDGA) avec NVIDIA GRID, Intel et AMD IOMMU
  - Virtualisation GPU avec NVIDIA GRID et AMD MxGPU

Pour les versions de XenServer prises en charge, consultez la section Liste de compatibilité matérielle de Citrix XenServer.

Utilisez l'outil Moniteur HDX pour valider l'opération et la configuration des technologies de visualisation HDX et pour diagnostiquer et résoudre les problèmes HDX. Pour télécharger l'outil et en apprendre davantage sur celui-ci, consultez https://taas.citrix.com/hdx/download/.

Accélération GPU pour OS de serveur Windows

November 8, 2018

HDX 3D Pro permet aux applications exigeantes en ressources graphiques exécutées dans de sessions d'OS de serveur Windows d'être restituées sur le processeur graphique du serveur (GPU). En déplaçant la restitution OpenGL, DirectX, Direct3D et Windows Presentation Foundation (WPF) sur le processeur graphique du serveur, l'unité centrale du serveur n'est pas ralentie par la restitution des graphiques. Par ailleurs, le serveur est capable de traiter davantage de graphiques car la charge est partagée entre le processeur graphique et l'unité centrale.

Windows Server étant un système d'exploitation multi-utilisateurs, un processeur graphique auquel accède XenApp peut être partagé par de multiples utilisateurs sans qu'une virtualisation du GPU (vGPU) ne soit nécessaire.

Pour les procédures qui impliquent la modification du registre, faites attention : la modification incorrecte du Registre peut entraîner des problèmes graves pouvant nécessiter de réinstaller votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Partage GPU

Le partage GPU active la restitution matérielle de l'unité de traitement graphique (GPU) des applications OpenGL et DirectX dans les sessions de bureau à distance ; il possède les caractéristiques suivantes :

- Peut être utilisée sur des machines bare metal ou virtuelles pour améliorer l'évolutivité et les performances des applications.
- Permet plusieurs sessions simultanées pour partager les ressources GPU (la plupart des utilisateurs ne requièrent pas les performances de restitution d'un processeur graphique dédié).
- Ne requiert aucun paramètre spécial.

Vous pouvez installer plusieurs processeurs graphiques sur un hyperviseur et affecter des VM à chacun de ces processeurs graphiques : soit installez une carte graphique possédant plus d'un processeur graphique, soit installez plusieurs cartes graphiques avec au moins un processeur graphique chacune. Le mélange de cartes graphiques hétérogènes sur le serveur n'est pas recommandé.

Les machines virtuelles requièrent un accès intermédiaire direct à un processeur graphique, qui est disponible avec Citrix XenServer, VMware vSphere vDGA et Intel GVT-d. Lorsque HDX 3D est utilisé avec un GPU Pass-through, chaque processeur graphique du serveur prend en charge une machine virtuelle multi-utilisateur.

Le partage GPU ne dépend pas d'une carte graphique spécifique.

- Lors de l'exécution sur un hyperviseur, sélectionnez une plate-forme matérielle et des cartes graphiques qui sont compatibles avec l'implémentation GPU Pass-through de votre hyperviseur. La liste matérielle qui a réussi le test de certification avec un GPU Pass-through XenServer est disponible dans la section Machines GPU Pass-through.
- Lors de l'exécution sur des machines bare metal, il est recommandé de n'activer qu'une seule carte vidéo par système d'exploitation. Si plusieurs processeurs graphiques sont installés sur le matériel, désactivez-les tous sauf un à l'aide de Device Manager.

L'évolutivité utilisant le partage GPU dépend de plusieurs facteurs :

- les applications étant exécutées ;
- la quantité de mémoire vive vidéo qu'elles consomment ;
- la puissance de traitement de la carte graphique.

certaines applications gèrent les insuffisances de RAM vidéo mieux que d'autres. Si le matériel devient extrêmement surchargé, ceci provoquera une instabilité ou un vidage du pilote de la carte graphique. Limitez le nombre d'utilisateurs simultanés pour éviter de tels problèmes.

Pour confirmer que l'accélération GPU se produit, utilisez un outil tiers tel que GPU-Z. GPU-Z est disponible sur https://www.techpowerup.com/gpuz/.

Restitution DirectX, Direct3D et WPF

La restitution DirectX, Direct3D et WPF est uniquement disponible sur les serveurs dotés d'un processeur graphique prenant en charge les versions DDI 9ex, 10 ou 11.

- Sur Windows Server 2008 R2, DirectX et Direct3D ne requièrent aucun paramètre spécial pour utiliser un seul processeur graphique.
- Sur Windows Server 2016 et Windows Server 2012, les sessions de Services Bureau à distance (RDS) des sessions sur le serveur hôte de session Bureau à distance utilisent le pilote de rendu de base Microsoft en tant qu'adaptateur par défaut. Pour utiliser le processeur graphique dans les sessions de services Bureau à distance dans Windows Server 2012, activez le paramètre Utiliser la carte graphique matérielle par défaut pour toutes les sessions des services Bureau à distance dans la stratégie de groupe Stratégie ordinateur local > Configuration ordinateur > Modèles d'administration> Composants Windows > Services Bureau à distance > Hôte de la session Bureau à distance > Environnement de session à distance.
- Pour activer les applications WPF pour effectuer la restitution à l'aide du GPU du serveur, créez les paramètres suivants dans le registre du serveur exécutant les sessions de système d'exploitation Windows Server :
  - [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\ Multiple Monitor Hook] "EnableWPFHook"=dword:00000001
  - [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\ Multiple Monitor Hook] "EnableWPFHook"=dword:00000001

Accélération de processeur graphique pour les applications CUDA ou OpenCL

L'accélération GPU d'applications CUDA et OpenCL exécutées dans une session utilisateur est désactivée par défaut.

Pour utiliser les fonctionnalités d'évaluation d'accélération CUDA, activez les paramètres de Registre suivants :

- [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] "OpenCL"=dword:0000
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] "OpenCL"=dword:00000001

Pour utiliser les fonctionnalités d'évaluation d'accélération OpenCL, activez les paramètres de Registre suivants :

- [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] "OpenCL"=dword:0000
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] "OpenCL"=dword:00000001

Accélération GPU pour OS de bureau Windows

January 23, 2019

Avec HDX 3D Pro vous pouvez mettre à disposition des applications au graphisme intensif dans le cadre des applications ou bureaux hébergés sur des machines avec OS de bureau. HDX 3D Pro prend en charge les ordinateurs hôtes physiques, (y compris les bureaux, les lames et les stations de travail en rack) et les technologies de virtualisation GPU Passthrough et GPU offertes par les hyperviseurs XenServer, vSphere et Hyper-V (Passthrough uniquement).

À l'aide de la fonctionnalité GPU Passthrough, vous pouvez créer des VM bénéficiant d'un accès exclusif à du matériel de traitement graphique dédié. Vous pouvez installer plusieurs processeurs graphiques sur l'hyperviseur et affecter individuellement des VM à chacun de ces processeurs graphiques.

À l'aide de la virtualisation GPU, plusieurs machines virtuelles peuvent accéder directement à la puissance de traitement graphique d'un processeur graphique physique unique. Le partage du matériel GPU offre des bureaux adaptés aux utilisateurs ayant des besoins complexes et exigeants en matière de design. La virtualisation GPU pour les cartes NVIDIA GRID (voir NVIDIA GRID) utilise les mêmes pilotes graphiques NVIDIA que ceux déployés sur des systèmes d'exploitation non virtualisés. La virtualisation GPU est également prise en charge pour les processeurs Intel de 5ème et 6ème génération avec Intel Iris Pro Graphics et Intel GVT-g. Pour de plus amples informations sur ces familles de processeurs Intel, consultez Processeurs Intel Core de 5ème génération et Processeurs Intel Core de 6ème génération. La virtualisation de GPU est également prise en charge pour les cartes serveur AMD FirePro S-Series, consultez Solution de virtualisation AMD Professional Graphics.

HDX 3D Pro offre les fonctionnalités suivantes :

- Compression approfondie H.264 adaptative pour des performances de réseau étendues et sans fil optimales. HDX 3D Pro utilise la compression H.264 plein écran basée sur l'UC en tant que technique de compression par défaut pour le codage. Le codage matériel est utilisé avec les cartes NVIDIA qui prennent en charge NVENC.
- Option de compression sans perte pour les cas d'utilisation spécialisés. HDX 3D Pro offre également un codec UC sans perte pour prendre en charge les applications pour lesquelles les graphiques gourmands en pixels sont nécessaires, comme l'imagerie médicale. La véritable compression sans perte est recommandée uniquement pour les scénarios d'utilisation spécifiques car elle consomme davantage de ressources réseau et de traitement.

  Lors de l'utilisation de la compression sans perte :

  - L'indicateur sans perte, une icône dans la barre d'état système, vous avertit si l'écran affiché est une trame avec ou sans perte. Cela est utile lorsque le paramètre de stratégie Qualité visuelle spécifie Sans perte si possible. L'indicateur sans perte devient vert lorsque les images envoyées sont sans perte.

  - Le commutateur sans perte permet à l'utilisateur de passer en mode Toujours sans perte à tout moment dans la session. Pour sélectionner ou désélectionner le mode sans perte à tout moment au cours d'une session, cliquez avec le bouton droit sur l'icône ou utilisez le raccourci ALT + MAJ + 1.

    Pour la compression sans perte : HDX 3D Pro utilise le codec sans perte pour la compression quel que soit le codec sélectionné au travers de la stratégie.

    Pour la compression avec perte : HDX 3D Pro utilise le codec original, soit celui par défaut, soit celui sélectionné via la stratégie.

    les paramètres du commutateur Sans perte ne sont pas conservés pour les sessions ultérieures. Pour utiliser le codec sans perte pour chaque connexion, sélectionnez Toujours sans perte dans le paramètre de stratégie Qualité visuelle.

- Vous pouvez remplacer le raccourci par défaut, ALT+MAJ+1, pour sélectionner ou désélectionner Sans perte dans une session. Configurez un nouveau paramètre de registre pour HKLM\SOFTWARE\Citrix\HDX3D\LLIndicator.
  - Nom : HKLM_HotKey, Type : chaîne
  - Le format pour configurer une combinaison de raccourcis est C=0|1, A=0|1, S=0|1, W=0|1, K=val. Les clés doivent être séparées par une virgule (,). L'ordre des touches n'est pas important.
  - A, C, S, W et K représentent des touches, où C=Contrôle, A=ALT, S=MAJ, W=Win et K=une touche valide. Les valeurs autorisées pour K sont 0-9, a-z, et tout code clavier virtuel. Pour de plus amples informations sur les codes clavier virtuel, consultez la section Virtual-Key Codes sur MSDN.
  - Par exemple :
    * Pour F10, définissez K=0x79
    * Pour Ctrl + F10, définissez C=1, K=0x79
    * Pour Alt + A, définissez A=1, K=a ou A=1, K=A ou K=A, A=1
    * Pour Ctrl + Alt + 5, définissez C=1, A=1, K=5 ou A=1, K=5, C=1
    * Pour Ctrl + Maj + F5, définissez A=1, S=1, K=0x74

> **Attention :**
>
> Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

- Prise en charge de multiples moniteurs haute résolution. Pour les machines avec OS de bureau, HDX 3D Pro prend en charge les machines utilisateur avec jusqu'à quatre moniteurs. Les utilisateurs peuvent organiser leurs moniteurs selon n'importe quelle configuration et peuvent

combiner des moniteurs ayant différentes résolutions et orientations. Le nombre de moniteurs n'est limité que par les capacités du processeur graphique de l'ordinateur hôte, de la machine utilisateur et de la bande passante disponible. HDX 3D Pro prend en charge toutes les résolutions de moniteur et n'est limité que par les capacités du processeur graphique sur l'ordinateur hôte.

HDX 3D Pro offre également une prise en charge limitée d'accès à plusieurs moniteurs pour les bureaux Windows XP. Pour de plus amples informations sur ce sujet, consultez la section VDA sur les machines exécutant Windows XP ou Windows Vista.

- Résolution dynamique. Vous pouvez redimensionner la fenêtre de bureau ou d'application virtuel(le) sur n'importe quelle résolution. **Remarque :** la seule méthode prise en charge permettant de changer la résolution consiste à redimensionner la fenêtre de session VDA. La modification de la résolution dans une session VDA (à l'aide de Panneau de configuration > Apparence et personnalisation > Affichage > Résolution d'écran) n'est pas prise en charge.
- Prise en charge de l'architecture NVIDIA GRID. HDX 3D Pro prend en charge les cartes NVIDIA GRID (voir NVIDIA GRID) pour GPU passthrough et le partage GPU. NVIDIA GRID vGPU permet à plusieurs machines virtuelles d'avoir un accès direct simultané à un GPU unique physique, à l'aide des mêmes pilotes graphiques NVIDIA qui sont déployés sur des systèmes d'exploitation non virtualisés.
- Prise en charge de VMware vSphere et VMware ESX à l'aide de l'accélération graphique virtuelle (vDGA) : vous pouvez utiliser HDX 3D Pro avec vDGA pour les RDS et les charges de travail VDI.
- Prise en charge de VMware vSphere/ESX à l'aide de NVIDIA GRID vGPU et AMD MxGPU.
- Prise en charge de Microsoft Hyper-V à l'aide de la technologie DDA de Windows Server 2016.
- Prise en charge de Data Center Graphics avec les processeurs Intel Xeon de la famille E3. HDX 3D Pro prend en charge plusieurs moniteurs (maximum de trois), l'occultation de console, une résolution personnalisée et une fréquence d'images élevée avec la famille de processeurs Intel prise en charge. Pour plus d'informations, veuillez consulter https://www.citrix.com/intel et https://www.intel.com/content/www/us/en/servers/data-center-graphics.html.
- Prise en charge d'AMD RapidFire sur les cartes pour serveur AMD FirePro S-series. HDX 3D Pro prend en charge plusieurs moniteurs (maximum de 6), l'occultation de la console, une résolution personnalisée et une haute fréquence d'images. Remarque : la prise en charge de HDX 3D Pro pour AMD MxGPU (virtualisation du GPU) fonctionne uniquement avec des vGPU VMWare vSphere. XenServer et Hyper-V sont pris en charge avec GPU passthrough. Pour plus d'informations, consultez la section Solution de virtualisation AMD.
- Accès à un encodeur vidéo haute performance pour les GPU NVIDIA et les processeurs graphiques Intel Iris Pro. Cette fonctionnalité est contrôlée par un paramètre de stratégie (activé par défaut) et autorise l'utilisation du codage matériel pour l'encodage H.264 (le cas

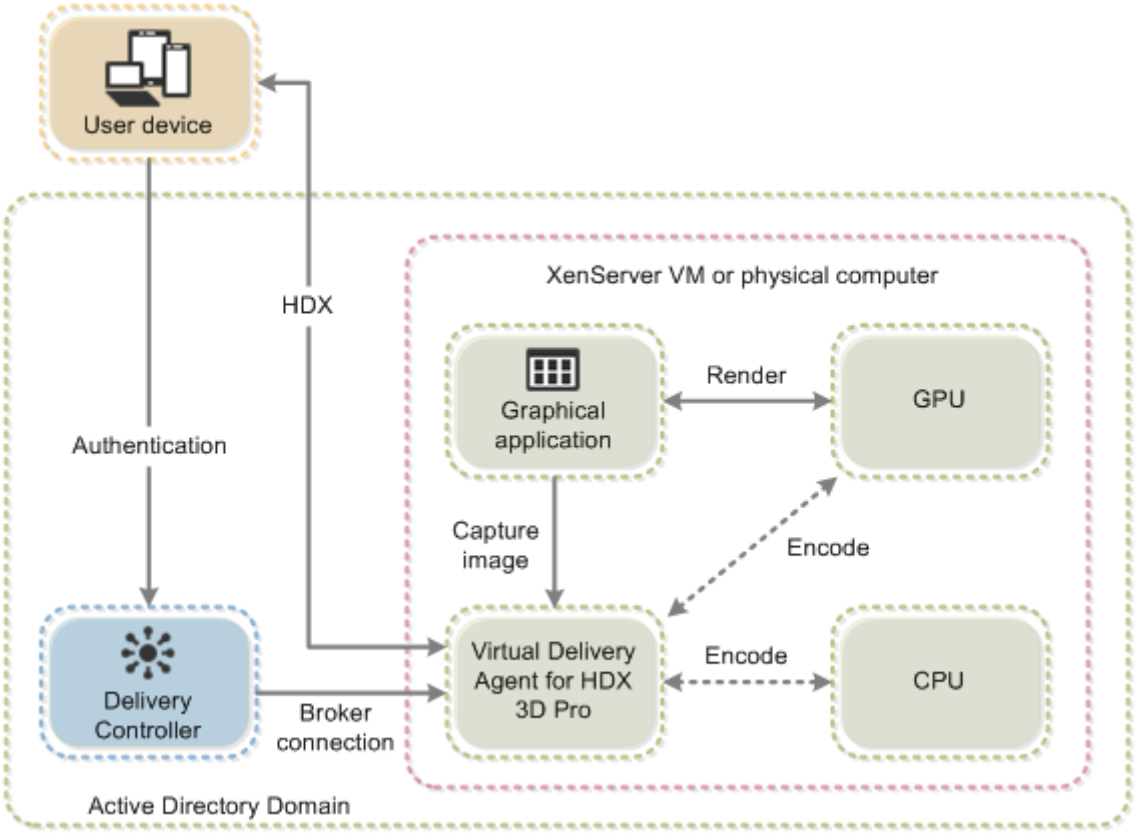
échéant). Si ce matériel n'est pas disponible, le VDA utilisera le codage basé sur l'UC avec le codec vidéo logiciel. Pour plus d'informations, veuillez consulter la section Paramètres de stratégie des graphiques.

Comme indiqué dans l'illustration suivante :

- Lorsqu'un utilisateur ouvre une session sur Citrix Receiver et accède au bureau ou à l'application virtuelle, le Controller authentifie l'utilisateur et contacte le VDA pour HDX 3D Pro afin de négocier une connexion à l'ordinateur qui héberge l'application graphique.

Le VDA pour HDX 3D Pro utilise le matériel approprié sur l'hôte pour compresser des vues du bureau complet ou de l'application graphique seule.

- Ces vues de bureau et d'application et les interactions de l'utilisateur avec elles sont transmises entre l'ordinateur hôte et la machine utilisateur via une connexion HDX directe entre Citrix Receiver et le VDA pour HDX 3D Pro.



Installer le VDA pour HDX 3D Pro

Lorsque vous utilisez l'interface graphique du programme d'installation pour l'installation d'un VDA pour OS de bureau Windows, sélectionnez Oui sur la page HDX 3D Pro. Lors de l'utilisation

de l'interface de ligne de commande, incluez l'option /enable_hdx_3d_pro avec la commande XenDesktop VdaSetup.exe.

Pour mettre à niveau HDX 3D Pro, désinstallez le composant HDX 3D for Professional Graphics et le VDA avant d'installer le VDA en mode HDX 3D Pro. De même, pour passer du mode standard de VDA pour OS Windows Desktop au mode 3D Pro, désinstallez le VDA standard, puis installez le VDA en mode HDX 3D Pro.

Mode standard	Mode HDX 3D Pro
Recommandé en général pour les bureaux virtuels sans accélération graphique matérielle et pour Remote PC Access.	Recommandé en général pour les bureaux de centre de données avec accélération graphique matérielle, sauf si plus de quatre moniteurs sont requis.
Tout GPU peut être utilisé pour Remote PC Access, avec certaines limitations de compatibilité de l'application : sur Windows 7, 8 et 8.1, accélération GPU pour niveaux de fonctionnalité DirectX jusqu'à 9.3. Certaines applications DirectX 10, 11 et 12 risquent de ne pas s'exécuter si elles ne gèrent pas le retour sur DirectX 9. Sur Windows 10, l'accélération GPU est fournie pour les applications DirectX 10, 11 et 12 fenêtrées. Les applications DX 9 sont restituées par WARP. Les applications DX ne peuvent pas être utilisées en mode plein écran. Accélération des applications OpenGL dans les sessions distantes si prise en charge par le fournisseur GPU (NVIDIA uniquement pour le moment).	Prend en charge l'accélération GPU avec tout processeur graphique ; toutefois l'occultation de console, les résolutions d'écran non standard et la prise en charge de moniteurs multiples réelle requièrent des graphiques NVIDIA GRID, Intel Iris Pro ou AMD RapidFire. Utilise le pilote du fournisseur de graphiques pour une compatibilité applicative optimale : toutes les API 3D (DirectX ou OpenGL) que le processeur graphique prend en charge. Prise en charge d'applications 3D plein écran avec Intel Iris Pro (Win10 uniquement), NVIDIA GRID et AMD RapidFire. Prise en charge d'API et d'extensions de pilote personnalisées. Par exemple, CUDA ou OpenCL.
Résolutions de moniteur arbitraires (limite déterminée par le système d'exploitation Windows et les performances) et jusqu'à huit moniteurs.	Prend en charge jusqu'à quatre moniteurs.
Encodage matériel H.264 disponible avec les processeurs graphiques Intel Iris Pro.	Encodage matériel H.264 disponible avec les processeurs graphiques Intel Iris Pro et les cartes NVIDIA.

Installer et mettre à niveau des pilotes NVIDIA

L'API GRID NVIDIA offre un accès direct au tampon de trame du GPU, fournissant le taux de trame le plus rapide possible pour une expérience utilisateur fluide et interactive. Si vous installez des pilotes NVIDIA avant d'installer un VDA avec HDX 3D Pro, NVIDIA GRID est activé par défaut.

Pour activer NVIDIA GRID sur une VM, désactivez Microsoft Basic Display Adapter dans le Gestionnaire de périphériques. Exécutez la commande suivante, puis redémarrez le VDA : **NVFBCEnable.exe -enable -noreset**

Si vous installez des pilotes NVIDIA après avoir installé un VDA avec HDX 3D Pro, NVIDIA GRID est désactivé. Activez NVIDIA GRID à l'aide de l'outil NVFBCEnable fourni par NVIDIA.

Pour désactiver NVIDIA GRID, exécutez la commande suivante, puis redémarrez le VDA : **NVFBCEnable.exe -disable -noreset**

Installer les pilotes graphiques Intel

Vous pouvez installer les pilotes graphiques Intel avant d'installer le VDA. L'étape suivante est requise uniquement si vous installez des pilotes Intel après avoir installé un VDA avec HDX 3D Pro, ou si le pilote Intel a été mis à jour.

Afin d'activer les pilotes Intel requis pour la prise en charge de moniteurs multiples, exécutez la commande suivante à l'aide de GfxDisplayTool.exe, puis redémarrez le VDA : **GfxDisplayTool.exe -vd enable**

GfxDisplayTool.exe est inclus avec le programme d'installation du VDA. L'exécutable GfxDisplayTool.exe se trouve dans C:\Program Files\Citrix\ICAServices.

> **Remarque :**
>
> La désinstallation des pilotes NVIDIA ou Intel dans les sessions ICA n'est pas prise en charge.

Optimiser l'expérience utilisateur de HDX 3D Pro

Pour utiliser HDX 3D Pro avec plusieurs moniteurs, assurez-vous que l'ordinateur hôte est configuré avec au moins autant de moniteurs que sont connectés aux machines utilisateur. Les moniteurs connectés à l'ordinateur hôte peuvent être physiques ou virtuels.

Ne connectez pas de moniteur (qu'il soit physique ou virtuel) à un ordinateur hôte alors qu'un utilisateur est connecté au bureau ou à l'application virtuel(le) fournissant l'application graphique. Car ceci peut provoquer une instabilité pour toute la durée de la session de l'utilisateur.

Faites savoir à vos utilisateurs que les modifications apportées à la résolution du bureau (par eux ou une application) ne sont pas prises en charge lorsqu'une session d'application graphique est en cours

d'exécution. Après fermeture de la session d'application, un utilisateur peut modifier la résolution de la fenêtre Desktop Viewer dans Citrix Receiver : Préférences de Desktop Viewer.

Lorsque plusieurs utilisateurs partagent une connexion disposant d'une bande passante limitée (par exemple dans une succursale), Citrix vous recommande d'utiliser le paramètre de stratégie Limite de bande passante de session générale pour limiter la bande passante disponible pour chaque utilisateur. Cela évite les trop fortes fluctuations de la bande passante au fur et à mesure que les utilisateurs ouvrent une session ou se déconnectent. Comme HDX 3D Pro s'adapte automatiquement pour utiliser toute la bande passante disponible, de fortes variations de celle-ci pendant les sessions des utilisateurs peuvent avoir un impact négatif sur les performances.

Ainsi, si 20 utilisateurs partagent une connexion de 60 Mbps, la bande passante disponible pour chaque utilisateur peut varier entre 3 Mbps et 60 Mbps en fonction du nombre d'utilisateurs simultanés. Pour optimiser l'expérience utilisateur dans ce scénario, déterminez la bande passante requise par utilisateur aux heures de pointe et limitez en permanence les utilisateurs à cette valeur.

Pour les utilisateurs de souris 3D, Citrix recommande d'augmenter la priorité du canal virtuel Generic USB Redirection à 0. Pour plus d'informations sur la modification de la priorité du canal virtuel, consultez l'article CTX128190.

Accélérateur logiciel OpenGL

November 8, 2018

L'accélérateur logiciel OpenGL est un logiciel de rastérisation pour des applications OpenGL telles que les applications ArcGIS, Google Earth, Nehe, Maya, Fusion, Voxler et CAD/CAM. Parfois, l'accélérateur logiciel OpenGL peut éliminer le besoin d'utiliser des cartes graphiques pour offrir une expérience utilisateur optimale lors de l'utilisation d'applications OpenGL.

> **Important**
>
> Nous fournissons l'accélérateur logiciel OpenGL *tel quel* et il doit être testé avec toutes les applications car il se peut qu'il ne prenne pas en charge certaines applications. Il peut apporter une solution au cas où le rastériseur Windows OpenGL ne fournirait pas des performances adéquates. Si l'accélérateur logiciel OpenGL prend en charge vos applications, vous pouvez l'utiliser pour éviter des investissements coûteux en matériel GPU.

L'accélérateur OpenGL logiciel est fourni dans le dossier Support du support d'installation et est pris en charge sur toutes les plates-formes valides de VDA.

Quand utiliser l'accélérateur logiciel OpenGL :

- Sur les serveurs sans matériel de traitement graphique, si les performances des applications OpenGL exécutées dans les machines virtuelles sur XenServer ou d'autres hyperviseurs posent

un problème. Pour certaines applications, l'accélérateur OpenGL surpasse la rastérisation logicielle OpenGL de Microsoft qui est incluse avec Windows car l'accélérateur OpenGL utilise SSE4.1 et AVX. L'accélérateur OpenGL prend également en charge les applications à l'aide des versions OpenGL jusqu'à la version 2.1.

- Pour les applications exécutées sur une station de travail, essayez tout d'abord la version par défaut de la prise en charge OpenGL fournie par la carte graphique de la station de travail. Si la carte graphique possède la dernière version disponible, elle met en général à disposition les meilleures performances possibles. Si la carte graphique est d'une version antérieure ou ne met pas à disposition des performances satisfaisantes, essayez d'utiliser l'accélérateur logiciel OpenGL.
- Les applications 3D OpenGL qui ne sont pas mises à disposition de manière adéquate à l'aide d'un logiciel de rastérisation sur l'UC peuvent bénéficier de l'accélération matérielle GPU OpenGL. Cette fonctionnalité peut être utilisée sur des machines bare metal ou virtuelles.

ThinWire

January 23, 2019

Introduction

Thinwire est la technologie de communication à distance d'écran par défaut de Citrix utilisée dans XenApp et XenDesktop.

La technologie de communication à distance d'écran permet aux graphiques générés sur une machine d'être transmis, généralement via un réseau, vers une autre machine.

Une solution de communication à distance d'écran performante doit fournir une expérience utilisateur hautement interactive, similaire à celle d'un PC local. Thinwire y parvient grâce à différentes techniques d'analyse et de compression d'image complexes et efficaces. Thinwire optimise la capacité à monter en charge du serveur et utilise moins de bande passante que les autres technologies de communication à distance d'écran.

Grâce à cet équilibre, Thinwire répond à la plupart des cas d'utilisation d'entreprise et est utilisé comme technologie de communication à distance d'écran par défaut dans XenApp et XenDesktop.

Thinwire ou Framehawk

Thinwire devrait être utilisé pour la mise à disposition de charges de travail de bureau standard, par exemple des bureaux ou des applications de productivité ou de navigateur. Thinwire est également

recommandé pour les scénarios à plusieurs moniteurs, haute résolution ou PPP élevé et pour les charges de travail avec un mélange de contenu vidéo et non-vidéo.

Framehawk devrait être utilisé pour les travailleurs mobiles sur des connexions sans fil haut débit avec lesquelles la perte de paquets peut être élevée par intermittence.

HDX 3D Pro

Dans sa configuration par défaut, Thinwire peut diffuser des graphiques 3D ou hautement interactifs ; cependant, l'activation du mode HDX 3D Pro lors de l'installation du VDA pour OS de bureau est une option recommandée pour de tels scénarios. Le mode 3D Pro configure Thinwire avec l'encodage H.264 plein écran pour la transmission de graphiques. Cette configuration offre une expérience plus fluide pour les graphiques 3D de qualité professionnelle. Pour de plus amples informations, consultez les sections HDX 3D Pro et Accélération GPU pour OS de bureau Windows.

Configuration requise et considérations

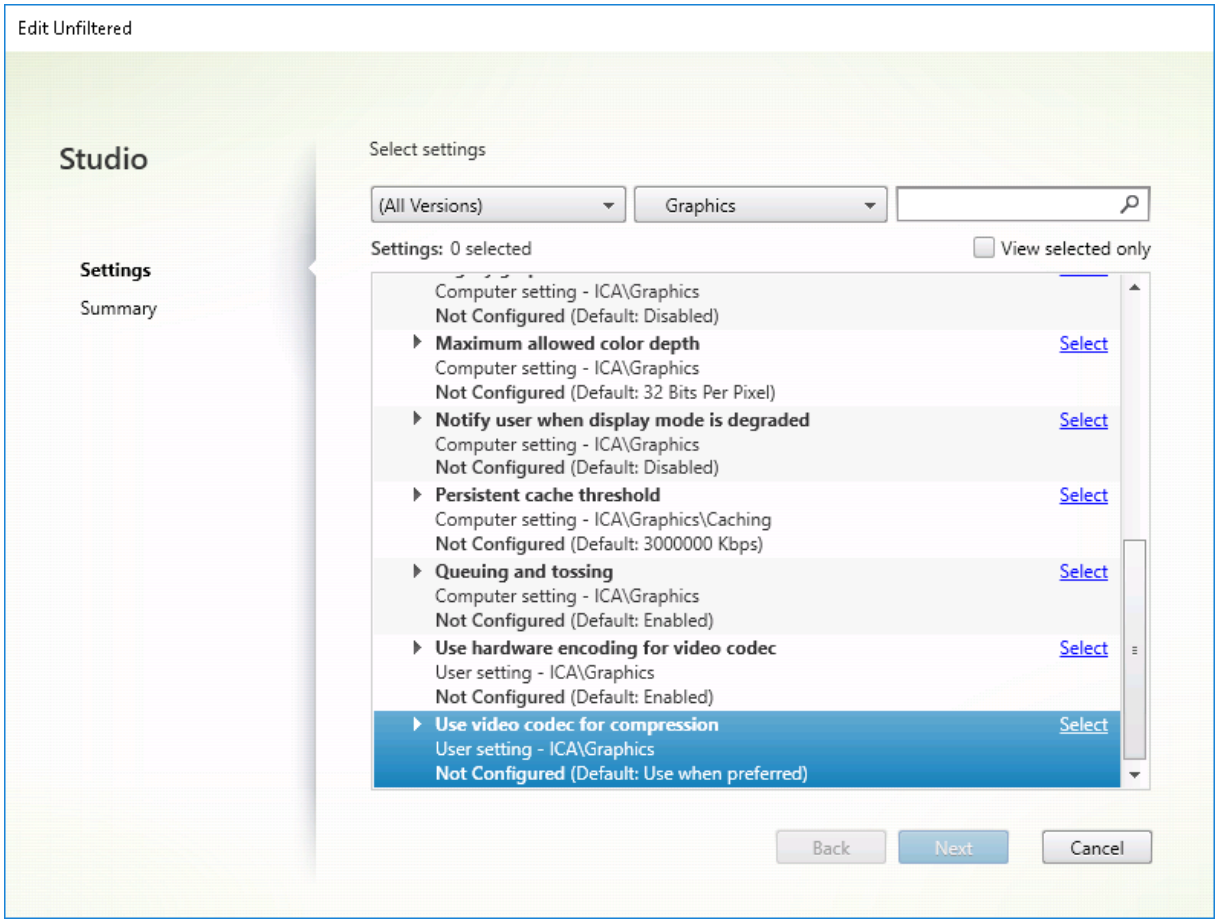
- Thinwire a été optimisé pour les systèmes d'exploitation les plus récents, y compris Windows Server 2012 R2, Windows Server 2016, Windows 7 et Windows 10. Pour Windows Server 2008 R2, le mode graphique d'ancienne génération est recommandé. Utilisez les modèles de stratégie Citrix intégrés, Montée en charge du serveur élevée - anciens systèmes d'exploitation et Optimisé pour les connexions WAN – anciens systèmes d'exploitation, pour mettre à disposition les combinaisons de paramètres de stratégie recommandées par Citrix pour ces cas d'utilisation.
- Le paramètre de stratégie qui détermine le comportement de Thinwire, **Utiliser codec vidéo pour la compression**, est disponible sur les versions VDA dans XenApp et XenDesktop 7.6 FP3 et versions ultérieures. L'option **Utiliser un codec vidéo au choix** est le paramètre par défaut pour les versions VDA de XenApp et XenDesktop 7.9 et versions ultérieures.
- Tous les Citrix Receiver prennent en charge Thinwire. Certains Citrix Receiver peuvent cependant prendre en charge des fonctionnalités de Thinwire que d'autres ne prennent pas en charge, par exemple, des graphiques 8 ou 16 bits pour une utilisation réduite de la bande passante. La prise en charge de ces fonctionnalités est automatiquement négociée par Citrix Receiver.
- Thinwire utilise davantage de ressources serveur (UC, mémoire) dans les scénarios à plusieurs moniteurs et haute résolution. Il est possible d'ajuster la quantité de ressources que Thinwire utilise ; cependant, l'utilisation de la bande passante peut augmenter en conséquence.
- Dans les scénarios à faible bande passante ou à latence élevée, il peut être utile d'activer les graphiques 8 ou 16 bits pour améliorer l'interactivité ; toutefois la qualité visuelle sera affectée, plus particulièrement avec un nombre de couleurs de 8 bits.

Configuration

Thinwire est la technologie de communication à distance d'écran par défaut.

Le paramètre de stratégie Graphiques suivant définit la valeur par défaut et fournit d'autres méthodes pour différents scénarios d'utilisation :

- Utiliser codec vidéo pour la compression
  - **Utiliser un codec vidéo au choix**. C'est le réglage par défaut. Aucune configuration supplémentaire n'est requise. Le maintien de ce paramètre en tant que valeur par défaut assure que Thinwire est sélectionné pour toutes les connexions Citrix, et est optimisé pour la capacité à monter en charge, la bande passante et une qualité d'image supérieure pour les charges de travail de bureau standard.
- Les autres options de ce paramètre de stratégie continueront à utiliser Thinwire en combinaison avec d'autres technologies pour différents scénarios d'utilisation. Par exemple :
  - **Pour les zones changeant constamment**. La technologie d'affichage adaptatif dans Thinwire identifie les images en mouvement (vidéo, 3D en mouvement) et utilise H.264 uniquement dans la partie de l'écran sur laquelle l'image est en mouvement.
  - **Pour l'écran entier**. Fournit Thinwire avec H.264 plein écran pour optimiser l'expérience utilisateur et la bande passante, particulièrement dans les cas dans lesquels les graphiques 3D sont fortement sollicités.



D'autres paramètres de stratégie, y compris les paramètres de stratégie Affichage visuel suivants, peuvent être utilisés pour optimiser les performances de la technologie de communication à distance d'écran et sont tous pris en charge par Thinwire :

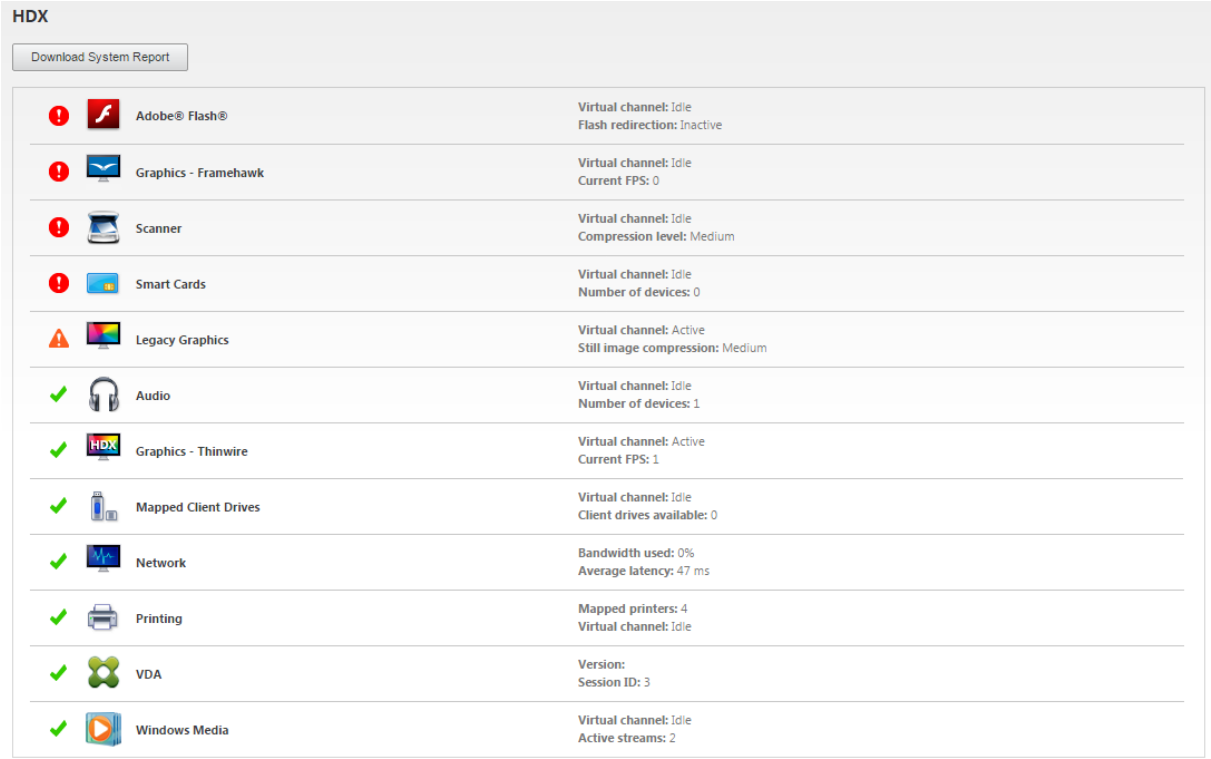
- Nombre de couleurs préféré pour les graphiques simples
- Taux de trames cible
- Qualité visuelle

Pour obtenir les combinaisons de paramètres de stratégie recommandées par Citrix pour différents scénarios d'utilisation, utilisez les modèles de stratégie Citrix intégrés. Les modèles **Montée en charge du serveur élevée** et **Expérience utilisateur très haute définition** utilisent tous les deux Thinwire avec les combinaisons de paramètres de stratégie les mieux adaptées aux priorités de votre organisation et aux attentes de vos utilisateurs.

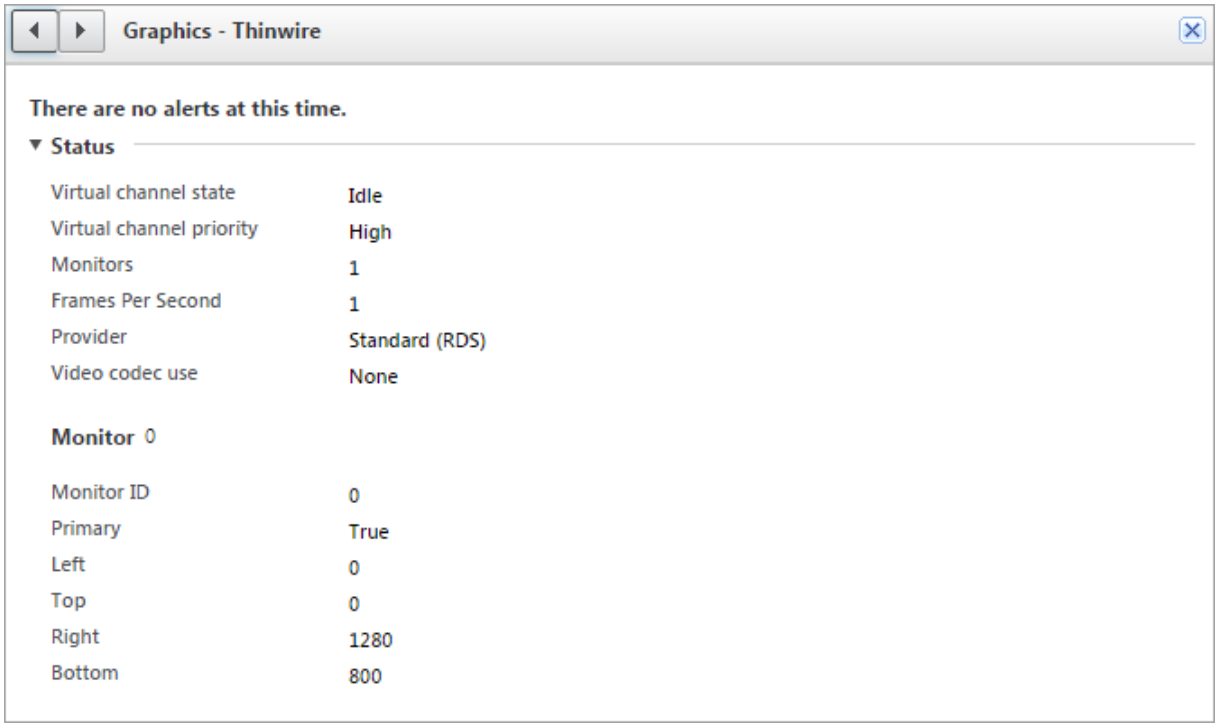
Contrôle de Thinwire

Vous pouvez contrôler l'utilisation et les performances de Thinwire depuis Citrix Director. La vue Détails du canal virtuel HDX contient des informations utiles pour la résolution des problèmes et le contrôle de Thinwire dans une session. Pour afficher les mesures liées à Thinwire :

1. Dans Director, recherchez un utilisateur, un ordinateur ou un point de terminaison, ouvrez une session active, puis cliquez sur **Détails**. Vous pouvez également sélectionner **Filtres** > **Sessions** > **Toutes les sessions**, ouvrir une session active et cliquer sur **Détails**.
2. Faites défiler l'écran vers le bas dans le panneau **HDX**.



1. Sélectionnez **Graphiques - Thinwire**.



Multimédia

February 28, 2019

La pile de la technologie HDX prend en charge la mise à disposition d'applications multimédias via deux approches complémentaires :

- Mise à disposition multimédia avec restitution côté serveur
- Redirection multimédia avec restitution côté client

Cette stratégie permet de vous assurer que vous pouvez mettre à disposition une gamme complète de formats multimédias, avec une expérience utilisateur optimale, lorsque vous maximisez la capacité à monter en charge du serveur pour réduire le coût par utilisateur.

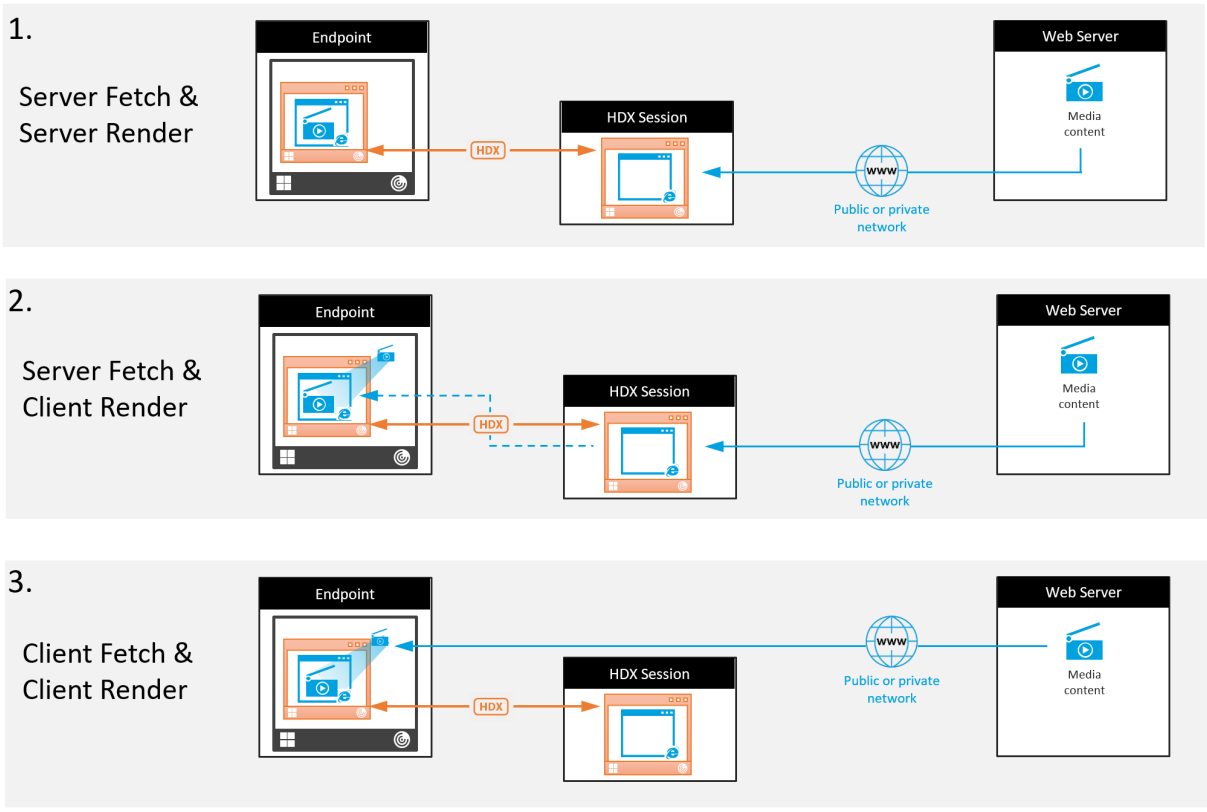
Avec la mise à disposition de multimédia restitué par le serveur, le contenu audio et vidéo est décodé et restitué sur le serveur XenApp ou XenDesktop par l'application. Le contenu est ensuite compressé et distribué via le protocole ICA au Citrix Receiver sur la machine utilisateur. Cette méthode fournit le taux de compatibilité le plus élevé avec différentes applications et différents formats multimédia. Le traitement des vidéos étant consommateur de ressources, la mise à disposition de multimédia par restitution sur le serveur bénéficie de l'accélération matérielle intégrée. Par exemple, la prise en charge de l'accélération de vidéo DirectX (DXVA) diminue la charge de l'UC en effectuant le décodage H.264 sur un matériel distinct. Les technologies Intel Quick Sync et NVIDIA NVENC fournissaient l'encodage H.264 avec accélération matérielle.

Étant donné que la plupart des serveurs ne proposent pas l'accélération matérielle pour la compression vidéo, la capacité à monter en charge du serveur est affectée si l'intégralité du traitement vidéo est effectué sur l'UC du serveur. Pour conserver une capacité à monter en charge élevée du serveur, de nombreux formats multimédias peuvent être redirigés vers la machine utilisateur pour une restitution locale. La redirection Windows Media déleste le serveur pour un large éventail de formats multimédia généralement associés avec Windows Media Player.

La redirection Flash permet de rediriger du contenu vidéo Adobe Flash vers un lecteur Flash exécuté localement sur la machine utilisateur.
Le contenu vidéo HTML5 est de plus en plus populaire et Citrix a introduit une technologie de redirection pour ce type de contenu.
En outre, vous pouvez appliquer les technologies de redirection de contact générales Redirection hôte vers client et Local App Access au contenu multimédia.

En combinant ces technologies, si vous ne configurez pas la redirection, HDX effectue la restitution côté serveur.
Si vous configurez la redirection, HDX utilise la méthode Récupération serveur et restitution client ou Récupération client et restitution client. Si ces méthodes échouent, HDX retourne à la restitution du côté serveur si nécessaire et est régi par la stratégie de prévention du retour.

Exemples de scénarios



Scénario 1. (Récupération serveur, restitution serveur) :

1. Le serveur récupère le fichier multimédia à partir de sa source, décode et présente le contenu sur un périphérique audio ou un périphérique d'affichage.
2. Le serveur extrait l'image ou le son présenté(e) depuis le périphérique d'affichage ou le périphérique audio respectivement.
3. Le serveur peut aussi le compresser et le transmettre ensuite au client.

Cette approche entraîne des coûts d'UC élevés, des coûts de bande passante élevés (si l'image ou le son extrait(e) n'est pas compressé(e) efficacement) et ne permet qu'une faible capacité à monter en charge.

Les canaux virtuels Audio et Thinwire utilisent cette approche. Cette approche a pour avantage de réduire la configuration matérielle et logicielle requise pour les clients. Avec cette approche, le décodage se produit sur le serveur et il fonctionne pour une plus grande variété de périphériques et de formats.

Scénario 2. (Récupération serveur, restitution client) :

Avec cette approche, le contenu multimédia doit pouvoir être intercepté avant d'être décodé et présenté au périphérique audio ou d'affichage. Le contenu audio/vidéo compressé est envoyé au client sur lequel il est ensuite décodé et présenté localement. L'avantage de cette approche est que le décodage et la présentation sont déchargés vers les machines clientes, réduisant les cycles d'UC sur le serveur.

Toutefois, elle requiert une configuration logicielle et matérielle supplémentaire pour le client. Le client doit pouvoir décoder chaque format qu'il est susceptible de recevoir.

Scénario 3. (Récupération client, restitution client) :

Avec cette approche, l'adresse URL du contenu multimédia doit pouvoir être interceptée avant d'être récupérée depuis la source. L'URL est envoyée au client sur lequel le contenu multimédia est récupéré, décodé et présenté localement. Cette approche repose sur un concept simple. Elle a pour avantage de diminuer les cycles d'UC sur le serveur et la bande passante car seules les commandes sont envoyées à partir du serveur. Toutefois, le contenu multimédia n'est pas toujours accessible par les clients.

Infrastructure et plate-forme

Les systèmes d'exploitation bureau (Windows, Mac OS X et Linux) offrent des infrastructures multimédias permettant le développement plus rapide et plus facile d'applications multimédias. Ce tableau répertorie certaines des infrastructures multimédias les plus populaires. Chaque infrastructure divise le traitement multimédia en plusieurs étapes et utilise une architecture basée sur pipeline.

Infrastructure	Plate-forme
DirectShow	Windows (98 et versions ultérieures)
Media Foundation	Windows (Vista et versions ultérieures)
Gstreamer	Linux
QuickTime	Mac OS X

Prise en charge double hop avec les technologies de redirection multimédia

Redirection de média	Prise en charge
Redirection HDX Flash	Non
Redirection Windows Media	Oui
Redirection vidéo HTML5	Oui
Redirection audio	No

Informations connexes

- Fonctionnalités audio
- Redirection Flash
- Redirection multimédia HTML5
- Redirection Windows Media
- Redirection de contenu générale

Fonctionnalités audio

January 23, 2019

Vous pouvez configurer et ajouter les paramètres de stratégie Citrix suivants pour une stratégie qui optimise les fonctionnalités audio HDX. Pour de plus amples informations sur l'utilisation et les relations et dépendances avec d'autres paramètres de stratégie, consultez la section Paramètres de stratégie audio et Paramètres de stratégie de bande passante et Paramètres de stratégie Connexions Multi-Stream.

> **Important**
>
> Bien qu'il soit conseillé de mettre à disposition le contenu audio à l'aide du protocole UDP plutôt que TCP, le cryptage audio UDP à l'aide de DTLS n'est disponible qu'entre NetScaler Gateway et Citrix Receiver. Par conséquent, il peut être préférable d'utiliser le transport TCP. TCP prend en charge le cryptage TLS de bout en bout depuis le VDA vers Citrix Receiver.

Qualité audio

En règle générale, une qualité sonore plus élevée consomme plus de bande passante et a une utilisation de l'UC serveur supérieure par le volume des données audio envoyées aux machines utilisateur. La compression du son vous permet d'équilibrer la qualité sonore sur les performances générales de session ; utilisez les paramètres de stratégie Citrix pour configurer les niveaux de compression à appliquer aux fichiers sonores.

Par défaut, le paramètre de stratégie de qualité audio est défini sur Élevée : audio à définition élevée lorsque le transport UDP est utilisé et sur Moyen - Optimisé pour la reconnaissance vocale lorsque le transport UDP (recommandé) est utilisé. Le paramètre Haute définition offre une qualité audio stéréo haute fidélité mais consomme plus de bande passante que les autres paramètres de qualité audio. N'utilisez pas cette qualité audio pour les chats vocaux ou les applications de chat vidéo (par exemple téléphones logiciels) non optimisés, car elle risque d'introduire une latence dans le chemin audio ne convenant pas aux communications en temps réel. Le paramètre de stratégie Optimisée pour le son de la voix est recommandé pour l'audio en temps réel, quel que soit le protocole de transport sélectionné.

Lorsque la bande passante est limitée, pour les connexions par satellite ou par modem par exemple, définir la qualité audio sur **Faible** permet de consommer le minimum de bande passante. Dans ce cas, créez des stratégies distinctes pour les utilisateurs sur connexions à faible bande passante afin que les utilisateurs sur connexions à bande passante élevée ne soient pas affectés.

Pour plus d'informations sur le paramètre, veuillez consulter la section Paramètres de stratégie audio. N'oubliez pas d'activer les Paramètres audio du client sur la machine utilisateur ; voir « Stratégies de configuration audio pour les machines utilisateur » dans cet article.

Redirection audio cliente

Pour autoriser des utilisateurs à recevoir l'audio d'une application sur un serveur au travers de haut-parleurs ou autres périphériques audio, (tels que des casques) sur la machine utilisateur, laissez le paramètre Redirection audio du client sur sa valeur par défaut (Autorisée).

Le mappage audio du client place une charge importante sur les serveurs et le réseau ; toutefois, l'interdiction de la redirection audio du client désactive toutes les fonctionnalités HDX audio.

Pour plus d'informations sur le paramètre, veuillez consulter la section Paramètres de stratégie audio. N'oubliez pas d'activer les Paramètres audio du client sur la machine utilisateur ; voir « Stratégies de configuration audio pour les machines utilisateur » dans cet article.

Redirection du microphone client

Pour permettre aux utilisateurs d'enregistrer de l'audio à l'aide de périphériques d'entrée tels que des microphones sur la machine utilisateur, laissez le paramètre Redirection du microphone client, sur sa valeur par défaut (Autorisée).

Pour des raisons de sécurité, les utilisateurs sont avertis si des serveurs non approuvés par leurs machines utilisateur essaient d'accéder à leurs microphones et peuvent choisir d'autoriser ou de refuser l'accès avant d'utiliser le microphone. Les utilisateurs peuvent désactiver cette alerte sur Citrix Receiver.

Pour plus d'informations sur le paramètre, veuillez consulter la section Paramètres de stratégie audio. N'oubliez pas d'activer les Paramètres audio du client sur la machine utilisateur ; voir « Stratégies de configuration audio pour les machines utilisateur » dans cet article.

Audio Plug N Play

Le paramètre de stratégie Plug N Play audio permet d'autoriser ou d'empêcher l'utilisation de plusieurs périphériques audio pour enregistrer et lire les sons. Cette option est **activée** par défaut. Plug N Play audio permet aux périphériques audio d'être reconnus même s'ils ne sont pas connectés tant que la session de l'utilisateur n'a pas été établie.

Ce paramètre s'applique uniquement aux machines équipées du système d'exploitation Windows Server.

Pour plus d'informations sur le paramètre, veuillez consulter la section Paramètres de stratégie audio.

Limite de bande passante de redirection audio et Pourcentage de limite de bande passante de redirection audio

Le paramètre de stratégie de Limite de bande passante de redirection audio spécifie la bande passante maximale (en kilobits par seconde) pour la lecture et l'enregistrement audio dans une session. Le paramètre Pourcentage de limite de bande passante de la redirection audio spécifie la bande passante maximale pour la redirection audio sous forme de pourcentage de la bande passante totale disponible. Par défaut, aucun maximum (zéro) n'est spécifié pour les deux paramètres. Si les deux paramètres sont configurés, celui possédant la limite de bande passante la plus basse est utilisé.

Pour plus d'informations sur le paramètre, veuillez consulter la section Paramètres de stratégie de bande passante. N'oubliez pas d'activer les Paramètres audio du client sur la machine utilisateur ; voir « Stratégies de configuration audio pour les machines utilisateur » dans cet article.

Transport en temps réel audio via UDP et Plage de port UDP audio

Par défaut,
Transport en temps réel audio via UDP est Autorisé (s'il est sélectionné au moment de l'installation), ouvrant un port UDP sur le serveur pour les connexions qui utilisent le transport en temps réel audio via UDP. Citrix recommande de configurer l'audio UDP/RTP pour vous assurer la meilleure expérience utilisateur possible dans le cas d'une surcharge du réseau ou une perte de paquets. Pour les fonctionnalités d'audio en temps réel telles que les applications softphone, l'audio UDP est désormais préférable à EDT. UDP permet une perte de paquets sans retransmission, évitant ainsi une latence supplémentaire sur les connexions avec perte de paquets élevée.

> **Important :**
>
> les données audio transmises via UDP ne sont pas cryptées lorsque NetScaler Access Gateway ne se trouve pas sur le chemin. Si NetScaler Access Gateway est configuré pour accéder aux ressources XenApp et XenDesktop, le trafic audio entre la machine de point de terminaison et NetScaler Access Gateway est sécurisé à l'aide du protocole DTLS.

La Plage de port UDP audio spécifie la plage de numéros de ports que le Virtual Delivery Agent (VDA) utilise pour échanger des données de paquet audio avec la machine utilisateur.

Par défaut, la plage se situe entre 16500 et 16509.

Pour plus d'informations sur le paramètre Transport en temps réel audio via UDP, voirParamètres de stratégie audio ; pour plus de détails sur Plage de port UDP audio, veuillez consulter la section Paramètres de stratégie Connexions Multi-Stream. N'oubliez pas d'activer les Paramètres audio du client sur la machine utilisateur ; voir « Stratégies de configuration audio pour les machines utilisateur » dans cet article.

Stratégies de configuration audio pour les machines utilisateur

1. Chargez les modèles de stratégie de groupe en suivant les instructions de Configuration avec le modèle d'administration d'objet de stratégie de groupe.
2. Dans l'éditeur de stratégie de groupe, développez Modèles d'administration > Composants Citrix > Citrix Receiver > Expérience utilisateur.
3. Pour les **paramètres audio du client**, sélectionnez **Non configuré**, **Activé** ou **Désactivé**.
    - **Non configuré**. Par défaut, la redirection audio est activée avec une qualité audio supérieure ou des paramètres audio personnalisés configurés précédemment.

- **Activé**. La redirection audio est activée avec les options sélectionnées.
- **Désactivé**. La redirection audio est désactivée.

4. Si vous sélectionnez **Activé**, choisissez une qualité audio. Pour l'audio UDP, utilisez **Moyenne** (valeur par défaut).
5. Pour l'audio UDP, sélectionnez **Activer le transport en temps réel** et définissez la plage de ports entrants à ouvrir dans le pare-feu Windows.
6. Pour utiliser l'audio UDP avec NetScaler Access Gateway, sélectionnez **Autoriser le transport en temps réel via NetScaler Gateway**. NetScaler Access Gateway doit être configuré avec DTLS. Pour de plus amples informations, consultez la section Audio UDP via un NetScaler Gateway.

En tant qu'administrateur, si vous n'avez pas de contrôle sur les machines de point de terminaison pour effectuer ces modifications, par exemple dans le cas de BYOD ou d'ordinateurs personnels, utilisez le fichier des attributs default.ica de StoreFront pour activer l'audio UDP.

1. Sur la machine StoreFront, ouvrez C:\inetpub\wwwroot\Citrix\<Nom magasin>\App_Data\default.ica à l'aide d'un éditeur de texte tel que Bloc-notes.
2. Ajoutez les entrées ci-dessous dans la section [Application].

```
; This is to enable Real-Time Transport
EnableRtpAudio=true
; This is to Allow Real-Time Transport Through gateway
EnableUDPThroughGateway=true
; This is to set audio quality to Medium
AudioBandwidthLimit=1-
; UDP Port range
RtpAudioLowestPort=16500
RtpAudioHighestPort=16509
```

Si vous activez l'audio UDP en modifiant le fichier default.ica, l'audio UDP est activé pour tous les utilisateurs qui utilisent ce magasin.

Éviter l'écho pendant les conférences multimédia

Les utilisateurs dans des conférences audio ou vidéo peuvent entendre un écho. Des échos se produisent généralement lorsque les haut-parleurs et les microphones sont trop proches l'un de l'autre. Pour cette raison, nous recommandons l'utilisation de casques pour les conférences audio et vidéo.

HDX offre une option d'annulation de l'écho (activée par défaut), qui réduit l'écho. L'efficacité de l'annulation de l'écho est liée à la distance entre les haut-parleurs et le microphone. Les périphériques ne doivent pas se trouver trop proches ou trop éloignés l'un de l'autre.

Vous pouvez modifier un paramètre de registre pour désactiver l'annulation de l'écho.

> **Avertissement**
>
> La modification incorrecte du Registre peut entraîner des problèmes graves pouvant nécessiter de réinstaller votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

1. À l'aide de l'Éditeur du Registre sur la machine utilisateur, sélectionnez l'une des options suivantes :
   - Ordinateurs 32 bits : HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advar
   - Ordinateurs 64 bits: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio\EchoCancellation
2. Modifiez le champ de données Valeur sur FALSE.

Softphones

Un softphone est un logiciel agissant en tant qu'interface téléphonique. Vous utilisez un softphone pour effectuer des appels via Internet à partir d'un ordinateur ou tout autre appareil intelligent. Avec un softphone, vous pouvez composer des numéros de téléphone et effectuer d'autres fonctions téléphoniques depuis un écran.

XenApp et XenDesktop prennent en charge plusieurs méthodes de mise à disposition de softphone.

- **Mode de contrôle**. Le softphone hébergé contrôle simplement un téléphone physique. Dans ce mode, aucun trafic audio ne transite via le serveur XenApp ou XenDesktop.
- **Prise en charge de softphone optimisé de HDX RealTime**. Le moteur multimédia est exécuté sur la machine utilisateur et le trafic VoIP circule en peer to peer. Par exemple, voir :
  - HDX RealTime Optimization Pack, qui optimise la mise à disposition de Microsoft Skype Entreprise et Lync.
  - Cisco Virtualization Experience Media Engine (VXME) pour Jabber.
  - Avaya VDI Communicator pour one-X Communicator et one-X Agent.
- **Local App Access**. Fonctionnalité de XenApp et XenDesktop qui permet à une application telle qu'un softphone de s'exécuter localement sur une machine utilisateur Windows tout en semblant être intégré au bureau virtuel/publié. L'intégralité du traitement audio s'effectue sur la machine utilisateur. Pour plus d'informations, voir Local App Access et redirection d'adresse URL.
- **Prise en charge de softphone générique de HDX RealTime.** VoIP-over-ICA.

Prise en charge de softphone générique

La prise en charge de softphone générique vous permet d'héberger un softphone non modifié sur XenApp ou XenDesktop dans le centre de données. Le trafic audio transite via le protocole Citrix ICA

(de préférence à l'aide d'UDP/RTP) vers la machine utilisateur exécutant Citrix Receiver.

La prise en charge de softphone générique est une fonction de HDX RealTime. Cette approche est particulièrement utile lorsque :

- Une solution optimisée pour la mise à disposition du softphone n'est pas disponible et l'utilisateur n'est pas sur une machine Windows sur laquelle Local App Access peut être utilisé.
- Le moteur multimédia requis pour la mise à disposition optimisée du softphone n'a pas été installé sur la machine utilisateur ou n'est pas disponible pour la version de système d'exploitation exécutée sur la machine utilisateur. Dans ce scénario, Generic HDX RealTime fournit une solution alternative.

Deux points doivent être prise en compte concernant la mise à disposition de softphone à l'aide de XenApp et XenDesktop :

- La manière dont l'application softphone est mise à disposition sur le bureau virtuel/publié.
- La manière dont l'audio est mis à disposition vers et depuis le casque, le microphone et les haut-parleurs de l'utilisateur ou le téléphone USB.

XenApp et XenDesktop incluent de nombreuses technologies pour prendre en charge la mise à disposition de softphone générique :

- Codec optimisé pour le son de la voix pour un codage rapide de l'audio en temps réel et une bande passante efficace.
- Pile audio avec latence faible.
- Tampon de gigue du côté serveur pour réguler l'audio lorsque la latence réseau fluctue.
- Identification des paquets (DSCP et WMM) pour la qualité de service.
  - Identification DSCP pour les paquets RTP (Couche 3)
  - Identification WMM pour le Wi-Fi

Les versions de Citrix Receiver pour Windows, Linux, Chrome et Mac sont également compatibles avec VoIP. Citrix Receiver pour Windows offre ces fonctionnalités :

- Tampon de gigue du côté serveur : régule l'audio lorsque la latence réseau fluctue.
- Annulation de l'écho : permet une plus grande variation de distance entre le micro et les haut-parleurs pour les travailleurs qui n'utilisent pas de casque.
- Audio Plug-n-Play : les appareils audio n'ont pas besoin d'être branchés avant le démarrage d'une session. Ils peuvent être branchés à tout moment.
- Routage du périphérique audio : les utilisateurs peuvent diriger la sonnerie vers les haut-parleurs, mais la voix vers leur casque.
- ICA Multi-stream : permet un routage flexible basé sur la qualité de service à travers le réseau.
- ICA prend en charge quatre flux TCP et deux flux UDP. Un des flux UDP prend en charge l'audio en temps réel sur RTP.

Vous trouverez un récapitulatif des fonctionnalités de Citrix Receiver dans le tableau des fonctionnalités de Citrix Receiver.

Configuration système recommandée

Logiciel et matériel client : pour une qualité audio optimale, nous vous recommandons la dernière version de Citrix Receiver et un casque de bonne qualité avec annulation de l'écho acoustique (AEC). Les versions de Citrix Receiver pour Windows, Linux et Mac prennent en charge VoIP. Dell Wyse offre également la prise en charge de VoIP pour ThinOS (WTOS).

Unité centrale : surveillez l'utilisation de l'UC sur le VDA pour déterminer s'il est nécessaire d'attribuer deux UC virtuelles à chaque machine virtuelle. La voix et la vidéo en temps réel consomment un grand nombre de données. La configuration de deux UC virtuelles réduit la latence causée par le basculement de thread. Par conséquent, nous vous recommandons de configurer deux UC virtuelles dans un environnement VDI XenDesktop.

Avoir deux UC virtuelles ne signifie pas nécessairement que le nombre d'UC physiques est doublé, car les UC physiques peuvent être partagées par différentes sessions.

Citrix Gateway Protocol (CGP), qui est utilisé pour la fonction de fiabilité de session, augmente également la consommation d'UC. Sur les connexions réseau de qualité élevée, vous pouvez désactiver cette fonctionnalité pour réduire la consommation d'UC sur le VDA. Les étapes précédentes peuvent ne pas être nécessaires sur un serveur puissant.

Audio UDP : la fonctionnalité Audio sur UDP fournit une excellente tolérance face aux congestions du réseau et à la perte de paquets. Nous vous recommandons de la préférer à TCP si elle est disponible.

Configuration LAN/WAN : une configuration correcte du réseau est indispensable à une bonne qualité audio en temps réel. En général, vous devez configurer des réseaux LAN virtuels (VLAN) car des paquets de diffusion excessifs peuvent introduire des effets de gigue. Les machines compatibles IPv6 peuvent générer de nombreux paquets de diffusion. Si la prise en charge IPv6 n'est pas nécessaire, vous pouvez désactiver IPv6 sur ces machines. Effectuez une configuration qui prendra en charge la qualité de service.

Paramètres pour les connexions WAN :
vous pouvez utiliser les chats audio via des connexions LAN et WAN. Sur une connexion WAN, la qualité audio dépend de la latence, de la perte de paquets et de la gigue sur la connexion. En cas de mise à disposition de softphones pour les utilisateurs d'une connexion WAN, nous recommandons l'utilisation de NetScaler SD-WAN entre le centre de données et le bureau à distance pour garantir une haute qualité de service. NetScaler SD-WAN prend en charge l'ICA multi-stream, y compris UDP. De plus, dans le cas d'un flux TCP unique, il est possible de distinguer les priorités de plusieurs canaux virtuels ICA pour vous assurer que les données audio en temps réel à priorité élevée soient traitées en priorité.

Utilisez Director ou HDX Monitor pour valider votre configuration HDX.

Connexions utilisateur à distance : NetScaler Gateway prend en charge DTLS pour mettre à disposition le trafic UDP/RTP en mode natif (sans encapsulation dans TCP).
Vous devez ouvrir les pare-feu de façon bidirectionnelle pour le trafic UDP sur le port 443.

Sélection codec et consommation de bande passante :
entre la machine utilisateur et le Virtual Delivery Agent (VDA) dans le centre de données, nous recommandons d'utiliser le paramètre de codec optimisé pour le son de la voix, également appelé audio de qualité moyenne. Entre la plate-forme VDA et l'adresse IP-PBX, le softphone utilise le codec configuré ou négocié, quel qu'il soit. Par exemple :

- G711 fournit un son de voix de très bonne qualité mais la bande passante doit être de 80 à 100 kilobits par seconde par appel (selon les charges de réseau Layer2).
- G729 fournit un son de voix de bonne qualité et la bande passante requise est faible, de 30 à 40 kilobits par seconde par appel (selon les charges de réseau Layer2).

Mise à disposition d'applications softphone sur le bureau virtuel

Il existe deux méthodes que vous pouvez utiliser pour mettre à disposition un softphone sur le bureau virtuel XenDesktop :

- L'application peut être installée sur l'image du bureau virtuel.
- L'application peut être distribuée en streaming sur le bureau virtuel à l'aide de Microsoft App□V. Cette approche présente des avantages en termes de gestion car elle évite d'encombrer l'image du bureau virtuel. Une fois diffusée en streaming sur le bureau virtuel, l'application s'exécute dans cet environnement comme si elle avait été installée de la manière habituelle. Les applications ne sont pas toutes compatibles avec App-V.

Mise à disposition audio vers et depuis la machine utilisateur

Generic HDX RealTime prend en charge deux méthodes de mise à disposition de contenu audio vers et depuis la machine utilisateur :

- **Canal virtuel audio Citrix**. Nous recommandons généralement le canal virtuel audio Citrix car il est conçu spécifiquement pour le transport audio.
- **Redirection USB générique**. Utile pour prendre en charge les périphériques audio avec boutons et/ou les périphériques d'interface utilisateur (HID) à écran, si la machine utilisateur se trouve sur un réseau LAN ou une connexion de type LAN vers le serveur XenApp ou XenDesktop.

Canal virtuel audio Citrix

Le canal virtuel audio Citrix (CTXCAM) bidirectionnel permet une mise à disposition efficace de l'audio via le réseau. Generic HDX RealTime récupère l'audio à partir du casque ou du micro de l'utilisateur, le compresse et le transmet via ICA vers l'application de softphone sur le bureau virtuel. De même, la sortie audio du softphone est compressée et envoyée dans l'autre direction vers le casque ou les haut-parleurs de l'utilisateur. Cette compression est indépendante de la compression utilisée par le softphone lui-même (telle que G.729 ou G.711). Elle est effectuée à l'aide du codec optimisé pour le son de la voix (qualité moyenne). Ses caractéristiques sont idéales pour le voice-over-IP (VoIP). Elle propose des temps de codage rapides et consomme uniquement environ 56 Kilobits par seconde de bande passante réseau (28 Kbit/s dans chaque direction), en utilisation maximale. Ce codec doit être

explicitement sélectionné dans la console Studio car il ne s'agit pas du codec audio par défaut. La valeur par défaut est le codec HD Audio (haute qualité). Ce codec est excellent pour les pistes audio stéréo haute fidélité mais le codage est plus lent qu'avec le codec optimisé pour le son de la voix.

Redirection USB générique

La technologie de redirection USB générique Citrix (canal virtuel CTXGUSB) offre un moyen générique d'accéder à distance aux périphériques USB, y compris les périphériques composites (audio plus HID) et les périphériques USB isochrones. Cette approche est limitée aux utilisateurs connectés au réseau LAN, car le protocole USB a tendance à être sensible à la latence du réseau et requiert une bande passante réseau considérable. La redirection USB isochrone fonctionne également bien lors de l'utilisation de certains softphones. Cette redirection fournit une qualité de voix excellente et une latence faible, mais le canal virtuel audio Citrix est recommandé car il est optimisé pour le trafic audio. L'exception principale concerne l'utilisation d'un périphérique audio avec boutons tel qu'un téléphone USB connecté à la machine utilisateur qui est connectée via LAN au centre de données. Dans ce cas, la redirection USB générique prend en charge les boutons du téléphone ou du casque permettant de contrôler les fonctionnalités en envoyant un signal au softphone. Cela n'est pas un problème avec les boutons qui fonctionnent localement sur la machine.

Redirection Flash

January 23, 2019

> **Important**
>
> Adobe a annoncé la fin de vie (EOL) de Flash le 25 juillet 2017. Adobe projette d'arrêter la mise à jour et la distribution du lecteur Flash à la fin de l'année 2020.
>
> Microsoft a annoncé qu'ils allaient progressivement abandonner la prise en charge de Flash dans Internet Explorer avant la date annoncée par Adobe. Ils supprimeront Flash de Windows d'ici la fin 2020. Lorsque cela se produira, les utilisateurs ne pourront plus activer ou exécuter Flash dans Internet Explorer.
>
> Citrix s'aligne avec la stratégie Microsoft et continue de maintenir et de prendre en charge la Redirection HDX Flash jusqu'à la fin de l'année 2020. Nous n'avons pas encore décidé les versions de XenApp et XenDesktop dans lesquelles le code de la Redirection Flash sera exclu, mais nous recommandons d'utiliser la Redirection vidéo HTML5 dès que possible. La Redirection vidéo HTML5 est idéale pour contrôler le contenu multimédia. Par exemple, des vidéos de communications d'entreprise, des vidéos de formation, ou lorsqu'un tiers héberge le contenu.
>
> Pour plus d'informations sur la redirection vidéo HTML5, consultez la section Redirection multimédia HTML5.

La redirection Flash transfère le traitement de la plupart du contenu Adobe Flash (y compris les animations, les vidéos et les applications) vers les réseaux locaux ou étendus des machines x86 Windows et Linux 32 bits des utilisateurs, ce qui réduit la charge serveur et réseau. Ce résultat augmente la capacité à monter en charge tout en garantissant une expérience utilisateur haute définition. Configuration de la redirection Flash requiert des paramètres côté client et côté serveur.

> **Avertissement :**
>
> la redirection Flash requiert une interaction significative entre la machine utilisateur et les composants serveur. Utilisez cette fonctionnalité uniquement dans des environnements dans lesquels la séparation de sécurité entre la machine utilisateur et le serveur n'est pas nécessaire. Vous pouvez également configurer des machines utilisateur pour pouvoir utiliser cette fonctionnalité uniquement avec des serveurs de confiance. Étant donné que la redirection Flash requiert l'installation du lecteur Adobe Flash Player sur la machine utilisateur, cette fonctionnalité doit uniquement être activée si le lecteur Flash Player lui-même est sécurisé.

La redirection Flash est prise en charge à la fois sur les clients et les serveurs. Si le client prend en charge la redirection Flash de deuxième génération, le contenu Flash est restitué sur le client. Les fonctionnalités de redirection Flash comprennent la prise en charge des connexions utilisateur sur le réseau étendu, le retour intelligent, et une liste de compatibilité d'adresses URL ; consultez la section ci-dessous pour plus de détails.

La redirection Flash utilise la journalisation d'événements Windows sur le serveur pour consigner les événements Flash. Le journal d'événements indique si la redirection Flash est utilisée et fournit des détails sur les problèmes. Voici une liste commune à tous les événements journalisés par la redirection Flash :

- La redirection Flash signale les événements au journal d'applications.
- Sur les systèmes Windows 10, Windows 8 et Windows 7, un journal spécifique à la redirection Flash s'affiche dans le nœud Journaux des applications et des services.
- La valeur Source est Flash.
- La valeur Catégorie est Aucune.

Pour les dernières mises à jour de compatibilité HDX Flash, reportez-vous à l'article CTX136588.

Configurer la redirection Flash sur le serveur

Pour configurer la redirection Flash sur le serveur, utilisez les paramètres de stratégie Citrix suivants : Pour de plus amples informations, consultez la section Paramètres de stratégie Redirection Flash.

- Par défaut, la redirection Flash est activée. Pour modifier ce comportement par défaut pour des pages Web individuelles et des instances Flash, utilisez le paramètre Liste de compatibilité d'adresses URL Flash.

- Retour intelligent Flash : détecte des instances de petits films Flash (telles que ceux fréquemment utilisés pour lire les publicités) et les restitue sur le serveur, au lieu de les rediriger pour restitution sur la machine utilisateur. Cette optimisation n'entraîne ni interruption, ni échec du chargement de la page Web ou de l'application Flash. Par défaut, le retour intelligent Flash est activé. Pour rediriger toutes les instances de contenu Flash pour la restitution sur la machine utilisateur, désactivez ce paramètre de stratégie. Notez que certains contenus Flash peuvent ne pas être redirigés correctement.
- La Liste d'adresse URL de récupération de contenu Flash côté serveur vous permet de spécifier des sites Web dont le contenu Flash doit être téléchargé vers le serveur puis transmis vers la machine utilisateur pour restitution. (Par défaut, la redirection Flash télécharge du contenu Flash directement vers la machine utilisateur avec récupération du contenu côté client.) Ce paramètre fonctionne en conjonction avec (et requiert) le paramètre Activer la récupération de contenu côté serveur sur la machine utilisateur et est conçu principalement pour être utilisé avec des sites intranet et des applications Flash internes ; consultez la section ci-dessous pour plus de détails. Il fonctionne également avec la plupart des sites Internet et peut être utilisé lorsque la machine utilisateur ne possède pas d'accès direct à Internet (par exemple, lorsque le serveur XenApp ou XenDesktop offre cette connexion).
  Remarque : la récupération de contenu côté serveur ne prend pas en charge les applications Flash utilisant le protocole RTMP (Real Time Messaging Protocol) ; au lieu de cela, la restitution côté serveur est utilisée, et prend en charge le protocole HTTP et HTTPS.
- La liste de compatibilité d'adresses URL Flash : spécifie l'emplacement où le contenu Flash provenant des sites Web répertoriés est restitué : sur la machine utilisateur, sur le serveur, ou bloqué.
- La liste de couleur d'arrière-plan Flash : vous permet de faire correspondre les couleurs des pages Web et des instances Flash, ce qui améliore l'apparence de la page Web lors de l'utilisation de la redirection Flash.

Configurer la redirection Flash sur la machine utilisateur

Installez Citrix Receiver et Adobe Flash Player sur la machine utilisateur. Aucune configuration supplémentaire n'est requise sur la machine utilisateur.

Vous pouvez modifier les paramètres par défaut à l'aide d'objets de stratégie de groupe Active Directory. Importez et ajoutez la Redirection HDX MediaStream Flash : modèle d'administration client (HdxFlashClient.adm), qui est disponible dans les dossiers suivants :

- Pour les ordinateurs 32 bits : %Program Files%\Citrix\ICA Client\Configuration\langue.
- Pour les ordinateurs 64 bits : %Program Files (x86)%\Citrix\ICA Client\Configuration\langue.

Les paramètres de stratégie s'affichent sous Modèles d'administration > Modèles d'administration classiques (ADM) > Redirection HDX MediaStream Flash - Client. Consultez la documentation Microsoft

Active Directory pour obtenir des détails sur les objets de stratégie de groupe et les modèles.

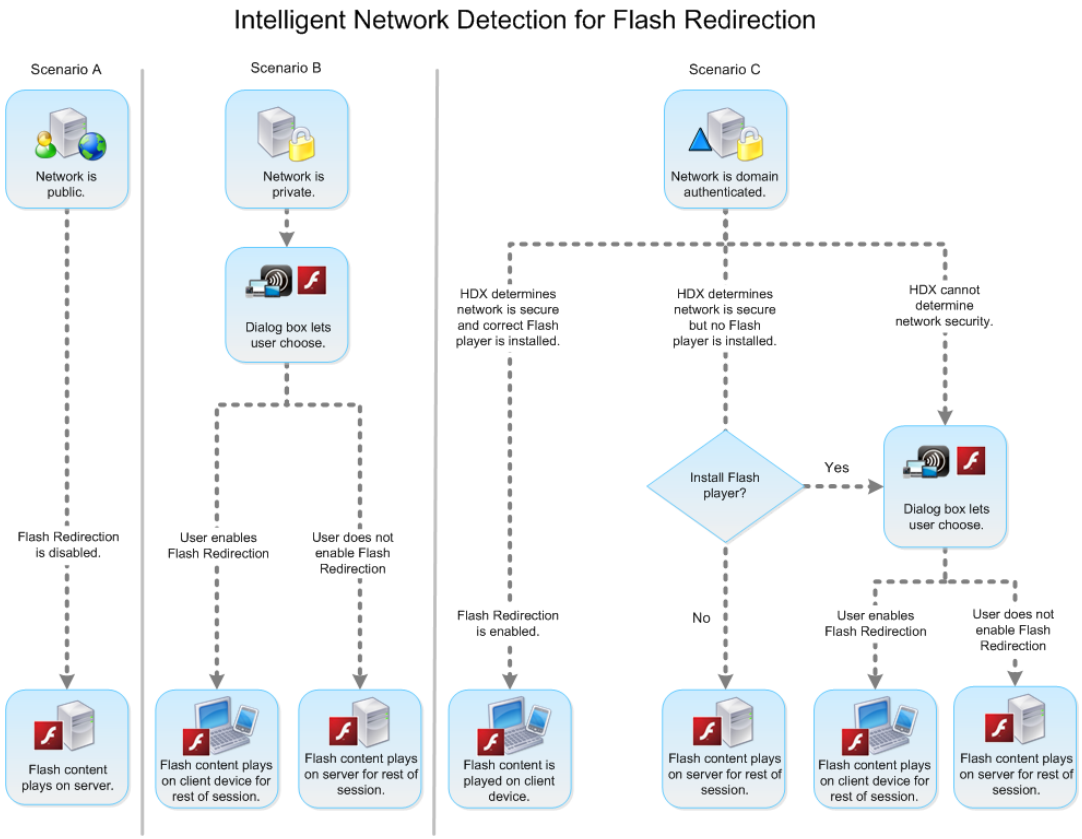
Modifier le moment où la redirection Flash est utilisée :

Le paramètre de stratégie Activer la redirection HDX MediaStream Flash sur la machine utilisateur, en conjonction avec les paramètres côté serveur, détermine si le contenu Adobe Flash est redirigé vers la machine utilisateur pour restitution locale. Par défaut, la redirection Flash est activée et utilise la détection réseau intelligente pour déterminer à quel moment lire le contenu Flash sur la machine utilisateur.

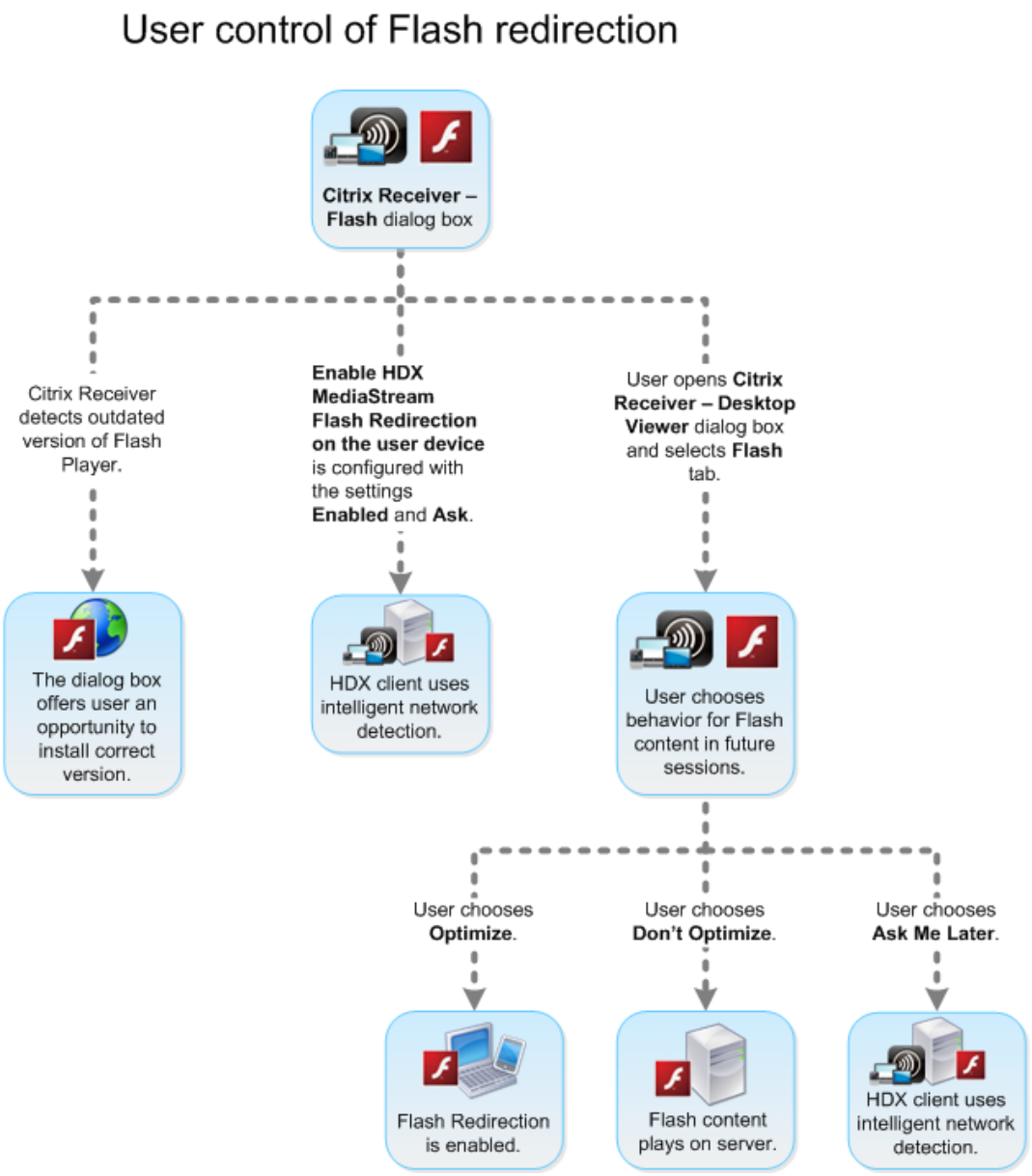
Si aucune configuration n'est définie et Desktop Lock est utilisé, la redirection Flash est activée sur la machine utilisateur par défaut.

Pour modifier le moment où la redirection Flash est utilisée ou pour désactiver la redirection Flash sur la machine utilisateur :

1. Dans la liste Paramètre, sélectionnez Activer la redirection Flash HDX MediaStream sur la machine utilisateur et cliquez sur paramètre de stratégie.
2. Sélectionnez Non configuré, Activé ou Désactivé.
3. Si vous sélectionnez Activé, choisissez une option dans la liste Utiliser la redirection HDX MediaStream Flash :
    - Pour utiliser la dernière version de la fonctionnalité de redirection Flash lorsque la configuration requise est présente, et retourner à la restitution côté serveur lorsqu'elle n'est pas utilisée, sélectionnez Uniquement avec la deuxième génération.
    - Pour toujours utiliser la redirection Flash, sélectionnez Toujours. Le contenu Flash est lu sur la machine utilisateur.
    - Pour ne jamais utiliser la redirection Flash, sélectionnez Jamais. Le contenu Flash est lu sur le serveur.
    - Pour utiliser la détection réseau intelligente pour évaluer le niveau de sécurité du réseau côté client pour déterminer le moment où utiliser la redirection Flash est approprié, sélectionnez Demander (la valeur par défaut). Si la sécurité du réseau ne peut pas être déterminée, l'utilisateur est invité à utiliser la redirection Flash. Si le niveau de sécurité réseau ne peut pas être déterminé, l'utilisateur est invité à choisir d'utiliser la redirection Flash. L'illustration suivante indique comment la redirection Flash est prise en charge pour les différents types de réseau.



Les utilisateurs peuvent remplacer la détection réseau intelligente à partir de la boîte de dialogue Citrix Receiver : Préférences de Desktop Viewer, en sélectionnant Optimiser ou Ne pas Optimiser dans l'onglet Flash. Les choix disponibles varient en fonction de la manière dont la redirection Flash est configurée sur la machine utilisateur, comme illustré ci-dessous.



Synchroniser les cookies HTTP côté client avec ceux côté serveur :

La synchronisation des cookies HTTP côté client avec ceux côté serveur est désactivée par défaut. Activez la synchronisation pour télécharger des cookies HTTP depuis le serveur ; ces cookies HTTP sont alors utilisés pour la récupération du contenu côté client et sont disponibles, pour des sites contenant du contenu Flash.

> **Remarque :**
>
> les cookies côté client ne sont pas remplacés lors de la synchronisation ; ils restent disponibles même si la stratégie de synchronisation est désactivée plus tard.

1. Dans la liste Paramètre, sélectionnez Activer la synchronisation des cookies HTTP côté client avec ceux côté serveur et cliquez sur paramètre de stratégie.

2. Sélectionnez Non configuré, Activé ou Désactivé (valeur par défaut).

Activer la récupération de contenu côté serveur :

Par défaut, la redirection Flash télécharge le contenu Flash directement vers la machine utilisateur où il est lu. L'activation de la récupération de contenu côté serveur provoque le téléchargement du contenu Flash vers le serveur, puis son envoi vers la machine utilisateur. À moins qu'il n'existe une stratégie de remplacement, telle qu'un site bloqué par le paramètre de stratégie Liste de compatibilité d'adresses URL Flash, le contenu Flash sera lu sur la machine utilisateur.

La récupération de contenu côté serveur est fréquemment utilisée lorsque la machine utilisateur se connecte à des sites internes via NetScaler Gateway et lorsque la machine utilisateur ne possède pas d'accès direct à Internet.

> **Remarque :**
>
> la récupération de contenu côté serveur ne prend pas en charge les applications Flash qui utilisent le protocole RTMP (Real Time Messaging Protocol). Au lieu de cela, la restitution côté serveur est utilisée pour de tels sites.

La redirection Flash prend en charge trois options, pour la récupération de contenu côté serveur. Deux de ces options permettent de mettre en cache du contenu côté serveur sur la machine utilisateur, ce qui améliore les performances car le contenu qui est réutilisé est déjà disponible sur la machine utilisateur pour restitution. le contenu présent dans ce cache est stocké séparément des autres contenus HTTP mis en cache sur la machine utilisateur.

Le retour vers la récupération de contenu côté serveur démarre automatiquement lorsque n'importe laquelle des options d'activation ci-dessus est sélectionnée et la récupération côté client de fichiers .swf échoue.

L'activation de la récupération de contenu côté serveur requiert des paramètres sur la machine cliente et le serveur.

1. Dans la liste Paramètre, sélectionnez Activer l'extraction de contenu côté serveur et cliquez sur paramètre de stratégie.
2. Sélectionnez Non configuré, Activé ou Désactivé (valeur par défaut). Si vous activez ce paramètre, choisissez une option dans la liste État de récupération de contenu côté serveur :

Option	Description
Désactivée	Désactive la récupération de contenu côté serveur et écrase le paramètre Liste d'adresse URL de récupération de contenu Flash côté serveur sur le serveur. Le retour vers la récupération de contenu côté est également désactivé.

Option	Description
Activée	Active la récupération de contenu côté serveur pour les pages Web et les applications Flash identifiées dans la Liste d'URL de récupération de contenu Flash côté serveur. Retour vers la récupération de contenu côté serveur est disponible, mais le contenu Flash n'est pas mis en cache.
Activée (mise en cache permanente)	Active la récupération de contenu côté serveur pour les pages Web et les applications Flash identifiées dans la Liste d'URL de récupération de contenu Flash côté serveur. Le retour vers la récupération de contenu côté est disponible. Le contenu obtenu via la récupération de contenu côté serveur est mis en cache sur la machine utilisateur et stocké d'une session à l'autre.
Activée (mise en cache temporaire)	Active la récupération de contenu côté serveur pour les pages Web et les applications Flash identifiées dans la Liste d'URL de récupération de contenu Flash côté serveur. Le retour vers la récupération de contenu côté est disponible. Le contenu obtenu via la récupération de contenu côté serveur est mis en cache sur la machine utilisateur et supprimé à la fin de la session.

3. Sur le serveur, activez le paramètre de stratégie Liste d'URL de récupération de contenu Flash côté serveur et remplissez-le avec des adresses URL cibles.

Rediriger les machines utilisateur vers d'autres serveurs pour la récupération de contenu côté client :

Pour rediriger une tentative d'obtention de contenu Flash à l'aide du paramètre Règles de réécriture d'URL pour la récupération de contenu côté client, qui est une fonctionnalité de redirection Flash de deuxième génération. Lors de la configuration de cette fonctionnalité, vous fournissez deux modèles d'adresse URL ; lorsque la machine utilisateur tente de récupérer du contenu provenant d'un site Web correspondant au premier modèle (le modèle d'adresse URL correspondant), le contenu est redirigé vers le site Web spécifié par le second modèle (le format de réécriture d'adresse URL).

Vous pouvez utiliser ce paramètre pour pallier les déficiences des réseaux de diffusion de contenu (CDN). Certains sites Web qui diffusent du contenu Flash utilisent la redirection CDN pour permettre à l'utilisateur d'obtenir le contenu à partir du groupe de serveurs contenant le même contenu le plus proche. Lors de l'utilisation de la fonctionnalité de récupération de contenu côté client de la redirection Flash, le contenu Flash est requis auprès de la machine utilisateur, tandis que le reste de la page Web sur laquelle le contenu Flash réside est requis par le serveur. Si CDN est utilisé, la requête serveur est redirigée vers le serveur le plus proche et la requête de la machine utilisateur suit le même chemin. Notez que cette valeur peut ne pas représenter l'emplacement le plus proche de la machine utilisateur ; selon la distance, il peut exister un délai significatif entre le chargement de la page Web et la lecture du contenu Flash.

1. Dans la liste Paramètre, sélectionnez Règles de réécriture d'URL pour la récupération de contenu côté client et cliquez sur paramètre de stratégie.
2. Sélectionnez Non configurée, Activée ou Désactivée. Non configurée est la valeur par défaut ; Désactivée provoque l'ignorance de toutes les règles de réécriture d'URL configurées dans l'étape suivante.
3. Si vous activez ce paramètre, cliquez sur Afficher. À l'aide d'une syntaxe d'expression régulière Perl, saisissez le modèle de correspondance d'adresse URL dans la zone Nom de valeur et le format de réécriture d'adresse URL dans la zone Valeur.

Vérification des versions minimum pour la redirection Flash

> **Avertissement**
>
> La modification incorrecte du Registre peut entraîner des problèmes graves pouvant nécessiter de réinstaller votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Vous pouvez ajouter des paramètres de registre pour spécifier la version minimale requise pour la redirection Flash pour les machines clientes qui accèdent à des VDA à l'aide de Citrix Receiver pour Windows et Citrix Receiver pour Linux. Cette fonctionnalité de sécurité permet de garantir qu'une version obsolète de Flash n'est pas utilisée.

ServerFlashPlayerVersionMinimum est une valeur de chaîne qui spécifie la version minimale du lecteur Flash Player sur le serveur ICA (VDA).

ClientFlashPlayerVersionMinimum est une valeur de chaîne qui spécifie la version minimale du lecteur Flash Player sur le client ICA (Citrix Receiver).

Ces chaînes de version peuvent être "10" ou "10.2" ou "10.2.140". Seuls les numéros de version majeur, mineur et de build sont comparés. Le numéro de révision est ignoré. Par exemple, pour une chaîne

de version de 10 avec spécification du numéro majeur uniquement, il est supposé que les numéros mineur et de build correspondent à zéro.

FlashPlayerVersionComparisonMask est une valeur DWORD qui, lorsqu'elle est définie sur 0, désactive la comparaison de la version du lecteur Flash Player sur le client ICA avec la version du lecteur Flash Player sur le serveur ICA. Le masque de comparaison a d'autres valeurs, mais ces dernières ne doivent pas être utilisées car la signification d'un masque autre que zéro peut changer. Il est recommandé de configurer le masque de comparaison sur zéro uniquement pour les clients souhaités. Il n'est pas recommandé de configurer le masque de comparaison sous les paramètres indépendants du client. Si un masque de comparaison n'est pas spécifié, la redirection Flash requiert que le client ICA ait un lecteur Flash Player de version supérieure ou égale à la version de Flash Player sur le serveur ICA. La comparaison s'effectue uniquement au niveau du numéro de version majeur du lecteur Flash.

Pour que la redirection s'effectue, les vérifications minimums de client et de serveur doivent réussir en plus de la vérification à l'aide du masque de comparaison.

La sous-clé ClientID0x51 spécifie Citrix Receiver pour Linux. La sous-clé ClientID0x1 spécifie Citrix Receiver pour Windows. Le nom de cette sous-clé est formé en ajoutant l'ID du produit client hexadécimal (sans les zéros du début) à la chaîne « ClientID ».

Exemple de configuration de registre VDA 32 bits :

[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer]
Paramètres indépendants du client

"ClientFlashPlayerVersionMinimum"="13.0" Version minimum requise pour le client ICA "ServerFlash-
PlayerVersionMinimum"="13.0" Version minimum requise pour le serveur ICA [HKEY_LOCAL_MACHINE\SOFTWARE
Paramètres du client ICA Windows

"ClientFlashPlayerVersionMinimum"="16.0.0" Spécifie la version minimum requise de Flash Player pour le client Windows [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServ
Paramètres du client ICA Linux

"FlashPlayerVersionComparisonMask"=dword:00000000 : désactive la comparaison de version pour le client Linux (vérifie que le client a une version de Flash Player plus récente que le serveur) "Client-FlashPlayerVersionMinimum"="11.2.0" : spécifie la version minimum de Flash Player pour le client Linux.

Exemple de configuration de registre VDA 64 bits :

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer]

"ClientFlashPlayerVersionMinimum"="13.0" "ServerFlashPlayerVersionMinimum"="13.0"[HKEY_LOCAL_MACHINE

"ClientFlashPlayerVersionMinimum"="16.0.0"[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMe

"FlashPlayerVersionComparisonMask"=dword:00000000 "ClientFlashPlayerVersionMinimum"="11.2.0"

Redirection multimédia HTML5

January 23, 2019

La redirection multimédia HTML5 étend les fonctionnalités de redirection multimédia de HDX MediaStream pour inclure des fonctions audio et vidéo HTML5. Face à la croissance de la distribution en ligne de contenu multimédia, plus particulièrement pour les appareils mobiles, l'industrie du navigateur a développé des manières plus efficaces de présenter du contenu audio et vidéo.

Flash a longtemps été la norme, mais ce logiciel requiert un plug-in, ne fonctionne pas sur tous les appareils et consomme davantage de batterie sur les appareils mobiles. Les sociétés telles que Youtube ou NetFlix.com et les versions plus récentes des navigateurs de Mozilla, Google et Microsoft se tournent vers HTML5, qui est devenu la nouvelle norme.

Le contenu multimédia basé sur HTML5 présente de nombreux avantages par rapport aux plug-ins propriétaires, y compris :

- Normes indépendantes de la société (W3C)
- Flux de travail DRM (Digital Rights Management) simplifié
- Meilleures performances sans les problèmes de sécurité causés par les plug-ins

Téléchargements HTTP progressifs

Le téléchargement HTTP progressif constitue une méthode de pseudo-streaming basée sur HTTP qui prend en charge HTML5. Dans un téléchargement progressif, le navigateur lit un seul fichier (codé selon une seule qualité) alors qu'il est en cours de téléchargement à partir d'un serveur Web HTTP. La vidéo est stockée sur le disque dur au fur et à mesure qu'elle est reçue et lue depuis le disque dur. Si vous regardez de nouveau la vidéo, le navigateur peut charger la vidéo à partir du cache.

Pour un exemple de téléchargement progressif, veuillez consulter la page de test de redirection vidéo HTML5. Utilisez les outils de développement de votre navigateur pour inspecter l'élément vidéo dans la page Web et trouver la source (un format de conteneur mp4) dans la balise vidéo HTML5 :

```
<video src="https://www.citrix.com/content/dam/citrix61/en_us/images/
offsite/html5-redirect.mp4"controls=""style="width:800px;"></video>
```

Comparaison entre HTML5 et Flash

Fonctionnalité	HTML5	Flash
Requiert un lecteur propriétaire	Non	Oui

Fonctionnalité	HTML5	Flash
S'exécute sur les appareils mobiles	Oui	Certains
Vitesse de fonctionnement sur différentes plates-formes	Élevée	Lente
Pris en charge par iOS	Oui	Non
Utilisation des ressources	Moins	Plus
Chargement plus rapide	Oui	Non

Exigences

Nous prenons en charge la redirection uniquement pour les téléchargements progressifs au format mp4. Nous ne prenons pas en charge les technologies WebM et ABS comme DASH/HLS.

Nous prenons en charge les fonctions suivantes :

- Restitution côté serveur
- Restitution client de récupération serveur
- Récupération et restitution côté client

Vous pourrez contrôler ces fonctions à l'aide de stratégies. Pour plus d'informations, veuillez consulter la section Paramètres de stratégie multimédia.

Versions minimales de Citrix Receiver :

- Citrix Receiver pour Windows 4.5
- Citrix Receiver pour Linux 13.5

Version minimale du navigateur VDA et version/build/SP du système d'exploitation Windows :

- **Internet Explorer 11.0**
  - Windows 10 x86 (1607 RS1) et x64 (1607 RS1)
  - Windows 7 x86 et x64
  - Windows Server 2016 RTM 14393 (1607)
  - Windows Server 2012 R2
  - Windows Server 2008 R2
- **Firefox 47** Ajoutez manuellement les certificats au magasin de certificats Firefox ou configurez Firefox pour rechercher les certificats à partir d'un magasin de certificats de confiance Windows. Pour plus d'informations, veuillez consulter https://wiki.mozilla.org/CA:AddRootToFirefox
  - Windows 10 x86 (1607 RS1) et x64 (1607 RS1)
  - Windows 7 x86 et x64

  - Windows Server 2016 RTM 14393 (1607)
  - Windows Server 2012 R2
  - Windows Server 2008 R2
- **Chrome 51**
  - Windows 10 x86 (1607 RS1) et x64 (1607 RS1)
  - Windows 7 x86 et x64
  - Windows Server 2016 RTM 14393 (1607)
  - Windows Server 2012 R2
  - Windows Server 2008 R2

Composants de la solution de redirection vidéo HTML5

- **HdxVideo.js :** hook JavaScript interceptant les commandes de vidéo sur le site Web. HdxVideo.js communique avec WebSocketService à l'aide de Secure WebSockets (SSL/TLS).
- **Certificats SSL WebSocket**
  - Pour l'autorité de certification (racine) : **Citrix XenApp/XenDesktop HDX In-Product CA** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp/XenDesktop Engineering; CN = Citrix XenApp/XenDesktop HDX In-Product CA)
    Emplacement : Certificats (ordinateur local) > Autorités de certification racines de confiance > Certificats.
  - Pour l'entité de fin (feuille) : **Citrix XenApp/XenDesktop HDX Service** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp/XenDesktop Engineering; CN = Citrix XenApp/XenDesktop HDX Service)
    Emplacement : Certificats (ordinateur local) > Personnel > Certificats.
- **WebSocketService.exe :** s'exécute sur le système local et effectue le mappage de session utilisateur et d'arrêt SSL. TLS Secure WebSocket écoutant le port 9001 127.0.0.1.
- **WebSocketAgent.exe :** s'exécute sur la session utilisateur et restitue la vidéo comme indiqué dans les commandes WebSocketService.

Activation de la redirection vidéo HTML5

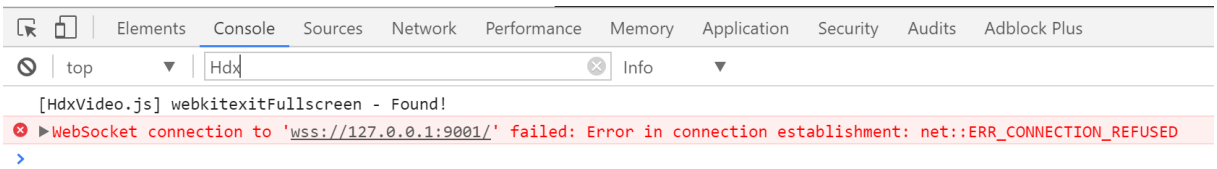
Dans cette version, cette fonctionnalité est disponible pour les pages Web contrôlées uniquement. Elle requiert l'ajout de JavaScript HdxVideo.js (fournie sur le support d'installation de XenDesktop et XenApp) aux pages web sur lesquelles le contenu multimédia HTML5 est disponible. Par exemple, des vidéos sur un site de formation interne.

Les sites Web tels que youtube.com, basés sur les technologies à débit adaptatif (par exemple, HTTP Live Streaming (HLS) et Dynamic Adaptive Streaming over HTTP (DASH)), ne sont pas pris en charge.

Pour plus d'informations, veuillez consulter la section Paramètres de stratégie multimédia.

Conseils de dépannage

Des erreurs peuvent se produire lorsque la page Web tente d'exécuter HdxVideo.js. Si JavaScript ne se charge pas, le mécanisme de redirection HTML5 échoue. Assurez-vous qu'il n'existe aucune erreur liée à HdxVideo.js en inspectant la console dans les fenêtres d'outil de développeur de votre navigateur. Par exemple :



Redirection Windows Media

November 8, 2018

La redirection Windows Media permet de contrôler et d'optimiser le mode de livraison en streaming des données audio et vidéo par les serveurs vers les utilisateurs. Par la lecture des fichiers d'exécution multimédia sur la machine utilisateur plutôt que sur le serveur, la redirection Windows Media réduit les besoins en bande passante pour la lecture de fichiers multimédia. La redirection Windows Media améliore les performances du lecteur Windows Media et les lecteurs compatibles exécutés sur des bureaux virtuels Windows.

Si la configuration requise pour la récupération de contenu Windows Media côté client n'est pas présente, la mise à disposition utilise automatiquement la récupération côté serveur. Cette méthode est transparente pour les utilisateurs. Vous pouvez utiliser XenDesktop Collector pour effectuer une trace Citrix diagnostic Facility (CDF) depuis HostMMTransport.dll pour déterminer la méthode utilisée.

La redirection Windows Media intercepte le pipeline multimédia au niveau du serveur hôte, capture les données multimédia dans leur format compressé natif et redirige le contenu vers la machine cliente. La machine cliente recrée ensuite le pipeline multimédia pour décompresser et restituer les données multimédia reçues depuis le serveur hôte. La redirection Windows Media fonctionne correctement sur les machines clientes exécutant un système d'exploitation Windows. Ces machines disposent de l'infrastructure multimédia requise pour reconditionner le pipeline multimédia tel qu'il était sur le serveur hôte. Les clients Linux utilisent des infrastructures open-source similaires pour reconditionner le pipeline multimédia.

Le paramètre de stratégie **Redirection Windows Media** contrôle cette fonctionnalité et est **Autorisé** par défaut. En général, ce paramètre améliore la qualité des données audio et vidéo restituées par le serveur à un niveau comparable à celui obtenu avec des applications exécutées localement sur les machines clientes. Dans de rares cas, la qualité obtenue avec la redirection Windows Media semble

inférieure à celle obtenue à l'aide de la compression ICA de base et des réglages audio standard. Vous pouvez désactiver cette fonctionnalité en ajoutant le paramètre **Redirection Windows Media** à une stratégie et en définissant sa valeur sur **Interdit**.

Pour de plus amples informations sur les paramètres de stratégie, consultez Paramètres de stratégie multimédia.

Redirection de contenu générale

February 28, 2019

La redirection de contenu vous permet de contrôler si les utilisateurs accèdent aux informations à l'aide d'applications publiées sur des serveurs ou d'applications exécutées localement sur les machines utilisateur.

Redirection de dossiers clients

La redirection de dossiers clients modifie la manière dont les fichiers côté client sont accessibles sur la session côté hôte. Lorsque vous activez uniquement le mappage de lecteur client sur le serveur, les volumes complets côté client sont automatiquement mappés sur les sessions en tant que liens UNC (Universal Naming Convention). Lorsque vous activez la redirection de dossiers clients sur le serveur et que l'utilisateur la configure sur la machine de bureau Windows, la partie du volume local spécifié par l'utilisateur est redirigée.

Redirection hôte vers client

La redirection hôte vers client peut être utilisée dans certains scénarios d'utilisation peu courants. En général, les autres méthodes de redirection de contenu sont préférables. Ce type de redirection est pris en charge uniquement sur les VDA avec OS de serveur (et non pas les VDA avec OS de bureau).

Local App Access et redirection d'adresse URL

Local App Access s'intègre en toute transparence avec les applications Windows installées localement dans un environnement de bureau hébergé sans passer d'un ordinateur à l'autre.

Considérations USB et lecteur client

La technologie HDX offre la **redirection USB générique** pour les périphériques spécialisés dont la prise en charge n'est pas optimisée ou n'est pas adaptée.

Informations connexes

- Redirection de dossiers clients
- Redirection hôte vers client
- Local App Access et redirection d'adresse URL

- Considérations USB et lecteur client
- Multimédia

Redirection de dossiers clients

February 28, 2019

La redirection de dossiers clients modifie la manière dont les fichiers côté client sont accessibles sur la session côté hôte. Lorsque vous activez uniquement le mappage de lecteur client sur le serveur, les volumes complets côté client sont automatiquement mappés sur les sessions en tant que liens UNC (Universal Naming Convention). Lorsque vous activez la redirection de dossiers clients sur le serveur et que l'utilisateur la configure sur la machine utilisateur, la partie du volume local spécifié par l'utilisateur est redirigée.

Seuls les dossiers spécifiés par l'utilisateur s'affichent sous forme de liens UNC dans les sessions au lieu du système de fichiers complet sur la machine utilisateur. Si vous désactivez les liens UNC via le registre, des dossiers clients apparaissent comme des lecteurs mappés au sein de la session.

La redirection de dossiers clients est prise en charge sur les machines avec OS de bureau Windows uniquement.

La redirection de dossiers clients d'un lecteur USB externe ne sera pas enregistrée suite à la déconnexion puis reconnexion de l'appareil.

Activez la redirection de dossiers clients sur le serveur. Ensuite, sur la machine cliente, spécifiez les dossiers à rediriger (l'application utilisée pour spécifier les options du dossier client est incluse avec Citrix Receiver fournie avec cette version).

> **Avertissement :**
>
> toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

1. Sur le serveur :
   a) Créez une clé : HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Client Folder Redirection.
   b) Créez une valeur REG_DWORD.
      - Nom : CFROnlyModeAvailable
      - Type : REG_DWORD
      - Données : définir sur 1
2. Sur la machine utilisateur :

a) Vérifiez que la dernière version de Citrix Receiver est installée.
b) À partir du répertoire d'installation de Citrix Receiver, démarrez CtxCFRUI.exe.
c) Sélectionnez le bouton radio Personnaliser et ajoutez, modifiez ou supprimez des dossiers.
d) Déconnectez-vous et reconnectez-vous à vos sessions pour que le paramètre prenne effet.

Redirection hôte vers client

February 28, 2019

La redirection de contenu vous permet de contrôler si les utilisateurs accèdent aux informations à l'aide d'applications publiées sur des serveurs ou d'applications exécutées localement sur les machines utilisateur.

Redirection hôte vers client est un type de redirection de contenu. Elle est prise en charge uniquement sur les VDA avec OS de serveur (et non pas les VDA avec OS de bureau).

- Lorsque la redirection hôte vers client est activée, les adresses URL sont interceptées sur le VDA de serveur puis envoyées vers la machine utilisateur. Le navigateur Web ou lecteur multimédia sur la machine utilisateur ouvre ces adresses URL.
- Si vous activez la redirection hôte vers client et que la machine utilisateur ne parvient pas à se connecter à l'adresse URL, cette dernière est redirigée vers le VDA de serveur.
- Lorsque la redirection hôte vers client est désactivée, les utilisateurs ouvrent les adresses URL à l'aide de navigateurs Web ou de lecteurs multimédias sur le VDA de serveur.
- Lorsque la redirection hôte vers client est activée, les utilisateurs ne peuvent pas la désactiver.

La redirection hôte vers client était précédemment connue sous le nom de **redirection serveur vers client**.

Quand utiliser la redirection hôte vers client

Vous pouvez envisager d'utiliser la redirection hôte vers client dans des cas spécifiques mais rares, à des fins de performances, de compatibilité ou de conformité. En général, les autres méthodes de redirection de contenu sont préférables.

Performances :

Vous pouvez utiliser la redirection hôte vers client pour les performances, de façon à ce qu'une application installée sur la machine utilisateur soit utilisée en priorité par rapport à une application installée sur le VDA.

N'oubliez pas que la redirection hôte vers client améliore les performances uniquement dans certaines conditions, car le VDA optimise déjà Adobe Flash et d'autres types de contenu multimédia. Tout

d'abord, envisagez les autres approches (paramètres de stratégie) indiquées dans les tableaux de cet article, plutôt que la redirection hôte vers client. Ces paramètres offrent plus de flexibilité et généralement une meilleure expérience utilisateur, plus particulièrement pour les machines utilisateur moins puissantes.

Compatibilité :

Vous pouvez utiliser la redirection hôte vers client pour des raisons de compatibilité dans les cas d'utilisation suivants :

- Vous utilisez des types de contenu autres que du code HTML ou multimédia (par exemple, une URL personnalisée).
- Vous utilisez un ancien format multimédia (tel que Real Media) qui n'est pas pris en charge par le lecteur multimédia du VDA avec la redirection multimédia.
- L'application du type de contenu est utilisée par un nombre limité d'utilisateurs qui disposent déjà de l'application sur leur machine utilisateur.
- Le VDA ne peut pas accéder à certains sites Web (par exemple, des sites Web internes à une autre organisation).

Conformité :

Vous pouvez utiliser la redirection hôte vers client pour des raisons de conformité dans les cas d'utilisation suivants :

- Le contrat de licence de l'application ou du contenu ne permet pas la publication par le VDA.
- La stratégie d'organisation n'autorise pas le chargement d'un document vers le VDA.

Certaines situations sont plus probables dans des environnements complexes et également si la machine utilisateur et le VDA appartiennent à différentes organisations.

Considérations sur la machine utilisateur

Les environnements peuvent comporter différents types de machines utilisateur.

Machine utilisateur	Situation ou environnement	Approche de redirection de contenu
Tablette	-	Toute approche (voir le tableau suivant)
Ordinateur portable	-	Toute approche (voir le tableau suivant)
Desktop PC	Les utilisateurs utilisent un large éventail d'applications installées sur la machine utilisateur	Toute approche (voir le tableau suivant)

Machine utilisateur	Situation ou environnement	Approche de redirection de contenu
Desktop PC	Les utilisateurs utilisent uniquement quelques applications connues installées sur la machine utilisateur	Local App Access
Desktop PC	Les utilisateurs n'utilisent aucune application installée sur la machine utilisateur	Redirection multimédia et/ou redirection Flash
Ordinateur de bureau	Le fournisseur prend en charge la redirection multimédia et/ou la redirection Flash	Redirection multimédia et/ou redirection Flash
Client fin	Le fournisseur prend en charge la redirection multimédia, la redirection Flash et la redirection hôte vers client	Toute approche (voir le tableau suivant)
Zéro client	Le fournisseur prend en charge la redirection multimédia et/ou la redirection Flash	Redirection multimédia et/ou redirection Flash

Utilisez les exemples suivants pour vous aider à choisir votre méthode de redirection de contenu.

Lien URL	Situation ou environnement	Approche de redirection de contenu
Document ou page Web	Le VDA ne peut pas accéder à l'URL	Redirection hôte vers client
Page Web	La page Web contient Adobe Flash	Redirection Flash
Flux ou fichier multimédia	Le VDA est doté d'un lecteur multimédia compatible	Redirection multimédia
Flux ou fichier multimédia	Le VDA n'est pas doté d'un lecteur multimédia compatible	Redirection hôte vers client

Lien URL	Situation ou environnement	Approche de redirection de contenu
Document	Le VDA ne dispose pas d'application pour ce type de document	Redirection hôte vers client
Document	Ne pas télécharger le document sur la machine utilisateur	Aucune redirection
Document	Ne pas charger le document sur le VDA	Redirection hôte vers client
Type d'URL personnalisée	Le VDA ne dispose pas d'application pour ce type d'adresse URL personnalisée	Redirection hôte vers client

Citrix Receiver pour Windows, Citrix Receiver pour Mac, Citrix Receiver pour Linux, Citrix Receiver pour HTML5 et Citrix Receiver pour Chrome prennent en charge la redirection hôte vers client.

Pour utiliser la redirection hôte vers client, la machine utilisateur doit disposer d'un navigateur Web, d'un lecteur multimédia ou d'une autre application qui convient pour le contenu. Si la machine utilisateur est un ordinateur de bureau, un client léger ou un client zéro, vérifiez qu'elle dispose des applications appropriées et qu'elle est suffisamment puissante.

Les machines utilisateur activées pour Local App Access utilisent un autre mécanisme pour la redirection de contenu, et ne requièrent pas la redirection de contenu hôte vers client.

Vous pouvez utiliser les stratégies Citrix pour empêcher la redirection de contenu hôte vers client pour les machines inadaptées.

Expérience des utilisateurs avec la redirection hôte vers client

La redirection hôte vers client est utilisée lorsque les adresses URL sont :

- intégrées en tant que liens hypertexte dans une application (par exemple, dans un message électronique ou un document) ;
- sélectionnées via les menus ou les boîtes de dialogue d'une application VDA, à condition que l'application utilise l'API Windows ShellExecuteEx ;
- tapées dans la boîte de dialogue Exécuter.

La redirection hôte vers client n'est pas utilisée pour les URL dans un navigateur Web (dans une page Web ou tapées dans la barre d'adresses du navigateur Web).

> **Remarque**
>
> Si les utilisateurs changent leur navigateur Web par défaut sur le VDA (par exemple, à l'aide de l'option Choisir les programmes par défaut), cette modification peut interférer avec la redirection hôte vers client pour les applications.

Lorsque la redirection de contenu hôte vers client est activée, l'application qui est ouvre l'URL dépend de la configuration de la machine utilisateur pour le type d'adresse URL et le type de contenu. Par exemple :

- Une URL HTTP avec un type de contenu HTML s'ouvre dans le navigateur Web par défaut.
- Une URL HTTP avec un type de contenu PDF peut s'ouvrir dans le navigateur Web par défaut, ou dans une autre application.

La redirection de contenu hôte vers client ne contrôle pas cette configuration de machine utilisateur. Si vous ne contrôlez pas la configuration de la machine utilisateur, vous pouvez utiliser la redirection Flash et la redirection multimédia, plutôt que la redirection de contenu hôte vers client.

Les types d'adresse URL suivants sont ouverts localement sur les machines utilisateur lorsque la redirection hôte vers client est activée :

- HTTP (Hypertext Transfer Protocol) ;
- HTTPS (Secure Hypertext Transfer Protocol) ;
- RTSP (Real Player et QuickTime) ;
- RTSPU (Real Player et QuickTime) ;
- PNM (ancienne version de Real Player) ;
- MMS (format multimédia de Microsoft).

Vous pouvez modifier la liste des types d'URL pour la redirection hôte vers client, supprimer et ajouter des types d'adresse URL, notamment les types d'adresse URL personnalisée.

Activer la redirection hôte vers client

L'activation de la redirection hôte vers client commence par l'activation d'un paramètre de stratégie Citrix.

Le paramètre de stratégie Redirection hôte vers client est situé dans la section Paramètres de stratégie de la redirection de fichier. Par défaut, ce paramètre est désactivé.

En outre, il peut être nécessaire de définir des clés de registre et une stratégie de groupe pour les VDA de serveur, en fonction du système d'exploitation du VDA.

- Si le VDA de serveur est Windows Server 2008 R2 SP1, vous n'avez pas besoin de définir les clés de registre ou la stratégie de groupe.
- Si le VDA de serveur est Windows Server 2012, Windows Server 2012 R2 ou Windows Server 2016, vous devez définir les clés de registre et la stratégie de groupe.

> **Avertissement**
>
> Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Modifications du registre

1. Copiez le texte entre « **Reg file start** » et « **Reg file end** » ci-dessous et collez-le dans Bloc-notes.
2. Enregistrez le fichier Bloc-notes avec **Enregistrer sous**, le type **Tous les fichiers** et le nom **ServerFTA.reg**.
3. Distribuez le fichier **ServerFTA.reg** aux serveurs à l'aide de la stratégie de groupe Active Directory.

```
--  Reg file start --

Éditeur de registre Windows version 5.00


[HKEY_CLASSES_ROOT\ServerFTAHTML\shell\open\command]

@="\"C:\\Program Files (x86)\\Citrix\\system32\\iexplore.exe\" %1"


[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ServerFTA]

@="ServerFTA"


[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ServerFTA\Capabilities]

"ApplicationDescription"="Server FTA URL."

"ApplicationIcon"="C:\\Program Files (x86)\\Citrix\\system32\\iexplore.
   exe,0"

"ApplicationName"="ServerFTA"


```



```
[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ServerFTA\Capabilities\
    URLAssociations]

"http"="ServerFTAHTML"

"https"="ServerFTAHTML"



[HKEY_LOCAL_MACHINE\SOFTWARE\RegisteredApplications]

"Citrix.ServerFTA"="SOFTWARE\\Citrix\\ServerFTA\\Capabilities"

-- Reg file end -- ---
```

Modifications de la stratégie de groupe

Créez un fichier XML. Copiez le texte entre **xml file start** et **xml file end** dans l'exemple, collez-le dans le fichier XML, puis enregistrez-le sous **ServerFTAdefaultPolicy.xml**.

```
-- xml file start --

<?xml version="1.0" encoding="UTF-8"?>

<DefaultAssociations>

<Association Identifier="http" ProgId="ServerFTAHTML" ApplicationName="
    ServerFTA" />

<Association Identifier="https" ProgId="ServerFTAHTML" ApplicationName=
    "ServerFTA" />

</DefaultAssociations>

-- xml file end -- ---
```

Depuis la Console de gestion des stratégies de groupe actuelle, accédez à : **Configuration ordinateur** > **Modèles d'administration** > **Composants Windows** > **Explorateur de fichiers** > **Définir un fichier de configuration des associations par défaut** et fournissez le fichier ServerFTAdefaultPolicy.xml que vous avez créé.

Modifier la liste des types d'URL pour la redirection hôte vers client

Pour modifier la liste des types d'URL pour la redirection hôte vers client, définissez la clé de registre suivante sur le VDA de serveur.

Clé : HKLM\Software\Wow6432Node\Citrix\SFTA

Pour supprimer des types d'adresse URL de la liste, définissez DisableServerFTA et NoRedirectClasses :

Nom : DisableServerFTA

Type : REG_DWORD

Données : 1

Nom : NoRedirectClasses
Type : REG_MULTI_SZ
Données : spécifiez une combinaison de ces valeurs : http, https, rtsp, rtspu, pnm ou mms. Tapez les valeurs multiples sur des lignes distinctes. Par exemple :

http

https

rtsp

Pour ajouter des types d'adresse URL à la liste, définissez ExtraURLProtocols :

Nom : ExtraURLProtocols

Type : REG_MULTI_SZ

Données : spécifiez toute combinaison de types d'URL. Chaque type d'URL doit inclure le suffixe :// ; séparez les valeurs multiples par des points-virgules. Par exemple :

customtype1://;customtype2://

Activer la redirection hôte vers client pour un ensemble spécifique de sites Web

Pour activer la redirection hôte vers client pour un ensemble spécifique de sites Web, définissez la clé de registre suivante sur le VDA de serveur.

Clé : HKLM\Software\Wow6432Node\Citrix\SFTA

Nom : ValidSites

Type : REG_MULTI_SZ

Données : spécifiez toute combinaison de noms de domaine complet (FQDN). Tapez les noms de domaine complets sur des lignes distinctes. Un nom de domaine complet peut inclure un caractère

générique à la position la plus à gauche. Cela correspond à un seul niveau de domaine, ce qui est compatible avec les règles définies dans RFC 6125. Par exemple :

```
www.example.com
```

```
*.example.com
```

Local App Access et redirection d'adresse URL

January 23, 2019

Introduction

Local App Access s'intègre en toute transparence avec les applications Windows installées localement dans un environnement de bureau hébergé sans passer d'un ordinateur à l'autre. Avec Local App Access, vous pouvez :

- Accédez aux applications installées localement sur un ordinateur portable, un PC ou tout autre périphérique physique directement à partir de votre bureau virtuel.
- Fournir une solution de mise à disposition d'applications flexible. Si les utilisateurs possèdent des applications locales que vous ne pouvez pas virtualiser ou qui ne sont pas gérées par le département informatique, ces applications se comporteront toujours comme si elles étaient installées sur un bureau virtuel.
- Éliminez la latence double-hop lorsque les applications sont hébergées séparément du bureau virtuel en plaçant le raccourci vers l'application publiée sur la machine Windows de l'utilisateur.
- Utiliser des applications telles que :
  - Logiciels de conférence vidéo tels que GoToMeeting.
  - Applications de niche ou spécialisées qui ne sont pas encore virtualisées.
  - Les applications et périphériques qui transfèrent des quantités très importantes de données depuis une machine utilisateur vers un serveur et à nouveau vers la machine utilisateur, comme les graveurs de DVD et les tuners TV.

Dans XenApp et XenDesktop, les sessions de bureau hébergées utilisent la redirection d'URL pour lancer les applications Local Access App. La redirection d'URL met l'application à disposition sous plusieurs adresses URL. Elle lance un navigateur local (en fonction de la liste noire d'adresses URL de votre navigateur) en cliquant sur des liens intégrés dans un navigateur dans une session de bureau. Si vous accédez à une URL qui n'est pas présente dans la liste noire, l'adresse URL est ouverte dans la session de bureau.

La redirection d'adresse URL ne fonctionne que pour les sessions de bureau, pas les sessions d'application. La seule fonctionnalité de redirection que vous pouvez utiliser pour des sessions d'application est la redirection de contenu hôte vers client, qui est un type de redirection de FTA

(Association de type de fichier) serveur. Cette FTA redirige certains protocoles vers le client, tels que http, https, rtsp ou mms. Par exemple, si vous voulez ouvrir uniquement des liens avec http, les liens s'ouvrent directement avec l'application cliente. Il n'y a aucune liste noire ou blanche d'adresses URL de prise en charge.

Lorsque Local App Access est activé pour les bureaux hébergés, les adresses URL qui sont affichées pour les utilisateurs en tant que liens depuis des applications exécutées localement, depuis les applications hébergées par l'utilisateur ou en tant que raccourcis sur le bureau sont redirigées de l'une des manières suivantes :

- À partir de l'ordinateur de l'utilisateur vers le bureau hébergé
- À partir du serveur XenApp vers l'ordinateur de l'utilisateur
- Restitué dans l'environnement dans lequel ils sont lancés (et non pas redirigés)

Pour spécifier le chemin d'accès de redirection du contenu de sites Web spécifiques, configurez la liste blanche et la liste noire d'adresses URL sur Virtual Delivery Agent. Ces listes contiennent des clés de Registre de chaînes multiples qui spécifient les paramètres de stratégie de redirection d'URL ; pour de plus amples informations, consultez la section Paramètres de stratégie Local App Access.

Les adresses URL peuvent être restituées sur le VDA avec les exceptions suivantes :

- Informations géographiques et relatives aux paramètres régionaux : sites Web qui requièrent des informations sur les paramètres régionaux, telles que msn.com ou news.google.com (ouvre une page spécifique au pays en fonction de l'emplacement géographique). À titre d'exemple, si le VDA est provisionné à partir d'un centre de données situé au Royaume-Uni et que le client se connecte depuis l'Inde, l'utilisateur s'attend à voir in.msn.com mais voit uk.msn.com.
- Contenu multimédia : les sites Web contenant du contenu multimédia riche, lorsqu'ils sont restitués sur la machine cliente, offrent aux utilisateurs une expérience native et permettent d'économiser la bande passante même dans les réseaux à latence élevée. Bien qu'il existe une fonctionnalité de redirection Flash, ceci effectue un complément en redirigeant les sites avec d'autres types multimédia comme Silverlight. Ceci est dans un environnement ultra sécurisé. En effet, les URL qui sont approuvées par l'administrateur sont exécutées sur la machine cliente tandis que le reste des URL sont redirigées vers le VDA.

En plus de la redirection d'URL, vous pouvez également utiliser la redirection FTA. L'association de types de fichier lance des applications locales lorsqu'un fichier est détecté dans la session. Si l'application locale est lancée, elle doit avoir accès au fichier pour l'ouvrir. Par conséquent, vous pouvez uniquement ouvrir des fichiers qui résident sur des partages réseau ou sur des lecteurs clients (avec CDM) à l'aide d'applications locales. Par exemple, lors de l'ouverture d'un fichier PDF, si un lecteur PDF est une application locale, le fichier s'ouvre à l'aide de ce lecteur PDF. Étant donné que l'application locale peut accéder au fichier directement, il n'y a pas de transfert réseau du fichier via ICA pour ouvrir ce dernier.

Configuration requise, considérations et limitations à prendre en compte

Local App Access est pris en charge sur les systèmes d'exploitation compatibles avec les VDA pour OS de serveur Windows et les VDA pour OS de bureau Windows, et requiert Citrix Receiver pour Windows version 4.1 (minimum). Les navigateurs Web pris en charge sont les suivants :

- Internet Explorer 11 Vous pouvez utiliser Internet Explorer versions 8, 9 ou 10, mais Microsoft prend en charge la version 11 (et Citrix vous recommande d'utiliser cette version).
- Firefox 3.5 à 21.0
- Chrome 10

Vérifiez les informations et les limitations suivantes lors de l'utilisation de Local App Access et de la redirection d'adresse URL.

- Local App Access est uniquement conçu pour les bureaux virtuels en mode plein écran couvrant tous les moniteurs comme suit :
  - L'expérience utilisateur pourrait prêter à confusion si Local App Access est utilisé avec un bureau virtuel qui s'exécute en mode fenêtre ou ne couvre pas tous les moniteurs.
  - Pour les utilisateurs équipés de plusieurs moniteurs, si un moniteur est agrandi, il devient le bureau par défaut pour toutes les applications lancées dans cette session, même si les applications suivantes sont lancées généralement sur l'autre moniteur.
  - Cette fonctionnalité prend en charge un VDA ; il n'y a pas d'intégration avec plusieurs VDA simultanés.
- Certaines applications peuvent se comporter de manière inattendue et affecter les utilisateurs :
  - Les utilisateurs risquent d'être déroutés par les lettres de lecteur, telles que C: local plutôt que le lecteur C: du bureau virtuel.
  - Les imprimantes disponibles dans le bureau virtuel ne sont pas disponibles pour les applications locales.
  - Les applications qui nécessitent des autorisations élevées ne peuvent pas être lancées en tant qu'applications hébergées sur le client.
  - Aucun traitement spécial pour les applications à instance unique (telles que le Lecteur Windows Media).
  - Les applications locales s'affichent avec le thème Windows de la machine locale.
  - Les applications en plein écran ne sont pas prises en charge. Cela inclut les applications qui s'ouvrent en plein écran, telles que des diaporamas PowerPoint, ou les visionneuses de photos couvrant la totalité du bureau.
  - Local App Access copie les propriétés de l'application locale (telles que les raccourcis sur le bureau et le menu Démarrer du client) sur le VDA ; cependant, il ne copie pas les autres propriétés, telles que les touches de raccourci et les attributs en lecture seule.
  - Les applications qui permettent de personnaliser la manière dont est géré le chevauchement des fenêtres peuvent avoir des résultats imprévisibles. Par exemple, certaines

fenêtres peuvent être masquées.
  - Les raccourcis ne sont pas pris en charge, y compris Ordinateur, Corbeille, Panneau de configuration, les raccourcis du lecteur réseau et les raccourcis de dossiers.
  - Les types de fichiers et fichiers suivants ne sont pas pris en charge : types de fichiers personnalisés, fichiers sans programmes associés, fichiers zippés et fichiers masqués.
  - Le regroupement de la barre des tâches n'est pas pris en charge pour les applications mixtes 32 bits et 64 bits hébergées sur le client ou le VDA, telles que le regroupement d'applications locales 32 bits avec des applications VDA 64 bits.
  - Les applications ne peuvent pas être lancées à l'aide de COM. Par exemple, si vous cliquez sur un document Office incorporé à une application Office, le lancement du processus ne peut pas être détecté et l'intégration de l'application locale échoue.
- Les scénarios double-hop, dans lesquels un utilisateur démarre un bureau virtuel à partir d'une autre session de bureau virtuel, ne sont pas pris en charge.
- La redirection d'URL prend uniquement en charge les adresses URL explicites (c'est-à-dire, celles qui apparaissant dans la barre d'adresse du navigateur ou celles détectées à l'aide de la barre de navigation du navigateur, selon le navigateur spécifique).
- La redirection d'adresses URL fonctionne uniquement avec les sessions de bureau, et non pas avec les sessions d'application.
- Le dossier du bureau local dans une session VDA n'autorise pas les utilisateurs à créer de nouveaux fichiers.
- Plusieurs instances d'une application exécutée localement se comportent conformément aux paramètres de barre des tâches établis pour le bureau virtuel. Les raccourcis vers des applications exécutées localement ne sont pas regroupés avec les instances en cours d'exécution de ces applications. Ils sont également non groupés avec les instances en cours d'exécution des applications hébergées ou les raccourcis épinglés pour les applications hébergées. Les utilisateurs ne peuvent fermer les fenêtres des applications exécutées localement qu'à partir de la barre des tâches. Bien que les utilisateurs puissent épingler les fenêtres d'applications locales à la barre des tâches et au menu Démarrer, les applications risquent de ne pas fonctionner de manière cohérente lors de l'utilisation de ces raccourcis.

Interaction avec Windows

L'interaction de Local App Access avec Windows comprend les comportements suivants.

- Comportement des raccourcis de Windows 8 et Windows Server 2012
  - Les applications Windows Store installées sur le client ne sont pas énumérées comme faisant partie des raccourcis Local App Access.
  - Les fichiers image et vidéo sont généralement ouverts par défaut à l'aide des applications du Windows Store. Toutefois, Local App Access énumère les applications du Windows Store et ouvre les raccourcis avec les applications du bureau.

- Programmes locaux
  - Pour Windows 7, le dossier est disponible dans le menu Démarrer.
  - Pour Windows 8, Programmes locaux est disponible uniquement lorsque l'utilisateur choisit **Toutes les applications** comme catégorie dans l'écran de démarrage. Les sous-dossiers ne sont pas tous affichés dans Programmes locaux.
- Fonctionnalités graphiques Windows 8 pour les applications
  - Les applications de bureau sont limitées à la zone de bureau et sont couvertes par l'écran d'accueil et les applications de style Windows 8.
  - Les applications Local App Access ne se comportent pas comme des applications de bureau en mode multi-écrans. En mode multi-écrans, l'écran d'accueil et le bureau s'affichent sur des moniteurs différents.
- Windows 8 et la redirection d'URL Local App Access
  - Étant donné que Windows 8 n'a aucun module complémentaire Internet Explorer activé, utilisez Internet Explorer sur le bureau pour activer la redirection d'adresse URL.
  - Dans Windows Server 2012, Internet Explorer désactive les modules complémentaires par défaut. Pour implémenter la redirection d'adresse URL, désactivez la configuration renforcée d'Internet Explorer. Réinitialisez ensuite les options d'Internet Explorer et redémarrez pour vous assurer que les modules complémentaires sont activés pour les utilisateurs standards.

Configurer Local App Access et la redirection d'adresse URL

Pour utiliser Local App Access et la redirection d'adresse URL à l'aide de Citrix Receiver :

- Installez Citrix Receiver sur la machine cliente locale. Vous pouvez activer les fonctionnalités lors de l'installation de Citrix Receiver ou vous pouvez activer le modèle Local App Access à l'aide de l'éditeur de stratégie de groupe.
- Définissez le paramètre de stratégie **Autoriser Local App Access** sur **Activé**. Vous pouvez également configurer les paramètres de stratégie de la liste blanche et la liste noire d'adresses URL pour la redirection d'adresses URL. Pour de plus amples informations, consultez la section Paramètres de stratégie Local App Access.

Activer Local App Access et la redirection d'adresses URL lors de l'installation de Citrix Receiver

Pour activer Local App Access et la redirection d'adresse URL pour toutes les applications locales :

1. Définissez le paramètre de stratégie **Autoriser Local App Access** sur **Activé**. Lorsque ce paramètre est activé, le VDA permet au client de décider si les raccourcis publiés par l'administrateur ou les raccourcis Local App Access sont activés dans la session. (Lorsque ce

paramètre est désactivé, les applications publiées par l'administrateur et les raccourcis Local App Access ne fonctionnent pas pour le VDA.) Ce paramètre de stratégie s'applique à la totalité de la machine, ainsi que la stratégie de redirection d'URL.

2. Activez Local App Access et la redirection d'adresses URL lors de l'installation de Citrix Receiver pour tous les utilisateurs d'une machine. Cette action enregistre également les modules complémentaires du navigateur requis pour la redirection d'adresses URL. À partir de l'invite de commandes, exécutez la commande appropriée pour installer Receiver avec l'option suivante :

   CitrixReceiver.exe /ALLOW_CLIENTHOSTEDAPPSURL=1

   CitrixReceiverWeb.exe /ALLOW_CLIENTHOSTEDAPPSURL=1

Pour activer le modèle Local App Access à l'aide de l'éditeur de stratégie de groupe

1. Exécutez **gpedit.msc**.
2. Sélectionnez la **configuration de l'ordinateur**. Cliquez avec le bouton droit de la souris sur **Modèles d'administration** et sélectionnez**Ajout/suppression de modèles > Ajouter**.
3. Ajoutez le modèle icaclient.adm se trouvant dans le dossier de Citrix Receiver Configuration (généralement dans c:\Program Files (x86)\Citrix\Online Plugin\Configuration). (Une fois le modèle icaclient.adm ajouté à la configuration de l'ordinateur, il est également disponible dans la configuration de l'utilisateur.)
4. Développez **Modèles d'administration > Modèles d'administration classiques (ADM) > Composants Citrix > Citrix Receiver > Expérience de l'utilisateur**.
5. Sélectionnez les **paramètres Local App Access**.
6. Sélectionnez **Activé** puis sélectionnez **Autoriser la redirection d'URL**. Pour la redirection d'adresse URL, enregistrez les modules complémentaires de navigateur à l'aide de la ligne de commande, comme décrit ci-dessous.

Fournir uniquement l'accès aux applications publiées

Pour fournir l'accès aux applications publiées uniquement :

1. Sur le serveur sur lequel le Delivery Controller est installé, exécutez **regedit.msc**.
   a) Naviguez jusqu'à HKLM\Software\Wow6432Node\Citrix\DesktopStudio.
   b) Ajoutez l'entrée ClientHostedAppsEnabled de REG_DWORD avec une valeur de 1. (Une valeur 0 désactive Local App Access).
2. Redémarrez le serveur Delivery Controller, puis redémarrez Studio.
3. Publiez les applications Local App Access.
   a) Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio, puis sélectionnez l'onglet Applications.
   b) Sélectionnez **Créer une application d'accès local** dans le volet Actions.

c) Sélectionnez le groupe de mise à disposition de bureaux.
d) Entrez le chemin d'accès complet de l'exécutable de l'application sur la machine locale de l'utilisateur.
e) Indiquez si le raccourci vers l'application locale sur le bureau virtuel sera visible dans le menu Démarrer, sur le bureau ou les deux.
f) Acceptez les valeurs par défaut sur la page Nom, puis vérifiez les paramètres.

4. Activez Local App Access et la redirection d'adresses URL lors de l'installation de Citrix Receiver pour tous les utilisateurs d'une machine. Cette action enregistre également les modules complémentaires du navigateur requis pour la redirection d'adresses URL. À partir de l'invite de commandes, exécutez la commande pour installer Citrix Receiver avec l'option suivante :
CitrixReceiver.exe /ALLOW_CLIENTHOSTEDAPPSURL=1
CitrixReceiverWeb.exe /ALLOW_CLIENTHOSTEDAPPSURL=1
5. Définissez le paramètre de stratégie **Autoriser Local App Access** sur **Activé**. Lorsque ce paramètre est activé, le VDA permet au client de décider si les raccourcis publiés par l'administrateur ou les raccourcis Local App Access sont activés dans la session. (Lorsque ce paramètre est désactivé, les applications publiées par l'administrateur et les raccourcis Local App Access ne fonctionnent pas pour le VDA.)

Enregistrer les modules complémentaires du navigateur

> **Remarque :**
>
> les modules complémentaires du navigateur requis pour la redirection d'adresse URL ne sont pas enregistrés automatiquement lorsque vous installez Citrix Receiver à partir de la ligne de commande avec l'option /ALLOW_CLIENTHOSTEDAPPSURL=1.

Vous pouvez utiliser les commandes suivantes pour enregistrer et annuler l'enregistrement d'un ou de plusieurs modules complémentaires :

- Pour enregistrer les composants sur une machine cliente : <*dossier-installation-client*>\redirector.exe /reg<*navigateur*>.
- Pour annuler l'enregistrement des composants sur une machine cliente : <*dossier-installation-client*>\redirector.exe /unreg<*navigateur*>.
- Pour enregistrer les composants sur un VDA :<*dossier-VDAinstallation*> \VDARedirector.exe /reg<*navigateur*>
- Pour annuler l'enregistrement des composants sur un VDA :<*dossier-VDAinstallation*> \VDARedirector.exe /unreg<*navigateur*>

où <*navigateur*> est IE, FF, Chrome ou tous.

Par exemple, la commande suivante enregistre les composants Internet Explorer sur une machine exécutant Citrix Receiver.

C:\Program Files\Citrix\ICA Client\redirector.exe/regIE

La commande suivante enregistre tous les composants d'un VDA avec OS Windows Server.

C:\Program Files (x86)\Citrix\System32\VDARedirector.exe /regAll

Interception d'adresses URL dans les navigateurs

- Par défaut, Internet Explorer redirige l'adresse URL entrée. Si l'adresse URL ne figure pas dans la liste noire mais est redirigée vers une autre adresse URL par le navigateur ou un site Web, l'adresse URL finale n'est pas redirigée, même si elle est présente dans la liste noire.

  Pour que la redirection d'adresse URL fonctionne correctement, activez le module complémentaire lorsque vous y êtes invité par le navigateur. Si les modules complémentaires utilisant les options Internet ou les modules complémentaires dans l'invite de commande sont désactivés, la redirection d'adresse URL ne fonctionne pas correctement.

- Les modules complémentaires Firefox redirigent toujours les adresses URL.

  Lorsqu'un module complémentaire est installé, Firefox vous invite à autoriser/empêcher l'installation du module complémentaire dans un nouvel onglet. Vous devez autoriser le module complémentaire pour que la fonctionnalité fonctionne.

- Le module complémentaire Chrome redirige toujours l'adresse URL finale qui est ouverte et non pas les adresses URL saisies.

  Les extensions ont été installées en externe. Si vous désactivez l'extension, la fonctionnalité de redirection d'adresse URL ne fonctionne pas dans Chrome. Si la redirection d'adresse URL est requise en mode Incognito, autorisez l'exécution de l'extension dans ce mode dans la page de paramètres du navigateur.

Configurer le comportement de l'application locale lors de la fermeture de session et de la déconnexion

1. Sur le bureau hébergé, exécutez **gpedit.msc**.
2. Naviguez jusqu'à HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Client Hosted Apps\Policies\Session State. Pour un système 64 bits, naviguez jusqu'à HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Citrix\C Hosted Apps\Policies\Session State.
3. Ajoutez l'entrée Terminate de REG_DWORD avec l'une des valeurs suivantes :
   - 1 : les applications locales continuent de s'exécuter lorsqu'un utilisateur ferme sa session ou se déconnecte de l'ordinateur virtuel. Lors de la reconnexion, les applications locales sont réintégrées si elles sont disponibles dans le bureau virtuel.
   - 3 : les applications locales se ferment lorsqu'un utilisateur ferme sa session ou se déconnecte de l'ordinateur virtuel.

Considérations USB et lecteur client

January 23, 2019

La technologie HDX offre une **prise en charge optimisée** pour la plupart des périphériques USB populaires, Parmi lesquelles :

- Moniteurs
- Souris
- Claviers
- Téléphones VoIP
- Casques
- Webcams
- Scanners
- Appareils photo
- Imprimantes
- Lecteurs
- Lecteurs de cartes à puce
- Tablettes graphiques
- Dispositifs de signature

La prise en charge optimisée offre une meilleure expérience utilisateur avec de meilleures performances et une bande passante plus efficace via un réseau étendu. La prise en charge optimisée est généralement la meilleure option, notamment dans les environnements à latence élevée ou avec des exigences de sécurité strictes.

La technologie HDX offre la **redirection USB générique** pour les périphériques spécialisés dont la prise en charge n'est pas optimisée ou n'est pas adaptée, par exemple :

- Le périphérique USB est doté d'autres fonctionnalités avancées ne faisant pas partie de la prise en charge optimisée, telles qu'une souris ou une webcam avec des boutons supplémentaires.
- Les utilisateurs ont besoin de fonctionnalités qui ne font pas partie de la prise en charge optimisée, telles que la gravure d'un CD.
- Le périphérique USB est un périphérique spécialisé, tel qu'un équipement de test et de mesure ou un contrôleur industriel.
- Une application requiert un accès direct au périphérique USB.
- Un seul pilote Windows est disponible pour le périphérique USB. Par exemple, un lecteur de carte à puce peut ne pas avoir de pilote pour Citrix Receiver pour Android.
- La version de Citrix Receiver n'offre pas de prise en charge optimisée pour ce type de périphérique USB.

Avec la redirection USB générique :

- Il n'est pas nécessaire pour les utilisateurs d'installer des pilotes de périphériques sur la machine

utilisateur.

- Les pilotes clients USB sont installés sur la machine VDA.

> **Remarque**
>
> - La redirection USB générique peut être utilisée conjointement avec la prise en charge optimisée. Si vous activez la redirection USB générique, configurez les paramètres de stratégie des périphériques USB Citrix pour la redirection USB générique et la prise en charge optimisée afin d'éviter un comportement incohérent et inattendu.
> - Le paramètre de stratégie Citrix Règles d'optimisation de périphérique USB client est un paramètre spécifique pour la redirection USB générique, pour un type de périphérique USB spécifique. Il ne s'applique pas à la prise en charge optimisée comme indiqué ici.
> - Redirection de périphérique Plug and Play USB client est une fonctionnalité liée qui fournit une prise en charge optimisée pour les périphériques tels que les appareils photo et les lecteurs multimédia qui utilisent le protocole PTP ou MTP. La redirection Plug and Play USB client ne fait pas partie de la redirection USB générique. La redirection Plug and Play USB client est disponible sur les OS de bureau uniquement.

Considérations sur les performances pour les périphériques USB

Avec la redirection USB générique, pour certains types de périphériques USB, la latence et la bande passante réseau peuvent affecter l'expérience utilisateur et le fonctionnement du périphérique USB. Par exemple, les périphériques soumis à des contraintes de temps risquent de ne pas fonctionner correctement avec des liens à faible bande passante et latence élevée. Utilisez la prise en charge optimisée autant que possible.

Certains périphériques USB requièrent une bande passante élevée pour être utilisables, par exemple une souris 3D (utilisée avec des applications 3D qui requièrent également une bande passante élevée en général). Vous pouvez éviter les problèmes de performances à l'aide de stratégies Citrix. Pour de plus amples informations, consultez la section Paramètres de stratégie de bande passante pour la redirection de périphérique USB client et Paramètres de stratégie Connexions Multi-Stream.

Considérations sur la sécurité pour les périphériques USB

Certains périphériques USB sont sécurisés par nature, par exemple, les lecteurs de carte à puce, les lecteurs d'empreintes digitales et les dispositifs de signature numérique. D'autres périphériques USB tels que les périphériques de stockage USB peuvent être utilisés pour transmettre des données qui peuvent être confidentielles.

Les périphériques USB sont souvent utilisés pour distribuer des logiciels malveillants. La configuration de Citrix Receiver, XenApp et XenDesktop peut réduire, mais pas éliminer, le risque lié à ces périphériques USB, que vous utilisiez la redirection USB générique ou la prise en charge optimisée.

> **Important**
>
> Pour les périphériques et les données sensibles, sécurisez toujours la connexion HDX à l'aide de TLS ou d'IPSec.
>
> Activez uniquement la prise en charge pour les périphériques USB dont vous avez besoin. Configurez à la fois la redirection USB générique et la prise en charge optimisée pour répondre à ce besoin.
>
> Fournissez des instructions aux utilisateurs pour qu'ils utilisent les périphériques USB en toute sécurité : utiliser uniquement des périphériques USB qui ont été obtenus auprès d'une source de confiance ; ne pas laisser les périphériques USB sans surveillance dans des environnements publics, un lecteur flash dans un cybercafé par exemple ; expliquer les risques liés à l'utilisation d'un périphérique USB sur plusieurs ordinateurs.

Compatibilité avec la redirection USB générique

La redirection USB générique est prise en charge pour les périphériques USB 2.0 et versions antérieures. La redirection USB générique est également prise en charge pour les périphériques USB 3.0 connectés à un port USB 2.0 ou USB 3.0. La redirection USB générique ne prend pas en charge les fonctionnalités USB introduites dans USB 3.0, telles que la vitesse.

Ces types de Citrix Receiver prennent en charge la redirection USB générique :

- Citrix Receiver pour Windows, voir Configuration de la prise en charge USB
- Citrix Receiver pour Mac, consultez la section Configuration de Citrix Receiver pour Mac
- Citrix Receiver pour Linux, consultez la section Optimiser
- Citrix Receiver pour Chrome OS, voir Nouveautés

Pour les versions de Citrix Receiver, reportez-vous au tableau des fonctionnalités de Citrix Receiver.

Si vous utilisez des versions antérieures de Citrix Receiver, reportez-vous à la documentation relative à Citrix Receiver afin de vérifier que la redirection USB générique est prise en charge. Reportez-vous à la documentation de Citrix Receiver pour connaître les restrictions sur les types de périphériques USB qui sont pris en charge.

La redirection USB générique est prise en charge pour les sessions de bureau à compter de VDA pour OS de bureau version 7.6 jusqu'à la version actuelle.

La redirection USB générique est prise en charge pour les sessions de bureau à compter de VDA pour OS de serveur version 7.6 jusqu'à la version actuelle, avec les restrictions suivantes :

- Le VDA doit exécuter Windows Server 2012 R2 ou Windows Server 2016.
- Seuls les scénarios à relais unique (single-hop) sont pris en charge. La redirection périphérique USB générique double-hop n'est pas prise en charge pour les sessions d'application hébergée de bureau.

- Les pilotes de périphérique USB doivent être entièrement compatibles avec Remote Desktop Session Host (RDSH) pour Windows 2012 R2, y compris la prise en charge complète de la virtualisation.

Certains types de périphériques USB ne sont pas pris en charge pour la redirection USB générique, car il n'est pas nécessaire de les rediriger :

- Modems USB.
- Cartes réseau USB.
- Concentrateurs USB. Les périphériques USB connectés à des concentrateurs USB sont gérés individuellement.
- Ports COM virtuels USB. Utilisez la redirection du port COM, plutôt que la redirection USB générique.

Pour de plus amples informations sur les périphériques USB qui ont été testés avec la redirection USB générique, veuillez consulter l'article CTX123569. Certains périphériques USB ne fonctionnent pas correctement avec la redirection USB générique.

Configurer la redirection USB générique

Vous pouvez contrôler les types de périphériques USB qui utilisent la redirection USB générique. Ce paramètre peut être configuré séparément :

- Sur le VDA, à l'aide des paramètres de stratégie Citrix. Pour de plus amples informations, consultez la section Redirection des lecteurs clients et de machines utilisateur et Paramètres de stratégie Périphériques USB dans la section Référence des paramètres de stratégie
- Dans Citrix Receiver, à l'aide de mécanismes liés à Citrix Receiver. À titre d'exemple, Citrix Receiver pour Windows est configuré avec des paramètres de registre qui peuvent être contrôlés par un modèle d'administration. Par défaut, la redirection USB est autorisée pour certaines classes de périphériques USB et refusée pour d'autres ; pour de plus amples informations, consultez la section Configuration de la prise en charge USB dans la documentation Citrix Receiver pour Windows.

Cette configuration séparée fournit une plus grande flexibilité. Par exemple :

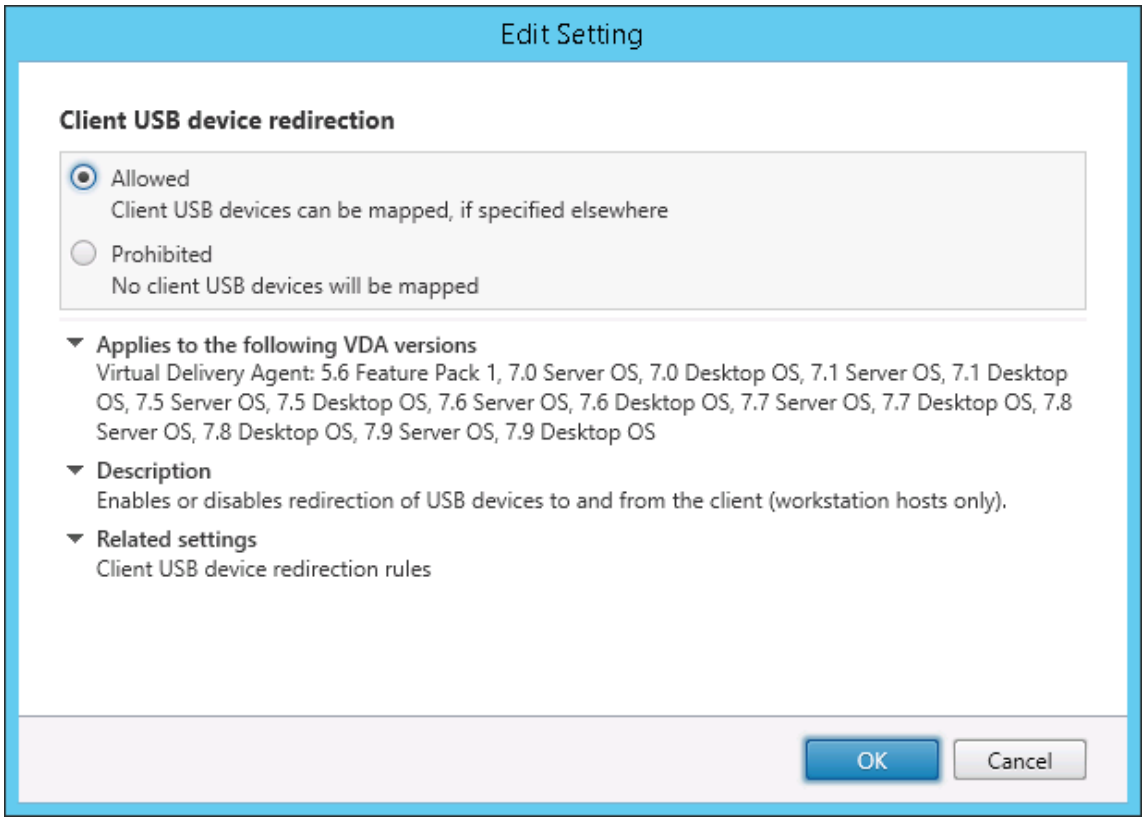
- Si deux organisations ou services distincts sont responsables de Citrix Receiver et du VDA, elles peuvent appliquer le contrôle séparément. Cela s'applique lorsqu'un utilisateur d'une organisation accède à une application située dans une autre organisation.
- Si des périphériques USB doivent être autorisés pour certains utilisateurs ou uniquement pour les utilisateurs se connectant via un réseau local (plutôt qu'avec NetScaler Gateway), cette configuration peut être contrôlée par des paramètres de stratégie Citrix.

Activer la redirection USB générique

Pour activer la redirection USB générique, configurez les paramètres de stratégie Citrix et Citrix Receiver.

Dans les paramètres de stratégie Citrix :

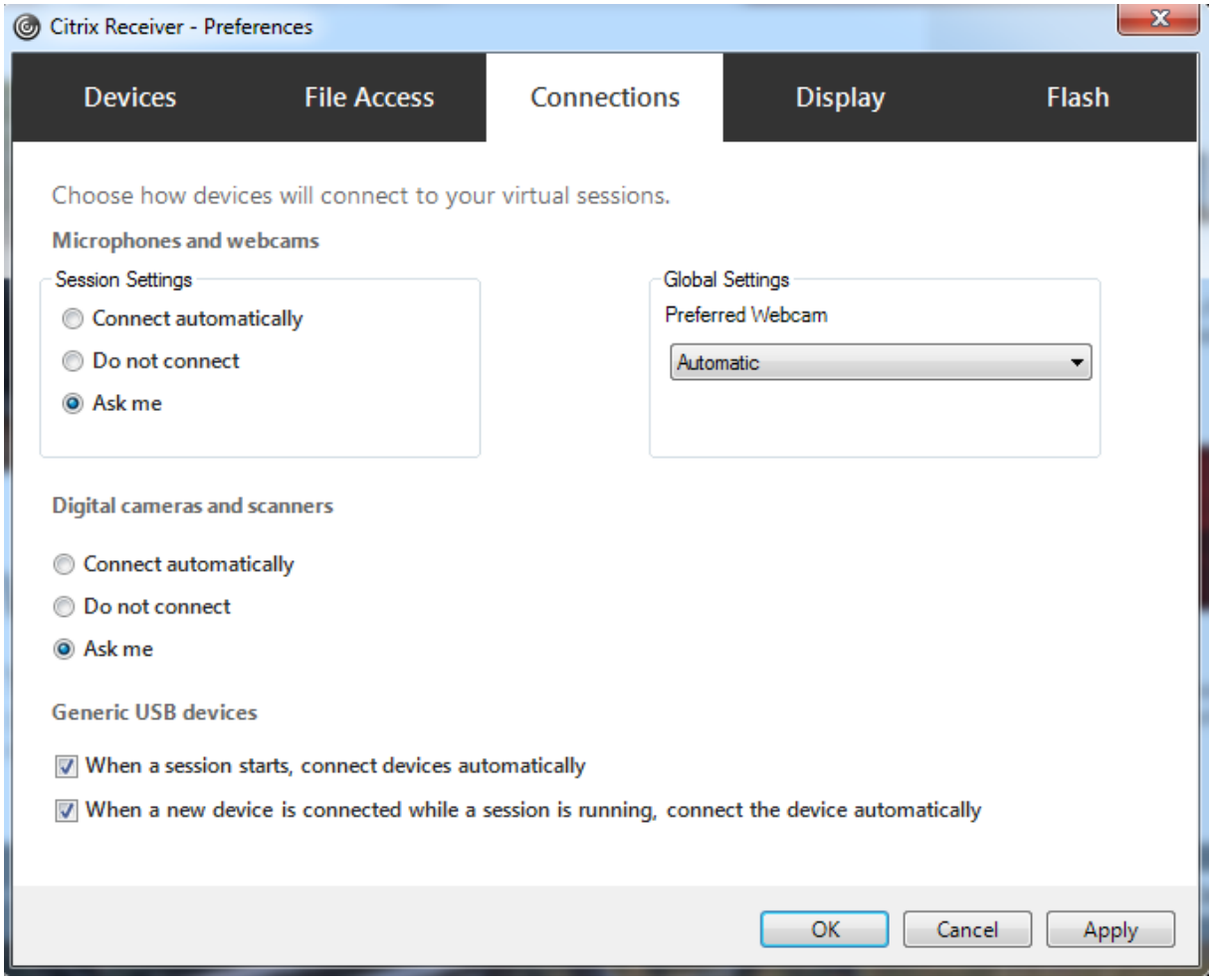
1. Ajoutez Redirection de périphérique USB client à une stratégie et définissez sa valeur sur **Autorisé**.



2. (Facultatif). Pour mettre à jour la liste des périphériques USB disponibles pour la redirection, ajoutez le paramètre Règles de redirection de périphérique USB client à une stratégie et spécifiez les règles de stratégie USB.

   Dans Citrix Receiver :

3. Activez la prise en charge USB lorsque vous installez Citrix Receiver sur les machines utilisateur. Vous pouvez effectuer cette opération à l'aide d'un modèle d'administration ou dans Citrix Receiver pour Windows > Préférences > Connexions.



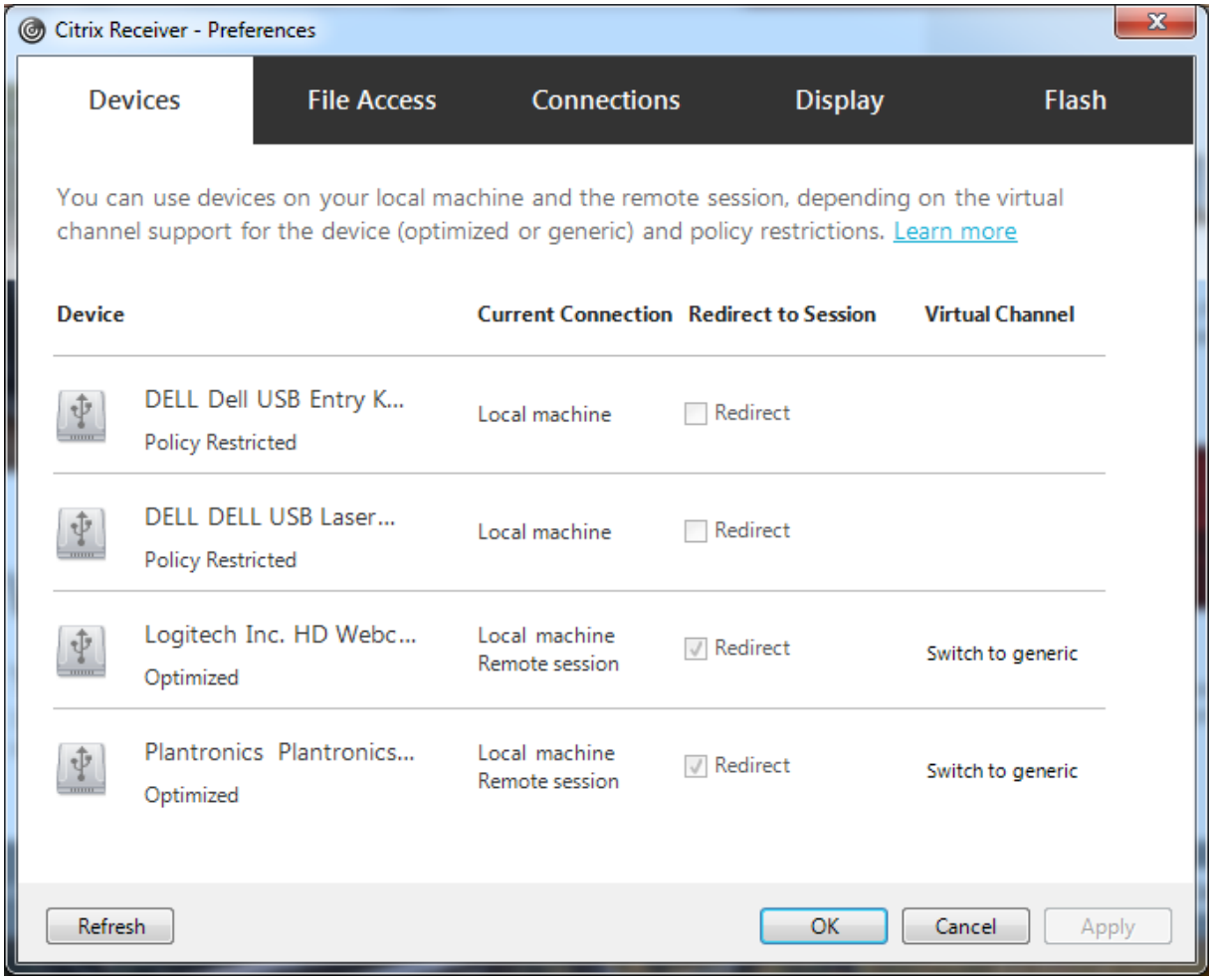
Si vous avez spécifié des règles de stratégie USB pour le VDA à l'étape précédente, spécifiez les mêmes règles de stratégie pour Citrix Receiver.

pour les clients légers, consultez le fabricant pour obtenir des détails sur la prise en charge USB et sur la configuration requise.

Configuration des types de périphériques USB disponibles pour la redirection USB générique

Les périphériques USB sont automatiquement redirigés lorsque la prise en charge USB est activée et que les paramètres de préférences de l'utilisateur USB sont définis pour la connexion automatique aux périphériques USB. Les périphériques USB sont également automatiquement redirigés lorsqu'ils se trouvent en mode Desktop Appliance et que la barre de connexion est absente.

Les utilisateurs peuvent rediriger explicitement les périphériques qui ne sont pas automatiquement redirigés en les sélectionnant dans la liste des périphériques USB. Les utilisateurs peuvent obtenir plus d'aide sur la marche à suivre dans l'article Citrix Receiver pour Windows, Afficher vos périphériques dans Desktop Viewer.



Pour utiliser la redirection USB générique plutôt que la prise en charge optimisée, vous pouvez :

- Dans Citrix Receiver, sélectionnez manuellement le périphérique USB qui devra utiliser la redirection USB générique et choisissez **Basculer en mode générique** dans l'onglet Périphériques de la boîte de dialogue Préférences.
- Sélectionnez automatiquement le périphérique USB qui devra utiliser la redirection USB générique en configurant la redirection automatique pour le type de périphérique USB (par exemple, AutoRedirectStorage=1), et définissez les paramètres de préférences de l'utilisateur sur la connexion automatique aux périphériques USB. Pour plus d'informations, veuillez consulter l'article CTX123015.

> **Remarque** :
>
> configurez la redirection USB générique pour une utilisation avec une webcam uniquement si la webcam n'est pas compatible avec la redirection multimédia HDX.

Pour empêcher les périphériques USB d'être répertoriés ou redirigés, vous pouvez spécifier des règles de périphérique pour Citrix Receiver et le VDA.

Pour la redirection USB générique, vous devez connaître au moins la classe et la sous-classe du pé-

riphérique USB. Tous les périphériques USB n'utilisent pas nécessairement une classe et une sous-classe de périphérique USB logiques. Par exemple :

- Les stylets utilisent la classe de périphérique de la souris.
- Les lecteurs de carte à puce peuvent utiliser la classe de périphérique définie par le fournisseur ou HID.

Pour un contrôle plus précis, vous aurez également besoin de connaître l'ID du fournisseur, l'ID du produit et l'ID de version. Vous pouvez obtenir ces informations auprès du fabricant du périphérique.

> **Important**
>
> Les périphériques USB malveillants peuvent présenter des caractéristiques de périphérique USB qui ne correspondent pas à l'utilisation prévue. Les règles de périphérique ne permettent pas d'empêcher ce comportement.

Vous pouvez contrôler les périphériques USB disponibles pour la redirection USB générique en spécifiant des règles de redirection de périphérique USB pour Citrix Receiver et le VDA qui remplaceront les règles de stratégie USB par défaut.

Pour le VDA :

- Modifiez les règles de remplacement de l'administrateur pour les machines avec OS de serveur à l'aide de règles de stratégie de groupe. La console de gestion des stratégies de groupe est incluse sur le support d'installation :
  - Pour x64 : dvd root \os\lang\x64\Citrix Policy\ CitrixGroupPolicyManagement_x64.msi
  - Pour x86 : dvd root \os\lang\x86\Citrix Policy\ CitrixGroupPolicyManagement_x86.msi

Sur Citrix Receiver pour Windows :

- Modifiez le registre de la machine utilisateur. Un modèle administratif (fichier ADM) est inclus dans le support d'installation pour vous permettre d'effectuer des modifications sur la machine utilisateur via une stratégie de groupe Active Directory :
  dvd root \os\lang\Support\Configuration\icaclient_usb.adm.

> **Avertissement**
>
> Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Les règles par défaut du produit sont stockées dans HKLM\SOFTWARE\Citrix\PortICA\GenericUSB\DeviceRules. ne modifiez pas les règles par défaut du produit. Au lieu de cela, utilisez-les pour créer des règles de remplacement de l'administrateur comme expliqué ci-dessous. Les règles de remplacement d'objets de stratégie de groupe de substitution sont évaluées avant les règles par défaut du produit.

Les règles de remplacement de l'administrateur sont stockées dans HKLM\SOFTWARE\Policies\Citrix\PortICA\Gene
Les règles de stratégies GPO sont au format **{Allow:|Deny:}** et sont suivies d'un ensemble d'expressions *tag=value* (balise=valeur) séparées par des espaces.

Les balises suivantes sont prises en charge :

Balise	Description
VID	ID fournisseur du descripteur de périphérique
PID	ID de produit du descripteur de périphérique
REL	ID de version du descripteur de périphérique
Classe	Classe du descripteur de périphérique ou d'un descripteur d'interface ; veuillez consulter le site Web USB sur https://www.usb.org/ pour les codes de classe USB disponibles
Sous-classe	Sous-classe du descripteur de périphérique ou d'un descripteur d'interface
Prot	Protocole à partir du descripteur de périphérique ou d'un descripteur d'interface

Lors de la création de nouvelles règles de stratégies, tenez compte de ce qui suit.

- Les règles ne sont pas sensibles à la casse.
- Les règles peuvent éventuellement comporter un commentaire, introduit par #, à la fin. Aucun délimiteur n'est requis et le commentaire est ignoré en cas de correspondance.
- Les espaces vides et les lignes de commentaires pures sont ignorés.
- L'espace est utilisé comme séparateur, mais il ne peut pas apparaître au milieu d'un nombre ou d'un identificateur. Par exemple, Deny: Class = 08 SubClass=05 est une règle valide, mais Deny: Class=0 Sub Class=05 ne l'est pas.
- Les balises doivent utiliser l'opérateur de correspondance =. Par exemple, VID=1230.
- Chaque règle doit commencer sur une nouvelle ligne ou faire partie d'une liste séparée par des points-virgules.

> **Remarque**
>
> si vous utilisez le fichier modèle ADM, vous devez créer des règles sur une seule ligne sous forme de liste séparée par des points-virgules.

Exemples :

- Cet exemple illustre une règle de stratégie USB définie par l'administrateur pour des identificateurs de fabricant et de produit :


```
Allow: VID=046D PID=C626 # Allow Logitech SpaceNavigator 3D Mouse
Deny: VID=046D # Deny all Logitech products
```

- Cet exemple illustre une règle de stratégie USB définie par l'administrateur pour une classe, une sous-classe et un protocole définis :

```
Deny: Class=EF SubClass=01 Prot=01 # Deny MS Active Sync devices
Allow: Class=EF SubClass=01 # Allow Sync devices
Allow: Class=EF # Allow all USB-Miscellaneous devices
```

Utiliser et supprimer des périphériques USB

Les utilisateurs peuvent se connecter un périphérique USB avant ou après le démarrage d'une session virtuelle.

Lors de l'utilisation de Citrix Receiver pour Windows, ce qui suit s'applique :

- Les périphériques connectés après démarrage d'une session apparaissent immédiatement dans le menu USB de Desktop Viewer.
- Si un périphérique USB n'est pas correctement redirigé, vous pouvez essayer de résoudre le problème en attendant que la session virtuelle ait démarré avant de connecter le périphérique.
- Pour éviter la perte de données, utilisez l'icône « Retirer le périphérique en toute sécurité » Windows avant de supprimer le périphérique USB.

Contrôles de sécurité pour les périphériques de stockage de masse USB

Une prise en charge optimisée est fournie pour les périphériques de stockage de masse USB. Elle fait partie du mappage des lecteurs clients XenApp et XenDesktop. Les lecteurs de la machine utilisateur sont automatiquement mappés vers les lettres de lecteur sur le bureau virtuel lorsque les utilisateurs ouvrent une session. Les lecteurs sont affichés sous la forme de dossiers partagés associés à des lettres de lecteur mappé. Pour configurer le mappage des lecteurs clients, utilisez le paramètre **Lecteurs amovibles clients** de la section Paramètres de stratégie de la redirection de fichier des Paramètres de stratégie ICA.

Avec les périphériques de stockage de masse USB, vous pouvez utiliser le mappage de lecteurs clients ou la redirection USB générique, ou les deux ; il vous suffit de les configurer dans les stratégies Citrix. Les principales différences sont les suivantes :

Fonctionnalité	Mappage des lecteurs clients	Redirection USB générique
Activée par défaut	Oui	Non

Fonctionnalité	Mappage des lecteurs clients	Redirection USB générique
Accès en lecture seule configurable	Oui	Non
Accès chiffré au périphérique	Oui, si le cryptage est déverrouillé avant l'accès au périphérique	Non
Le périphérique peut être retiré en toute sécurité au cours d'une session	Non	Oui, étant donné que les utilisateurs suivent les recommandations du système d'exploitation pour un retrait en toute sécurité.

Si la redirection USB générique et les stratégies de mappage de lecteurs clients sont activées, alors lorsqu'un périphérique de stockage de masse est inséré avant ou après le démarrage d'une session, il sera redirigé à l'aide du mappage de lecteur client. Lorsque la redirection USB générique et les stratégies de mappage de lecteurs clients sont activées et qu'un périphérique est configuré pour une redirection automatique (voir https://support.citrix.com/article/CTX123015) et un périphérique de stockage de masse est inséré avant ou après le démarrage d'une session, il sera redirigé à l'aide d'USB générique.

> **Remarque**
>
> La redirection USB est prise en charge sur les connexions de bande passante faible, par exemple de 50 Kbps ; toutefois, la copie de fichiers volumineux ne fonctionnera pas.

Contrôler l'accès aux fichiers avec le mappage de lecteurs clients

Vous pouvez contrôler si les utilisateurs peuvent copier des fichiers à partir de leurs environnements virtuels vers leurs machines utilisateur. Par défaut, les fichiers et dossiers sur les lecteurs clients mappés sont disponibles en mode de lecture/écriture au sein de la session.

Pour empêcher les utilisateurs d'ajouter ou de modifier des fichiers et dossiers sur les lecteurs clients mappés, activez le paramètre de stratégie **Accès en lecture unique sur le lecteur client**. Lorsque vous ajoutez ce paramètre à une stratégie, vérifiez que le paramètre **Redirection de lecteur client** est défini sur **Autorisé** et est également ajouté à la stratégie.

Imprimer

February 28, 2019

La gestion des imprimantes dans votre environnement est un processus à plusieurs étapes :

1. Familiarisation avec les concepts d'impression, si ce n'est pas déjà le cas.
2. Planifiez votre architecture d'impression. Cela comprend l'analyse des besoins de votre entreprise, votre infrastructure d'impression existante, la façon dont vos utilisateurs et applications interagissent avec l'impression aujourd'hui et le modèle de gestion de l'impression qui s'applique le mieux à votre environnement.
3. Configurez votre environnement d'impression en sélectionnant une méthode de provisioning de l'imprimante et en créant des stratégies pour déployer votre solution d'impression. Mettez à jour des stratégies lorsque de nouveaux employés ou serveurs sont ajoutés.
4. Testez la configuration du pilote d'impression avant de le déployer auprès des utilisateurs.
5. Gérez votre environnement d'impression Citrix en gérant des pilotes d'imprimante et en optimisant les performances d'impression.
6. Résolvez les problèmes qui peuvent se produire.

Concepts d'impression

Avant de commencer à planifier votre déploiement, assurez-vous que vous comprenez ces concepts majeurs pour l'impression :

- Les types suivants de provisioning de l'imprimante sont disponibles
- comment les tâches sont routées ;
- les bases de la gestion de pilotes d'impression.

Concepts d'impression créés sur les concepts d'impression Windows. Pour configurer et gérer l'impression correctement dans votre environnement, vous devez comprendre le fonctionnement de l'impression réseau et cliente Windows et ce que cela signifie en comportement d'impression dans cet environnement.

Processus d'impression

Dans cet environnement, toutes les impressions sont lancées (par l'utilisateur) sur les machines hébergeant les applications. Les tâches d'impression sont redirigées via le serveur d'impression réseau ou la machine utilisateur vers le périphérique d'impression.

Il n'existe aucun espace de travail permanent pour les utilisateurs de bureaux et d'applications virtuels. Lorsqu'une session se termine, l'espace de travail de l'utilisateur est supprimé, et tous les

paramètres doivent être recréés au début de chaque session. Par conséquent, chaque fois qu'un utilisateur démarre une nouvelle session, le système doit recréer l'espace de travail de l'utilisateur.

Lorsqu'un utilisateur effectue l'impression :

- Détermine les imprimantes à fournir à l'utilisateur. Ceci est appelé provisioning de l'impression ;
- restaure les préférences d'impression de l'utilisateur ;
- détermine la nature de l'imprimante par défaut pour la session.

Vous pouvez personnaliser la manière dont vous souhaitez réaliser ces tâches en configurant des options pour le provisioning de l'impression, le routage des tâches d'impression, la rétention des propriétés d'imprimante et la gestion de pilotes. Veillez à évaluer la manière dont les paramètres des options peuvent modifier les performances d'impression dans votre environnement, ainsi que l'expérience de l'utilisateur.

Provisioning de l'impression

Le processus par lequel les imprimantes sont mises à disposition dans une session est appelé provisioning. Le provisioning de l'imprimante est généralement traité de manière dynamique. En d'autres termes, les imprimantes qui s'affichent dans une session ne sont pas prédéterminées et stockés. Au lieu de cela, les imprimantes sont assemblées et basées sur les stratégies, au fur et à mesure que la session est créée lors de l'ouverture de session et la reconnexion. Par conséquent, les imprimantes peuvent changer selon la stratégie, l'emplacement de l'utilisateur, et les modifications de réseau, s'ils sont reflétés dans les stratégies. Par conséquent, les utilisateurs itinérants vers un autre emplacement peuvent voir les modifications apportées à leur espace de travail.

Le système surveille également les imprimantes côté client et ajuste dynamiquement les imprimantes créées automatiquement dans les sessions en fonction des ajouts, suppressions et modifications apportées aux imprimantes côté client. Cette découverte dynamique des imprimantes présente un avantage pour les utilisateurs itinérants lorsqu'ils se connectent à partir de divers périphériques.

Les méthodes les plus courantes de provisioning de l'imprimante sont :

- **Serveur d'impression universelle** : le serveur d'impression universelle Citrix fournit la prise en charge de l'impression universelle pour les imprimantes réseau. Le serveur d'impression universelle utilise le pilote d'impression universelle. Cette solution vous permet d'utiliser un pilote unique sur une machine avec OS de serveur pour permettre l'impression réseau à partir de n'importe quel périphérique.

Citrix recommande d'utiliser le serveur d'impression universelle Citrix pour les scénarios de serveur d'impression distants. Le serveur d'impression universelle transfère la tâche d'impression sur le réseau selon un format optimisé et compressé, réduisant ainsi l'utilisation du réseau et améliorant l'expérience utilisateur.

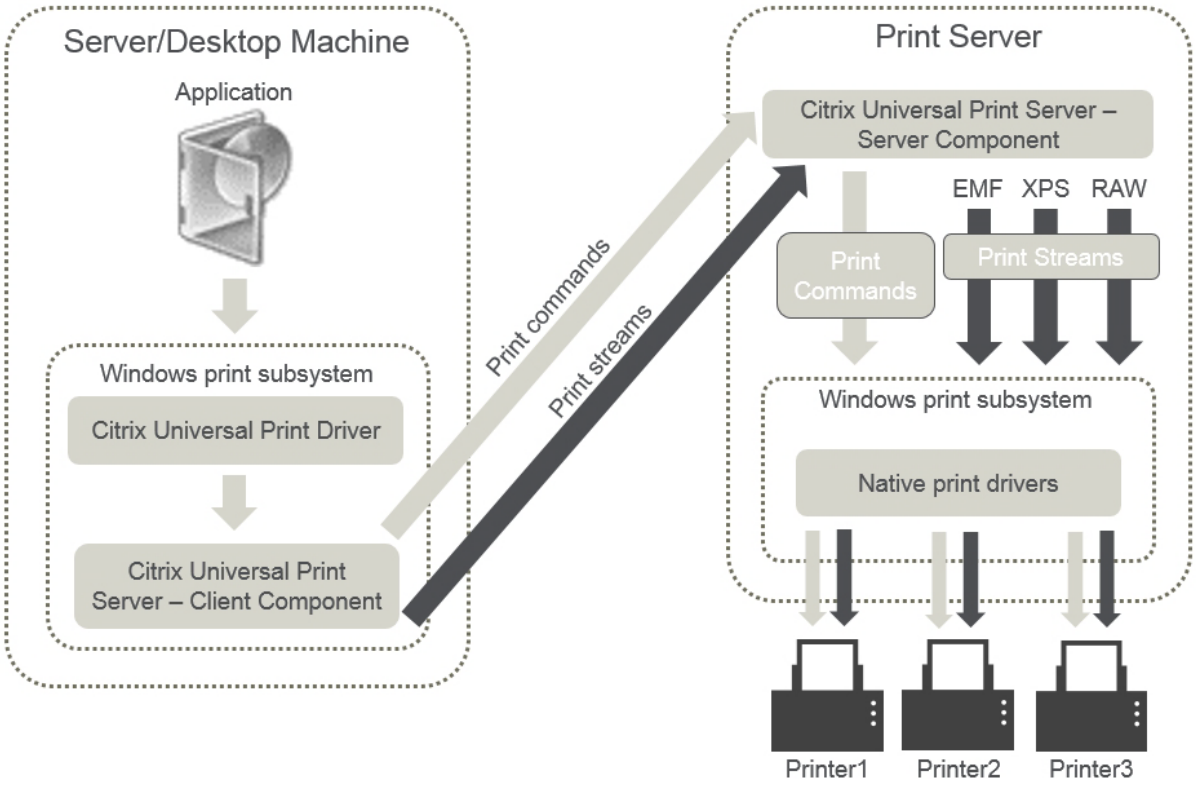
La fonctionnalité Serveur d'impression universelle comprend :

Un composant client, **UPClient** : activez UPClient sur chaque machine d'OS de serveur qui fournit des imprimantes réseau de session et utilise le pilote d'imprimante universel.

Un composant serveur, **UPServer** : installez UPServer sur chaque serveur d'impression qui fournit des imprimantes réseau de session et utilise le pilote d'impression universel pour les imprimantes de session (que les imprimantes de session soient approvisionnées de manière centralisée ou non).

Pour la configuration requise du serveur d'impression universelle et les détails d'installation, reportez-vous aux articles Configuration système requise et Installation.

L'illustration suivante affiche le flux de travail classique pour un réseau en fonction de l'imprimante réseau dans un environnement qui utilise le serveur d'impression universelle.



Lorsque vous activez le Serveur d'impression universelle Citrix, toutes les imprimantes réseau connectées en tirent parti automatiquement via la découverte automatique.

> **Remarque :**
> le Serveur d'impression universelle est également pris en charge pour VDI-in-a-Box 5.3. Pour plus d'informations sur l'installation du serveur d'impression universelle avec VDI-in-a-Box, reportez-vous à la documentation VDI-in-a-Box.

- **Création automatique** : le terme *Création automatique* fait référence aux imprimantes crées automatiquement au début de chaque session. À la fois les imprimantes réseaux distantes et les

imprimantes clientes locales peuvent être créées automatiquement. Envisagez la création automatique uniquement de l'imprimante cliente par défaut pour les environnements possédant un grand nombre d'imprimantes par utilisateur. La création automatique d'un plus petit nombre d'imprimantes utilise moins de traitement de mémoire et de processeur sur les machines avec OS de serveur. La réduction des imprimantes créées automatiquement permet également de réduire les durées d'ouverture de session de l'utilisateur.

Les imprimantes créées automatiquement sont basées sur :

- les imprimantes installées sur la machine utilisateur ;
- toutes les stratégies qui s'appliquent à la session.

  Les paramètres de stratégie de création automatique vous permettent de limiter le nombre ou le type d'imprimantes créées automatiquement. Par défaut, les imprimantes mises à disposition dans les sessions lors de la configuration automatique de toutes les imprimantes sur la machine cliente, y compris celles connectées localement et les imprimantes réseau.

Après que l'utilisateur ait mis fin à la session, les imprimantes de cette session sont supprimées.

La création automatique de l'imprimante cliente et réseau possède une maintenance associée. Par exemple, l'ajout d'une imprimante requiert que vous effectuiez les opérations suivantes :

- Mettre à jour le paramètre de stratégie Imprimantes de session.
- Ajouter le pilote à toutes les machines avec OS de serveur utilisant le paramètre de stratégie Mappage et compatibilité du pilote d'imprimante.

Routage des tâches d'impression

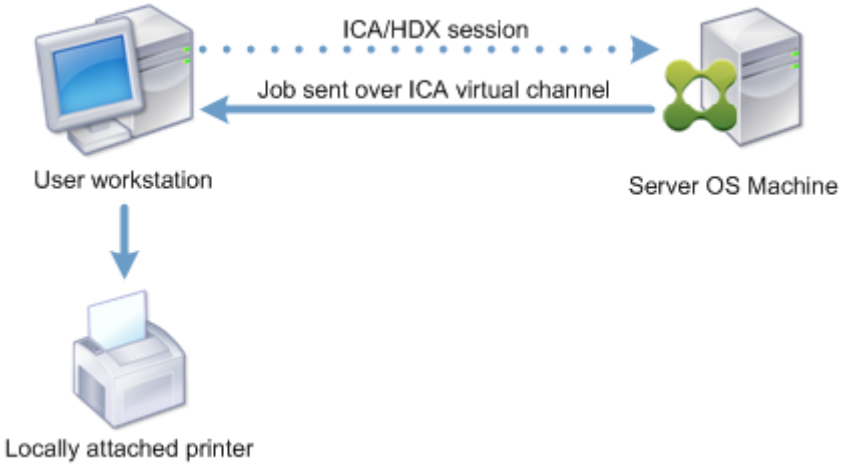
Le terme piste d'impression regroupe à la fois le chemin suivant lequel les tâches d'impression sont routées et l'emplacement dans lequel les tâches d'impression sont spoulées. Les deux aspects de ce concept sont importants. Le routage affecte le trafic réseau. La mise en file d'attente affecte l'utilisation des ressources locales sur la machine qui traite la tâche d'impression.

Dans cet environnement, les tâches d'impression peuvent prendre deux chemins d'accès vers un périphérique d'impression : via le client ou via un serveur d'impression réseau. Ces chemins d'accès sont appelées piste d'impression cliente et piste d'impression réseau. Le chemin d'accès sélectionné par défaut dépend du type d'imprimante utilisé.

Imprimantes connectées localement

Le système route les tâches vers des imprimantes connectées localement à partir de la machine avec OS de serveur, au travers du client, puis vers le périphérique d'impression. Le protocole ICA optimise

et compresse le trafic de la tâche d'impression. Lorsqu'un périphérique d'impression est connecté localement à la machine utilisateur, les tâches d'impression sont routées via le canal virtuel ICA.



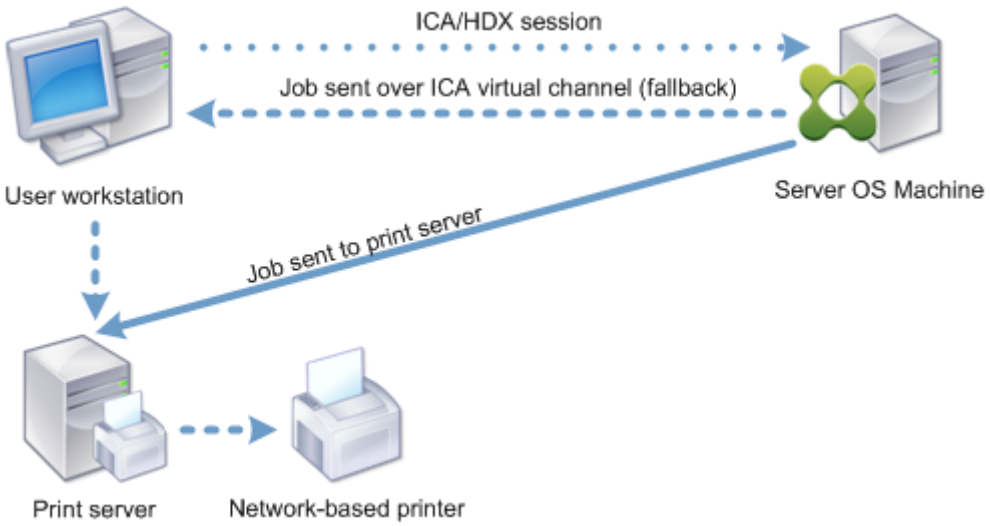
Imprimantes réseau

Par défaut, toutes les tâches d'impression sont destinées à la route d'imprimantes réseau à partir de la machine avec OS de serveur, au travers du réseau, et directement vers le serveur d'impression. Cependant, les tâches d'impression sont routées automatiquement via la connexion ICA dans les cas suivants :

- Si le bureau virtuel ou l'application ne peuvent pas contacter le serveur d'impression.
- Si le pilote d'imprimante natif n'est pas disponible sur la machine avec OS de serveur.

Si le serveur d'impression universelle n'est pas activé, la configuration de la piste d'impression cliente pour l'impression réseau est utile pour les connexions à faible bande passante, telles que les réseaux étendus, qui peuvent bénéficier de l'optimisation et de la compression du trafic résultant en l'envoi de tâches via la connexion ICA.

La piste d'impression cliente vous permet également de limiter le trafic ou de restreindre la bande passante allouée aux tâches d'impression. Si le routage de tâches via la machine utilisateur n'est pas possible, tel que pour les clients légers sans les fonctionnalités d'impression, la qualité de service doit être configurée pour favoriser le trafic ICA/HDX et assurer une bonne expérience de l'utilisateur dans les sessions.



Gestion des pilotes d'impression

Le pilote d'imprimante universelle Citrix (UPD) est un pilote d'imprimante indépendant du périphérique, qui est compatible avec la plupart des imprimantes. Le pilote UPD Citrix est constitué de deux composants :

Composant serveur. Le pilote d'imprimante universelle Citrix est installé dans le cadre de l'installation de VDA XenApp ou XenDesktop. Le VDA installe les pilotes suivants avec le pilote UPD Citrix : « Citrix Universal Printer » (pilote EMF) et « Citrix XPS Universal Printer » (pilote XPS).

Name	Processor	Type
Citrix Universal Printer	x64	Type 3 - User Mode
Citrix XPS Universal Printer	x64	Type 3 - User Mode

Lorsqu'une tâche d'impression est initiée, le pilote enregistre la sortie de l'application et l'envoie, sans qu'aucune modification ne soit apportée au périphérique de destination.

Composant client. Le pilote d'imprimante universelle Citrix est installé dans le cadre de l'installation de Citrix Receiver. Il récupère le flux d'impression entrant pour la session XenApp ou XenDesktop. Il transmet ensuite le flux d'impression au sous-système d'impression locale où la tâche d'impression est restituée à l'aide des pilotes d'imprimante spécifiques au périphérique. Outre le pilote d'imprimante universelle Citrix, le pilote d'imprimante universelle PDF Citrix peut être installé séparément avec Citrix Receiver pour HTML5 et de Citrix Receiver pour Chrome.

Le pilote d'imprimante universelle Citrix prend en charge les formats d'impression suivants :

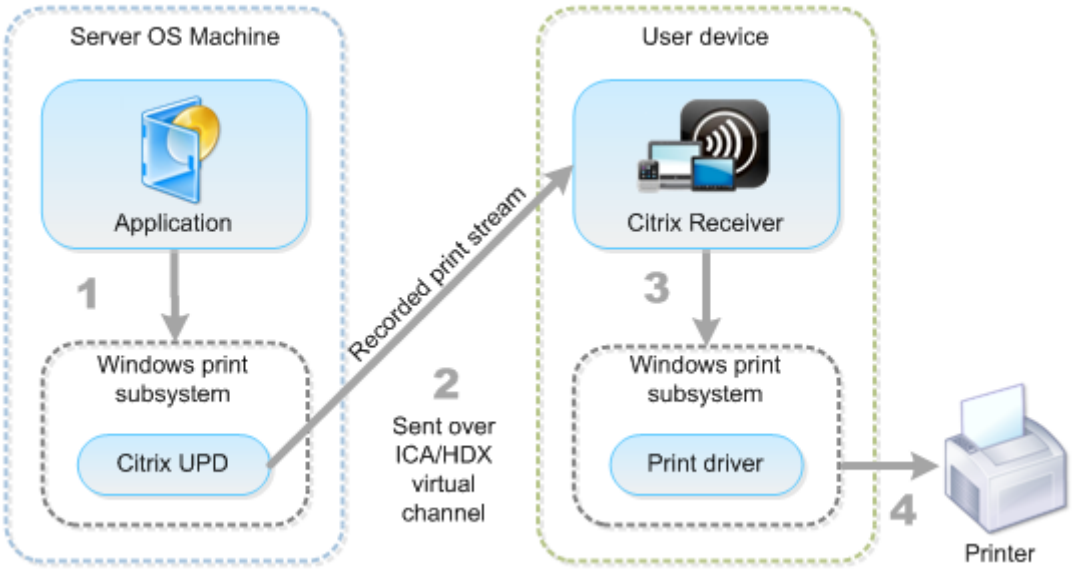
- Enhanced Metafile Format (**EMF**), valeur par défaut. EMF est la version 32 bits de Windows Metafile Format (WMF). Le pilote EMF peut uniquement être utilisé par les clients Windows.
- XML Paper Specification (**XPS**). Le pilote XPS utilise XML pour créer un « papier électronique » indépendant de la plate-forme utilisée similaire au format PDF d'Adobe.

- Printer Command Language (**PCL5c** et **PCL4**). PCL est un protocole d'impression développé par Hewlett-Packard pour les imprimantes à jet d'encre. Il est utilisé pour l'impression de texte et de graphiques de base et est largement pris en charge sur les périphériques HP LaserJet et multifonctions.
- PostScript (**PS**). PostScript est un langage informatique qui peut être utilisé pour l'impression de texte et de graphiques vectoriels. Ce pilote est largement utilisé avec les imprimantes et multifonctions de base.

Les pilotes PS et PCL sont plus adaptés lors de l'utilisation de machines non Windows, avec un client Mac ou UNIX par exemple. L'ordre dans lequel le pilote d'imprimante universelle Citrix tente d'utiliser les pilotes peut être modifié à l'aide du paramètre de stratégie Préférence de pilote universel.

Le pilote d'imprimante universelle Citrix (pilotes EMF et XPS) prend en charge les fonctionnalités d'impression avancées, telles que l'agrafage et la sélection de l'alimentation papier. Ces fonctionnalités sont disponibles si le pilote natif les rend disponibles à l'aide de la technologie d'impression de Microsoft. Le pilote natif doit utiliser les mots clés du schéma d'impression standard dans le fichier XML des fonctionnalités d'impression. Si des mots-clés non standard sont utilisés, les fonctionnalités d'impression avancées ne sont pas disponibles à l'aide du pilote d'imprimante universelle Citrix.

L'illustration suivante affiche les composants du pilote d'impression universelle et un flux de travail typique pour une imprimante connectée localement sur un périphérique.

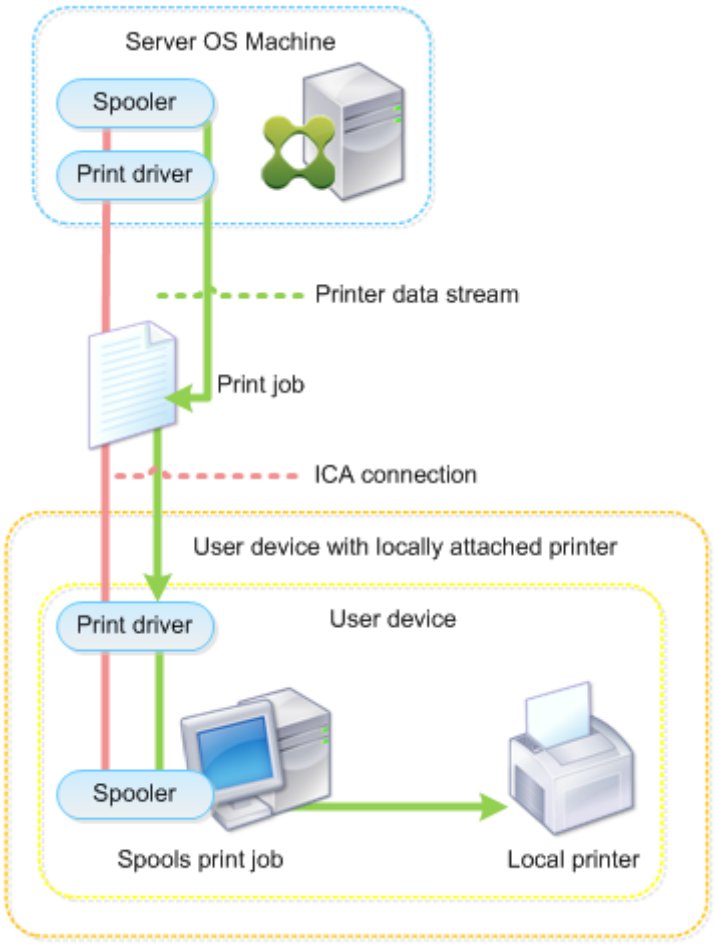


Lors de la planification de votre stratégie de gestion de pilote, déterminez si vous allez prendre en charge le pilote d'impression universelle, le pilote spécifique à la machine, ou les deux. Si vous prenez en charge les pilotes standards, vous devrez également déterminer :

Lors de la création automatique des imprimantes, si le système détecte une nouvelle imprimante locale connectée à une machine utilisateur, il vérifie la présence du pilote d'imprimante requis sur la

machine avec OS de serveur. Par défaut, si un pilote natif Windows n'est pas disponible, le système utilise le pilote d'impression universelle.

Le pilote d'imprimante de la machine avec OS de serveur et le pilote de la machine utilisateur doivent correspondre pour que l'impression réussisse. Le diagramme qui suit démontre comment le pilote d'imprimante est utilisé à deux endroits pour l'impression cliente.



- Les types de pilotes à prendre en charge.
- Indiquez si vous devez installer les pilotes d'imprimante automatiquement lorsqu'ils sont manquants sur les machines avec OS de serveur.
- Indiquer s'il faut créer des listes de compatibilité du pilote.

Contenu associé

- Exemple de configuration d'impression
- Meilleures pratiques, considérations de sécurité et opérations par défaut
- Imprimer les stratégies et préférences
- Provisionner les imprimantes

- Gérer l'environnement d'impression

Exemple de configuration d'impression

February 28, 2019

Le choix d'options de configuration d'impression les plus appropriées à vos besoins et à l'environnement peut simplifier l'administration. Bien que la configuration d'impression par défaut permet aux utilisateurs d'imprimer dans la plupart des environnements, les valeurs par défaut peuvent ne pas fournir la meilleure expérience utilisateur attendue ou l'utilisation du réseau et de surcharge de gestion pour votre environnement.

Votre configuration d'impression dépend des facteurs suivants :

- Les besoins de votre entreprise et votre infrastructure d'impression existante.

  Concevez votre configuration d'impression selon les besoins de votre organisation. Votre implémentation d'impression existante (capacité des utilisateurs à ajouter des imprimantes, quels utilisateurs ont accès à quelles imprimantes, etc) peut être un guide utile lors de la définition de la configuration de l'impression.

- Si votre entreprise possède des stratégies de sécurité qui réservent des imprimantes pour certains utilisateurs (par exemple, des imprimantes pour le département des ressources humaines ou finance).

- Si les utilisateurs doivent imprimer alors qu'ils sont éloignés de leur emplacement de travail principal ; par exemple, les travailleurs qui se déplacent entre stations de travail ou sont en voyage d'affaire.

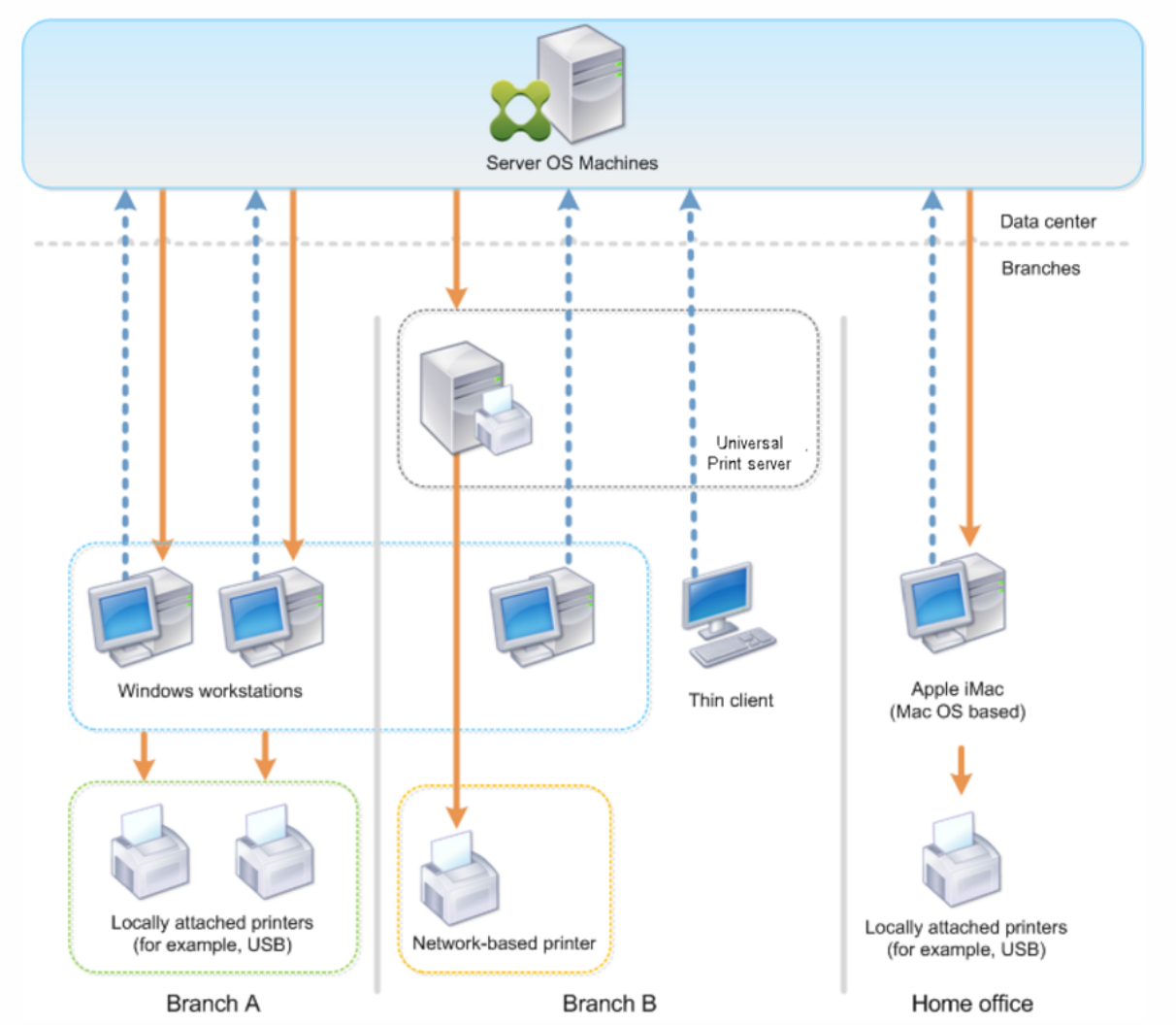
Lors de la conception de votre configuration d'impression, essayez de fournir aux utilisateurs la même expérience en session qu'ils rencontrent lorsqu'ils impriment depuis leurs machines utilisateur locales.

Exemple de déploiement d'impression

L'illustration suivante affiche le déploiement pour ces cas d'utilisation :

- **Succursale A :** une petite succursale à l'étranger avec quelques stations de travail Windows. Chaque utilisateur station de travail possède une imprimante privée, connectée localement.
- **Succursale B :** une succursale importante avec des clients légers et des stations de travail Windows. Pour une meilleure efficacité, les utilisateurs de cette succursale partagent des imprimantes réseau (une par étage). Des serveurs d'impression Windows situés dans la succursale gèrent les files d'attente d'impression.

- **Bureau à domicile :** un bureau à domicile avec une machine utilisateur Mac OS qui accède à l'infrastructure Citrix de l'entreprise. La machine utilisateur dispose d'une imprimante connectée localement.



Les sections suivantes décrivent les configurations qui réduisent la complexité de l'environnement et simplifient sa gestion.

Imprimantes créées automatiquement et pilote d'imprimante universelle Citrix

Dans la succursale A, tous les utilisateurs travaillent sur des stations de travail Windows, par conséquent, les imprimantes clientes créées automatiquement et le pilote d'imprimante universelle sont utilisés. Ces technologies fournissent ces avantages :

- Performances : les tâches d'impression sont fournies via le canal ICA d'impression et les données d'impression peuvent être compressées pour économiser la bande passante.

Pour vous assurer qu'un seul utilisateur imprimant un document important ne peut dégrader les performances de session des autres utilisateurs, une stratégie Citrix est configurée pour spécifier la bande passante d'impression maximale.

Une autre solution consiste à tirer parti d'une connexion multi-stream ICA, dans laquelle le trafic d'impression est transféré vers une autre connexion TCP à basse priorité. Multi-stream ICA est une option lorsque la qualité de service (QoS) n'est pas implémentée sur la connexion de réseau étendu.

- Flexibilité : l'utilisation du pilote d'imprimante universelle Citrix assure que toutes les imprimantes connectées à un client peuvent également être utilisées à partir d'un bureau virtuel ou la session d'application sans intégrer un nouveau pilote d'imprimante dans le centre de données.

Serveur d'impression universelle Citrix

Dans la succursale B, toutes les imprimantes sont basées sur le réseau et leurs files d'attente sont gérées sur un serveur d'impression Windows, et le Serveur d'impression universelle Citrix est ainsi le plus efficace de la configuration.

Tous les pilotes d'imprimante requis sont installés et gérés sur le serveur d'impression par les administrateurs locaux. Le mappage des imprimantes dans le bureau virtuel ou la session d'application fonctionne comme suit :

- Pour les stations de travail Windows : l'équipe informatique locale permet aux utilisateurs de connecter l'imprimante réseau à leurs stations de travail Windows. Cela permet aux utilisateurs d'imprimer à partir des applications installées localement.

  Lors d'une session application ou de bureau virtuel, les imprimantes de session configurées localement sont énumérées via la création automatique. Le bureau virtuel ou l'application se connectent au serveur d'impression en tant que connexion réseau directe si possible.

  Les composants du serveur d'impression universelle Citrix sont installés et activés, ainsi les pilotes d'imprimante natifs ne sont pas requis. Si un pilote est mis à jour ou une file d'attente d'imprimante est modifiée, aucune configuration supplémentaire n'est requise dans le centre de données.

- Pour les clients fins : pour les utilisateurs des clients légers, les imprimantes doivent être connectées au sein de la session de bureau virtuel ou d'application. Pour fournir aux utilisateurs l'expérience d'impression la plus simple, les administrateurs configurent une stratégie Citrix Imprimante de session unique par étage pour connecter une imprimante par étage en tant qu'imprimante par défaut.

  Pour vous assurer que l'imprimante appropriée est connectée, même si les utilisateurs itinèrent entre les étages, les stratégies sont filtrées en fonction du sous-réseau ou du nom du client

léger. Cette configuration, appelée impression de proximité, permet la maintenance du pilote d'imprimante locale (en fonction du modèle d'administration déléguée).

Si une file d'attente d'imprimante doit être modifiée ou ajoutée, les administrateurs Citrix doivent modifier la stratégie Imprimante de session correspondante au sein de l'environnement.

Étant donné que le trafic d'impression réseau sera envoyé en dehors du canal virtuel ICA, la qualité de service (QoS) est implémentée. Le trafic réseau entrant et sortant sur les ports utilisés par le trafic ICA/HDX sont prioritaires sur tous les autres trafics réseau. Cette configuration permet d'assurer que les sessions utilisateur ne sont pas affectées par les tâches d'impression importantes.

Imprimantes créées automatiquement et pilote d'imprimante universelle Citrix

Pour les bureaux à domicile sur lesquels les utilisateurs travaillent sur des stations de travail non standard et utilisent des périphériques d'impression non gérés, l'approche la plus simple consiste à utiliser les imprimantes clientes créées automatiquement et le pilote d'imprimante universelle.

Récapitulatif du déploiement

Dans le récapitulatif, l'exemple de déploiement est configuré comme suit :

- Aucun des pilotes d'imprimante n'est installé sur les machines avec OS de serveur. Seul le pilote d'imprimante universelle Citrix est utilisé. Le retour à l'impression native et l'installation automatique des pilotes d'imprimantes est désactivé.
- Une stratégie est configurée pour créer automatiquement toutes les imprimantes clientes pour tous les utilisateurs. Les machines avec OS de serveur se connecteront directement aux serveurs d'impression par défaut. La seule configuration requise est l'activation des composants du serveur d'impression universelle.
- Une stratégie d'imprimante de session est configurée pour chaque étage de la succursale B et appliquée à tous les clients légers de l'étage respectif.
- QoS est implémentée pour la succursale B afin d'assurer une excellente expérience utilisateur.

Meilleures pratiques, considérations de sécurité et opérations par défaut

February 28, 2019

Recommandations

De nombreux facteurs déterminent la meilleure solution d'impression pour un environnement particulier. Certaines de ces recommandations risquent de ne pas s'appliquer à votre site.

- Utilisez le Serveur d'impression universelle Citrix.
- Utilisez le pilote d'imprimante universelle ou les pilotes natifs Windows.
- Réduisez le nombre de pilotes d'imprimante installés sur les machines avec OS de serveur.
- Utilisez le mappage de pilote pour les pilotes natifs.
- Ne jamais installer de pilotes d'imprimante non testés sur un site de production.
- Évitez de la mise à jour de pilote. Essayez toujours de désinstaller un pilote, redémarrer le serveur d'impression, puis installer le pilote de remplacement.
- Désinstallez les pilotes non utilisées ou utilisez la stratégie Mappage et compatibilité du pilote d'imprimante pour empêcher la création d'imprimantes avec le pilote.
- Essayez d'éviter d'utiliser la version 2 des pilotes en mode noyau.
- Pour savoir si un modèle d'imprimante est pris en charge, contactez le fabricant ou consultez le guide du produit Citrix Ready sur www.citrix.com/ready.

  En général, les pilotes d'imprimante fourni par Microsoft sont testées avec les services Terminal Server et sont garantis de fonctionner avec Citrix. Toutefois, avant d'utiliser un pilote d'impression tiers, consultez votre fournisseur de pilote d'imprimante pour que le pilote soit certifié pour les services Terminal Server par le programme Windows Hardware Quality Labs (WHQL). Citrix ne certifie pas les pilotes d'imprimante.

Considérations de sécurité

Les solutions d'impression Citrix sont sécurisées dès leur conception.

- Le service du Gestionnaire d'impression Citrix surveille en permanence et répond aux événements de session, tels que l'ouverture et la fermeture de session, la déconnexion, la reconnexion et la terminaison d'une session. Il gère les demandes de service en imitant la session utilisateur courante.
- L'impression Citrix affecte un espace de noms unique à chaque imprimante dans une session.
- L'impression Citrix définit le descripteur de sécurité par défaut pour les imprimantes créées automatiquement pour vous assurer que les imprimantes clientes créées automatiquement dans une session ne sont pas accessibles aux utilisateurs exécutés dans d'autres sessions. Par défaut, les utilisateurs administratifs ne peuvent pas accidentellement d'imprimer vers une autre session d'imprimante cliente, même s'ils peuvent afficher et ajuster manuellement les permissions des imprimantes clientes.

Opérations d'impression par défaut

Par défaut, si vous ne configurez aucune règle de stratégie, le comportement d'impression est le suivant :

- La fonctionnalité Serveur d'impression universelle est désactivée.
- Toutes les imprimantes configurées sur la machine utilisateur sont automatiquement créées au début de chaque session.

  Ce comportement est équivalent à la configuration du paramètre de stratégie Citrix Créer automatiquement les imprimantes clientes avec l'option Créer automatiquement toutes les imprimantes clientes.
- Le système route toutes les tâches d'impression mises en file d'attente sur les imprimantes connectées localement vers les machines clientes en tant que tâches d'impression clientes (c'est-à-dire, via le canal ICA et au travers de la machine utilisateur).
- Le système route toutes les tâches d'impression mises en file d'attente vers les imprimantes réseau directement depuis les machines avec OS de serveur. Si le système ne peut pas router les tâches sur le réseau, il les routera au travers de la machine utilisateur sous la forme d'une tâche d'impression cliente redirigée.

  Ce comportement est équivalent à la désactivation du paramètre de stratégie Citrix Diriger les connexions vers les serveurs d'impression.
- Le système tente de stocker les propriétés d'impression, une combinaison des préférences d'impression de l'utilisateur et des paramètres d'impression spécifiques à la machine, sur la machine cliente. Si le client ne prend pas en charge cette opération, le système stocke les propriétés d'impression dans les profils utilisateur sur la machine avec OS de serveur.

  Ce comportement est équivalent à la configuration du paramètre de stratégie Citrix Rétention des propriétés de l'imprimante avec l'option Contenu dans le profil uniquement si non enregistré sur le client.
- Le système utilise la version de Windows du pilote d'imprimante si elle est disponible sur la machine avec OS de serveur. Si le pilote d'imprimante n'est pas disponible, le système tente d'installer le pilote à partir du système d'exploitation Windows. Si le pilote n'est pas disponible sous Windows, il utilise un pilote d'impression universelle Citrix.

  Ce comportement est équivalent à l'activation du paramètre de stratégie Citrix Installation automatique de pilotes d'imprimante fournis avec Windows et à la configuration du paramètre Impression universelle avec l'option Utiliser l'impression universelle uniquement si le pilote requis n'est pas disponible.

  L'activation de l'installation automatique de pilotes d'imprimante fournis avec Windows peut entraîner l'installation de nombreux pilotes d'imprimante natifs.

Remarque : si vous n'êtes pas sûr des paramètres par défaut de livraison pour l'impression, vous pouvez les afficher en créant une nouvelle stratégie et en définissant toutes les règles de stratégie d'impression sur Activé. L'option qui s'affiche est l'option par défaut.

Journalisation permanente

Une fonctionnalité de journalisation permanente est disponible pour le serveur d'impression et le sous-système d'impression sur le VDA.

Pour regrouper les journaux au format ZIP pour l'envoi par e-mail, ou pour charger automatiquement les journaux vers Citrix Insight Services, utilisez l'applet de commande PowerShell **Start-TelemetryUpload**.

Stratégies et préférences d'impression

November 9, 2018

Lorsque les utilisateurs accèdent aux imprimantes à partir des applications publiées, vous pouvez configurer des stratégies Citrix pour spécifier :

- comment les imprimantes sont approvisionnées (ou ajoutées aux sessions) ;
- comment les tâches sont routées ;
- comment les pilotes d'imprimante sont gérés.

Vous pouvez posséder plusieurs configurations d'impression pour différentes machines utilisateur, utilisateurs ou tout autre objet sur lequel les stratégies sont filtrées.

La plupart des fonctions d'impression sont configurées au travers des paramètres de stratégie d'impression Citrix. Les paramètres d'impression sont conformes au comportement de stratégie Citrix standard :

XenDesktop peut écrire les paramètres de l'imprimante dans l'objet d'imprimante à la fin de la session ou sur le périphérique d'impression cliente, étant donné que le compte réseau de l'utilisateur possède les permissions suffisantes. Par défaut, Citrix Receiver utilise les paramètres stockés dans l'objet d'imprimante de la session, avant de rechercher dans d'autres emplacements les paramètres et préférences.

Par défaut, le magasin store, ou conserve, des propriétés d'imprimante sur la machine utilisateur (si elle est prise en charge par la machine) ou dans le profil utilisateur de la machine avec OS de serveur. Lorsqu'un utilisateur modifie les propriétés de l'imprimante au cours d'une session, ces modifications sont mises à jour dans le profil de l'utilisateur sur la machine. La prochaine fois que l'utilisateur ouvre une session ou se reconnecte, la machine utilisateur hérite de ces paramètres conservés. En

d'autres termes, les modifications apportées aux propriétés de l'imprimante sur la machine utilisateur n'affectent pas la session courante tant que l'utilisateur n'a pas fermé puis rouvert une session.

Emplacements des préférence d'impression

Dans les environnements d'impression Windows, les modifications apportées aux préférences d'impression peuvent être stockées sur l'ordinateur local ou dans un document. Dans cet environnement, lorsque les utilisateurs modifient leurs paramètres d'impression, ils peuvent être stockés aux emplacements suivants :

- **Sur la machine utilisateur elle-même :** les utilisateurs Windows peuvent modifier les paramètres d'un périphérique sur la machine utilisateur en cliquant avec le bouton droit de la souris sur l'imprimante dans le Panneau de configuration, en sélectionnant Préférences d'impression. Par exemple, si Paysage est sélectionné en tant qu'orientation de page de l'imprimante, paysage est désormais enregistré en tant que préférence d'orientation de page par défaut pour cette imprimante.
- **Dans un document :** dans les programmes de traitement de texte et de publication assistée par ordinateur, les paramètres du document, tels que l'orientation de page, sont souvent stockés à l'intérieur des documents. Par exemple, une fois un document placé dans la file d'attente d'un document, Microsoft Word stocke généralement les préférences d'impression spécifiées, telles que l'orientation de page, et le nom de l'imprimante dans le document. Ces paramètres s'affichent par défaut la prochaine fois que vous imprimez ce document.
- **À partir des modifications effectuées par un utilisateur lors d'une session :** le système conserve uniquement les modifications apportées aux paramètres d'impression d'une imprimante créée automatiquement si la modification a été apportée dans le Panneau de configuration dans la session ; c'est-à-dire, sur la machine avec OS de serveur.
- **Sur la machine avec OS de serveur :** ce sont les paramètres par défaut associés à un pilote d'imprimante spécifique sur la machine.

Les paramètres préservés dans tout environnement Windows varient selon l'emplacement dans lequel l'utilisateur a effectué les modifications. Ceci signifie également que les paramètres d'impression qui s'affichent à un endroit, tel qu'un tableur, peuvent être différents de ceux qui s'affichent à d'autres endroits, tels que des documents. Ainsi, les paramètres d'impression appliqués à une imprimante spécifique peuvent changer dans une session.

Hiérarchie des préférences d'impression des utilisateurs

Les préférences d'impression pouvant être stockées à plusieurs endroits, le système les traite selon une priorité spécifique. Il est également important de noter que les paramètres de la machine sont traités différemment des paramètres du document (et ont habituellement priorité sur ces derniers).

Par défaut, le système applique toujours tout paramètre d'impression modifié par un utilisateur lors d'une session, c'est-à-dire, les paramètres conservés, avant de considérer tout autre paramètre. Lorsque l'utilisateur effectue l'impression, le système fusionne et applique les paramètres de l'imprimante par défaut stockés sur la machine avec OS de serveur avec tout paramètre d'imprimante cliente ou conservé.

Enregistrement des préférences d'impression de l'utilisateur

Citrix vous recommande de ne pas modifier l'emplacement de stockage des propriétés de l'imprimante. Le paramètre par défaut, qui enregistre les propriétés de l'imprimante sur la machine cliente, est la manière la plus facile d'assurer des propriétés d'impression cohérentes. Si le système n'a pas pu enregistrer les propriétés sur la machine utilisateur, il retourne automatiquement au profil utilisateur sur la machine avec OS de serveur.

Vérifiez le paramètre de stratégie Conservation des propriétés d'imprimante si ces scénarios s'appliquent :

- Si vous utilisez des plug-ins d'ancienne génération qui n'autorisent pas les utilisateurs à stocker des propriétés d'imprimante sur une machine utilisateur.
- Si vous utilisez des profils obligatoires sur votre réseau Windows et que vous souhaitez conserver les propriétés d'imprimante de l'utilisateur.

Provisionner les imprimantes

February 28, 2019

Serveur d'impression universelle Citrix

Lorsque vous déterminez la meilleure solution d'impression pour votre environnement, tenez compte de ce qui suit :

- Le serveur d'impression universelle fournit des fonctionnalités ne sont pas disponibles pour le fournisseur d'impression Windows : la mise en cache des images et des polices, la compression avancée, l'optimisation et la prise en charge de la qualité de service (QoS).
- Le pilote d'impression universelle prend en charge les paramètres indépendants de machine publics définis par Microsoft. Si les utilisateurs ont besoin d'accéder à des paramètres qui sont spécifiques au fabricant d'un pilote d'impression, le Serveur d'impression universelle associé à un pilote natif Windows peut être la meilleure solution. Avec cette configuration, vous conservez les avantages du Serveur d'impression universelle tout en offrant aux utilisateurs l'accès

aux fonctionnalités d'impression spécialisées. Un compromis à prendre en compte est que les pilotes natifs Windows nécessitent une certaine maintenance.

- Le serveur d'imprimante universel Citrix fournit une prise en charge de l'impression universelle pour les imprimantes réseau. Le serveur d'impression universelle utilise le pilote d'impression universelle, un seul pilote sur la machine avec OS de serveur qui permet l'impression locale ou réseau à partir de n'importe quel périphérique, y compris des clients légers et des tablettes.

Pour utiliser le Serveur d'impression universelle avec un pilote natif Windows, activez le serveur d'impression universelle. Par défaut, si le pilote natif Windows est disponible, il est utilisé. Sinon, le pilote d'impression universelle est utilisé. Pour spécifier les modifications apportées à ce comportement, par exemple pour utiliser uniquement les pilotes natifs Windows ou le pilote d'impression universelle, mettez à jour le paramètre de stratégie Utilisation du pilote d'impression universelle.

Installer le serveur d'impression universelle

Pour utiliser le serveur d'impression universelle, installez le composant UpsServer sur vos serveurs d'impression, comme décrit dans les documents d'installation et configurez-le. Pour de plus amples informations, consultez la section Installer les composants principaux et Installer à l'aide de la ligne de commande.

Dans les environnements dans lesquels vous voulez déployer le composant UPClient séparément, par exemple avec **XenApp 6.5** :

1. Téléchargez le package autonome XenApp et XenDesktop Virtual Delivery Agent (VDA) pour OS de bureau ou de serveur Windows.
2. Extrayez le VDA à l'aide des instructions de ligne de commande décrites dans la section Installer à l'aide de la ligne de commande.
3. Installez les composants requis depuis \Image-Full\Support\VcRedist_2013_RTM
    - Vcredist_x64 / vcredist_x86
        - Exécutez x86 pour 32 bits uniquement, et les deux packages pour les déploiements 64 bits
4. Installez le composant requis cdf depuis \Image-Full\x64\Virtual Desktop Components ou \Image-Full\x86\Virtual Desktop Components.
    - Cdf_x64 / Cdf_x86
        - x86 pour 32 bits, x64 pour 64 bits
5. Localisez le composant UPClient dans \Image-Full\x64\Virtual Desktop Components ou \Image-Full\x86\Virtual Desktop Components.
6. Installez le composant UPClient en extrayant et en lançant le MSI du composant.
7. Un redémarrage est nécessaire après l'installation du composant UPClient.

Refuser de prendre part au programme CEIP pour le serveur d'impression universelle

Vous êtes automatiquement inscrit au Programme d'amélioration de l'expérience utilisateur Citrix (CEIP) lorsque vous installez le serveur d'impression universelle. Le premier chargement de données s'effectue sept jours après la date et heure d'installation.

Pour ne plus participer au programme CEIP, modifiez la clé de registre **HKLM\Software\Citrix\Universal Print Server\CEIPEnabled** et définissez la valeur **DWORD** sur **0**.

Pour participer à nouveau, définissez la valeur DWORD sur 1.

> **Attention :**
>
> Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Pour de plus amples informations, consultez Citrix Insight Services.

Configurer le serveur d'impression universelle

Utilisez les paramètres de stratégie Citrix suivants pour configurer le serveur d'impression universelle. Pour plus d'informations, reportez-vous à l'aide des paramètres de stratégie à l'écran.

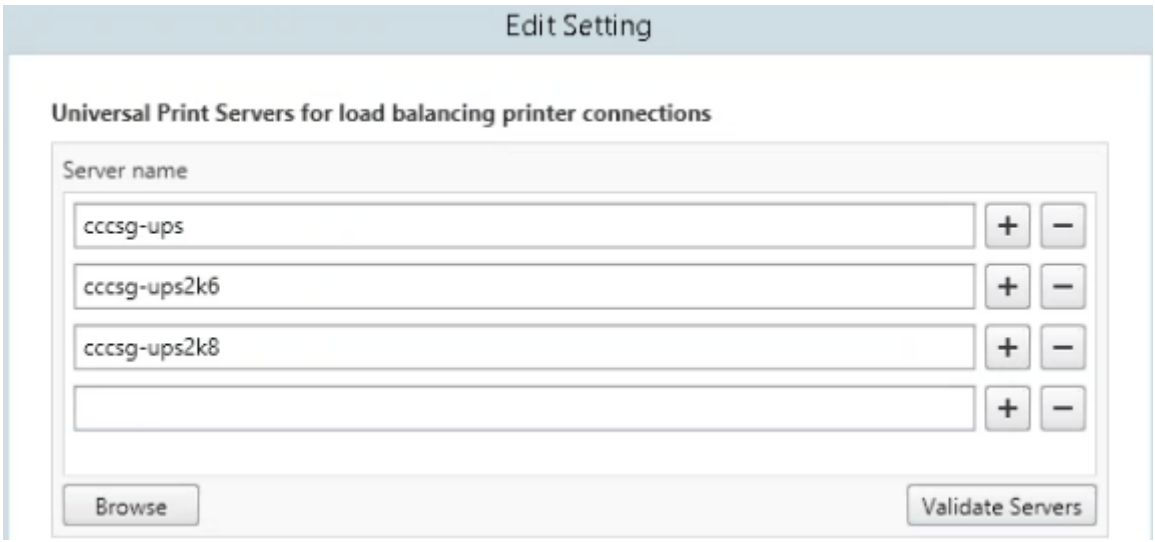
- **Serveur d'impression universelle activé**. Le serveur d'impression universelle est désactivé par défaut. Lorsque vous activez le serveur d'impression universelle, vous pouvez choisir d'utiliser le fournisseur d'impression Windows si le serveur d'impression universelle n'est pas disponible. Après avoir installé le serveur d'impression universelle, un utilisateur peut ajouter et énumérer des imprimantes réseau au travers des interfaces du fournisseur d'impression Windows et du fournisseur Citrix.
- **Port (CGP) du flux de données d'impression du serveur d'impression universelle**. Spécifie le numéro de port TCP utilisé par l'écouteur CGP (Common Gateway Protocol) du flux de données d'impression Serveur d'impression universelle. Valeurs par défaut **7229**.
- **Port (HTTP/SOAP) du service Web du serveur d'impression universelle**. Spécifie le numéro de port TCP utilisé par l'écouteur Serveur d'impression universelle pour les requêtes HTTP/-SOAP entrantes. Valeurs par défaut **8080**.

Pour modifier le port par défaut HTTP 8080 pour les communications du serveur d'impression universelle vers des VDA XenApp et XenDesktop, le registre suivant doit également être créé et la valeur du numéro de port doit être modifiée sur l'ordinateur du serveur d'impression universelle :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\PrintingPolicies
"UpsHttpPort"=DWORD:

Ce numéro de port doit correspondre à la stratégie HDX, le port du service Web du serveur d'impression universelle (HTTP/SOAP), dans Studio.

- **Limite de bande passante d'entrée du flux d'impression du serveur d'impression universelle (kbps)**. Spécifie la limite supérieure (en kilobits par seconde) pour le transfert des données d'impression mises à disposition depuis chaque tâche d'impression vers le Serveur d'impression universelle à l'aide de CGP. La valeur par défaut est 0 (illimitée).
- **Serveurs d'impression universelle d'équilibrage de la charge**. Ce paramètre dresse la liste des serveurs d'impression universelle à utiliser pour répartir la charge des connexions aux imprimantes établies lors du lancement de la session, après l'évaluation d'autres paramètres de stratégie d'impression Citrix. Pour optimiser la durée de création des imprimantes, Citrix recommande que les mêmes imprimantes partagées soient installées sur tous les serveurs d'impression.



- **Seuil au-delà duquel les serveurs d'impression universelle sont hors service**. Indique la durée pendant laquelle l'équilibrage de charge attend le rétablissement de la connexion à un serveur d'impression universelle avant de considérer que le serveur est hors connexion et de répartir sa charge sur d'autres serveurs d'impression disponibles. Le délai par défaut est de 180 secondes.

Une fois les stratégies d'impression modifiées sur le Delivery Controller, l'application des modifications de stratégie aux VDA peut prendre quelques minutes.

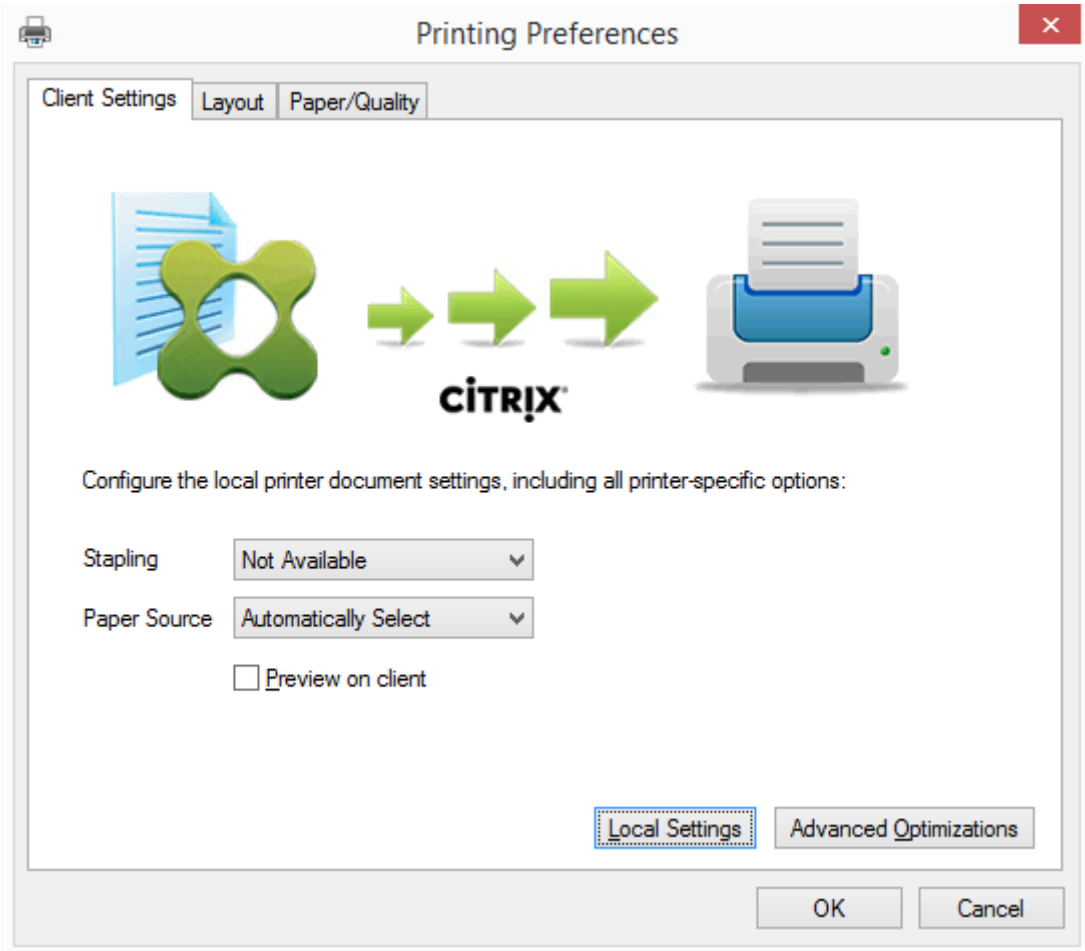
Interactions avec d'autres paramètres de stratégie : le serveur d'impression universelle respecte les autres paramètres de stratégie d'impression Citrix et interagit avec eux comme indiqué dans le tableau suivant. Les informations fournies supposent que si le paramètre de stratégie Serveur d'impression universelle est activé, les composants Serveur d'impression universelle sont installés, et les paramètres de stratégie sont appliqués.

Paramètre de stratégie	lnteraction
Redirection d'imprimante cliente, Créer automatiquement les imprimantes clientes	Si le Serveur d'impression réseau est activé, les imprimantes réseau clientes peuvent être créées à l'aide du pilote d'imprimante universelle, au lieu des pilotes natifs. Les utilisateurs aperçoivent le même nom d'imprimante qu'avant.
Imprimantes de session	Lors de l'utilisation de la solution du serveur d'impression universelle Citrix, les paramètres de stratégie du pilote d'imprimante universelle sont appliqués.
Connexions directes au serveur d'impression	Lorsque le serveur d'impression réseau est activé et que le paramètre de stratégie d'utilisation des pilotes d'imprimante universelle est configuré pour utiliser l'impression universelle uniquement, une connexion d'imprimante réseau directe peut être créée sur le serveur d'impression, à l'aide du pilote d'impression universelle.
Préférence UPD	Prend en charge les pilotes EMF et XPS.

Effets sur les interfaces utilisateur : le pilote d'impression universelle Citrix utilisé par le serveur d'impression universelle désactive les contrôles d'interface utilisateur suivants :

- dans la boîte de dialogue Propriétés d'imprimante, le bouton Paramètres d'imprimante local ;
- dans la boîte de dialogue Propriétés du document, les boutons Paramètres d'imprimante locale et Aperçu sur le client.

Le pilote d'imprimante universelle Citrix (pilotes EMF et XPS) prend en charge les fonctionnalités d'impression avancées, telles que l'agrafage et l'alimentation papier. L'utilisateur peut sélectionner les options Agrafage ou Alimentation papier dans la boîte de dialogue d'impression UDP personnalisée si le client ou les imprimantes réseau qui sont mappés sur le pilote d'imprimante universelle (UDP) dans la session prennent en charge ces fonctionnalités.



Pour configurer les paramètres d'imprimante non standard, tels que l'agrafage et le code PIN, sélectionnez **Paramètres locaux** dans la boîte de dialogue d'impression du pilote d'imprimante universelle pour les imprimantes mappées par le client qui utilisent le pilote Citrix EMF ou XPS. La boîte de dialogue **Préférences d'impression** de l'imprimante mappée est affichée en dehors de la session sur la machine cliente, ce qui permet à l'utilisateur de modifier les options d'imprimante, et les paramètres modifiés sont utilisés dans la session active lors de l'impression de ce document.

Ces fonctionnalités sont disponibles si le pilote natif les rend disponibles à l'aide de la technologie d'impression de Microsoft. Le pilote natif doit utiliser les mots clés du schéma d'impression standard dans le fichier XML des fonctionnalités d'impression. Si des mots-clés non standard sont utilisés, les fonctionnalités d'impression avancées ne seront pas disponibles à l'aide du pilote d'imprimante universelle Citrix.

Lors de l'utilisation du serveur d'impression universelle, l'assistant d'ajout d'imprimante du fournisseur d'impression Citrix est le même que l'assistant d'ajout d'imprimante du fournisseur d'impression Windows, avec les exceptions suivantes :

- Lors de l'ajout d'une imprimante par nom ou adresse, vous pouvez fournir un numéro de port HTTP/SOAP pour le serveur d'impression. Ce numéro de port devient une partie du nom

d'imprimante et apparaît dans les affichages.
- Si le paramètre de stratégie d'utilisation du pilote d'impression universelle Citrix spécifie que l'impression universelle doit être utilisée, le nom du pilote d'imprimante universelle s'affiche lors de la sélection d'une imprimante. Le fournisseur d'impression Windows ne peut utiliser le pilote d'impression universelle.

Le fournisseur d'impression Citrix ne prend pas en charge la restitution côté client.

Pour de plus amples informations sur le serveur d'impression universelle, consultez l'article CTX200328.

Imprimantes clientes créées automatiquement

Ces solutions d'impression universelle sont fournies pour les imprimantes clientes :

- **Imprimante universelle Citrix** : une imprimante générique créée au début des sessions qui n'est associée à aucun périphérique d'impression. L'imprimante universelle Citrix n'est pas requise pour énumérer les imprimantes clientes disponibles lors de l'ouverture de session, ce qui permet de réduire considérablement l'utilisation des ressources et de diminuer les durées d'ouverture de session de l'utilisateur. L'imprimante universelle peut imprimer sur n'importe quel périphérique d'impression côté client.

  L'imprimante universelle Citrix peut ne pas fonctionner pour toutes les machines utilisateur ou Citrix Receiver de votre environnement. L'imprimante universelle Citrix requiert un environnement Windows et ne prend pas en charge Citrix Offline Plug-in ou les applications livrées en streaming vers le client. Utilisez les imprimantes clientes créées automatiquement et le pilote d'impression universelle pour de tels environnements.

  Si vous souhaitez utiliser une solution d'impression universelle pour Citrix Receivers non Windows, utilisez l'un des autres pilotes d'impression universelle, qui sont basés sur postscript/PCL et sont automatiquement installés.

- **Pilotes d'impression universelle Citrix** : un pilote d'imprimante indépendant du périphérique. Si vous configurez un pilote d'impression universelle Citrix, le système utilise un pilote d'impression EMF par défaut.

  Le pilote d'impression universelle Citrix peut alors créer des tâches d'impression plus petites à l'inverse des pilotes d'imprimante plus anciens ou moins avancés. Toutefois, un pilote spécifique à la machine peut être nécessaire pour optimiser les tâches d'impression pour une imprimante spécialisée.

Configurer l'impression universelle : utilisez les paramètres de stratégie Citrix suivants pour configurer l'impression universelle. Pour plus d'informations, reportez-vous à l'aide des paramètres de stratégie à l'écran.

- Utilisation du pilote d'impression universelle Indique quand utiliser l'impression universelle.
- Créer automatiquement l'imprimante universelle générique. Active ou désactive la création automatique de l'objet d'imprimante universelle Citrix générique pour les sessions lorsqu'une machine utilisateur compatible avec l'impression universelle est en cours d'utilisation. Par défaut, l'objet Imprimante universelle générique n'est pas créé automatiquement.
- Préférence de pilote universel Spécifie l'ordre dans lequel le système tente d'utiliser les pilotes d'impression universelle, en commençant par la première entrée de la liste. Vous pouvez ajouter, modifier ou supprimer des pilotes et changer leur ordre dans la liste.
- Préférence d'aperçu d'impression universelle. Spécifie s'il convient d'utiliser la fonction d'aperçu d'impression pour les imprimantes universelles génériques ou créées automatiquement.
- Mode de traitement EMF de l'impression universelle. Contrôle la méthode de traitement du fichier de spoul EMF sur la machine utilisateur Windows. Par défaut, les enregistrements EMF sont spoulés directement sur l'imprimante. Le spoulage directement vers l'imprimante permet au spouleur de traiter les enregistrements plus rapidement et utiliser moins de ressources d'UC.

Vous trouverez des stratégies supplémentaires dans la section Optimiser les performances d'impression. Pour modifier les valeurs par défaut des paramètres tels que la taille du papier, la qualité du papier, la couleur, l'impression recto verso et le nombre de copies, consultez l'article CTX113148.

Créer automatiquement des imprimantes depuis la machine de l'utilisateur : au début de la session, le système crée automatiquement toutes les imprimantes sur la machine utilisateur par défaut. Vous pouvez contrôler quels types, le cas échéant, d'imprimantes sont provisionnés auprès des utilisateurs et empêchent la création automatique.

Utilisez le paramètre de stratégie
Citrix Créer automatiquement les imprimantes clientes pour contrôler la création automatique. Vous pouvez spécifier l'un des éléments suivants :

- toutes les imprimantes visibles pour la machine cliente, y compris les imprimantes connectées localement et les imprimantes réseau, sont créées automatiquement au début de chaque session (valeur par défaut) ;
- toutes les imprimantes locales connectées physiquement à la machine cliente sont créées automatiquement ;
- seule l'imprimante par défaut de la machine cliente est créée automatiquement.
- La création automatique est désactivée pour toutes les imprimantes clientes

Le paramètre Créer automatiquement les imprimantes clientes nécessite que le paramètre Redirection d'imprimante cliente soit Autorisé (valeur par défaut).

Attribuer les imprimantes réseau aux utilisateurs

Par défaut, les imprimantes réseau de la machine cliente sont créées automatiquement au début des sessions. Le système vous permet de réduire le nombre d'imprimantes réseau énumérées et mappées en spécifiant les imprimantes réseau à créer dans chaque session. Certaines de ces imprimantes sont appelées Imprimantes de session.

Vous pouvez filtrer des stratégies d'imprimante de session par adresse IP pour offrir l'impression de proximité. L'impression de proximité permet aux utilisateurs se trouvant dans une plage d'adresses IP spécifiée d'accéder automatiquement aux périphériques d'impression réseau existant dans la même plage. L'impression de proximité est fournie par le Serveur d'impression universelle Citrix et ne nécessite pas la configuration décrite dans cette section.

L'impression de proximité peut impliquer le scénario suivant :

- Le réseau d'entreprise interne fonctionne avec un serveur DHCP qui attribue automatiquement les adresses IP aux utilisateurs.
- Tous les services d'une entreprise possèdent des plages d'adresses IP désignées uniques.
- Des imprimantes réseau existent dans la plage d'adresses IP de chaque service.

Lorsque l'impression de proximité est configurée et un employé voyage d'un service à un autre, aucune autre configuration du périphérique d'impression n'est requise. Lorsque la machine utilisateur est reconnue dans la plage d'adresse IP du nouveau service, elle a accès à toutes les imprimantes réseau de cette plage.

Configurer des imprimantes spécifiques devant être redirigées dans les sessions : pour créer des imprimantes attribuées à l'administrateur, configurez le paramètre de stratégie
Citrix Imprimantes de session. Ajoutez une imprimante réseau à cette stratégie à l'aide de l'une des méthodes suivantes :

- Entrez le chemin UNC de l'imprimante au format \\nomserveur\nomimprimante.
- Rechercher un emplacement d'imprimante sur le réseau.
- Recherchez des imprimantes sur un serveur spécifique. Entrez le nom du serveur selon le format \\nomserveur et cliquez sur Parcourir.

> **Important :**
>
> Le serveur fusionne tous les paramètres d'imprimantes de session activés de toutes les stratégies appliquées en commençant par celles dont la priorité est la plus élevée. Lorsqu'une imprimante est configurée dans plusieurs objets de stratégie, les paramètres personnalisés par défaut ne sont utilisés qu'à partir de l'objet de stratégie ayant la plus haute priorité dans laquelle cette imprimante est configurée.

Les imprimantes réseau créées à l'aide du paramètre Imprimantes de session peuvent varier selon les conditions dans lesquelles la session a été initiée, en appliquant un filtre sur les objets comme les sous-réseaux.

Spécifiez une imprimante réseau par défaut pour une session : par défaut, l'imprimante principale de l'utilisateur est utilisée comme imprimante par défaut pour la session. Utilisez le paramètre de stratégie Citrix Imprimante par défaut pour changer la façon dont l'imprimante par défaut sur la machine utilisateur est établie dans une session.

1. Sur la page de paramètres Imprimante par défaut, sélectionnez un paramètre pour Choisir l'imprimante par défaut du client :
    - Nom d'imprimante réseau. Les imprimantes ajoutées avec le paramètre de stratégie Imprimantes de session s'affichent dans ce menu. Sélectionnez l'imprimante réseau à utiliser comme valeur par défaut de cette stratégie.
    - Ne pas ajuster l'imprimante par défaut de l'utilisateur. Utilise le réglage du profil utilisateur courant pour l'imprimante par défaut. Pour plus d'informations, reportez-vous à l'aide des paramètres de stratégie à l'écran.
2. Appliquez la stratégie au groupe d'utilisateurs (ou autres objets filtrés) que vous souhaitez attribuer.

Configurer l'impression de proximité : l'impression de proximité est également fournie par le Serveur d'impression universelle Citrix, qui ne nécessite pas la configuration décrite ici.

1. Créez une stratégie distincte pour chaque sous-réseau (ou pour correspondre à l'emplacement de l'imprimante).
2. Dans chacune de ces stratégies, ajoutez les imprimantes de l'emplacement géographique de ce sous-réseau au paramètre Imprimantes de session.
3. Attribuez au paramètre Imprimante par défaut la valeur Ne pas ajuster l'imprimante par défaut de l'utilisateur.
4. Filtrez les stratégies par adresse IP cliente. Veillez à mettre à jour ces stratégies pour refléter les modifications apportées aux plages d'adresses IP DHCP.

Gérer l'environnement d'impression

January 23, 2019

La gestion de votre environnement d'impression comprend :

- Gestion des pilotes d'imprimante
- Optimisation des performances d'impression
- Affichage de l'imprimante et gestion des files d'attente d'impression

Gestion des pilotes d'imprimantes

Pour réduire les coûts administratifs et les éventuels problèmes de pilote d'impression, Citrix vous recommande d'utiliser le pilote d'imprimante universelle Citrix.

Si la création automatique échoue, par défaut, le système installe un pilote d'imprimante natif Windows fourni avec Windows. Si un pilote n'est pas disponible, le système retourne au pilote d'impression universelle. Pour de plus amples informations sur les valeurs par défaut du pilote d'imprimante, veuillez consulter la section Recommandations, considérations en matière de sécurité et opérations par défaut.

Si le pilote d'impression universelle Citrix n'est pas une option pour tous les scénarios, mappez les pilotes d'imprimante pour réduire la quantité de pilotes installés sur les machines avec OS de serveur. En outre, le mappage des pilotes d'imprimante vous permet de :

- autoriser les imprimantes spécifiques à utiliser uniquement les pilotes d'impression universelle Citrix ;
- autoriser ou empêcher la création d'imprimantes avec un pilote spécifique ;
- remplacer les pilotes d'imprimante appropriés par des pilotes altérés ou périmés ;
- remplacer un pilote disponible sur le serveur Windows par un nom de pilote client.

Empêcher l'installation automatique des pilotes d'imprimante : l'installation automatique de pilotes d'impression doit être désactivée pour assurer la cohérence entre les machines avec OS de serveur. Cela peut être assuré au travers des stratégies Citrix, Microsoft ou les deux. Pour empêcher l'installation automatique des pilotes d'imprimante natifs Windows, désactivez le paramètre de stratégie Citrix Installation automatique de pilotes d'imprimante fournis avec Windows.

Mappage des pilotes d'imprimante des clients : chaque client fournit des informations sur les imprimantes côté client au cours de l'ouverture de session, notamment le nom du pilote d'imprimante. Lors de la création automatique de l'imprimante client, le nom des pilotes d'imprimantes des serveurs Windows sont sélectionnés de manière à correspondre aux noms des modèles d'imprimante fournis par le client. Le processus de création automatique utilise ensuite les pilotes d'imprimantes identifiés et disponibles de manière à créer les files d'impression des clients redirigés.

Le processus général de définition des règles de remplacement de pilotes et de modification des paramètres d'impression pour les pilotes d'imprimantes clientes mappées est le suivant .

1. Pour spécifier les règles de remplacement des pilotes pour les imprimantes clientes créées automatiquement, configurez le paramètre de stratégie Citrix Mappage et compatibilité du pilote d'imprimante en ajoutant le nom du pilote d'imprimante cliente et en sélectionnant le pilote de serveur à utiliser à la place du pilote d'imprimante cliente dans le menu Rechercher un pilote d'imprimante. Vous pouvez utiliser des caractères génériques dans ce paramètre. Par exemple, pour obliger toutes les imprimantes HP à utiliser un pilote spécifique, spécifiez HP* dans le paramètre de stratégie.
2. Pour interdire un pilote d'imprimante, sélectionnez le nom de pilote et choisissez le paramètre Ne pas créer.
3. Le cas échéant, vous pouvez modifier un mappage existant, supprimer un mappage ou modifier l'ordre des entrées de pilote dans la liste.

4. Pour modifier les paramètres d'impression pour les pilotes d'imprimantes clientes mappées, sélectionnez le pilote d'imprimante, cliquez sur Paramètres, puis spécifiez les paramètres tels que la qualité d'impression, l'orientation et la couleur. Si vous spécifiez une option d'impression que le pilote d'imprimante ne prend pas en charge, cette option n'a aucun effet. Ce paramètre écrase les paramètres d'imprimante définis par l'utilisateur durant une session précédente.
5. Citrix vous recommande de tester le comportement des imprimantes en détail après le mappage des pilotes, car certaines fonctionnalités d'imprimante peuvent être disponibles uniquement avec un pilote spécifique.

Lorsque les utilisateurs ouvrent une session, le système vérifie la liste de compatibilité des pilotes d'imprimantes clients avant de configurer les imprimantes clientes.

Optimiser les performances d'impression

Pour optimiser les performances d'impression, utilisez le Serveur d'impression universelle et un pilote d'impression universelle. Les stratégies suivantes contrôlent l'optimisation et la compression de l'impression :

- Valeurs par défaut de l'optimisation de l'impression universelle. Spécifie les valeurs par défaut de l'imprimante universelle lorsqu'elle est créée pour une session :
  - Qualité d'image souhaitée spécifie la limite de compression d'image par défaut appliquée à l'impression universelle. Par défaut, Qualité standard est activée, signifiant que les utilisateurs peuvent uniquement imprimer des images à l'aide des compressions standard ou de qualité réduite.
  - Activer la compression lourde active ou désactive la réduction de la bande passante au-delà du niveau de compression défini par l'option Qualité d'image souhaitée, sans perte de qualité d'image. Par défaut, la compression intensive est désactivée.
  - Les paramètres Cache d'image et de police spécifient si oui ou non vous pouvez cacher des images et des polices qui s'affichent plusieurs fois dans le flux d'impression, assurant ainsi que chaque image ou police est envoyée à l'imprimante une seule fois. Par défaut, les images incorporées et les polices sont mises en cache.
  - Autoriser les non-administrateurs à modifier ces paramètres spécifie si les utilisateurs peuvent ou non modifier les paramètres d'optimisation d'impression dans une session. Par défaut, les utilisateurs ne sont pas autorisés à modifier les paramètres par défaut d'optimisation de l'impression.
- Limite de compression d'image de l'impression universelle. Définit la qualité maximale et le niveau de compression minimal disponibles pour les images imprimées avec le pilote d'imprimante universelle. Par défaut, la limite de compression d'image est définie sur Meilleure qualité (compression sans perte).
- Limite de qualité d'impression de l'impression universelle. Spécifie le nombre maximal de points par pouce (dpi) disponible pour l'impression dans la session. Par défaut, aucune limite

n'est spécifiée.

Par défaut, toutes les tâches d'impression sont destinées à la route d'imprimantes réseau à partir de la machine avec OS de serveur, au travers du réseau, et directement vers le serveur d'impression. Envisagez le routage des tâches d'impression via la connexion ICA si le réseau possède une certaine latence ou une bande passante limitée. Pour ce faire, désactivez le paramètre de stratégie Citrix Connexions directes aux serveurs d'impression. Les données envoyées aux clients via la connexion ICA sont compressées. Les transmissions de données sur le réseau étendu nécessitent donc moins de bande passante.

Améliorer les performances de session en limitant la bande passante d'impression : lors de l'impression de fichiers depuis des machines avec OS de serveur vers les imprimantes utilisateur, il se peut que d'autres canaux virtuels (vidéo, par exemple) peuvent rencontrer une baisse des performances en raison de compétition de la bande passante, spécialement si les utilisateurs accèdent à des serveurs via des réseaux lents. Pour empêcher ce type de dégradation, vous pouvez limiter la bande passante utilisée par l'impression cliente. En limitant la vitesse de transfert des données d'impression, vous pouvez augmenter la bande passante disponible dans le flux de données HDX pour le transfert des données vidéo et des informations relatives aux frappes clavier et aux clics de souris.

Important : si une limite de bande passante d'impression est définie, elle est respectée même lorsqu'aucun autre canal n'est utilisé.

Utilisez les paramètres d'imprimante de la stratégie Citrix
Bande passante pour configurer les limites de session de bande passante d'impression. Pour définir les limites pour le site, réalisez cette tâche à l'aide de Studio. Pour définir les limites pour des serveurs individuels, effectuez cette tâche à l'aide de la console de gestion des stratégies de groupe dans Windows localement sur chaque machine avec OS de serveur.

- Le paramètre Limite de bande passante de redirection d'imprimante permet de spécifier la bande passante en kilobits par seconde (kbps) disponible pour l'impression.
- Le paramètre Pourcentage de limite de bande passante de redirection de l'imprimante permet de limiter la bande passante disponible pour l'impression à un pourcentage de la bande passante générale disponible.

  Remarque : pour spécifier la bande passante sous forme de pourcentage à l'aide du paramètre Pourcentage de limite de bande passante de redirection de l'imprimante, activez également le paramètre
  Limite de bande passante de session générale.

  Si vous entrez des valeurs pour les deux paramètres, le paramètre le plus restrictif (ayant la valeur la plus faible) est appliqué.

Pour obtenir des informations en temps réel sur la bande passante d'impression, utilisez Citrix Director.

Équilibrer la charge des serveurs d'impression universelle

La solution de serveur d'impression universelle peut monter en charge en ajoutant davantage de serveurs d'impression dans la solution d'équilibrage de charge. Il n'existe aucun point de défaillance unique car chaque VDA dispose de son propre équilibreur de charge pour répartir la charge d'impression auprès de tous les serveurs d'impression.

Utilisez les paramètres de stratégie, Serveurs d'impression universelle d'équilibrage de la charge et Seuil au-delà duquel les serveurs d'impression universelle sont hors service, pour répartir la charge de l'impression auprès de tous les serveurs d'impression dans la solution d'équilibrage de charge.

En cas de défaillance imprévue d'un serveur d'impression, le mécanisme de basculement de l'équilibreur de charge de chaque VDA répartit automatiquement les connexions d'imprimantes attribuées aux serveurs d'impression défaillants aux autres serveurs d'impression disponibles de façon à ce que toutes les sessions existantes et entrantes fonctionnent normalement sans affecter l'expérience de l'utilisateur et sans nécessiter l'intervention immédiate de l'administrateur.

Les administrateurs peuvent surveiller l'activité des serveurs d'impression d'équilibrage de charge à l'aide d'un ensemble de compteurs de performances pour suivre les indicateurs suivants sur le VDA :

- Liste des serveurs d'impression dont la charge est équilibrée sur le VDA et leur état (disponible, indisponible)
- Nombre de connexions d'imprimantes acceptées par chaque serveur d'impression
- Nombre d'échecs de connexions d'imprimantes sur chaque serveur d'impression
- Nombre de connexions d'imprimantes actives sur chaque serveur d'impression
- Nombre de connexions d'imprimantes en attente sur chaque serveur d'impression

Afficher et gérer les files d'attente d'impression

Le tableau suivant récapitule l'emplacement d'affichage des imprimantes et de gestion des files d'attente dans votre environnement.

	Piste d'impression	Emplacement
Imprimantes clientes (imprimantes connectées à la machine utilisateur)	Piste d'impression cliente	UAC activé : Composant logiciel enfichable Gestion d'impression dans la console Microsoft Management Console ; UAC désactivé : Pré-Windows 8 : Panneau de configuration, Windows 8 : Composant logiciel enfichable Gestion de l'impression
Imprimantes réseau (Imprimantes sur un serveur d'impression réseau)	Piste d'impression réseau	UAC activé : Serveur d'impression > Composant logiciel enfichable Gestion de l'impression dans la console Microsoft Management Console ; UAC désactivé : Serveur d'impression > Panneau de configuration
Imprimantes réseau (Imprimantes sur un serveur d'impression réseau)	Piste d'impression cliente	UAC activé : Serveur d'impression > Composant logiciel enfichable Gestion d'impression dans la console Microsoft Management Console ; UAC désactivé : Pré-Windows 8 : Panneau de configuration, Windows 8 : Composant logiciel enfichable Gestion de l'impression
Imprimantes serveur réseau locales (Imprimantes d'un serveur d'impression réseau qui sont ajoutées à une machine avec OS de serveur)	Piste d'impression réseau	UAC activé : Serveur d'impression > Panneau de configuration ; UAC désactivé : Serveur d'impression > Panneau de configuration

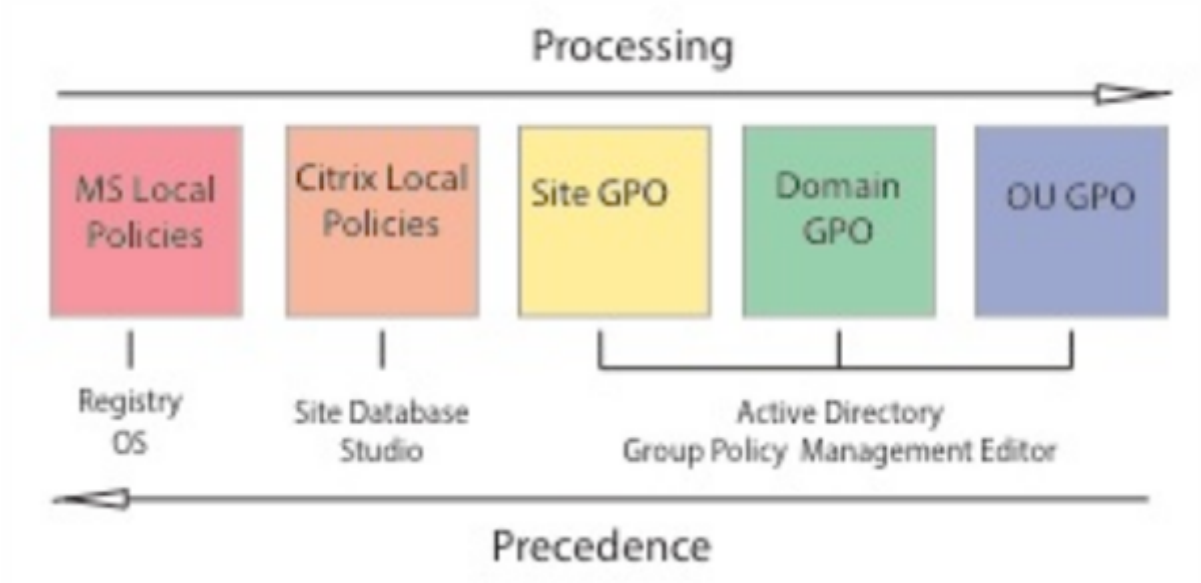
> **Remarque :**
>
> Les files d'attente d'impression des imprimantes réseau utilisant la piste d'impression réseau sont privées et ne peuvent être gérées au travers du système.

Stratégies

November 9, 2018

Les stratégies sont un ensemble de paramètres qui définissent la façon dont les sessions, la bande passante et la sécurité sont gérées pour un groupe d'utilisateurs, de machines, ou de types de connexion.

Vous pouvez appliquer des paramètres de stratégie à des machines physiques et virtuelles ou à des utilisateurs. Vous pouvez appliquer des paramètres à des utilisateurs individuels au niveau local ou dans les groupes de sécurité dans Active Directory. Les configurations définissent des critères et des règles spécifiques. Si vous n'attribuez pas spécifiquement les stratégies, les paramètres sont appliqués à toutes les connexions.



Vous pouvez appliquer des stratégies sur différents niveaux du réseau. Les paramètres de stratégie placés au niveau de l'objet de stratégie de groupe de l'unité d'organisation prennent la plus haute priorité sur le réseau. Les stratégies au niveau de l'objet de stratégie de groupe du domaine remplacent les stratégies au niveau de l'objet de stratégie de groupe du site, qui remplacent les stratégies en conflit sur les deux niveaux Microsoft et Stratégies locales Citrix.

Toutes les stratégies locales Citrix sont créées et gérées dans la console Citrix Studio et stockées dans la base de données du site. Les stratégies de groupe sont créées et gérées à l'aide de la console de

gestion des stratégies de groupe Microsoft (GPMC) et stockées dans Active Directory. Les stratégies locales Microsoft sont créées dans le système d'exploitation Windows et sont stockées dans le Registre.

Studio utilise un assistant de modélisation pour aider les administrateurs à comparer les paramètres de configuration dans les modèles et stratégies pour vous aider à éliminer tout paramètre en conflit ou redondant. Les administrateurs peuvent définir leurs objets de stratégie de groupe à l'aide de GPMC pour configurer les paramètres et les appliquer à un ensemble cible d'utilisateurs à différent niveaux du réseau.

Ces objets de stratégie de groupe sont enregistrés dans Active Directory, et l'accès à l'administration de ces paramètres est limité pour la plupart des services informatiques pour des raisons de sécurité.

Les paramètres sont fusionnés selon leur priorité et leur condition. Tout paramètre désactivé remplace un paramètre d'une priorité plus faible activé. Tout paramètre de stratégie non configuré est ignoré et ne remplace pas les paramètres de priorité inférieure.

Les stratégies locales peuvent également être en conflit avec des stratégies de groupe dans Active Directory, qui peuvent se remplacer entre elles, selon le cas.

Toutes les stratégies sont traitées dans l'ordre suivant :

1. L'utilisateur ouvre une session sur une machine à l'aide des informations d'identification de domaine.
2. Les informations d'identification sont envoyées au contrôleur de domaine.
3. Active Directory applique toutes les stratégies (utilisateur final, point de terminaison, unité d'organisation et domaine).
4. L'utilisateur ouvre une session sur Receiver et accède à une application ou à un bureau.
5. Citrix et les stratégies Microsoft sont traitées pour l'utilisateur et la machine qui héberge la ressource.
6. Active Directory détermine la priorité pour les paramètres de stratégie. Il les applique ensuite aux registres de la machine de point de terminaison et à la machine hébergeant la ressource.
7. L'utilisateur ferme sa session sur la ressource. Les stratégies Citrix pour l'utilisateur et la machine de point de terminaison ne sont plus actives.
8. L'utilisateur ferme sa session sur la machine utilisateur, ce qui libère les stratégies utilisateur de l'objet de stratégie de groupe.
9. L'utilisateur éteint le périphérique, ce qui libère les stratégies de machine de l'objet de stratégie de groupe.

Lorsque vous créez des stratégies pour des groupes d'utilisateurs, des périphériques et des machines, certains membres peuvent avoir différents besoins et auraient besoin d'exceptions à certains paramètres de stratégie. Les exceptions sont effectuées via des filtres dans Studio et le GPMC qui déterminent ce qui est affecté par la stratégie.

> **Remarque**
>
> Nous ne prenons pas en charge le mélange de stratégies Windows et Citrix dans le même objet de stratégie de groupe.

Utilisation des stratégies

January 23, 2019

Configurez des stratégies Citrix pour contrôler l'accès utilisateur ou les environnements de session. Les stratégies Citrix constituent la méthode la plus efficace pour contrôler les paramètres de connexion, de sécurité et de bande passante. Vous pouvez créer des stratégies relatives à des groupes d'utilisateurs, des machines ou des types de connexion spécifiques. Chaque stratégie peut contenir plusieurs paramètres.

Outils pour l'utilisation de stratégies Citrix

Vous pouvez utiliser les outils suivants pour fonctionner avec les stratégies Citrix.

- **Studio** : si vous êtes un administrateur Citrix ne disposant pas de permissions de gérer la stratégie de groupe, utilisez Studio pour créer des stratégies pour votre site. Les stratégies créés avec Studio sont enregistrées dans la base de données du site et les mises à jour sont déployées vers le bureau virtuel soit lorsque celui-ci s'enregistre auprès du broker, soit lorsque l'utilisateur se connecte à ce bureau virtuel.
- **Éditeur de stratégie de groupe locale** (composant logiciel enfichable Microsoft Management Console) : si votre environnement réseau utilise Active Directory et que vous avez l'autorisation de gérer la stratégie de groupe, vous pouvez utiliser l'éditeur de stratégie de groupe local pour créer des stratégies pour votre site. Les paramètres que vous configurez affectent les objets de stratégie de groupe que vous spécifiez via la console de gestion des stratégies de groupe.
  Important : vous devez utiliser l'éditeur de stratégie de groupe local pour configurer certains paramètres de stratégie, y compris ceux associés à l'enregistrement des VDA auprès d'un Controller et ceux associés aux serveurs Microsoft App-V.

Ordre de traitement et priorité des stratégies

Les paramètres de stratégie de groupe sont traités dans l'ordre suivant :

1. GPO local
2. Objet de stratégie de groupe du site XenApp ou XenDesktop (stocké dans la base de données du site)

3. GPO au niveau du site
4. GPO au niveau du domaine
5. Unités d'organisation

Cependant, si un conflit se produit, les paramètres de stratégie qui sont traités en dernier peuvent remplacer ceux qui sont traités en premier. Ceci signifie que les paramètres de stratégie sont prioritaires dans l'ordre suivant :

1. Unités d'organisation
2. GPO au niveau du domaine
3. GPO au niveau du site
4. Objet de stratégie de groupe du site XenApp ou XenDesktop (stocké dans la base de données du site)
5. GPO local

Par exemple, un administrateur Citrix utilise Studio pour créer une stratégie (Stratégie A) qui active la redirection de fichier client pour les employés du département Ventes de l'entreprise. Pendant ce temps, un autre administrateur utilise l'éditeur de stratégie de groupe pour créer une stratégie (Stratégie B) qui désactive la redirection de fichier client pour les employés des ventes. Lorsque les employés des ventes ouvrent une session sur les bureaux virtuels, la Stratégie B est appliquée et la Stratégie A est ignorée car la Stratégie B a été traitée au niveau du domaine et la Stratégie A a été traitée au niveau du GPO de site XenApp ou XenDesktop.

Toutefois lorsqu'un utilisateur lance une session ICA ou RDP (Protocole Bureau à distance), les paramètres de la session Citrix remplacent les mêmes paramètres configurés dans une stratégie Active Directory ou à l'aide de la Configuration d'hôte de session Bureau à distance. Ceci comprend les paramètres liés aux paramètres de connexion client RDP standard tels que Papier peint du bureau, Animation de menu et Afficher le contenu de la fenêtre lors d'un cliquer déplacer.

Lors de l'utilisation de plusieurs stratégies, vous pouvez établir des priorités pour les stratégies qui contiennent des paramètres conflictuels ; voir Comparer, donner un ordre de priorité, modéliser et résoudre les problèmes des stratégies pour plus de détails.

Flux de travail des stratégies Citrix

Le processus de configuration des stratégies est le suivant :

1. Créez la stratégie.
2. Configurez les paramètres de stratégie.
3. Affectez la stratégie aux objets machine et utilisateur.
4. Définissez l'ordre de priorité de la stratégie.
5. Vérifiez la stratégie effective en exécutant l'assistant Modélisation de stratégie de groupe Citrix.

Naviguer vers les stratégies et paramètres Citrix

Dans l'éditeur de stratégie de groupe local, les stratégies et les paramètres apparaissent dans deux catégories : Configuration ordinateur et Configuration utilisateur. Chaque catégorie a un nœud Stratégies Citrix. Consultez la documentation Microsoft pour plus de détails sur la navigation et l'utilisation de ce composant logiciel enfichable.

Dans Studio, les paramètres de stratégie sont triés dans des catégories en fonction de la fonctionnalité ou fonction qu'ils affectent. Par exemple, la section Profile Management contient des paramètres de stratégie pour Profile Management.

- Les paramètres Ordinateur (paramètres de stratégie s'appliquant aux machines) définissent le comportement des bureaux virtuels et sont appliqués lorsqu'un bureau virtuel démarre. Ces paramètres s'appliquent même s'il n'y a pas de session utilisateur active sur le bureau virtuel. Les paramètres utilisateur définissent l'expérience de l'utilisateur lors de la connexion à l'aide du protocole ICA. Les stratégies utilisateur sont appliquées lorsqu'un utilisateur se connecte ou se reconnecte à l'aide du protocole ICA. Les stratégies utilisateur ne sont pas appliquées si un utilisateur se connecte à l'aide de RDP ou ouvre une session directement sur la console.

  Pour accéder aux stratégies, paramètres ou modèles, sélectionnez Stratégies dans le panneau de navigation de Studio.

  - L'onglet **Stratégies** répertorie toutes les stratégies. Lorsque vous sélectionnez une stratégie, les onglets de droite affichent : Présentation (nom, priorité, statut activé/désactivé et description), Paramètres (liste des paramètres configurés) et Attribués à (objets utilisateur et machine auxquels la stratégie est actuellement affectée). Pour de plus amples informations, consultez la section Créer des stratégies.
  - L'onglet **Modèles** répertorie des modèles fournis par Citrix et personnalisés que vous avez créés. Lorsque vous sélectionnez un modèle, les onglets de droite affichent : Description (la raison pour laquelle vous souhaitez utiliser le modèle) et Paramètres (liste des paramètres configurés). Pour plus d'informations, veuillez consulter la section Modèles de stratégie.
  - L'onglet **Comparaison** vous permet de comparer les paramètres d'une stratégie ou d'un modèle avec ceux des autres stratégies ou modèles. Par exemple, il se peut que vous souhaitiez vérifier les valeurs des paramètres pour assurer la compatibilité avec les meilleures pratiques. Pour plus d'informations, consultez la section Comparer, donner un ordre de priorité, modéliser et résoudre les problèmes des stratégies.
  - À partir de l'onglet **Modélisation**, vous pouvez simuler des scénarios de connexion avec les stratégies Citrix. Pour plus d'informations, consultez la section Comparer, donner un ordre de priorité, modéliser et résoudre les problèmes des stratégies.

  Pour rechercher un paramètre dans une stratégie ou un modèle :

  1. Sélectionnez la stratégie ou le modèle.

2. Sélectionnez Modifier la stratégie ou Modifier le modèle dans le volet Actions.
3. Sur la page Paramètres, commencez à taper le nom du paramètre.

Vous pouvez affiner votre recherche en sélectionnant une version spécifique du produit, en sélectionnant une catégorie (par exemple, Bande passante), ou en sélectionnant la case à cocher Afficher sélectionné uniquement ou en sélectionnant pour ne rechercher que les paramètres qui ont été ajoutés à la stratégie sélectionnée. Pour une recherche non filtrée, sélectionnez Tous les paramètres.

- Pour rechercher un paramètre dans une stratégie :

1. Sélectionnez la stratégie.
2. Sélectionnez l'onglet Paramètres, commencez à taper le nom du paramètre.

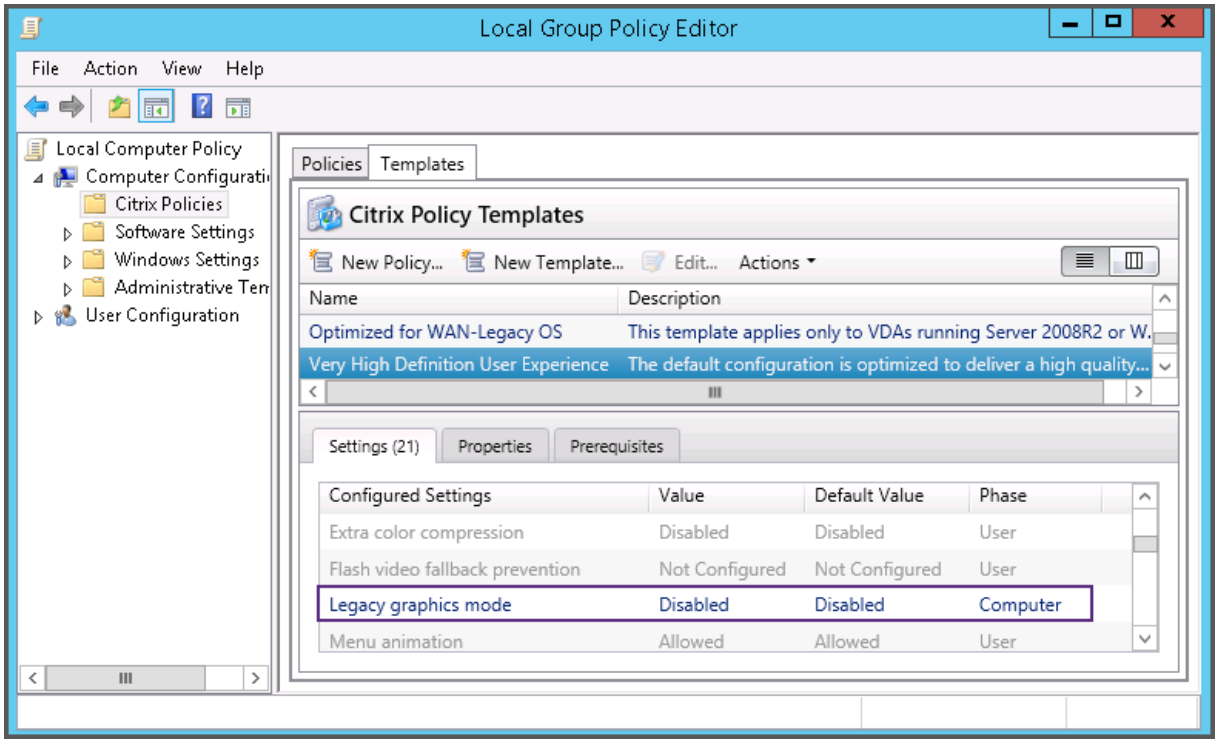
Vous pouvez affiner votre recherche en sélectionnant une version spécifique du produit ou en sélectionnant une catégorie. Pour une recherche non filtrée, sélectionnez Tous les paramètres.

Une stratégie, une fois qu'elle a été créée, est complètement indépendante du modèle utilisé. Vous pouvez utiliser le champ Description d'une nouvelle stratégie pour le suivi de la source modèle utilisé.

Dans Studio, les stratégies et les modèles sont affichés dans une liste unique, qu'ils contiennent des paramètres Utilisateur, Ordinateur ou les deux types de paramètres et peuvent être appliqués à l'aide de filtres Utilisateur et Ordinateur.

Dans l'éditeur de stratégie de groupe, les paramètres Ordinateur et Utilisateur doivent être appliqués séparément, même s'ils ont été créés à partir d'un modèle qui contient les deux types de paramètres. Dans cet exemple, vous choisissez d'utiliser le paramètre Expérience utilisateur très haute définition dans Configuration ordinateur :

- Le Mode graphique d'ancienne génération est un paramètre Ordinateur qui sera utilisé dans une stratégie créée à partir de ce modèle.
- Les paramètres Utilisateur, grisés, ne seront pas utilisés dans une stratégie créée à partir de ce modèle.



Modèles de stratégie

November 9, 2018

Les modèles sont utilisés pour créer des stratégies à partir d'un point de départ prédéfini. Les modèles Citrix incorporés, optimisés pour des environnements ou des conditions réseau spécifiques, peuvent être utilisés en tant que :

- Source pour créer vos propres stratégies et modèles à partager entre les sites.
- Référence pour comparer en toute facilité les résultats entre déploiements en vous permettant de faire état des résultats, par exemple, « …lors de l'utilisation du modèle Citrix x ou y… »
- Méthode permettant de transmettre des stratégies au support Citrix ou à des tiers de confiance en important ou exportant des modèles.

Les modèles de stratégies peuvent être importés ou exportés. Pour de plus amples informations sur les modèles et/ou sur les mises à jour apportées aux modèles incorporés, consultez l'article CTX202000.

Pour les considérations à prendre en compte lors de l'utilisation de modèles pour créer des stratégies, veuillez consulter l'article CTX202330.

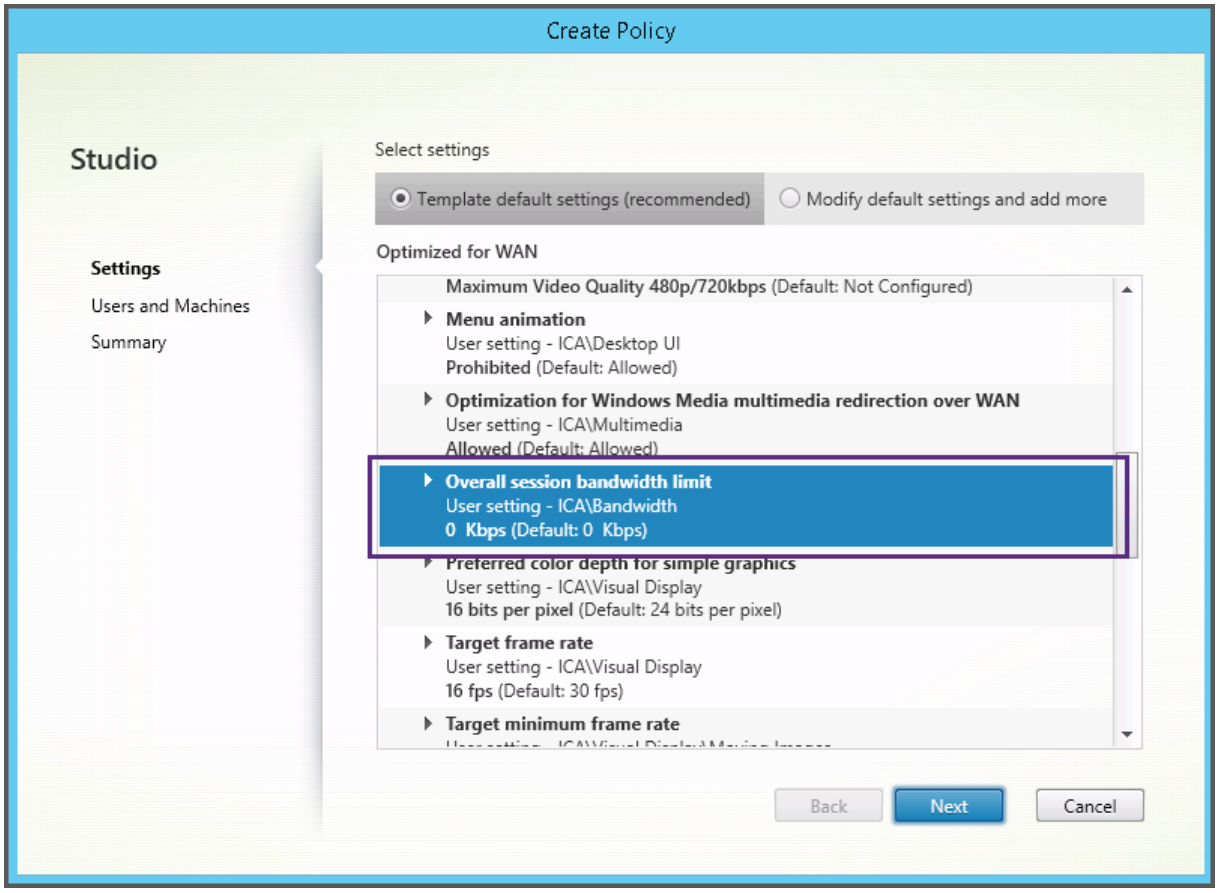
Modèles Citrix incorporés

Les modèles de stratégie suivants sont disponibles :

- **Expérience utilisateur très haute définition**. Ce modèle applique les paramètres par défaut ce qui optimise l'expérience utilisateur. Utilisez ce modèle dans les scénarios dans lesquels plusieurs stratégies sont traitées par ordre de priorité.
- **Montée en charge du serveur élevée**. Appliquez ce modèle pour économiser les ressources du serveur. Ce modèle assure un excellent compromis entre expérience utilisateur et montée en charge du serveur. Il offre une expérience utilisateur des plus satisfaisantes tout en augmentant le nombre d'utilisateurs que vous pouvez héberger sur un seul serveur. Ce modèle n'utilise pas le codec vidéo pour la compression de graphiques et empêche la génération de multimédia côté serveur.
- **Montée en charge du serveur élevée - anciens systèmes d'exploitation**. Ce modèle de montée en charge du serveur élevée s'applique uniquement aux VDA exécutant Windows Server 2008 R2 ou Windows 7 et versions antérieures. Ce modèle s'appuie sur le Mode graphique d'ancienne génération qui est plus efficace pour ces systèmes d'exploitation.
- **Optimisé pour NetScaler SD-WAN.** Appliquez ce modèle pour les utilisateurs qui travaillent depuis des succursales avec NetScaler SD-WAN pour optimiser la mise à disposition de XenDesktop. (NetScaler SD-WAN est la nouvelle appellation de CloudBridge).
- **Optimisé pour les connexions WAN**. Ce modèle est conçu pour les utilisateurs qui travaillent dans des succursales (connexions WAN partagées) ou depuis des sites distants utilisant des connexions à faible bande passante qui accèdent à des applications dotées d'interfaces graphiques simples et contenant très peu de contenu multimédia. Ce modèle optimise l'efficacité de la bande passante au détriment de l'expérience de lecture vidéo et de la montée en charge du serveur.
- **Optimisé pour les connexions WAN – anciens systèmes d'exploitation**. Ce modèle s'applique uniquement aux VDA exécutant Windows Server 2008 R2 ou Windows 7 et versions antérieures. Ce modèle s'appuie sur le Mode graphique d'ancienne génération qui est plus efficace pour ces systèmes d'exploitation.
- **Sécurité et contrôle**. Utilisez ce modèle dans les environnements dans lesquels la tolérance aux risques est faible, de façon à limiter les fonctionnalités activées par défaut dans XenApp et XenDesktop. Ce modèle contient des paramètres qui désactivent l'accès à l'impression, au Presse-papiers, aux périphériques, au mappage de lecteurs, à la redirection de port et à l'accélération Flash sur les machines utilisateur. L'application de ce modèle peut consommer plus de bande passante et réduire le nombre d'utilisateurs par serveur.

Bien que nous recommandions d'utiliser les modèles Citrix intégrés avec leurs paramètres par défaut, vous trouverez des paramètres pour lesquels aucune valeur spécifique n'a été recommandée, par exemple « Limite de bande passante de session générale », inclus dans les modèles Optimisé pour les connexions WAN. Dans ce cas, le modèle expose le paramètre de façon à faire comprendre à

l'administrateur que ce paramètre est susceptible de s'appliquer au scénario.



Si vous travaillez avec un déploiement (gestion de la stratégie et VDA) antérieur à XenApp et XenDesktop 7.6 FP3, et avez besoin de modèles Montée en charge du serveur élevée et Optimisé pour les connexions WAN, utilisez les anciennes versions de systèmes d'exploitation de ces modèles lorsqu'ils s'appliquent.

> **Remarque**
>
> Les modèles incorporés sont créés et mis à jour par Citrix. vous ne pouvez ni modifier ni supprimer ces modèles.

Créer et gérer des modèles à l'aide de Studio

Pour créer un nouveau modèle à partir d'un autre modèle :

1. Sélectionnez **Stratégies** dans le volet de navigation Studio.
2. Cliquez sur l'onglet **Modèles**, puis sélectionnez le modèle depuis lequel vous souhaitez créer le nouveau modèle.
3. Sélectionnez **Créer un modèle** dans le volet Actions.

4. Sélectionnez et configurez les paramètres de stratégie que vous souhaitez inclure dans le modèle. Supprimez tout paramètre existant qui ne devrait pas être inclus. Entrez un nom pour le modèle.

Lorsque vous cliquez sur **Terminer**, le nouveau modèle s'affiche sur la page de l'onglet **Modèles**.

Pour créer un nouveau modèle à partir d'une stratégie :

1. Sélectionnez **Stratégies** dans le volet de navigation Studio.
2. Sélectionnez l'onglet **Stratégies**, puis sélectionnez la stratégie à partir de laquelle vous souhaitez créer le nouveau modèle.
3. Sélectionnez **Enregistrer en tant que modèle** dans le volet Actions.
4. Sélectionnez et configurez tout nouveau paramètre de stratégie que vous souhaitez inclure dans le modèle. Supprimez tout paramètre existant qui ne devrait pas être inclus. Entrez un nom et une description pour le modèle, puis cliquez sur **Terminer**.

Pour importer un modèle :

1. Sélectionnez **Stratégies** dans le volet de navigation Studio.
2. Sélectionnez l'onglet **Modèles**, puis sélectionnez **Importer un modèle**.
3. Sélectionnez le fichier de modèle à importer, puis cliquez sur **Ouvrir**. Si vous importez un modèle du même nom qu'un modèle existant, vous pouvez choisir de remplacer le modèle existant ou d'enregistrer le modèle sous un nom différent qui est généré automatiquement.

Pour exporter un modèle :

1. Sélectionnez **Stratégies** dans le volet de navigation Studio.
2. Sélectionnez l'onglet **Modèles**, puis sélectionnez **Exporter le modèle**.
3. Sélectionnez l'emplacement dans lequel vous souhaitez enregistrer le modèle, puis cliquez sur **Enregistrer**.

Un fichier .gpt est créé à l'emplacement spécifié.

Créer et gérer des modèles à l'aide de l'éditeur de stratégie de groupe

Dans l'éditeur de stratégie de groupe, développez le nœud
Configuration ordinateur ou
Configuration utilisateur. Développez le nœud
Stratégies, puis sélectionnez
Stratégies Citrix. Choisissez l'action appropriée ci-dessous.

Tâche	Instruction
Créer un nouveau modèle à partir d'une stratégie existante	Sur l'onglet Stratégies, sélectionnez la stratégie et sélectionnez Actions > Enregistrer en tant que modèle.
Créer une nouvelle stratégie à partir d'un modèle existant	Sur l'onglet Modèles, sélectionnez le modèle, puis cliquez sur Nouvelle stratégie.
Créer un nouveau modèle à partir d'un modèle existant	Sur l'onglet Modèles, sélectionnez le modèle, puis cliquez sur Nouveau modèle.
Importer un modèle	Sur l'onglet Modèles, sélectionnez Actions > Importer.
Exporter un modèle	Sur l'onglet Modèles, sélectionnez Actions > Exporter.
Afficher les paramètres du modèle	Sur l'onglet Modèles, sélectionnez le modèle, puis cliquez sur l'onglet Paramètres.
Afficher un récapitulatif des propriétés du modèle	Sur l'onglet Modèles, sélectionnez le modèle, puis cliquez sur l'onglet Propriétés.
Afficher les prérequis du modèle	Sur l'onglet Modèles, sélectionnez le modèle, puis cliquez sur l'onglet Pré-requis.

Modèles et Administration déléguée

Les modèles de stratégie sont stockés sur la machine sur laquelle le pack de gestion des stratégies a été installé. Cette machine est soit la machine Delivery Controller, soit la machine de gestion des objets de stratégie de groupe (et non la base de données du site XenApp et XenDesktop). Cela signifie que les fichiers de modèle de stratégie sont contrôlés par les autorisations administratives Windows plutôt que par les rôles et les étendues d'administration déléguée du site.

Par conséquent, un administrateur disposant d'autorisations en lecture seule dans le site peut, par exemple, créer de nouveaux modèles. Cependant, les modèles étant des fichiers locaux, aucune modification n'est apportée à votre environnement.

Les modèles personnalisés sont uniquement visibles par le compte utilisateur qui les a créés et stockés dans le profil Windows de l'utilisateur. Pour exposer davantage un modèle personnalisé, créez une stratégie à partir de ce dernier ou exportez-le sur un emplacement partagé.

Créer des stratégies

February 28, 2019

Avant de créer une stratégie, déterminez quel groupe d'utilisateurs ou de périphériques doit être affecté par celle-ci. Il se peut que vous souhaitiez créer une stratégie basée sur la fonction de l'utilisateur, son type de connexion, sa machine utilisateur ou son emplacement géographique. Vous pouvez aussi utiliser le même critère que vous utilisez pour les stratégies de groupe Windows Active Directory.

Si vous avez déjà créé une stratégie qui s'applique à un groupe, envisagez de la modifier et de configurer les paramètres appropriés au lieu de créer une autre stratégie. Évitez de créer une stratégie uniquement pour activer un paramètre spécifique ou pour exclure certains utilisateurs de l'application de la stratégie.

Lorsque vous créez une nouvelle stratégie, vous pouvez la baser sur les paramètres d'un modèle de stratégie et personnaliser les paramètres selon vos besoins, ou vous pouvez la créer, sans utiliser de modèle et ajouter tous les paramètres nécessaires.

Dans Citrix Studio, les nouvelles stratégies créées sont réglées sur Désactivé, sauf si la case à cocher Activer la stratégie est explicitement sélectionnée.

Paramètres de stratégie

Les paramètres de stratégie peuvent être activés, désactivés ou non configurés. Par défaut, les paramètres de stratégie ne sont pas configurés, c'est-à-dire qu'ils ne sont pas ajoutés à une stratégie. Les paramètres ne sont appliqués que lorsqu'ils sont ajoutés à une stratégie.

Les paramètres de stratégie peuvent affichés l'un des états suivants :

- Autorisé ou Interdit permet ou empêche l'action contrôlée par le paramètre. Dans certains cas, les utilisateurs sont autorisés ou non à gérer l'action du paramètre dans la session. Par exemple, si le paramètre Animation de menu est défini sur Autorisé, les utilisateurs peuvent contrôler les animations de menu dans leur environnement client.
- Activé ou Désactivé active ou désactive le paramètre. Si vous désactivez un paramètre, celui-ci n'est pas activé dans les stratégies de priorité inférieure.

De plus, certains paramètres contrôlent l'efficacité des paramètres dépendants. Par exemple, Redirection de lecteur client contrôle le fait que les utilisateurs sont autorisés ou non à accéder aux lecteurs de leurs machines. Pour permettre aux utilisateurs d'accéder à leurs lecteurs réseau, ce paramètre ainsi que le paramètre Lecteurs réseau clients doivent être ajoutés à la stratégie. Si le paramètre Redirection de lecteur client est désactivé, les utilisateurs ne pourront pas accéder à leurs lecteurs réseau même si le paramètre Lecteurs réseau clients est activé.

En général, les modifications apportées au paramètre de stratégie qui affectent les machines se produisent lorsque le bureau virtuel redémarre ou lorsqu'un utilisateur ouvre une session. Les modifications apportées au paramètre de stratégie qui affectent les utilisateurs se produisent la prochaine fois que les utilisateurs ouvrent une session. Si vous utilisez Active Directory, les paramètres de stratégie sont mis à jour lorsque Active Directory réévalue les stratégies à intervalles de 90 minutes et ils sont appliqués lorsque le bureau virtuel redémarre ou qu'un utilisateur ouvre une session.

Pour certains paramètres de stratégie, vous pouvez entrer ou sélectionner une valeur lorsque vous ajoutez ce paramètre à une stratégie. Vous pouvez limiter la configuration du paramètre en sélectionnant Utiliser une valeur par défaut ; ceci désactive la configuration du paramètre et ne permet à la valeur par défaut du paramètre d'être utilisé lorsque la stratégie est appliquée, quelle que soit la valeur entrée avant la sélection de l'option Utiliser la valeur par défaut.

Recommandations :

- Attribuez des stratégies aux groupes plutôt qu'aux utilisateurs individuels. Si vous attribuez des stratégies aux groupes, les attributions seront mises à jour automatiquement lorsque vous ajouterez des utilisateurs au groupe ou en supprimerez.
- N'activez pas les paramètres de conflit ou de chevauchement dans la configuration d'hôte de session Bureau à distance. Dans certains cas, la configuration d'hôte de session Bureau à distance offre une fonctionnalité similaire pour les paramètres de stratégie Citrix. Chaque fois que possible, maintenez la cohérence de tous les paramètres (activés ou désactivés) pour faciliter la résolution des problèmes.
- Désactivez les stratégies non utilisées. Les stratégies sans paramètres ajoutés génèrent un traitement inutile.

Affectations de stratégie

Lors de la création d'une stratégie, vous l'attribuez à certains objets utilisateur et ordinateur, cette stratégie est appliquée aux connexions selon des critères ou des règles spécifiques. En général, vous pouvez ajouter à une stratégie autant d'affectations que vous le souhaitez, selon une combinaison de critères. Si vous ne spécifiez pas les affectations, la stratégie est appliquée à toutes les connexions.

Le tableau suivant répertorie les affectations disponibles :

Nom de l'affectation	Applique une stratégie basée sur
Access Control	Conditions de contrôle d'accès au travers desquelles un client se connecte. Type de connexion : si vous souhaitez appliquer la stratégie aux connexions établies avec ou sans NetScaler Gateway. Nom de batterie NetScaler Gateway : nom du serveur virtuel NetScaler Gateway. Condition d'accès : nom de la stratégie d'analyse de point de terminaison ou de session à utiliser.
Citrix CloudBridge	Indique si une session utilisateur est lancée au travers de Citrix CloudBridge. **Remarque :** vous pouvez ajouter une seule affectation Citrix CloudBridge à une stratégie.
Adresse IP cliente	Adresse IP de la machine cliente utilisée pour se connecter à la session. Exemples IPv4 : 12.0.0.0, 12.0.0.*, 12.0.0.1-12.0.0.70, 12.0.0.1/24 ; Exemples IPv6 : 2001:0db8:3c4d:0015:0:0:abcd:ef12, 2001:0db8:3c4d:0015::/54
Nom du client	Nom de la machine utilisateur. Concordance exacte : ClientABCName. Utilisation du caractère générique : Client*Name
Groupe de mise à disposition	Appartenance à un groupe de mise à disposition.
Type de groupe de mise à disposition	Type de bureau ou d'application : bureau privé, bureau partagé, application privée ou application partagée.
Unité d'organisation (UO)	Unité d'organisation.
Balise	Balises. **Remarque :** pour vous assurer que les stratégies sont correctement appliquées lors de l'utilisation de balises, installez la correction disponible sur l'article CTX142439.
Utilisateur ou groupe	Nom d'utilisateur ou de groupe.

Lorsque les utilisateurs ouvrent une session, toutes les stratégies correspondant aux affectations pour

la connexion sont identifiées. Les stratégies sont triées dans un ordre de priorité et plusieurs instances de tous les paramètres sont comparées. Chaque paramètre est appliqué selon l'ordre de priorité de la stratégie. Un paramètre de stratégie qui est désactivé prévaut sur un paramètre activé doté d'une priorité plus faible. Les paramètres de stratégie qui ne sont pas configurés sont ignorés.

Important : lorsque vous configurez les stratégies Active Directory et Citrix avec la Console de gestion des stratégies de groupe, il est possible que les filtres et les paramètres ne soient pas appliqués comme prévu. Pour plus d'informations, consultez l'article CTX127461.

Une stratégie appelée « Non filtrée » est fournie par défaut.

- Si vous utilisez Studio pour gérer les stratégies Citrix, les paramètres que vous ajoutez à la stratégie Non filtrée sont appliqués à l'ensemble des serveurs, des bureaux et des connexions d'un site.
- Si vous utilisez l'éditeur de stratégie de groupe pour gérer les stratégies Citrix, les paramètres que vous ajoutez à la stratégie Non filtrée sont appliqués à tous les sites et à toutes les connexions qui se trouvent dans l'étendue des Objets de stratégie de groupe qui contiennent la stratégie. Par exemple, L'UO Ventes contient un GPO appelé Ventes-FR qui comprend tous les membres de l'équipe de vente française. Le GPO Ventes-FR est configuré à l'aide d'une stratégie Unfiltered qui comprend plusieurs paramètres de stratégie utilisateur. Lorsque le directeur des Ventes FR ouvre une session sur le site, les paramètres de la stratégie Non filtrée sont automatiquement appliqués à la session car l'utilisateur est membre du GPO Ventes-FR.

Un mode d'affectation détermine si la stratégie s'applique uniquement aux connexions qui ne correspondent pas aux critères d'affectation. Si le mode est défini sur
Autoriser (valeur par défaut), la stratégie s'applique uniquement aux connexions correspondant aux critères d'affectation. Si le mode est défini sur
Refuser, la stratégie s'applique si la connexion ne correspond pas aux critères d'affectation. Les exemples suivants illustrent la manière dont les modes d'affectation affectent les stratégies Citrix lorsque plusieurs affectations sont présentes.

- **Exemple : affectations de types similaires avec des modes différents :** dans les stratégies comportant deux affectations du même type, un défini sur Autoriser et un défini sur Refuser, l'affectation définie sur Refuser a priorité, étant donné que la connexion satisfait les deux affectations. Par exemple :

  La stratégie 1 comprend les affectations suivantes :

  - L'affectation A spécifie le groupe Ventes et le mode est défini sur Autoriser.
  - L'affectation B spécifie le compte du directeur des ventes et le mode est défini sur Refuser.

  Le mode de l'affectation B étant défini sur Refuser, la stratégie n'est pas appliquée lorsque le directeur des ventes ouvre une session sur le site, bien que l'utilisateur soit membre du groupe Ventes.

- **Exemple : affectations de types différents avec des modes similaires :** dans les stratégies comportant deux affectations ou plus de types différents, défini sur Autoriser, la connexion doit satisfaire au moins une affectation de chaque type afin que la stratégie soit appliquée. Par exemple :

  La stratégie 2 comprend les affectations suivantes :

  - l'affectation C est une affectation utilisateur qui spécifie le groupe Ventes et le mode est défini sur Autoriser ;
  - l'affectation D est une affectation d'adresse IP cliente qui spécifie 10.8.169.* (le réseau d'entreprise) et le mode est défini sur Autoriser.

  Lorsque le directeur des ventes ouvre une session sur le site depuis son bureau, la stratégie est appliquée car la connexion satisfait les deux affectations.

  La stratégie 3 comprend les affectations suivantes :

  - l'affectation E est une affectation utilisateur qui spécifie le groupe Ventes et le mode est défini sur Autoriser ;
  - l'affectation F est une affectation de type contrôle d'accès qui spécifie les conditions de connexion NetScaler Gateway et le mode est défini sur Autoriser.

  Lorsque le directeur des ventes ouvre une session sur le site depuis le bureau, la stratégie n'est pas appliquée car la connexion ne satisfait pas l'affectation F.

Créer une nouvelle stratégie basée sur un modèle à l'aide de Studio

1. Sélectionnez Stratégies dans le volet de navigation Studio.
2. Sélectionnez l'onglet Modèles, puis sélectionnez un modèle.
3. Sélectionnez Créer une stratégie à partir du modèle dans le volet Actions.
4. Par défaut, la nouvelle stratégie utilise tous les paramètres par défaut dans le modèle (le bouton radio Utiliser les paramètres de modèles par défaut est sélectionné). Si vous souhaitez modifier les paramètres, sélectionnez le bouton radio Modifier les valeurs par défaut et ajouter des paramètres, puis ajoutez ou supprimez des paramètres.
5. Spécifiez comment appliquer la stratégie en sélectionnant l'une des options suivantes :
   - Attribuer aux objets Utilisateur et Machine sélectionnés, puis sélectionnez les objets utilisateur et machine auquel la stratégie s'applique.
   - Attribuer tous les objets d'un site pour appliquer la stratégie à tous les objets utilisateur et machine dans le site.
6. Entrez un nom pour la stratégie (ou acceptez la valeur par défaut) ; considérez appeler la stratégie en fonction de ce qu'elle affecte, par exemple, Service finance ou Utilisateurs distants. Facultativement, ajoutez une description.

La stratégie est activée par défaut, vous pouvez la désactiver. Si vous activez la stratégie, vous pouvez l'appliquer immédiatement aux utilisateurs ouvrant une session. Si vous désactivez la stratégie, elle n'est pas appliquée. Si vous avez besoin de définir la priorité de la stratégie ou d'ajouter des paramètres ultérieurement, considérez désactiver cette stratégie jusqu'à ce que vous soyez prêt à l'appliquer.

Créer une nouvelle stratégie à l'aide de Studio

1. Sélectionnez Stratégies dans le volet de navigation Studio.
2. Sélectionnez l'onglet Stratégies.
3. Sélectionnez Créer une stratégie dans le volet Actions.
4. Ajoutez et configurez les paramètres de stratégie.
5. Spécifiez comment appliquer la stratégie en choisissant l'une des options suivantes :
   - Attribuer aux objets Utilisateur et Machine sélectionnés, puis sélectionnez les objets utilisateur et machine auquel la stratégie s'applique.
   - Attribuer tous les objets d'un site pour appliquer la stratégie à tous les objets utilisateur et machine dans le site.
6. Entrez un nom pour la stratégie (ou acceptez la valeur par défaut) ; considérez appeler la stratégie en fonction de ce qu'elle affecte, par exemple, Service finance ou Utilisateurs distants. Facultativement, ajoutez une description.

   La stratégie est activée par défaut, vous pouvez la désactiver. Si vous activez la stratégie, vous pouvez l'appliquer immédiatement aux utilisateurs ouvrant une session. Si vous désactivez la stratégie, elle n'est pas appliquée. Si vous avez besoin de définir la priorité de la stratégie ou d'ajouter des paramètres ultérieurement, considérez désactiver cette stratégie jusqu'à ce que vous soyez prêt à l'appliquer.

Créer et gérer les stratégies à l'aide de l'éditeur de stratégie de groupe

Dans l'éditeur de stratégie de groupe, développez le nœud
Configuration ordinateur ou
Configuration utilisateur. Développez le nœud
Stratégies, puis sélectionnez
Stratégies Citrix. Choisissez l'action appropriée ci-dessous.

Tâche	Instruction
Créer une nouvelle stratégie	Dans l'onglet Stratégies, cliquez sur Nouveau.

Tâche	Instruction
Modifier une stratégie existante	Sur l'onglet Stratégies, sélectionnez la stratégie et cliquez sur Modifier.
Modifier la priorité d'une stratégie existante	Sur l'onglet Stratégies, sélectionnez la stratégie et cliquez sur Plus élevée ou Plus basse.
Afficher des informations récapitulatives sur une stratégie	Sur l'onglet Stratégies, sélectionnez la stratégie et cliquez sur l'onglet Synthèse.
Afficher et modifier les paramètres d'une stratégie	Sur l'onglet Stratégies, sélectionnez la stratégie et cliquez sur l'onglet Paramètres.
Afficher et modifier les filtres d'une stratégie	Sur l'onglet Stratégies, sélectionnez la stratégie et cliquez sur l'onglet Filtres.
Activer ou désactiver une stratégie	Sur l'onglet Stratégies, sélectionnez la stratégie, puis sélectionnez soit Actions > Activer ou Actions > Désactiver.
Créer une nouvelle stratégie à partir d'un modèle existant	Sur l'onglet Modèles, sélectionnez le modèle, puis cliquez sur Nouvelle stratégie.

Comparer, donner un ordre de priorité, modéliser et résoudre les problèmes des stratégies

January 23, 2019

Vous pouvez utiliser plusieurs stratégies pour personnaliser votre environnement afin de répondre aux besoins des utilisateurs, qui varient selon leur fonction, leur emplacement géographique ou leur type de connexion. Par exemple, pour des raisons de sécurité, il se peut vous deviez imposer des restrictions aux groupes d'utilisateurs qui travaillent régulièrement avec des données confidentielles. Vous pouvez créer une stratégie qui empêche les utilisateurs d'enregistrer les fichiers confidentiels sur leurs lecteurs clients locaux. Toutefois, si certains membres du groupe d'utilisateurs ont besoin de l'accès à leurs lecteurs locaux, vous pouvez créer une autre stratégie spécialement pour ces utilisateurs. Vous pouvez ensuite définir l'ordre de ces deux stratégies afin de définir laquelle des deux est prioritaire.

Lorsque vous utilisez plusieurs stratégies, vous devez déterminer comment leur accorder des priorités, créer des exceptions et visualiser la stratégie effective en cas de conflit.

En général, les stratégies ont priorité sur les paramètres similaires configurés pour la totalité du site, pour des Delivery Controller spécifiques ou sur la machine cliente. L'exception à ce principe est

la sécurité. Le paramètre de cryptage le plus élevé de votre environnement, y compris le système d'exploitation, et le paramètre d'observation le plus restrictif remplace toujours les autres paramètres et stratégies.

Les stratégies Citrix interagissent avec celles que vous définissez dans votre système d'exploitation. Dans un environnement Citrix, les paramètres Citrix remplacent les mêmes paramètres configurés dans une stratégie Active Directory ou à l'aide de la Configuration d'hôte de session Bureau à distance. Ceci comprend les paramètres liés aux paramètres de connexion client RDP (Remote Desktop Protocol) standard tels que Papier peint du bureau, Animation de menu et Afficher le contenu de la fenêtre lors d'un cliquer déplacer. Certains paramètres de stratégie, tels que Secure ICA, doivent correspondre à ceux du système d'exploitation. Si un niveau plus élevé de cryptage prioritaire est défini autre part, les paramètres de stratégie Secure ICA que vous spécifiez dans la stratégie ou lorsque vous mettez à disposition une application ou des bureaux peuvent être remplacés.

Par exemple, les paramètres de cryptage que vous spécifiez lorsque vous créez des groupes de mise à disposition devraient être au même niveau que les paramètres de cryptage que vous avez spécifié au travers de votre environnement.

Remarque : dans le second hop d'un scénario double-hop, lorsqu'un VDA avec OS de bureau se connecte à un VDA avec OS de serveur, les stratégies Citrix s'appliquent sur le VDA avec OS de bureau comme s'il s'agissait de la machine utilisateur. À titre d'exemple, si des stratégies sont définies pour mettre en cache les images sur la machine utilisateur, les images mises en cache pour le second hop dans un scénario double-hop sont mises en cache sur machine sur laquelle est installé le VDA avec OS de bureau.

Comparer les stratégies et les modèles

Vous pouvez comparer les paramètres d'une stratégie ou d'un modèle avec ceux des autres stratégies ou modèles. Par exemple, il se peut que vous deviez vérifier des valeurs de paramètres afin d'assurer la compatibilité avec les meilleures pratiques. Vous pouvez également comparer les paramètres d'une stratégie ou d'un modèle avec les paramètres par défaut fournis par Citrix.

1. Sélectionnez Stratégies dans le volet de navigation Studio.
2. Cliquez sur l'onglet Comparaison puis cliquez sur Sélectionner.
3. Sélectionnez les stratégies ou les modèles à comparer. Pour inclure les valeurs par défaut dans la comparaison, sélectionnez la case à cocher Comparer aux paramètres par défaut.
4. Après avoir cliqué sur Comparer, les paramètres configurés sont affichés dans les colonnes.
5. Pour afficher tous les paramètres, sélectionnez Afficher tous les paramètres. Pour revenir à la vue par défaut, sélectionnez Afficher les paramètres courants.

Définir les priorités des stratégies

La définition de priorités de stratégies vous permet de définir quelles sont les stratégies qui prévalent lorsqu'elles présentent des conflits de paramètres. Lorsque les utilisateurs ouvrent une session, toutes les stratégies correspondant aux affectations pour la connexion sont identifiées. Les stratégies sont triées dans un ordre de priorité et plusieurs instances de tous les paramètres sont comparées. Chaque paramètre est appliqué selon l'ordre de priorité de la stratégie.

Vous définissez la priorité des stratégies en leur donnant des numéros de priorité différents dans Studio. Par défaut, la priorité d'une nouvelle stratégie est plus faible que celle d'une stratégie déjà existante. Lorsque deux stratégies à appliquer ont des règles entrant en conflit, la stratégie dotée de la plus haute priorité (la valeur 1 représentant la plus haute priorité) prévaut sur la stratégie dotée de la priorité la plus faible. Les paramètres sont combinés selon leur priorité et leur condition, par exemple si le paramètre est désactivé ou activé. Tout paramètre désactivé remplace un paramètre de plus faible priorité qui est activé. Les paramètres de stratégie qui ne sont pas configurés sont ignorés ; ils ne l'emportent pas sur les paramètres dotés d'une priorité plus faible.

1. Sélectionnez Stratégies dans le volet de navigation Studio. Assurez-vous que l'onglet Stratégies est sélectionné.
2. Sélectionnez une stratégie.
3. Sélectionnez Priorité inférieure ou Priorité supérieure dans le volet Actions.

Exceptions

Après avoir créé des stratégies pour des groupes d'utilisateurs, des machines utilisateur ou des machines, vous constaterez peut-être qu'il est nécessaire de définir, pour certains membres de ces groupes, des exceptions à certains paramètres de stratégie. Vous pouvez créer des exceptions en :

- créant une stratégie uniquement pour ces membres de groupe qui ont besoin des exceptions, et en plaçant la priorité d'une stratégie en plus haute position que la stratégie de tout le groupe ;
- utilisant le mode Refuser pour une attribution ajoutée à la stratégie.

Une affectation avec le mode défini sur
Refuser applique une stratégie uniquement aux connexions qui ne correspondent pas aux critères d'affectation. Par exemple, une stratégie contient les affectations suivantes :

- L'affectation A est une affectation d'adresse IP cliente qui spécifie la plage 208.77.88.* et le mode est défini sur Autoriser.
- L'affectation B est une affectation utilisateur qui spécifie un compte utilisateur particulier et le mode est défini sur Refuser.

La stratégie est appliquée à tous les utilisateurs qui ouvrent une session sur le site avec des adresses IP se trouvant dans la plage spécifiée dans l'affectation A. Cependant, la stratégie n'est pas appliquée

à l'ouverture de session de l'utilisateur sur le site lorsque le compte utilisateur est spécifié dans l'affectation B, bien que l'ordinateur de l'utilisateur se voit attribuer une adresse IP dans la plage spécifiée dans l'affectation A.

Déterminer les stratégies qui s'appliquent à une connexion

Il arrive parfois qu'une connexion ne réponde pas comme prévu car plusieurs stratégies s'appliquent. Si une stratégie à priorité élevée s'applique également à la connexion, elle peut remplacer les paramètres configurés dans la stratégie d'origine. Vous pouvez déterminer le résultat final de la combinaison des paramètres de stratégie pour une connexion en calculant l'ensemble de stratégies résultant.

Vous pouvez calculer l'ensemble de stratégies résultant de plusieurs façons :

- Utilisez l'assistant Modélisation de stratégie de groupe Citrix pour simuler un scénario de connexion et déterminer comment appliquer les stratégies Citrix. Vous pouvez spécifier les conditions d'un scénario de connexion, telles qu'un contrôleur de domaine, des utilisateurs, des valeurs d'évidence d'affectation de stratégie Citrix et des paramètres d'environnement simulé comme une connexion réseau lente. Le rapport créé par l'assistant répertorie les stratégies Citrix susceptibles de s'appliquer dans le scénario. Si vous êtes connecté au Controller en tant qu'utilisateur du domaine, l'assistant calcule l'ensemble de stratégies résultant en utilisant les paramètres de stratégie du site et les objets de stratégie de groupe (GPO) Active Directory.
- Utilisez l'outil Résultats de stratégie de groupe pour créer un rapport décrivant les stratégies Citrix en vigueur pour un utilisateur et un contrôleur donnés. L'outil Résultats de stratégie de groupe vous aide à évaluer l'état actuel des objets de stratégie de groupe dans votre environnement et génère un rapport décrivant de quelle façon ces objets, y compris les stratégies Citrix, sont appliqués à un utilisateur et à un contrôleur donnés.

Vous pouvez lancer l'assistant Modélisation de stratégie de groupe Citrix depuis le panneau Actions de Studio. Vous pouvez lancer les deux outils à partir de la Console de gestion des stratégies de groupe dans Windows.

Si vous exécutez l'assistant Modélisation de stratégie de groupe Citrix ou l'outil Résultats de stratégie de groupe à partir de la Console de gestion des stratégies de groupe, les paramètres de stratégie de site créés avec Studio ne sont pas inclus dans l'ensemble de stratégies résultant.

Pour être certain d'obtenir l'ensemble de stratégies résultant le plus complet, Citrix vous recommande de lancer l'assistant Modélisation de stratégie de groupe Citrix depuis Studio, sauf si vous ne créez des stratégies qu'avec la Console de gestion des stratégies de groupe.

Utiliser l'assistant Modélisation de stratégie de groupe Citrix

Ouvrez l'Assistant Modélisation de stratégie de groupe Citrix à l'aide de l'une des options suivantes :

- Sélectionnez Stratégies dans le panneau de navigation de Studio, sélectionnez l'onglet Modélisation, puis sélectionnez Démarrer l'assistant de modélisation dans le volet Actions.
- Démarrez la console de gestion des stratégies de groupe (gpmc.msc), cliquez avec le bouton droit de la souris sur le nœud Modélisation de stratégie de groupe Citrix dans l'arborescence et sélectionnez Assistant Modélisation de stratégie de groupe Citrix.

Suivez les instructions de l'assistant pour sélectionner le contrôleur de domaine, les utilisateurs, les ordinateurs, les paramètres d'environnement et les critères d'affectation Citrix à utiliser dans la simulation. Lorsque vous cliquez sur Terminer, l'assistant produit un rapport sur les résultats de modélisation. Dans Studio, le rapport apparaît dans le panneau du milieu, sous l'onglet Modélisation.

Pour afficher le rapport, sélectionnez Afficher le rapport de modélisation.

Résolution des problèmes de stratégies

Les utilisateurs, adresses IP et autres objets affectés peuvent posséder plusieurs stratégies qui s'appliquent de manière simultanée. Ceci peut entraîner des conflits lorsqu'une stratégie ne se comporte pas de manière attendue. Lorsque vous exécutez l'assistant Modélisation de stratégie de groupe Citrix ou l'outil Résultats de stratégie de groupe, il se peut que vous découvriez qu'aucune stratégie n'est appliquée aux connexions utilisateur. Dans ce cas, les utilisateurs se connectant à leurs applications et bureaux dans des conditions correspondant aux critères d'évaluation de stratégie ne sont affectés par aucun paramètre de stratégie. Ceci se produit lorsque :

- aucune stratégie ne possède d'affectation correspondant au critère d'évaluation de stratégie ;
- les stratégies correspondant à l'affectation ne possèdent aucun paramètre configuré ;
- les stratégies correspondant à l'affectation sont désactivées.

Si vous souhaitez appliquer des paramètres de stratégie à des connexions répondant aux critères spécifiés, effectuez les opérations suivantes :

- Les stratégies que vous souhaitez appliquer à ces connexions sont activées.
- Les stratégies que vous souhaitez appliquer possèdent les paramètres appropriés configurés.

Paramètres de stratégie par défaut

January 23, 2019

Les tableaux suivants répertorient les paramètres de stratégie, leur valeur par défaut, et les versions de Virtual Delivery Agent (VDA) auxquelles ils s'appliquent.

ICA

Name	Paramètre par défaut	VDA
Redirection de Presse-papiers client	Autorisé	Toutes les versions VDA
Démarrages de bureau	Interdit	VDA pour OS de serveur 7 jusqu'à la version actuelle
EDT	Désactivé	VDA 7.13. Voir Transport adaptatif.
Expiration de délai de la connexion à l'écouteur ICA	120000 millisecondes	VDA 5, 5.5, 5.6 FP1, VDA pour OS de bureau 7 jusqu'à la version actuelle
Numéro de port de l'écouteur ICA	1494	Toutes les versions VDA
Lancement de programmes non publiés lors de la connexion du client	Interdit	VDA pour OS de serveur 7 jusqu'à la version actuelle
Formats autorisés d'écriture dans le Presse-papiers client	Aucun format spécifié	VDA 7.6 jusqu'à la version actuelle
Restreindre l'écriture dans le Presse-papiers client	Interdit	VDA 7.6 jusqu'à la version actuelle
Restreindre l'écriture dans le Presse-papiers de session	Interdit	VDA 7.6 jusqu'à la version actuelle
Formats autorisés d'écriture dans le Presse-papiers de session	Aucun format spécifié	VDA 7.6 jusqu'à la version actuelle

ICA/Mise à disposition Adobe Flash/Redirection Flash

Name	Paramètre par défaut	VDA
Prévention du retour à la vidéo Flash	Non configuré	VDA 7.6 FP3 jusqu'à la version actuelle
Erreur *.swf de prévention du retour à la vidéo Flash		VDA 7.6 FP3 jusqu'à la version actuelle

ICA/Audio

Name	Paramètre par défaut	VDA
Audio Plug N Play	Autorisé	VDA pour OS de serveur 7 jusqu'à la version actuelle
Qualité audio	Élevé - audio haute définition	Toutes les versions VDA
Redirection audio cliente	Autorisé	Toutes les versions VDA
Redirection du microphone client	Autorisé	Toutes les versions VDA

ICA/Reconnexion automatique des clients

Name	Paramètre par défaut	VDA
Reconnexion automatique des clients	Autorisé	Toutes les versions VDA
Authentification de la reconnexion automatique des clients	Ne pas requérir d'authentification	Toutes les versions VDA
Journalisation de la reconnexion automatique des clients	Ne pas journaliser les événements de reconnexion automatique	Toutes les versions VDA

ICA/Bande passante

Name	Paramètre par défaut	VDA
Limite de bande passante de redirection audio	0 kbps	Toutes les versions VDA
Pourcentage de limite de bande passante de la redirection audio	0	Toutes les versions VDA

Name	Paramètre par défaut	VDA
Limite de bande passante de redirection du périphérique USB client	0 kbps	VDA 5,5, 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Pourcentage de limite de bande passante de redirection du périphérique USB client	0	VDA 5,5, 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Limite de bande passante de redirection du Presse-papiers	0 kbps	Toutes les versions VDA
Pourcentage de la limite de la bande passante de redirection du Presse-papiers	0	Toutes les versions VDA
Limite de bande passante pour la redirection du port COM	0 kbps	Toutes les versions VDA ; pour le VDA 7.0 jusqu'à la version 7.8, configurez ce paramètre en utilisant le Registre.
Pourcentage de limite de bande passante de redirection du port COM	0	Toutes les versions VDA ; pour le VDA 7.0 jusqu'à la version 7.8, configurez ce paramètre en utilisant le Registre.
Limite de bande passante de redirection de fichier	0 kbps	Toutes les versions VDA
Pourcentage de limite de bande passante de redirection de fichier	0	Toutes les versions VDA
Limite de bande passante d'accélération multimédia HDX MediaStream	0 kbps	VDA 5.5, 5.6 FP1, VDA pour OS de serveur 7 et VDA pour OS de bureau 7 à versions VDA pour OS de serveur et VDA pour OS de bureau courantes

Name	Paramètre par défaut	VDA
Pourcentage de limite de bande passante d'accélération multimédia HDX MediaStream	0	VDA 5,5, 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Limite de bande passante pour la redirection du port LPT	0 kbps	Toutes les versions VDA ; pour le VDA 7.0 jusqu'à la version 7.8, configurez ce paramètre en utilisant le Registre.
Pourcentage de limite de bande passante de redirection du port LPT	0	Toutes les versions VDA ; pour le VDA 7.0 jusqu'à la version 7.8, configurez ce paramètre en utilisant le Registre.
Limite de bande passante globale de session	0 kbps	Toutes les versions VDA
Limite de bande passante de redirection d'imprimante	0 kbps	Toutes les versions VDA
Pourcentage de limite de bande passante de redirection de l'imprimante	0	Toutes les versions VDA
Limite de bande passante de redirection du périphérique TWAIN	0 kbps	VDA 5,5, 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Pourcentage de limite de bande passante de redirection du périphérique TWAIN	0	VDA 5,5, 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle

ICA/Capteurs clients

Name	Paramètre par défaut	VDA
Cette option permet aux applications d'utiliser l'emplacement physique de la machine cliente.	Interdit	VDA 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle

ICA/IU de bureau

Name	Paramètre par défaut	VDA
Redirection Desktop Composition	Désactivé (7.6 FP3 jusqu'à la version actuelle), Activé (5.6 à 7.6 FP2)	VDA 5.6, VDA pour OS de bureau 7 jusqu'à la version actuelle
Qualité graphique de redirection Desktop Composition	Modéré	VDA 5.6, VDA pour OS de bureau 7 jusqu'à la version actuelle
Papier peint du bureau	Autorisé	Toutes les versions VDA
Animation de menu	Autorisé	Toutes les versions VDA
Afficher le contenu de la fenêtre lors d'un cliquer déplacer	Autorisé	Toutes les versions VDA

ICA/Contrôle de l'utilisateur final

Name	Paramètre par défaut	VDA
Calcul des boucles ICA	Activée	Toutes les versions VDA
Intervalle de calcul des boucles ICA	15 secondes	Toutes les versions VDA
Calcul des boucles ICA pour les connexions inactives	Désactivée	Toutes les versions VDA

ICA/Expérience de bureau améliorée

Name	Paramètre par défaut	VDA
Expérience de bureau améliorée	Autorisé	VDA pour OS de serveur 7 jusqu'à la version actuelle

ICA/Redirection de fichier

Name	Paramètre par défaut	VDA
Connecter automatiquement les lecteurs clients	Autorisé	Toutes les versions VDA
Redirection de lecteur client	Autorisé	Toutes les versions VDA
Lecteurs fixes clients	Autorisé	Toutes les versions VDA
Lecteurs de disquette clients	Autorisé	Toutes les versions VDA
Lecteurs réseau clients	Autorisé	Toutes les versions VDA
Lecteurs optiques clients	Autorisé	Toutes les versions VDA
Lecteurs amovibles clients	Autorisé	Toutes les versions VDA
Redirection hôte vers client	Désactivée	VDA pour OS de serveur 7 jusqu'à la version actuelle
Préserver les lettres de lecteurs clients	Désactivée	VDA 5, 5.5, 5.6 FP1, VDA pour OS de bureau 7 jusqu'à la version actuelle
Accès en lecture unique sur le lecteur client	Désactivée	VDA 5,5, 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Redirection vers les dossiers spéciaux	Autorisé	Déploiements Interface Web uniquement ; VDA pour OS de serveur 7 jusqu'à la version actuelle
Utiliser les écritures asynchrones	Désactivée	Toutes les versions VDA

ICA/graphiques

Name	Paramètre par défaut	VDA
Autoriser la compression visuelle sans perte	Désactivée	VDA 7.6 jusqu'à la version actuelle
Limite de mémoire d'affichage	65536 Ko	VDA 5, 5.5, 5.6 FP1, VDA pour OS de bureau 7 jusqu'à la version actuelle
Préférence de dégradation du mode d'affichage	Réduire d'abord le nombre de couleurs	Toutes les versions VDA
Aperçu de fenêtres dynamiques	Activée	VDA 5,5, 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Cache d'image	Activée	VDA 5,5, 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Mode graphique d'ancienne génération	Désactivée	VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Nombre de couleurs maximal autorisé	32 bits par pixel	Toutes les versions VDA
Notifier l'utilisateur lorsque le mode d'affichage se dégrade	Désactivée	VDA pour OS de serveur 7 jusqu'à la version actuelle
Mise en file d'attente et ballotage	Activée	Toutes les versions VDA
Utiliser codec vidéo pour la compression	Utiliser un codec vidéo au choix	VDA 7.6 FP3 jusqu'à la version actuelle
Utiliser le codage matériel pour le codec vidéo	Activée	VDA 7.11 jusqu'à la version actuelle

ICA/graphiques/mise en cache

Name	Paramètre par défaut	VDA
Seuil de cache permanent	3 000 000 bps	VDA pour OS de serveur 7 jusqu'à la version actuelle

ICA/graphiques/Framehawk

Name	Paramètre par défaut	VDA
Canal d'affichage Framehawk	Désactivée	VDA 7.6 FP2 jusqu'à la version actuelle
Plage de ports du canal d'affichage Framehawk	3224, 3324	VDA 7.6 FP2 jusqu'à la version actuelle

ICA/Persistance

Name	Paramètre par défaut	VDA
Délai d'expiration de persistance ICA	60 secondes	Toutes les versions VDA
Persistances ICA	Ne pas envoyer de messages de persistance ICA	Toutes les versions VDA

ICA/Local App Access

Name	Paramètre par défaut	VDA
Autoriser Local App Access	Interdit	VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Liste noire de redirection d'adresse URL	Aucun site n'est spécifié.	VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle

Name	Paramètre par défaut	VDA
Liste blanche de redirection d'adresse URL	Aucun site n'est spécifié.	VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle

ICA/Expérience mobile

Name	Paramètre par défaut	VDA
Affichage de clavier automatique	Interdit	VDA 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Démarrer le bureau tactile	Autorisé	VDA 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle. Ce paramètre est désactivé et n'est pas disponible pour les machines Windows 10 et Windows Server 2016.
Contrôler la zone combinée	Interdit	VDA 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle

ICA/multimédia

Name	Paramètre par défaut	VDA
Redirection vidéo HTML5	Interdit	VDA 7.12 jusqu'à la version actuelle

Name	Paramètre par défaut	VDA
Limiter la qualité de la vidéo	Non configuré	VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Conférences multimédia	Autorisé	Toutes les versions VDA
Optimisation de la redirection multimédia de Windows Media sur un réseau étendu	Autorisé	VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Utiliser GPU pour l'optimisation de la redirection multimédia Windows Media sur un réseau étendu	Interdit	VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Prévention du retour à Windows Media	Non configuré	VDA 7.6 FP3 jusqu'à la version actuelle
Récupération de contenu côté client Windows Media	Autorisé	VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Redirection Windows Media	Autorisé	Toutes les versions VDA
Taille de tampon de redirection Windows Media	5 secondes	VDA 5, 5.5, 5.6 FP1
Utilisation de la taille de tampon de redirection Windows Media	Désactivée	VDA 5, 5.5, 5.6 FP1

ICA/Connexions Multi-Stream

Name	Paramètre par défaut	VDA
Audio sur UDP	Autorisé	VDA pour OS de serveur 7 jusqu'à la version actuelle

Name	Paramètre par défaut	VDA
Plage de port UDP audio	16500, 16509	VDA 5,5, 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Stratégie Multi-Port	Le port principal (2598) a une priorité élevée	VDA 5,5, 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Paramètre d'ordinateur Multi-Stream	Désactivée	VDA 5,5, 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Paramètre utilisateur Multi-Stream	Désactivée	VDA 5,5, 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle

ICA/Redirection de ports

Name	Paramètre par défaut	VDA
Connecter automatiquement les ports COM du client	Désactivée	Toutes les versions VDA ; pour le VDA 7.0 jusqu'à la version 7.8, configurez ce paramètre en utilisant le Registre.
Connecter automatiquement les ports LPT du client	Désactivée	Toutes les versions VDA ; pour le VDA 7.0 jusqu'à la version 7.8, configurez ce paramètre en utilisant le Registre.

Name	Paramètre par défaut	VDA
Redirection de port COM client	Interdit	Toutes les versions VDA ; pour le VDA 7.0 jusqu'à la version 7.8, configurez ce paramètre en utilisant le Registre.
Redirection de port LPT client	Interdit	Toutes les versions VDA ; pour le VDA 7.0 jusqu'à la version 7.8, configurez ce paramètre en utilisant le Registre.

ICA/Impression

Name	Paramètre par défaut	VDA
Redirection d'imprimante cliente	Autorisé	Toutes les versions VDA
Imprimante par défaut	Définir l'imprimante par défaut sur l'imprimante principale du client	Toutes les versions VDA
Attributions d'imprimantes	L'imprimante actuelle de l'utilisateur est utilisée comme imprimante par défaut pour la session.	Toutes les versions VDA
Préférence de journalisation des événements de création automatique des imprimantes	Journaliser les erreurs et les avertissements	Toutes les versions VDA
Imprimantes de session	Aucune imprimante n'est spécifiée.	Toutes les versions VDA
Attendre la création d'imprimantes (bureau)	Désactivée	Toutes les versions VDA

ICA/Impression/Imprimantes clientes

Name	Paramètre par défaut	VDA
Créer automatiquement les imprimantes clientes	Création automatique de toutes les imprimantes clientes	Toutes les versions VDA
Créer automatiquement l'imprimante universelle générique	Désactivée	Toutes les versions VDA
Noms des imprimantes clientes	Noms d'imprimantes standards	Toutes les versions VDA
Diriger les connexions vers les serveurs d'impression	Activée	Toutes les versions VDA
Mappage et compatibilité du pilote d'imprimante	Aucune règle n'est spécifiée.	Toutes les versions VDA
Rétention des propriétés d'imprimante	Conservées dans le profil seulement si pas enregistrées sur la machine cliente	Toutes les versions VDA
Imprimantes clientes conservées et restaurées	Autorisé	VDA 5, 5.5, 5.6 FP1

ICA/Impression/Pilotes

Name	Paramètre par défaut	VDA
Installation automatique de pilotes d'imprimante fournis par défaut	Activée	Toutes les versions VDA
Préférence de pilote universel	EMF ; XPS ; PCL5c ; PCL4 ; PS	Toutes les versions VDA
Utilisation du pilote d'impression universelle	Utiliser l'impression universelle uniquement si le pilote requis n'est pas disponible	Toutes les versions VDA

ICA/Impression/Serveur d'impression universelle

Name	Paramètre par défaut	VDA
Activer le serveur d'impression universelle	Désactivée	Toutes les versions VDA
Port (CGP) du flux de données d'impression du serveur d'impression universelle	7229	Toutes les versions VDA
Limite de bande passante d'entrée du flux d'impression du serveur d'impression universelle (kpbs)	0	Toutes les versions VDA
Port (HTTP/SOAP) du service Web du serveur d'impression universelle	8080	Toutes les versions VDA
Serveurs d'impression universelle d'équilibrage de la charge		VDA 7.9 jusqu'à la version actuelle
Seuil au-delà duquel les serveurs d'impression universelle sont hors service	180 (secondes)	VDA 7.9 jusqu'à la version actuelle

ICA/Impression/Impression universelle

Name	Paramètre par défaut	VDA
Mode de traitement de l'impression universelle EMF	Spouler directement vers l'imprimante	Toutes les versions VDA
Limite de compression d'image de l'impression universelle	Meilleure qualité (compression sans perte)	Toutes les versions VDA

Name	Paramètre par défaut	VDA
Valeur par défaut d'optimisation de l'impression universelle	Compression d'image : Qualité d'image désirée = Qualité standard, Activer la compression lourde = False. Cache d'image et de police : Autoriser la mise en cache des images incorporées = True, Autoriser la mise en cache des polices incorporées = True. Autoriser les non-administrateurs à modifier ces paramètres = False	Toutes les versions VDA
Préférence d'aperçu d'impression universelle	Ne pas utiliser l'aperçu pour les imprimantes créées automatiquement ou universelles génériques	Toutes les versions VDA
Limite de qualité d'image de l'impression universelle	Durée illimitée	Toutes les versions VDA

ICA/sécurité

Name	Paramètre par défaut	VDA
Niveau de cryptage minimum SecureICA	De base	VDA pour OS de serveur 7 jusqu'à la version actuelle

ICA/Limites de serveur

Name	Paramètre par défaut	VDA
Intervalle d'horloge inactive du serveur	0 millisecondes	VDA pour OS de serveur 7 jusqu'à la version actuelle

ICA/Limites de session

Name	Paramètre par défaut	VDA
Horloge de session déconnectée	Désactivée	VDA 5, 5.5, 5.6 FP1, VDA pour OS de bureau 7 jusqu'à la version actuelle
Intervalle d'horloge de session déconnectée	1440 minutes	VDA 5, 5.5, 5.6 FP1, VDA pour OS de bureau 7 jusqu'à la version actuelle
Minuteur de connexion de session	Désactivée	VDA 5, 5.5, 5.6 FP1, VDA pour OS de bureau 7 jusqu'à la version actuelle
Intervalle de minuteur de connexion de session (Session connection timer interval)	1440 minutes	VDA 5, 5.5, 5.6 FP1, VDA pour OS de bureau 7 jusqu'à la version actuelle
Minuteur de session inactive	Activé	VDA 5, 5.5, 5.6 FP1, VDA pour OS de bureau 7 jusqu'à la version actuelle
Intervalle de minuteur de session inactive	1440 minutes	VDA 5, 5.5, 5.6 FP1, VDA pour OS de bureau 7 jusqu'à la version actuelle

ICA/Fiabilité de session

Name	Paramètre par défaut	VDA
Connexions de fiabilité de session	Autorisé	Toutes les versions VDA
Numéro de port de la fiabilité de session	2598	Toutes les versions VDA
Expiration de délai de la fiabilité de session	180 secondes	Toutes les versions VDA

ICA/Contrôle de fuseau horaire

Name	Paramètre par défaut	VDA
Estimer l'heure locale pour les clients d'ancienne génération	Activée	VDA pour OS de serveur 7 jusqu'à la version actuelle
Utilisation de l'heure locale du client	Utiliser le fuseau horaire du serveur	Toutes les versions VDA

Périphériques ICA/TWAIN

Name	Paramètre par défaut	VDA
Redirection de périphérique TWAIN client	Autorisé	VDA 5,5, 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Niveau de compression TWAIN	Modéré	VDA 5,5, 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle

Périphériques ICA/USB

Name	Paramètre par défaut	VDA
Règles d'optimisation des périphériques USB clients	Activé (VDA 7.6 FP3 jusqu'à la version actuelle), Désactivé (VDA 7.11 jusqu'à la version actuelle). Par défaut, aucune règle n'est spécifiée.	VDA 7.6 FP3 jusqu'à la version actuelle
Redirection de périphérique USB client	Interdit	Toutes les versions VDA
Règles de redirection des périphériques USB clients	Aucune règle n'est spécifiée.	Toutes les versions VDA

Name	Paramètre par défaut	VDA
Redirection de périphérique Plug and Play USB client	Autorisé	VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle

ICA/Affichage visuel

Name	Paramètre par défaut	VDA
Nombre de couleurs préféré pour les graphiques simples	24 bits par pixel	VDA 7.6 FP3 jusqu'à la version actuelle
Taux de trames cible	30 fps	Toutes les versions VDA
Qualité visuelle	Modéré	VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle

ICA/Affichage visuel/Images en mouvement

Name	Paramètre par défaut	VDA
Qualité d'image minimale	Normale	VDA 5,5, 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Compression d'images en mouvement	Activée	VDA 5,5, 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle

Name	Paramètre par défaut	VDA
Niveau de compression progressif	Aucun	VDA 5,5, 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Valeur de seuil de compression progressif	2147483647 kbps	VDA 5,5, 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Taux de trame minimum cible	10 fps	VDA 5,5, 5.6 FP1, VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle

ICA/Affichage visuel/Images fixes

Name	Paramètre par défaut	VDA
Compression couleur supplémentaire	Désactivée	Toutes les versions VDA
Seuil de compression de couleur supplémentaire	8192 Kbits/s	Toutes les versions VDA
Compression lourde	Désactivée	Toutes les versions VDA
Niveau de compression avec perte	Modéré	Toutes les versions VDA
Valeur de seuil de compression avec perte	2147483647 kbps	Toutes les versions VDA

/

Name	Paramètre par défaut	VDA
Connexions WebSockets	Interdit	VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Numéro de port WebSockets	8008	VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Liste de serveurs d'origine approuvés WebSockets	Le caractère générique est utilisé pour faire confiance à toutes les adresses URL Receiver pour Web.	VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle

Gestion de la charge

Name	Paramètre par défaut	VDA
Tolérance d'ouvertures de session simultanée	2.	VDA pour OS de serveur 7 jusqu'à la version actuelle
Utilisation UC	Désactivée	VDA pour OS de serveur 7 jusqu'à la version actuelle
Priorité de processus exclue de l'utilisation UC	Inférieure à la normale ou Basse	VDA pour OS de serveur 7 jusqu'à la version actuelle
Utilisation du disque	Désactivée	VDA pour OS de serveur 7 jusqu'à la version actuelle
Nombre maximum de sessions	250	VDA pour OS de serveur 7 jusqu'à la version actuelle
Utilisation de mémoire	Désactivée	VDA pour OS de serveur 7 jusqu'à la version actuelle
Charge de base d'utilisation mémoire	Charge zéro : 768 Mo	VDA pour OS de serveur 7 jusqu'à la version actuelle

Profile Management/Paramètres avancés

Name	Paramètre par défaut	VDA
Désactiver la configuration automatique	Désactivée	Toutes les versions VDA
Fermer la session de l'utilisateur si un problème se produit	Désactivée	Toutes les versions VDA
Nombre de tentatives d'accès à des fichiers verrouillés	5	Toutes les versions VDA
Traiter les cookies Internet à la fermeture de session	Désactivée	Toutes les versions VDA

Profile Management/Paramètres de base

Name	Paramètre par défaut	VDA
Réécriture active	Désactivée	Toutes les versions VDA
Activer Profile Management	Désactivée	Toutes les versions VDA
Groupes exclus	Désactivé. Tous les membres des groupes d'utilisateurs sont traités.	Toutes les versions VDA
Prise en charge des profils déconnectés	Désactivée	Toutes les versions VDA
Chemin d'accès au magasin de l'utilisateur	Windows	Toutes les versions VDA
Traiter les connexions des administrateurs locaux	Désactivée	Toutes les versions VDA
Groupes traités	Désactivé. Tous les membres des groupes d'utilisateurs sont traités.	Toutes les versions VDA

Profile Management/Paramètres multi-plateformes

Name	Paramètre par défaut	VDA
Paramètres multi-plateformes des groupes d'utilisateurs	Désactivé. Tous les groupes d'utilisateurs spécifiés dans Groupes traités sont traités	Toutes les versions VDA
Activer les paramètres multi-plateformes	Désactivée	Toutes les versions VDA
Chemin d'accès aux définitions multi-plateformes	Désactivé. Aucun chemin n'est spécifié.	Toutes les versions VDA
Chemin d'accès au magasin des paramètres multi-plateformes	Désactivé. Windows\PM_CM est utilisé.	Toutes les versions VDA
Source utilisée pour créer les paramètres multi-plateformes	Désactivée	Toutes les versions VDA

Profile Management/Système de fichiers/Exclusions

Name	Paramètre par défaut	VDA
Liste d'exclusion - répertoires	Désactivé. Tous les dossiers du profil utilisateur sont synchronisés.	Toutes les versions VDA
Liste d'exclusion - fichiers	Désactivé. Tous les fichiers du profil utilisateur sont synchronisés.	Toutes les versions VDA

Profile Management/Système de fichiers/Synchronisation

Name	Paramètre par défaut	VDA
Répertoires à synchroniser	Désactivé. Seuls les dossiers non exclus sont synchronisés.	Toutes les versions VDA
Fichiers à synchroniser	Désactivé. Seuls les fichiers non exclus sont synchronisés.	Toutes les versions VDA

Name	Paramètre par défaut	VDA
Dossiers en miroir	Désactivé. Aucun dossier n'est mis en miroir.	Toutes les versions VDA

Profile Management/Redirection de dossiers

Name	Paramètre par défaut	VDA
Accorder l'accès administrateur	Désactivée	Toutes les versions VDA
Inclure le nom de domaine	Désactivée	Toutes les versions VDA

Profile Management/Redirection de dossiers/AppData(Roaming)

Name	Paramètre par défaut	VDA
Chemins d'accès au dossier AppData(Roaming)	Désactivé. Aucun emplacement n'est spécifié.	Toutes les versions VDA
Paramètres de redirection du dossier AppData(Roaming)	Le contenu est redirigé vers le chemin UNC spécifié dans les paramètres de stratégie AppData(Roaming)	Toutes les versions VDA

Profile Management/Redirection de dossiers/Contacts

Name	Paramètre par défaut	VDA
Chemin d'accès au dossier Contacts	Désactivé. Aucun emplacement n'est spécifié.	Toutes les versions VDA
Paramètres de redirection du dossier Contacts	Le contenu est redirigé vers le chemin UNC spécifié dans les paramètres de stratégie Chemin Contacts	Toutes les versions VDA

Profile Management/Redirection de dossiers/Bureau

Name	Paramètre par défaut	VDA
Chemin d'accès au dossier Bureau	Désactivé. Aucun emplacement n'est spécifié.	Toutes les versions VDA
Paramètres de redirection du dossier Bureau	Le contenu est redirigé vers le chemin UNC spécifié dans les paramètres de stratégie Chemin Bureau	Toutes les versions VDA

Profile Management/Redirection de dossiers/Documents

Name	Paramètre par défaut	VDA
Chemin d'accès au dossier Mes documents	Désactivé. Aucun emplacement n'est spécifié.	Toutes les versions VDA
Paramètres de redirection du dossier Mes documents	Le contenu est redirigé vers le chemin UNC spécifié dans les paramètres de stratégie Chemin Documents.	Toutes les versions VDA

Profile Management/Redirection de dossiers/Téléchargements

Name	Paramètre par défaut	VDA
Chemin d'accès au dossier Téléchargements	Désactivé. Aucun emplacement n'est spécifié.	Toutes les versions VDA
Paramètres de redirection du dossier Téléchargements	Le contenu est redirigé vers le chemin UNC spécifié dans les paramètres de stratégie Chemin Téléchargements	Toutes les versions VDA

Profile Management/Redirection de dossiers/Favoris

Name	Paramètre par défaut	VDA
Chemin d'accès au dossier Favoris	Désactivé. Aucun emplacement n'est spécifié.	Toutes les versions VDA
Paramètres de redirection du dossier Favoris	Le contenu est redirigé vers le chemin UNC spécifié dans les paramètres de stratégie Chemin Favoris	Toutes les versions VDA

Profile Management/Redirection de dossiers/Liens

Name	Paramètre par défaut	VDA
Chemin d'accès au dossier Liens	Désactivé. Aucun emplacement n'est spécifié.	Toutes les versions VDA
Paramètres de redirection du dossier Liens	Le contenu est redirigé vers le chemin UNC spécifié dans les paramètres de stratégie Chemin Liens	Toutes les versions VDA

Profile Management/Redirection de dossiers/Musique

Name	Paramètre par défaut	VDA
Chemin d'accès au dossier Ma musique	Désactivé. Aucun emplacement n'est spécifié.	Toutes les versions VDA
Paramètres de redirection du dossier Ma musique	Le contenu est redirigé vers le chemin UNC spécifié dans les paramètres de stratégie Chemin Musique	Toutes les versions VDA

Profile Management/Redirection de dossiers/Photos

Name	Paramètre par défaut	VDA
Chemin d'accès au dossier Mes images	Désactivé. Aucun emplacement n'est spécifié.	Toutes les versions VDA
Paramètres de redirection du dossier Mes images	Le contenu est redirigé vers le chemin UNC spécifié dans les paramètres de stratégie Chemin Photos	Toutes les versions VDA

Profile Management/Redirection de dossiers/Jeux enregistrés

Name	Paramètre par défaut	VDA
Chemin d'accès au dossier Parties enregistrées	Désactivé. Aucun emplacement n'est spécifié.	Toutes les versions VDA
Paramètres de redirection du dossier Parties enregistrées	Le contenu est redirigé vers le chemin UNC spécifié dans les paramètres de stratégie Chemin Jeux enregistrés	Toutes les versions VDA

Profile Management/Redirection de dossiers/Recherches

Name	Paramètre par défaut	VDA
Chemin d'accès au dossier Recherches	Désactivé. Aucun emplacement n'est spécifié.	Toutes les versions VDA
Paramètres de redirection du dossier Recherches	Le contenu est redirigé vers le chemin UNC spécifié dans les paramètres de stratégie Chemin Recherches	Toutes les versions VDA

Profile Management/Redirection de dossiers/Menu Démarrer

Name	Paramètre par défaut	VDA
Chemin d'accès au menu Démarrer	Désactivé. Aucun emplacement n'est spécifié.	Toutes les versions VDA
Paramètres de redirection du menu Démarrer	Le contenu est redirigé vers le chemin UNC spécifié dans les paramètres de stratégie Chemin Menu Démarrer	Toutes les versions VDA

Profile Management/Redirection de dossiers/Vidéo

Name	Paramètre par défaut	VDA
Chemin d'accès au dossier Vidéo	Désactivé. Aucun emplacement n'est spécifié.	Toutes les versions VDA
Paramètres de redirection pour la vidéo	Le contenu est redirigé vers le chemin UNC spécifié dans les paramètres de stratégie Chemin Vidéo	Toutes les versions VDA

Profile Management/Paramètres du journal

Name	Paramètre par défaut	VDA
Actions Active Directory	Désactivée	Toutes les versions VDA
Informations courantes	Désactivée	Toutes les versions VDA
Avertissements courants	Désactivée	Toutes les versions VDA
Activer la journalisation	Désactivée	Toutes les versions VDA
Actions du système de fichiers	Désactivée	Toutes les versions VDA
Notifications du système de fichiers	Désactivée	Toutes les versions VDA
Fermeture de session	Désactivée	Toutes les versions VDA
Ouverture de session	Désactivée	Toutes les versions VDA
Taille maximale du fichier journal	1048576	Toutes les versions VDA

Name	Paramètre par défaut	VDA
Chemin vers le fichier journal	Désactivé. Les fichiers journaux sont enregistrés à l'emplacement par défaut ; %System-Root%\System32\Logfiles\UserProfileManager.	Toutes les versions VDA
Informations utilisateur personnalisées	Désactivée	Toutes les versions VDA
Valeurs de stratégie à l'ouverture et fermeture de session	Désactivée	Toutes les versions VDA
Actions du registre	Désactivée	Toutes les versions VDA
Différences de registre à la fermeture de session	Désactivée	Toutes les versions VDA

Management/Profile Management/Traitement des profils

Name	Paramètre par défaut	VDA
Délai avant la suppression des profils du cache	0	Toutes les versions VDA
Supprimer les profils mis en cache localement à la fermeture de session	Désactivée	Toutes les versions VDA
Gestion des conflits de profils locaux	Utiliser profil local	Toutes les versions VDA
Migration des profils existants	Locaux et itinérants	Toutes les versions VDA
Chemin d'accès au profil modèle	Désactivé. Les nouveaux profils utilisateur sont créés à partir du profil utilisateur par défaut sur la machine sur laquelle un utilisateur ouvre une session.	Toutes les versions VDA
Le profil modèle remplace le profil local	Désactivée	Toutes les versions VDA

Name	Paramètre par défaut	VDA
Le profil modèle remplace le profil itinérant	Désactivée	Toutes les versions VDA
Profil modèle utilisé en tant que profil Citrix obligatoire pour toutes les ouvertures de session	Désactivée	Toutes les versions VDA

Profile Management/Registre

Name	Paramètre par défaut	VDA
Liste d'exclusion	Désactivé. Toutes les clés de registre dans la ruche HKCU sont traitées lorsqu'un utilisateur ferme sa session.	Toutes les versions VDA
Liste d'inclusion	Désactivé. Toutes les clés de registre dans la ruche HKCU sont traitées lorsqu'un utilisateur ferme sa session.	Toutes les versions VDA

Profile Management/Profils utilisateur streamés

Name	Paramètre par défaut	VDA
Toujours mettre en cache	Désactivée	Toutes les versions VDA
Toujours mettre en cache la taille	0 Mo	Toutes les versions VDA
Streaming des profils	Désactivée	Toutes les versions VDA
Groupes des profils utilisateurs streamés	Désactivé. Tous les profils utilisateur d'une unité d'organisation sont traités normalement.	Toutes les versions VDA

Name	Paramètre par défaut	VDA
Délai d'expiration des fichiers de verrous de la zone d'attente (jours)	1 jour	Toutes les versions VDA

Receiver

Name	Paramètre par défaut	VDA
Liste de comptes StoreFront	Aucun magasin n'est spécifié.	VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle

Virtual Delivery Agent

Name	Paramètre par défaut	VDA
Masque réseau IPv6 d'enregistrement du contrôleur	Aucun masque réseau n'est spécifié.	VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Port d'enregistrement du contrôleur	80	Toutes les versions VDA
SID de contrôleur	Aucun SID n'est spécifié.	Toutes les versions VDA
Controller	Aucun contrôleur n'est spécifié.	Toutes les versions VDA
Activer la mise à jour automatique des contrôleurs	Activée	VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle
Uniquement utiliser l'enregistrement du contrôleur IPv6	Désactivée	VDA pour OS de serveur 7 jusqu'à la version actuelle, VDA pour OS de bureau 7 jusqu'à la version actuelle

Name	Paramètre par défaut	VDA
GUID de site	Aucun GUID n'est spécifié.	Toutes les versions VDA

Virtual Delivery Agent/HDX 3D Pro

Name	Paramètre par défaut	VDA
Activer sans perte	Activée	VDA 5.5, 5.6 FP1
Paramètres de qualité HDX 3D Pro		VDA 5.5, 5.6 FP1

Virtual Delivery Agent/Surveillance

Name	**Paramètre par défaut**	**VDA**
Activer le suivi des processus	Désactivée	VDA 7.11 jusqu'à la version actuelle
Activer le suivi des ressources	Activée	VDA 7.11 jusqu'à la version actuelle

IP virtuelle

Name	Paramètre par défaut	VDA
Prise en charge du bouclage d'adresse IP virtuelle	Désactivée	VDA 7.6 jusqu'à la version actuelle
Liste de programmes de bouclage virtuel d'adresse IP virtuelle	Aucun	VDA 7.6 jusqu'à la version actuelle

Référence des paramètres de stratégie

January 23, 2019

Les stratégies contiennent des paramètres qui sont mis en œuvre lorsqu'elles sont appliquées. Les de-

scriptions de cette section indiquent également si des paramètres supplémentaires sont requis pour activer une fonctionnalité ou sont similaires à un paramètre.

Référence rapide

Les tableaux suivants présentent les paramètres que vous pouvez configurer au sein d'une stratégie. Recherchez la tâche que vous souhaitez effectuer dans la colonne de gauche, puis situez le paramètre qui lui correspond dans la colonne de droite.

Audio

Pour cette tâche	Utilisez ce paramètre de stratégie
Spécifier si l'utilisation de plusieurs périphériques audio est autorisée	Audio Plug N Play
Spécifier si l'entrée audio des microphones sur la machine utilisateur est autorisée	Redirection du microphone client
Contrôler la qualité audio sur la machine utilisateur	Qualité audio
Contrôler le mappage audio vers les haut-parleurs sur la machine utilisateur	Redirection audio cliente

Bande passante des machines utilisateur

Pour limiter la bande passante utilisée pour	Utilisez ce paramètre de stratégie
Mappage audio client	Limite de bande passante de redirection audio ou Pourcentage de limite de bande passante de redirection audio
La copie et le collage à l'aide du Presse-papiers local	Limite de bande passante de redirection du Presse-papiers ou Pourcentage de limite de bande passante de redirection du Presse-papiers
L'accès aux lecteurs clients locaux dans les sessions	Limite de bande passante de redirection de fichier ou Pourcentage de limite de bande passante de redirection de fichier

Pour limiter la bande passante utilisée pour	Utilisez ce paramètre de stratégie
Accélération multimédia HDX MediaStream	Limite de bande passante d'accélération multimédia HDX MediaStream ou Pourcentage de limite de bande passante d'accélération multimédia HDX MediaStream
Session cliente	Limite de bande passante globale de session
Impression	Limite de bande passante de redirection d'imprimante ou Pourcentage de limite de bande passante de redirection de l'imprimante
Périphériques TWAIN (appareils photo, scanners, etc.)	Limite de bande passante de redirection du périphérique TWAIN ou Pourcentage de limite de bande passante de redirection du périphérique TWAIN
Périphériques USB	Limite de bande passante de redirection du périphérique USB client ou Pourcentage de limite de bande passante de redirection du périphérique USB client

Redirection des lecteurs clients et de machines utilisateur

Pour cette tâche	Utilisez ce paramètre de stratégie
Spécifier si les lecteurs de la machine utilisateur sont connectés lorsque les utilisateurs se connectent au serveur	Connecter automatiquement les lecteurs clients
Contrôler le transfert des données copiées ou coupées entre le serveur et le Presse-papiers local	Redirection de Presse-papiers client
Déterminer la méthode de mappage des lecteurs de la machine utilisateur	Redirection de lecteur client
Contrôler si les disques durs locaux des utilisateurs sont disponibles dans une session	Lecteurs fixes clients et Redirection de lecteur client
Contrôler si les lecteurs de disquette locaux des utilisateurs sont disponibles dans une session	Lecteurs de disquette clients et Redirection du lecteur client

Pour cette tâche	Utilisez ce paramètre de stratégie
Contrôler si les lecteurs réseau des utilisateurs sont disponibles dans une session	Lecteurs réseau clients et Redirection du lecteur client
Contrôler si les lecteurs de CD, de DVD ou Blu-ray locaux des utilisateurs sont disponibles dans une session	Lecteurs optiques clients et Redirection du lecteur client
Contrôler si les lecteurs amovibles locaux des utilisateurs sont disponibles dans une session	Lecteurs amovibles clients et Redirection de lecteur client
Contrôler si les périphériques TWAIN des utilisateurs, tels que les scanners et les appareils photo, sont disponibles dans une session et contrôler la compression des transferts de données d'image	Redirection de périphérique TWAIN client et redirection de compression TWAIN
Contrôler si les périphériques USB sont disponibles dans une session	Redirection de périphérique USB client et règles de redirection de périphérique USB client
Améliorer la vitesse d'écriture et de copie des fichiers sur les disques clients via des réseaux étendus	Utiliser les écritures asynchrones

Redirection de contenu

Pour cette tâche	Utilisez ce paramètre de stratégie
Choisir d'utiliser ou non la redirection de contenu des serveurs vers la machine utilisateur	Redirection hôte vers client

IU de bureau

Pour cette tâche	Utilisez ce paramètre de stratégie
Choisir d'utiliser ou non le papier peint du bureau dans les sessions des utilisateurs	Papier peint du bureau
Afficher le contenu d'une fenêtre pendant son déplacement	Afficher le contenu de la fenêtre lors d'un cliquer déplacer

Graphiques et multimédia

Pour cette tâche	Utilisez ce paramètre de stratégie
Choisir le nombre maximal de trames par seconde envoyées depuis les bureaux virtuels vers les machines utilisateur	Taux de trames cible
Contrôler la qualité visuelle des images affichées sur la machine utilisateur	Qualité visuelle
Indiquer si le contenu Flash est rendu dans les sessions	Comportement Flash par défaut
Indiquer si les sites Web peuvent afficher du contenu Flash lors de l'accès aux sessions	Liste d'adresse URL de récupération de contenu Flash côté serveur ; Liste de compatibilité d'adresses URL Flash ; Paramètre de stratégie de prévention du retour à la vidéo Flash ; Erreur *.swf de prévention du retour à la vidéo Flash
Contrôler la compression de la vidéo rendue par le serveur	Utiliser codec vidéo pour la compression ; Utiliser le codage matériel pour le codec vidéo
Contrôler la diffusion du contenu Web multimédia HTML5 pour les utilisateurs	Redirection vidéo HTML5

Définition des priorités du trafic réseau multi-stream

Pour cette tâche	Utilisez ce paramètre de stratégie
Spécifier les ports pour le trafic ICA au travers de plusieurs connexions et établir des priorités de réseau	Stratégie Multi-Port
Activer la prise en charge des connexions multi-stream entre les serveurs et les machines utilisateur	Multi-Stream (paramètres ordinateur et utilisateur)

Imprimer

Pour cette tâche	Utilisez ce paramètre de stratégie
Contrôler la création des imprimantes clientes sur la machine utilisateur	Créer automatiquement les imprimantes clientes et Redirection d'imprimante cliente
Choisir l'emplacement où les propriétés de l'imprimante sont stockées	Rétention des propriétés d'imprimante
Définir si le client ou le serveur traite les requêtes d'impression	Diriger les connexions vers les serveurs d'impression
Indiquer si les utilisateurs peuvent accéder aux imprimantes connectées à leurs machines utilisateur	Redirection d'imprimante cliente
Contrôler l'installation des pilotes Windows natifs lors de la création automatique des imprimantes client et réseau	Installation automatique de pilotes d'imprimante fournis par défaut
Indiquer quand utiliser le pilote d'imprimante universel	Utilisation du pilote d'impression universelle
Choisir une imprimante en fonction des informations de la session de l'utilisateur itinérant	Imprimante par défaut
Équilibrer la charge et définir le seuil de basculement pour les serveurs d'impression universels	Serveurs d'impression universelle d'équilibrage de la charge Seuil au-delà duquel les serveurs d'impression universelle sont hors service

> Remarque :
>
> Les stratégies ne peuvent pas être utilisées pour activer un écran de veille dans une session de bureau ou d'application. Pour les utilisateurs qui ont besoin d'économiseurs d'écran, l'économiseur d'écran peut être implémenté sur la machine utilisateur.

Paramètres de stratégie ICA

February 28, 2019

La section ICA contient des paramètres de stratégie liés aux connexions de l'écouteur ICA et au mappage vers le Presse-papiers.

Transport adaptatif

Ce paramètre autorise ou empêche le transport de données via l'EDT comme transport principal et le retour vers TCP.

Par défaut, le transport adaptatif est défini sur **Désactivé** et TCP est toujours utilisé.

1. Dans Studio, activez le paramètre de stratégie HDX adaptive transport (il est désactivé par défaut). Nous recommandons de ne pas activer cette fonctionnalité en tant que stratégie universelle pour tous les objets du site.
2. Pour activer le paramètre de stratégie, définissez la valeur sur **Préféré** et cliquez sur **OK**.

Préféré. Le transport adaptatif via EDT est utilisé autant que possible, avec retour vers TCP.

Mode de diagnostic. EDT est activé de force et le retour vers TCP est désactivé. Nous vous recommandons de n'utiliser ce paramètre qu'à des fins de dépannage.

Désactivé. TCP est activé de force et EDT est désactivé.

Pour plus d'informations, consultez la section Transport adaptatif.

Délai d'attente de lancement des applications

Ce paramètre spécifie le délai d'attente en millisecondes pendant lequel une session attend que la première application démarre. Si le démarrage de l'application dépasse ce délai, la session se termine.

Vous pouvez choisir le délai par défaut (10 000 millisecondes) ou spécifier un nombre de millisecondes.

Redirection de Presse-papiers client

Ce paramètre permet d'autoriser ou d'empêcher le mappage du Presse-papiers sur la machine utilisateur au Presse-papiers du serveur.

Par défaut, la redirection du Presse-papiers est autorisée.

Pour empêcher le transfert des données par couper-coller entre une session et le Presse-papiers local, sélectionnez Interdire. Les utilisateurs peuvent toujours couper-coller des données entre les applications exécutées dans les sessions.

Une fois ce paramètre autorisé, configurez la bande passante maximale que le Presse-papiers peut consommer dans une connexion cliente en utilisant le paramètre Limite de bande passante de redirection du Presse-papiers ou Pourcentage de limite de la bande passante de redirection du Presse-papiers.

Formats autorisés d'écriture dans le Presse-papiers client

Lorsque le paramètre Restreindre écriture dans le Presse-papiers client est activé, les données du Presse-papiers hôte ne peuvent pas être partagées avec le point de terminaison client. Vous pouvez utiliser ce paramètre pour autoriser des formats de données spécifiques à être partagés avec le Presse-papiers de point de terminaison client. Pour utiliser ce paramètre, activez-le et ajoutez les formats spécifiques à autoriser.

Les formats de Presse-papiers suivantes sont définis par le système :

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

Les formats de Presse-papiers suivants sont prédéfinis dans XenApp et XenDesktop :

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8

Le format HTML est désactivé par défaut. Pour activer cette fonctionnalité :

- Assurez-vous que le paramètre **Redirection de Presse-papiers client** est autorisé.
- Assurez-vous que le paramètre **Restreindre écriture dans le Presse-papiers client** est activé.

- Ajoutez une entrée pour **CF_HTML** (et les formats que vous souhaitez prendre en charge) dans **Formats d'écriture autorisés dans le Presse-papiers client**.

Remarque : l'activation de la prise en charge de la copie Presse-papiers du format HTML (CF_HTML) copie les scripts (s'ils existent) depuis la source du contenu copié vers la destination. Assurez-vous que vous faites confiance à la source avant d'effectuer la copie. Si vous copiez un contenu contenant des scripts, ils ne seront actifs que si vous enregistrez le fichier de destination en tant que fichier HTML et l'exécutez.

Des formats personnalisés supplémentaires peuvent être ajoutés. Le nom de format personnalisé doit correspondre aux formats à enregistrer avec le système. Les noms de format sont sensibles à la casse.

Ce paramètre ne s'applique pas si soit Redirection de Presse-papiers client soit Restreindre l'écriture dans le Presse-papiers client est défini sur Interdit.

Démarrages de bureau

Ce paramètre autorise ou empêche les utilisateurs qui ne sont pas des administrateurs d'un groupe d'utilisateurs DirectAccess dans un VDA de se connecter à une session sur ce VDA à l'aide d'une connexion ICA.

Par défaut, les utilisateurs qui ne sont pas des administrateurs ne peuvent pas se connecter à ces sessions.

Ce paramètre n'a aucun effet sur les utilisateurs qui ne sont pas des administrateurs d'un groupe d'utilisateurs DirectAccess dans un VDA et qui utilisent une connexion Bureau à distance. Ces utilisateurs peuvent se connecter au VDA que ce paramètre soit activé ou désactivé. Ce paramètre n'a aucun effet sur les utilisateurs qui ne sont pas des administrateurs n'appartenant pas à un groupe d'utilisateurs DirectAccess dans un VDA. Ces utilisateurs peuvent se connecter au VDA que ce paramètre soit activé ou désactivé.

Expiration de délai de la connexion à l'écouteur ICA

Remarque : ce paramètre ne s'applique que pour les Virtual Delivery Agent 5.0, 5.5 et 5.6 Feature Pack 1.

Ce paramètre spécifie le temps d'attente maximal d'établissement d'une connexion utilisant le protocole ICA.

Par défaut, le temps d'attente maximal est de 120 000 millisecondes, soit deux minutes.

Numéro de port de l'écouteur ICA

Ce paramètre spécifie le numéro de port TCP/IP utilisé par le protocole ICA sur le serveur.

Le numéro port est défini par défaut sur 1494.

Les numéros de port doivent être compris entre 0 et 65535 et ne doit pas entrer en conflit avec d'autres ports identifiés. Si vous modifiez le numéro de port, redémarrez le serveur pour prendre en compte la nouvelle valeur. Si vous modifiez le numéro de port sur le serveur, vous devez également le modifier sur chaque Citrix Receiver ou plug-in qui se connecte à ce serveur.

Lancement de programmes non publiés lors de la connexion du client

Ce paramètre spécifie si les applications initiales peuvent être lancées via RDP sur le serveur.

Par défaut, le lancement d'applications via RDP sur le serveur n'est pas autorisé.

Retard du démarrage de vérification de fermeture de session

Ce paramètre spécifie la durée pendant laquelle retarder le démarrage de la vérification de fermeture de session. Cette stratégie permet de définir le délai (en secondes) pendant lequel une session client attend avant de déconnecter la session.

Ce paramètre augmente également le temps nécessaire à un utilisateur pour se déconnecter du serveur.

Restreindre l'écriture dans le Presse-papiers client

Si ce paramètre est Autorisé, les données du Presse-papiers hôte ne peuvent être partagées avec le point de terminaison client. Vous pouvez autoriser des formats spécifiques en activant le paramètre Formats autorisés d'écriture dans le Presse-papiers client.

Par défaut, cette option est définie sur Interdit.

Restreindre l'écriture dans le Presse-papiers de session

Si ce paramètre est Autorisé, les données du Presse-papiers client ne peuvent être partagées dans la session utilisateur. Vous pouvez autoriser des formats spécifiques en activant le paramètre Formats autorisés d'écriture dans le Presse-papiers de session.

Par défaut, cette option est définie sur Interdit.

Formats autorisés d'écriture dans le Presse-papiers de session

Lorsque le paramètre Restreindre l'écriture dans le Presse-papiers de session est défini sur Autorisé, les données du Presse-papiers client ne peuvent être partagées avec les applications de session. Vous pouvez utiliser ce paramètre pour autoriser des formats de données spécifiques à être partagés avec le Presse-papiers de session.

Les formats de Presse-papiers suivantes sont définis par le système :

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

Les formats de Presse-papiers suivants sont prédéfinis dans XenApp et XenDesktop :

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8

Le format HTML est désactivé par défaut. Pour activer cette fonctionnalité :

- Assurez-vous que le paramètre **Redirection de Presse-papiers client** est autorisé.
- Assurez-vous que le paramètre **Restreindre écriture dans le Presse-papiers** de session est activé.

- Ajoutez une entrée pour **CF_HTML** (et les formats que vous souhaitez prendre en charge) dans **Formats d'écriture autorisés dans le Presse-papiers de session**.

Remarque : l'activation de la prise en charge de la copie Presse-papiers du format HTML (CF_HTML) copie les scripts (s'ils existent) depuis la source du contenu copié vers la destination. Assurez-vous que vous faites confiance à la source avant d'effectuer la copie. Si vous copiez un contenu contenant des scripts, ils ne seront actifs que si vous enregistrez le fichier de destination en tant que fichier HTML et l'exécutez.

Des formats personnalisés supplémentaires peuvent être ajoutés. Le nom de format personnalisé doit correspondre aux formats à enregistrer avec le système. Les noms de format sont sensibles à la casse.

Ce paramètre ne s'applique pas si le paramètre Redirection de Presse-papiers client ou le paramètre Restreindre l'écriture dans le Presse-papiers de session est défini sur Interdit.

Paramètres de stratégie Reconnexion automatique des clients

November 9, 2018

La section Reconnexion automatique des clients contient des paramètres de stratégie permettant de contrôler la reconnexion automatique des sessions.

Reconnexion automatique des clients

Ce paramètre permet d'activer ou de désactiver la reconnexion automatique par un même client après l'interruption d'une connexion.

Pour Citrix Receiver pour Windows 4.7 et versions ultérieures, la reconnexion automatique des clients utilise uniquement les paramètres de stratégie de Citrix Studio. Les mises à jour de ces stratégies dans Studio synchronisent la reconnexion automatique des clients du serveur vers le client. Avec les versions antérieures de Citrix Receiver pour Windows, pour configurer la reconnexion automatique des clients, utilisez une stratégie Studio et modifiez le Registre ou le fichier default.ica.

L'activation de la reconnexion automatique des clients permet aux utilisateurs de retrouver leur session dans l'état dans lequel elle se trouvait lors de l'interruption de la connexion. La fonction de reconnexion automatique détecte les connexions interrompues, puis reconnecte les utilisateurs à leurs sessions.

Si le cookie Citrix Receiver contenant la clé de l'ID de session et les informations d'identification n'est pas utilisé, la reconnexion automatique peut entraîner le démarrage d'une nouvelle session, plutôt que la reconnexion à une session existante. Le cookie n'est pas utilisé s'il a expiré, par exemple en raison d'un délai de reconnexion ou si les informations d'identification doivent être à nouveau entrées.

La reconnexion automatique du client n'est pas déclenchée lorsqu'un utilisateur se déconnecte volontairement de sa session.

Une fenêtre de session est grisée lorsqu'une reconnexion est en cours. Un minuteur affiche la durée restante avant la reconnexion de la session. Une fois que la session a expiré, elle est déconnectée.

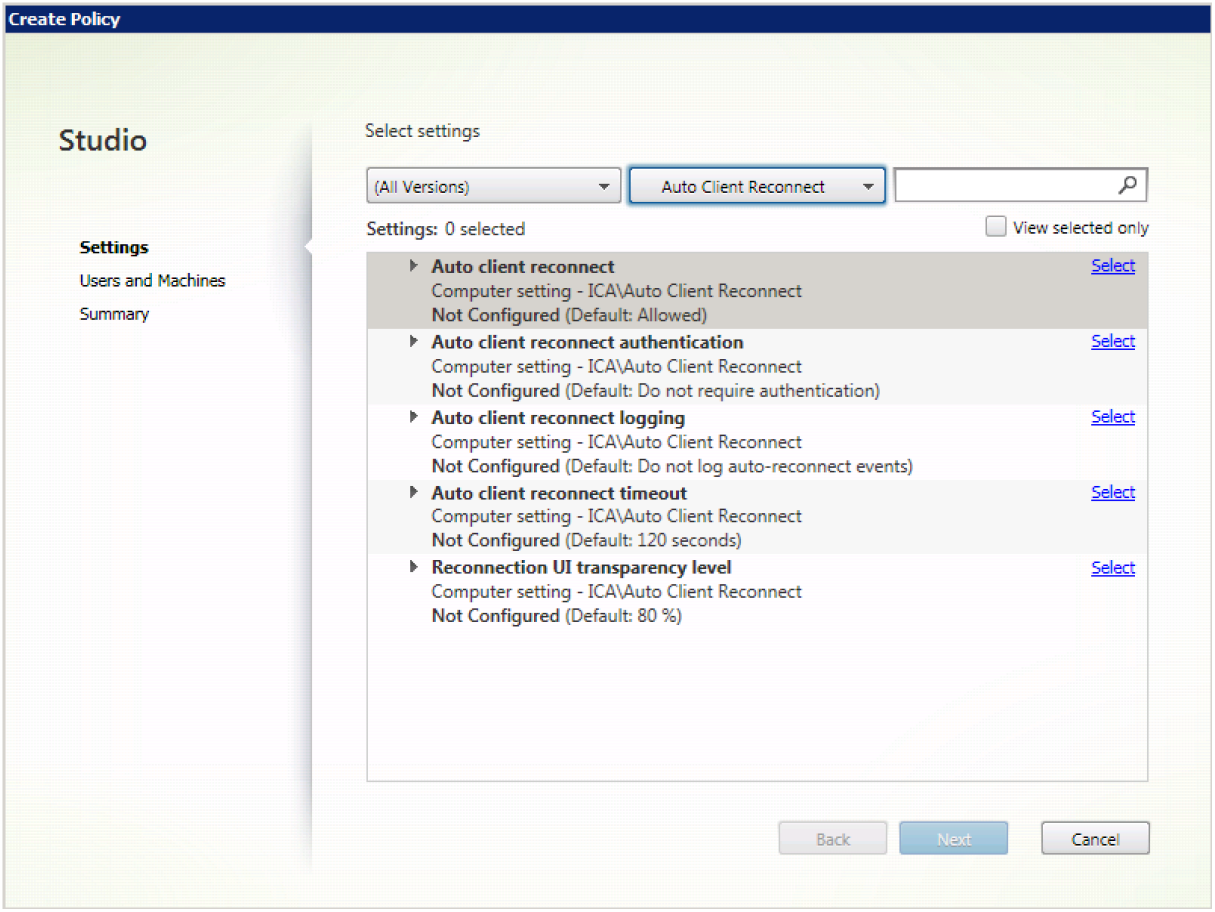
Pour les sessions d'application, lorsque la reconnexion automatique est autorisée, un minuteur s'affiche dans la zone de notification, indiquant le temps restant avant la reconnexion de la session. Citrix Receiver essaie de reconnecter une session jusqu'à ce que la reconnexion réussisse ou que l'utilisateur annule la tentative de reconnexion.

Pour les sessions de bureau, si la reconnexion automatique est autorisée, Citrix Receiver tente de se reconnecter à la session pendant une période de temps spécifiée, à moins que la reconnexion réussisse ou que l'utilisateur annule la tentative de reconnexion. Par défaut, cette durée est de cinq minutes. Pour modifier ce délai, modifiez la stratégie.

Par défaut, la reconnexion automatique des clients est autorisée.

Pour désactiver la reconnexion automatique des clients :

1. Démarrez Citrix Studio.
2. Ouvrez la stratégie **Reconnexion automatique des clients**.
3. Définissez la stratégie sur **Interdit**.



Authentification de la reconnexion automatique des clients

Ce paramètre requiert une authentification pour les reconnexions automatiques des clients.

Lorsqu'un utilisateur ouvre initialement une session, ses informations d'identification sont cryptées, stockées dans la mémoire et un cookie est créé contenant la clé de cryptage. Le cookie est envoyé à Citrix Receiver. Si ce paramètre est configuré, les cookies ne sont pas utilisés. Au lieu de cela, une boîte de dialogue s'affiche auprès des utilisateurs, leur demandant de fournir leurs informations d'identification lorsque Citrix Receiver tente de se reconnecter automatiquement.

Par défaut, l'authentification n'est pas requise.

Authentification de la reconnexion automatique des clients

1. Démarrez Citrix Studio.
2. Ouvrez la stratégie **Authentification de la reconnexion automatique des clients**.
3. Active ou désactive l'authentification.
4. Cliquez sur **OK**.

Journalisation de la reconnexion automatique des clients

Ce paramètre permet d'activer ou de désactiver l'enregistrement des reconnexions automatiques des clients dans le journal d'événements.

Lorsqu'elle est activée, le Journal système du ou des serveurs reçoit les informations relatives aux échecs et aux réussites des tentatives de reconnexion automatique. Un site ne fournit pas de journal combinant les événements de reconnexion de tous les serveurs.

Par défaut, la journalisation est désactivée.

Journalisation de la reconnexion automatique des clients

1. Démarrez Citrix Studio.
2. Ouvrez la stratégie **Journalisation de la reconnexion automatique des clients**.
3. Activez ou désactivez la journalisation.
4. Cliquez sur **OK**.

Délai de reconnexion automatique des clients

Par défaut, le délai de reconnexion automatique des clients est réglé sur 120 secondes, la valeur maximale configurable pour le délai de reconnexion automatique des clients est de 300 secondes.

Délai de reconnexion automatique des clients

1. Démarrez Citrix Studio.
2. Ouvrez la stratégie **Délai de reconnexion automatique des clients**.
3. Modifiez la valeur du délai d'expiration.
4. Cliquez sur **OK**.

Niveau de transparence de l'interface durant la reconnexion

Vous pouvez utiliser la stratégie Studio pour configurer le niveau d'opacité appliqué à la fenêtre de session XenApp ou XenDesktop lors du minutage de la reconnexion de fiabilité de session.

Par défaut, la transparence de l'interface durant la reconnexion est définie sur 80 %.

Pour modifier le niveau d'opacité de l'interface durant la reconnexion :

1. Démarrez Citrix Studio.
2. Ouvrez la stratégie **Niveau de transparence de l'interface durant la reconnexion**.
3. Modifiez la valeur.
4. Cliquez sur **OK**.

Paramètres de stratégie audio

February 28, 2019

La section Audio contient des paramètres de stratégie pour autoriser une machine utilisateur à recevoir et à envoyer des données audio dans une session sans altérer les performances.

Transport en temps réel audio via UDP

Ce paramètre permet ou empêche la transmission et la réception des données audio entre le VDA et la machine utilisateur sur RTP via le protocole UDP (User Datagram Protocol). Lorsque ce paramètre est désactivé, l'audio est envoyé et reçu sur TCP.

Par défaut, l'audio sur UDP est autorisé.

Audio Plug N Play

Ce paramètre autorise ou empêche l'utilisation de plusieurs machines audio destinées à enregistrer et lire du son.

Par défaut, l'utilisation de plusieurs périphériques audio est autorisée.

Ce paramètre s'applique uniquement aux machines équipées du système d'exploitation Windows Server.

Qualité audio

Ce paramètre spécifie le niveau de qualité sonore reçu dans les sessions utilisateur.

Par défaut, la qualité audio est définie sur Élevée : audio à définition élevée.

Pour contrôler la qualité du son, choisissez l'une des options suivantes :

- Sélectionnez Faible : pour les connexions à basse vitesse pour les connexions disposant d'une faible bande passante. Les sons envoyés à la machine utilisateur sont compressés jusqu'à 16 Kbps. Cette compression a pour effet de dégrader la qualité sonore de manière significative mais permet des performances convenables pour une connexion disposant d'une bande passante faible.
- Sélectionnez Moyenne : optimisée pour le son de la voix pour mettre à disposition des applications Voix sur IP (VoIP), des applications multimédia pour des connexions réseau difficiles avec des lignes à moins de 512 Kbps, ou dans lesquelles les pertes de paquets sont importantes du fait de l'encombrement. Ce codec offre des temps de codage très rapides, ce qui est idéal pour

une utilisation avec des softphones et des applications de communications unifiées lorsque le traitement multimédia doit s'effectuer du côté serveur.

L'audio envoyé vers la machine utilisateur est compressé jusqu'à 64 Kbps. Cette compression s'accompagne d'une baisse modérée de la qualité de l'audio restitué sur la machine utilisateur, tout en offrant une faible latence et consommant une faible bande passante. Si la qualité VoIP n'est pas satisfaisante, assurez-vous que le paramètre de stratégie transport en temps réel audio via UDP est défini sur Autorisé.

À l'heure actuelle, le protocole RTP via UDP n'est pris en charge que lorsque cette qualité audio est sélectionnée. Utilisez également cette qualité audio pour la mise à disposition d'applications multimédia dans les connexions réseau difficiles comme les lignes très basses (moins de 512 Kbps) et en cas de congestion et de perte de paquets sur le réseau.

- Pour les connexions disposant d'une bande passante élevée et pour lesquelles la qualité sonore est importante, sélectionnez Élevée : audio haute définition. Les sons sont alors transmis aux clients à leurs taux d'origine. Les sons sont compressés à un niveau de qualité similaire à la qualité CD et utilisent une bande passante maximale de 112 Kbps. La transmission d'une telle quantité de données peut solliciter l'UC de façon intensive et provoquer un engorgement du réseau.

La bande passante n'est utilisée que lors d'un enregistrement ou d'une lecture. Si les deux opérations sont effectuées en même temps, la consommation en bande passante est doublée.

Pour spécifier la quantité maximale de bande passante, configurez le paramètre Limite de bande passante de la redirection audio ou Pourcentage de limite de bande passante de la redirection audio.

Redirection audio cliente

Ce paramètre spécifie si les applications hébergées sur le serveur peuvent lire des sons par l'intermédiaire d'un périphérique audio installé sur la machine utilisateur. Ce paramètre spécifie également si les utilisateurs peuvent enregistrer l'entrée audio.

Par défaut, la redirection audio est autorisée.

Après avoir activé ce paramètre, vous pouvez limiter la bande passante utilisée par la lecture ou l'enregistrement audio. Le fait de limiter la bande passante utilisée par l'audio peut améliorer les performances des applications, mais aussi dégrader la qualité sonore. La bande passante n'est utilisée que lors d'un enregistrement ou d'une lecture. Si les deux opérations sont effectuées en même temps, la consommation de bande passante est doublée. Pour spécifier la quantité maximale de bande passante, configurez le paramètre Limite de bande passante de la redirection audio ou Pourcentage de limite de bande passante de la redirection audio.

Sur les machines équipées d'un système d'exploitation Windows Server, vous devez également vous

assurer que le paramètre Plug N Play audio est Activé pour prendre en charge plusieurs périphériques audio.

Important : l'interdiction de la redirection audio du client désactive toutes les fonctionnalités HDX audio.

Redirection du microphone client

Ce paramètre active ou désactive la redirection du microphone client. Lorsqu'il est activé, les clients peuvent utiliser des microphones pour enregistrer l'entrée audio dans une session.

Par défaut, la redirection du microphone est autorisée.

Pour des raisons de sécurité, les utilisateurs sont avertis si des serveurs non approuvés par leurs machines clientes essaient d'accéder à leurs micros. Les utilisateurs peuvent alors accepter ou refuser l'accès. Les utilisateurs peuvent désactiver l'alerte sur Citrix Receiver.

Sur les machines équipées d'un système d'exploitation Windows Server, vous devez également vous assurer que le paramètre Plug N Play audio est Activé pour prendre en charge plusieurs périphériques audio.

Si le paramètre Redirection audio du client est désactivé sur la machine cliente, cette règle n'a aucun effet.

Paramètres de stratégie de bande passante

January 23, 2019

La section Bande passante contient des paramètres de stratégie pour éviter les problèmes de performances liés à l'utilisation de la bande passante des sessions clientes.

> Important :
>
> L'utilisation de ces paramètres de stratégie avec les paramètres de stratégie Multi-Stream peut produire des résultats inattendus. Si vous utilisez les paramètres Multi-Stream dans une stratégie, assurez-vous que ces paramètres de stratégie de limite de bande passante ne sont pas inclus.

Limite de bande passante de redirection audio

Ce paramètre spécifie la bande passante maximale autorisée, en kilobits par seconde, pour la lecture ou l'enregistrement de données audio dans une session utilisateur.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre Pourcentage de limite de bande passante de la redirection audio, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Pourcentage de limite de bande passante de la redirection audio

Ce paramètre spécifie la limite de bande passante maximale autorisée pour la lecture ou l'enregistrement de données audio sous forme de pourcentage de la bande passante totale de session.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre Limite de bande passante de la redirection audio, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Si vous configurez ce paramètre, vous devez également configurer le paramètre Limite de bande passante globale de session qui spécifie la bande passante totale disponible pour les sessions clientes.

Limite de bande passante de redirection du périphérique USB client

Ce paramètre spécifie la bande passante maximale autorisée, en kilobits par seconde, pour la redirection des périphériques USB vers et depuis le client.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre Pourcentage de limite de bande passante de redirection du périphérique USB client, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Pourcentage de limite de bande passante de redirection du périphérique USB client

Ce paramètre spécifie la bande passante maximale autorisée pour la redirection de périphériques USB vers et depuis le client sous forme de pourcentage de la bande passante totale de session.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre Limite de bande passante de redirection du périphérique USB client, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Si vous configurez ce paramètre, vous devez également configurer le paramètre Limite de bande passante globale de session qui spécifie la bande passante totale disponible pour les sessions clientes.

Limite de bande passante de redirection du Presse-papiers

Ce paramètre spécifie la bande passante maximale autorisée, en kilobits par seconde, pour le transfert des données entre une session et le Presse-papiers local.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre Pourcentage de limite de la bande passante de redirection du Presse-papiers, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Pourcentage de la limite de la bande passante de redirection du Presse-papiers

Ce paramètre spécifie la bande passante maximale autorisée pour le transfert de données entre une session et le Presse-papiers local sous forme de pourcentage de la bande passante totale de session.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre Limite de bande passante de redirection du Presse-papiers, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Si vous configurez ce paramètre, vous devez également configurer le paramètre Limite de bande passante globale de session qui spécifie la bande passante totale disponible pour les sessions clientes.

Limite de bande passante pour la redirection du port COM

Remarque : pour Virtual Delivery Agent 7.0 à 7.8, configurez ce paramètre à l'aide du registre ; consultez la section
Configurer les paramètres de redirection du port COM et LPT à l'aide du Registre.

Ce paramètre spécifie la bande passante maximale autorisée, en kilobits par seconde, pour l'accès à un port COM dans une connexion cliente. Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre Pourcentage de limite de bande passante de redirection du port COM, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Pourcentage de limite de bande passante de redirection du port COM

Remarque : pour Virtual Delivery Agent 7.0 à 7.8, configurez ce paramètre à l'aide du registre ; consultez la section
Configurer les paramètres de redirection du port COM et LPT à l'aide du Registre.

Ce paramètre spécifie la bande passante maximale autorisée pour l'accès aux ports COM dans une connexion cliente, sous forme de pourcentage de la bande passante totale de session.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre Limite de bande passante pour la redirection du port COM, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Si vous configurez ce paramètre, vous devez également configurer le paramètre Limite de bande passante globale de session qui spécifie la bande passante totale disponible pour les sessions clientes.

Limite de bande passante de redirection de fichier

Ce paramètre spécifie la bande passante maximale autorisée, en kilobits par seconde, pour l'accès à un lecteur client dans une session utilisateur.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre Pourcentage de limite de bande passante de redirection de fichier, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Pourcentage de limite de bande passante de redirection de fichier

Ce paramètre spécifie la limite de bande passante maximale autorisée pour l'accès aux lecteurs clients sous forme de pourcentage de la bande passante totale de session.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre Limite de bande passante de redirection de fichier, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Si vous configurez ce paramètre, vous devez également configurer le paramètre Limite de bande passante globale de session qui spécifie la bande passante totale disponible pour les sessions clientes.

Limite de bande passante d'accélération multimédia HDX MediaStream

Ce paramètre spécifie la bande passante maximale autorisée, en kilobits par seconde, pour la mise à disposition d'audio et de vidéo à l'aide de l'accélération multimédia HDX MediaStream.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre Pourcentage de limite de bande passante d'accélération multimédia HDX MediaStream, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Pourcentage de limite de bande passante d'accélération multimédia HDX MediaStream

Ce paramètre spécifie la bande passante maximale autorisée pour la mise à disposition d'audio et de vidéo à l'aide de l'Accélération multimédia HDX MediaStream sous forme de pourcentage de la bande passante totale de session.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre Limite de bande passante d'accélération multimédia HDX MediaStream, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Si vous configurez ce paramètre, vous devez également configurer le paramètre Limite de bande passante globale de session qui spécifie la bande passante totale disponible pour les sessions clientes.

Limite de bande passante pour la redirection du port LPT

Remarque : pour Virtual Delivery Agent 7.0 à 7.8, configurez ce paramètre à l'aide du registre ; consultez la section
Configurer les paramètres de redirection du port COM et LPT à l'aide du Registre.

Ce paramètre spécifie la bande passante maximale autorisée, en kilobits par seconde, pour les tâches d'impression utilisant un port LPT dans une session utilisateur unique.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre Pourcentage de limite de bande passante de redirection du port LPT, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Pourcentage de limite de bande passante de redirection du port LPT

Remarque : pour Virtual Delivery Agent 7.0 à 7.8, configurez ce paramètre à l'aide du registre ; consultez la section
Configurer les paramètres de redirection du port COM et LPT à l'aide du Registre.

Ce paramètre spécifie la limite de bande passante pour les tâches d'impression utilisant un port LPT dans une session cliente unique sous forme de pourcentage de la bande passante totale de session.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre Limite de bande passante pour la redirection du port LPT, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Si vous configurez ce paramètre, vous devez également configurer le paramètre Limite de bande passante globale de session qui spécifie la bande passante totale disponible pour les sessions clientes.

Limite de bande passante globale de session

Ce paramètre spécifie la bande passante totale disponible, en kilobits par seconde, pour les sessions utilisateur.

La limite de bande passante maximale exécutoire est de 10 Mbps (10 000 Kbps). Par défaut, aucun maximum (zéro) n'est spécifié.

Le fait de limiter la bande passante utilisée par une connexion cliente peut améliorer les performances lorsque d'autres applications en dehors de la connexion cliente sont en concurrence et que la bande passante disponible est réduite.

Limite de bande passante de redirection d'imprimante

Ce paramètre spécifie la bande passante maximale autorisée, en kilobits par seconde, pour l'accès aux imprimantes clientes dans une session utilisateur.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre Pourcentage de limite de bande passante de redirection de l'imprimante, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Pourcentage de limite de bande passante de redirection de l'imprimante

Ce paramètre spécifie la bande passante maximale autorisée pour l'accès aux imprimantes clientes sous forme de pourcentage de la bande passante totale de session.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre Limite de bande passante de redirection d'imprimante, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Si vous configurez ce paramètre, vous devez également configurer le paramètre Limite de bande passante globale de session qui spécifie la bande passante totale disponible pour les sessions clientes.

Limite de bande passante de redirection du périphérique TWAIN

Ce paramètre spécifie la bande passante maximale autorisée, en kilobits par seconde, pour le contrôle des périphériques d'images TWAIN à partir d'applications publiées.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre Pourcentage de limite de bande passante de redirection du périphérique TWAIN, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Pourcentage de limite de bande passante de redirection du périphérique TWAIN

Ce paramètre spécifie la bande passante maximale autorisée pour le contrôle des périphériques d'images TWAIN à partir d'applications publiées sous forme de pourcentage de la bande passante totale de session.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre Limite de bande passante de redirection du périphérique TWAIN, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Si vous configurez ce paramètre, vous devez également configurer le paramètre Limite de bande passante globale de session qui spécifie la bande passante totale disponible pour les sessions clientes.

Paramètres de stratégie Redirection bidirectionnelle du contenu

January 23, 2019

La section Redirection bidirectionnelle du contenu contient des paramètres de stratégie permettant d'activer ou de désactiver la redirection client vers hôte et hôte vers URL client. Les stratégies de serveur sont définies dans Studio et les stratégies clients sont définies depuis le modèle d'administration de l'objet de stratégie de groupe Citrix Receiver.

Bien que Citrix offre également une redirection hôte vers client et Local App Access pour la redirection client vers URL, nous vous recommandons d'utiliser la redirection bidirectionnelle du contenu pour les clients Windows joints à un domaine.

La redirection bidirectionnelle du contenu requiert XenApp ou XenDesktop 7.13 ou versions ultérieures plus Citrix Receiver pour Windows 4.7 ou versions ultérieures.

> **Important**
>
> - Assurez-vous que les règles de redirection n'entraînent pas une configuration en boucle. Par exemple, les règles de client sur le VDA sont définies sur https://www.citrix.com, et les règles de VDA sur le client sont définies sur la même adresse URL, ce qui peut entraîner une exécution en boucle infinie.
> - Nous prenons en charge uniquement les points de terminaison associés à un domaine.
> - La redirection d'URL prend uniquement en charge les adresses URL explicites (URL qui ap-

paraissant dans la barre d'adresse du navigateur ou celles détectées à l'aide de la barre de navigation du navigateur, selon le navigateur spécifique). Nous ne prenons pas en charge les raccourcis de lien.
- La redirection bidirectionnelle du contenu prend en charge uniquement Internet Explorer 8 à 11. Internet Explorer doit être utilisé à la fois sur la machine utilisateur et sur le VDA.
- Le module complémentaire de navigateur Internet Explorer est requis pour la Redirection bidirectionnelle du contenu. Pour plus d'informations, consultez la section Enregistrer les modules complémentaires du navigateur.
- Aucun mécanisme de retour n'est disponible si la redirection échoue en raison de problèmes de démarrage de session.
- Si deux applications avec le même nom d'affichage sont configurées avec des comptes StoreFront multiples, un nom d'affichage du compte StoreFront principal est utilisé pour démarrer.
- Prend en charge Citrix Receiver pour Windows uniquement.
- Une nouvelle fenêtre de navigateur s'affiche uniquement lorsque l'adresse URL est redirigée sur le client. Lorsque l'adresse URL est redirigée sur le VDA, et que le navigateur est déjà ouvert, l'adresse URL redirigée s'ouvre dans le nouvel onglet.
- Prend en charge les liens intégrés dans les fichiers, y compris les documents, les e-mails et les PDF.
- Cette fonctionnalité fonctionne sur les sessions de bureau et les sessions d'application, contrairement à la redirection d'adresse URL de Local App Access, qui fonctionne uniquement sur les sessions de bureau.
- Si Local App Access est activé pour la redirection d'adresse URL (sur le VDA ou le client), la redirection bidirectionnelle du contenu ne prend pas effet.

Redirection hôte vers client et hôte vers hôte

Utilisez Studio pour configurer les stratégies de redirection hôte vers client (client) et hôte vers hôte (VDA).

Par défaut, la redirection de contenu bidirectionnel est **interdite**.

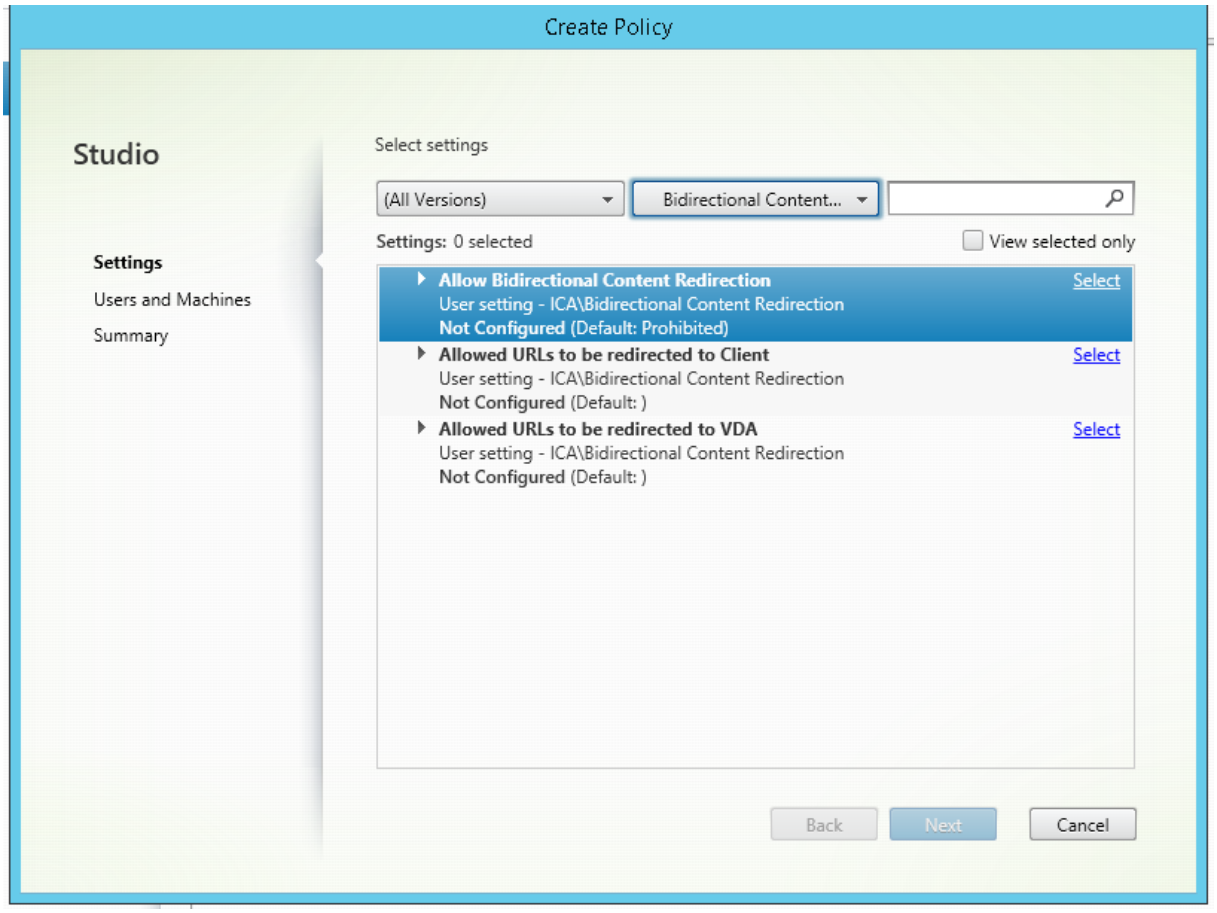
Pour activer la redirection bidirectionnelle du contenu

Lorsque vous incluez des adresses URL, vous pouvez spécifier une adresse URL ou une liste d'adresses URL séparées par un point-virgule. Vous pouvez utiliser un astérisque (*) comme caractère générique dans le nom de domaine. Par exemple :

```
https://*.citrix.com;https://www.google.com
```

1. Démarrez Citrix Studio.

2. Ouvrez la stratégie **Redirection bidirectionnelle du contenu**.
3. Sélectionnez **Autoriser la redirection bidirectionnelle du contenu**, choisissez **Autorisée** et **OK**. Si vous n'autorisez pas cette option, vous ne pouvez pas effectuer cette procédure.
4. Sélectionnez **URL autorisées à être redirigées sur le client** et spécifiez une adresse URL, une liste d'adresses URL, ou choisissez la valeur par défaut.
5. Sélectionnez **URL autorisées à être redirigées sur le VDA** et spécifiez une adresse URL, une liste d'adresses URL, ou choisissez la valeur par défaut.



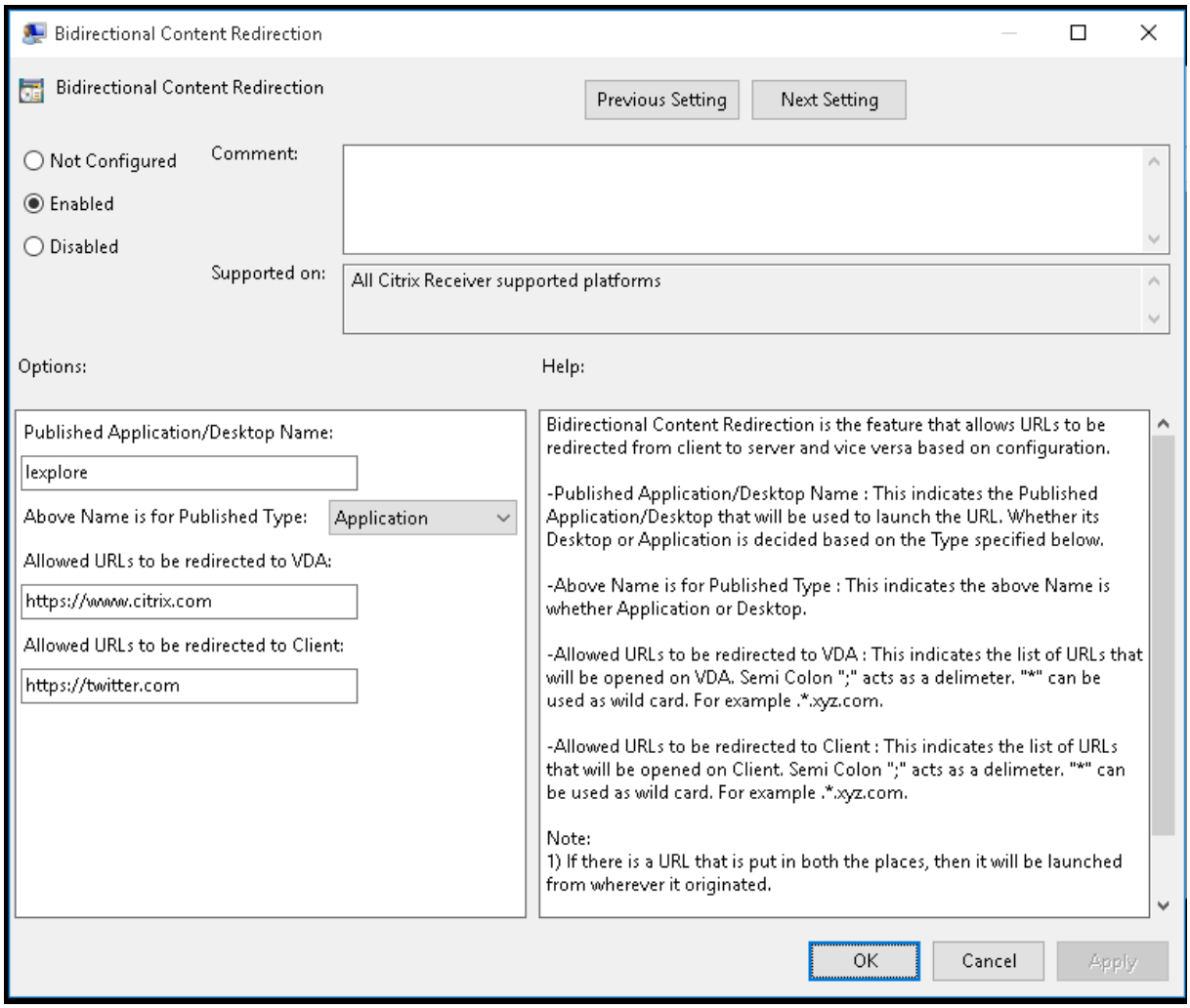
Redirection client vers hôte (VDA) et client vers client

Utilisez le modèle d'administration Objet de stratégie de groupe Citrix Receiver pour configurer la redirection client vers hôte (VDA) et client vers client (client).

Pour activer la redirection bidirectionnelle du contenu

Lorsque vous incluez des adresses URL, vous pouvez spécifier une adresse URL ou une liste d'adresses URL séparées par un point-virgule. Vous pouvez utiliser un astérisque (*) comme caractère générique.

Pour plus d'informations, consultez la section Configuration de la redirection bidirectionnelle du contenu dans la documentation de Citrix Receiver.



Enregistrer les modules complémentaires du navigateur

Le module complémentaire de navigateur Internet Explorer est requis pour la Redirection bidirectionnelle du contenu.

Vous pouvez utiliser les commandes suivantes pour enregistrer et annuler l'enregistrement du module complémentaire Internet Explorer :

- Pour enregistrer le module complémentaire Internet Explorer sur une machine cliente : `<client-installation-folder>`\redirector.exe /regIE
- Pour annuler l'enregistrement du module complémentaire Internet Explorer sur une machine cliente : `<client-installation-folder>`\redirector.exe /unregIE
- Pour enregistrer le module complémentaire Internet Explorer sur un VDA : `<VDAinstallation-folder>`\VDARedirector.exe regIE

- Pour annuler l'enregistrement du module complémentaire Internet Explorer sur un VDA : <VDAinstallation-folder>\VDARedirector.exe /unregIE

Par exemple, la commande suivante enregistre le module Internet Explorer sur une machine exécutant Citrix Receiver.

C:\Program Files\Citrix\ICA Client\redirector.exe/regIE

La commande suivante enregistre le module Internet Explorer sur un VDA avec OS Windows Server.

C:\Program Files (x86)\Citrix\System32\VDARedirector.exe /regIE

Paramètres de stratégie Capteurs clients

February 28, 2019

La section Capteurs clients contient des paramètres de stratégie permettant de contrôler la manière dont les informations de capteurs d'appareils mobiles sont gérées dans une session utilisateur.

Autoriser les applications à utiliser l'emplacement physique de la machine cliente

Ce paramètre détermine si les applications exécutées dans une session sur un appareil mobile sont autorisées à utiliser l'emplacement physique de la machine cliente.

Par défaut, l'utilisation des informations d'emplacement est interdite.

Lorsque ce paramètre est interdit, les tentatives par une application de récupération des informations d'emplacement retournent une valeur de « permission refusée ».

Lorsque ce paramètre est activé, un utilisateur peut interdire l'utilisation des informations d'emplacement en refusant une requête de Citrix Receiver pour accéder à l'emplacement. Les appareils Android et iOS invitent la saisie des informations d'emplacement lors de la première requête de chaque session.

Lors du développement d'applications hébergées qui utilisent le paramètre
Permettre aux applications d'utiliser l'emplacement physique de la machine cliente, considérez ce qui suit :

- Une application pour laquelle l'emplacement est activé ne devrait pas compter sur la disponibilité des informations d'emplacement, car :
  - Il se peut qu'un utilisateur n'ait pas accès aux informations d'emplacement.
  - Il se peut que l'emplacement ne soit pas disponible ou soit modifié lors de l'exécution de l'application.
  - Il se peut qu'un utilisateur se connecte à la session d'application depuis une machine différente qui ne prend pas en charge les informations d'emplacement.

- Une application pour laquelle l'emplacement est activé doit :
  - posséder la fonctionnalité d'emplacement désactivée par défaut ;
  - offrir une option utilisateur pour permettre ou interdire la fonctionnalité lors de l'exécution de l'application ;
  - offrir une option utilisateur pour effacer les données d'emplacement cachées par l'application. (Citrix Receiver ne cache pas les données d'emplacement.)
- Une application pour laquelle l'emplacement est activé doit gérer la précision des informations d'emplacement afin que les données acquises soient appropriées aux fins de l'application et se conforme aux régulations dans tous les territoires appropriés.
- Une connexion sécurisée (par exemple, en utilisant TLS ou un VPN) devrait être mise en application lors de l'utilisation des services d'emplacement. Citrix Receiver devrait se connecter aux serveurs de confiance.
- Considérez l'obtention de conseils juridiques quant à l'utilisation des services d'emplacement.

Paramètres de stratégie Interface utilisateur de bureau

November 9, 2018

La section UI de bureau contient des paramètres de stratégie qui contrôlent les effets visuels, tels que le papier peint du bureau, les animations de menu et le glisser-déplacer des images, pour gérer la bande passante utilisée dans les connexions clientes. Vous pouvez améliorer les performances des applications sur un réseau étendu en limitant la consommation de la bande passante.

Redirection Desktop Composition

Ce paramètre indique s'il faut utiliser la capacité de traitement de l'unité de traitement graphique (GPU) ou intégré processeur graphique (IGP) sur la machine utilisateur pour la restitution des graphiques DirectX locaux pour offrir aux utilisateurs une expérience de bureau Windows plus fluide. Lorsque cette option est activée, la redirection de la composition du bureau offre une expérience Windows très réactive tout en conservant une évolutivité élevée sur le serveur.

Par défaut, la redirection Desktop Composition est désactivée.

Pour désactiver la redirection Desktop Composition et réduire la bande passante requise dans les sessions utilisateur, sélectionnez Désactivée lorsque vous ajoutez ce paramètre à une stratégie.

Qualité graphique de redirection Desktop Composition

Ce paramètre spécifie la qualité des graphiques utilisés pour la redirection Desktop Composition.

Par défaut, ce paramètre est défini sur Élevée.

Choisissez entre les qualités Élevée, Moyenne, Basse ou Sans perte.

Papier peint du bureau

Ce paramètre autorise ou empêche l'affichage du papier-peint dans les sessions utilisateur.

Par défaut, les sessions utilisateur peuvent afficher le papier peint.

Pour désactiver le papier peint et réduire la bande passante requise dans les sessions utilisateur, sélectionnez Interdit lorsque vous ajoutez ce paramètre à la stratégie.

Animation de menu

Ce paramètre autorise ou empêche les animations de menu dans les sessions utilisateur.

Par défaut, l'animation de menu est autorisée.

L'animation de menu est un paramètre de préférence personnelle Microsoft destiné à faciliter l'accès. Lorsque cette option est activée, elle entraîne l'affichage d'un menu après un bref délai, en effectuant un défilement ou un fondu. Une icône de flèche s'affiche en bas du menu. Le menu s'affiche lorsque vous placez la souris sur cette flèche.

L'animation de menu est activée sur un bureau si ce paramètre de stratégie est réglé sur Autorisé et que le paramètre de préférence personnelle de Microsoft est activé.

Remarque : toute modification apportée au paramètre de préférence personnelle de Microsoft est apportée au bureau. Cela signifie que si le bureau est défini pour ignorer les modifications à la fin de la session, même si un utilisateur a activé les animations de menu dans une session, l'animation de menu ne sera pas disponible dans les prochaines sessions sur le bureau. Pour les utilisateurs qui nécessitent l'animation de menu, activez le paramètre Microsoft dans l'image principale du bureau ou assurez-vous que le bureau conserve les modifications apportées par l'utilisateur.

Afficher le contenu de la fenêtre lors d'un cliquer déplacer

Ce paramètre autorise ou empêche l'affichage des contenus de fenêtre lors d'un glisser-déplacer d'une fenêtre au travers de l'écran.

Par défaut, l'affichage du contenu de la fenêtre est autorisé.

S'il a la valeur Autorisé, la fenêtre entière semble se déplacer lorsque vous la faites glisser. S'il a la valeur Interdit, seul le contour de la fenêtre semble se déplacer jusqu'à ce que vous relâchiez le bouton.

Paramètres de stratégie Contrôle de l'utilisateur final

November 9, 2018

La section Contrôle de l'utilisateur final contient des paramètres de stratégie permettant de mesurer le trafic de session.

Calcul des boucles ICA

Ce paramètre détermine si les calculs de boucle ICA sont exécutés pour les connexions actives.

Par défaut, les calculs des connexions actives sont activés.

Par défaut, chaque initiation de mesure des boucles ICA est retardée jusqu'à l'apparition de trafic indiquant une interaction avec l'utilisateur. Ce retard, dont la longueur peut s'avérer indéfinie, est conçu pour empêcher que la mesure des boucles ICA devienne la seule raison du trafic ICA.

Intervalle de calcul des boucles ICA

Ce paramètre spécifie la fréquence d'exécution (en secondes) des calculs des boucles ICA.

Par défaut, les boucles ICA sont calculées toutes les 15 secondes.

Calcul des boucles ICA pour les connexions inactives

Ce paramètre détermine si les calculs de boucle ICA sont exécutés pour les connexions inactives.

Par défaut, les calculs ne sont pas exécutés pour les connexions inactives.

Par défaut, chaque initiation de mesure des boucles ICA est retardée jusqu'à l'apparition de trafic indiquant une interaction avec l'utilisateur. Ce retard, dont la longueur peut s'avérer indéfinie, est conçu pour empêcher que la mesure des boucles ICA devienne la seule raison du trafic ICA.

Paramètre de stratégie Expérience de bureau améliorée

November 9, 2018

Les sessions du paramètre de stratégie Expérience de bureau améliorée exécutées sur des systèmes d'exploitation serveur afin de ressembler à des bureaux Windows 7 locaux, offrant aux utilisateurs une expérience de bureau améliorée.

Par défaut, ce paramètre est autorisé.

Si un profil utilisateur avec un thème Windows Classic existe déjà sur le bureau virtuel, l'activation de cette stratégie n'offre pas une expérience utilisateur améliorée pour cet utilisateur. Si un utilisateur, avec un profil utilisateur de thème Windows 7, ouvre une session sur un bureau virtuel exécutant Windows Server 2012 pour lequel cette stratégie n'est soit pas configurée soit désactivée, cet utilisateur aperçoit un message d'erreur indiquant l'échec d'application du thème.

Dans les deux cas, la réinitialisation du profil utilisateur résout le problème.

Si la stratégie change d'un état activé à désactivé sur un bureau virtuel avec des sessions utilisateur actives, l'apparence de ces sessions est incohérente avec l'expérience de bureau Windows 7 et Windows Classic. Pour éviter ce problème, assurez-vous de redémarrer le bureau virtuel après la modification de ce paramètre de stratégie. Vous devez également supprimer tous les profils itinérants sur le bureau virtuel. Citrix recommande également de supprimer tous les profils d'utilisateur sur le bureau virtuel pour éviter des incohérences entre les profils.

Si vous utilisez des profils d'utilisateurs itinérants dans votre environnement, assurez-vous que la fonctionnalité Expérience de bureau améliorée est activée ou désactivée pour tous les bureaux virtuels qui partagent un profil.

Citrix ne recommande pas de partager les profils itinérants entre bureaux virtuels exécutant des systèmes d'exploitation serveur et des systèmes d'exploitation clients. Les profils des systèmes d'exploitation clients et serveurs diffèrent et le partage des profils itinérants sur les deux types de systèmes d'exploitation peut provoquer des incohérences dans les propriétés de profil lorsqu'un utilisateur passe de l'un à l'autre.

Paramètres de stratégie de la redirection de fichier

November 9, 2018

La section Redirection de fichier contient les paramètres de stratégie liés au mappage des lecteurs clients et à leur optimisation.

Connecter automatiquement les lecteurs clients

Ce paramètre autorise ou empêche la connexion automatique des lecteurs clients lorsque les utilisateurs ouvrent une session.

Par défaut, la connexion automatique est autorisée.

Lorsque vous ajoutez ce paramètre à une stratégie, assurez-vous d'activer les paramètres pour les types de lecteurs que vous souhaitez connecter automatiquement. Par exemple, pour permettre la connexion automatique des lecteurs de CD-ROM des utilisateurs, configurez ce paramètre ainsi que le paramètre Lecteurs optiques clients.

Les paramètres de stratégie suivants sont associés :

- Redirection de lecteur client
- Lecteurs de disquette clients
- Lecteurs optiques clients
- Lecteurs fixes clients
- Lecteurs réseau clients
- Lecteurs amovibles clients

Redirection de lecteur client

Ce paramètre active ou désactive la redirection de lecteur depuis et vers les lecteurs de la machine utilisateur.

Par défaut, la redirection de fichiers est activée.

Lorsqu'il est activé, les utilisateurs peuvent enregistrer des fichiers dans tous leurs lecteurs clients. Lorsqu'il est désactivé, la redirection des fichiers est interdite, quel que soit l'état des paramètres de redirection de fichiers individuels tels que Lecteurs de disquette clients et Lecteurs réseau clients.

Les paramètres de stratégie suivants sont associés :

- Lecteurs de disquette clients
- Lecteurs optiques clients
- Lecteurs fixes clients
- Lecteurs réseau clients
- Lecteurs amovibles clients

Lecteurs fixes clients

Ce paramètre autorise ou empêche les utilisateurs d'accéder à des fichiers ou d'en enregistrer sur les lecteurs de disque fixes de la machine utilisateur.

Par défaut, l'accès aux lecteurs fixes clients est autorisé.

Lorsque que vous ajoutez ce paramètre à une stratégie, vérifiez que le paramètre Redirection de lecteur client est présent et défini sur Autorisé. Si ces paramètres sont désactivés, les lecteurs fixes clients ne sont pas mappés et les utilisateurs ne peuvent pas y accéder manuellement, quel que soit l'état du paramètre Lecteurs de disque fixe clients.

Pour être certain que les lecteurs de disque fixe sont automatiquement connectés lorsque les utilisateurs ouvrent une session, configurez le paramètre Connecter automatiquement les lecteurs clients.

Lecteurs de disquette clients

Ce paramètre autorise ou empêche les utilisateurs d'accéder à des fichiers ou d'en enregistrer sur les lecteurs de disquette de la machine utilisateur.

Par défaut, l'accès aux lecteurs de disquette clients est autorisé.

Lorsque que vous ajoutez ce paramètre à une stratégie, vérifiez que le paramètre Redirection de lecteur client est présent et défini sur Autorisé. Si ces paramètres sont désactivés, les lecteurs de disquette clients ne sont pas mappés et les utilisateurs ne peuvent pas y accéder manuellement, quel que soit l'état du paramètre Lecteurs de disquette clients.

Pour garantir la connexion automatique des lecteurs de disquette lors de l'ouverture de session des utilisateurs, configurez le paramètre Connecter automatiquement les lecteurs clients.

Lecteurs réseau clients

Ce paramètre autorise ou empêche les utilisateurs d'accéder à des fichiers ou d'en enregistrer sur les lecteurs réseau (distants) par l'intermédiaire de la machine utilisateur.

Par défaut, l'accès aux lecteurs réseau clients est autorisé.

Lorsque que vous ajoutez ce paramètre à une stratégie, vérifiez que le paramètre Redirection de lecteur client est présent et défini sur Autorisé. Si ces paramètres sont désactivés, les lecteurs réseau clients ne sont pas mappés et les utilisateurs ne peuvent pas y accéder manuellement, quel que soit l'état du paramètre Lecteurs réseau clients.

Pour garantir la connexion automatique des lecteurs réseau lors de l'ouverture de session des utilisateurs, configurez le paramètre Connecter automatiquement les lecteurs clients.

Lecteurs optiques clients

Ce paramètre autorise ou empêche les utilisateurs d'accéder à des fichiers ou d'en enregistrer sur les lecteurs de CD-ROM, DVD-ROM et BD-ROM de la machine utilisateur.

Par défaut, l'accès aux lecteurs optiques clients est autorisé.

Lorsque que vous ajoutez ce paramètre à une stratégie, vérifiez que le paramètre Redirection de lecteur client est présent et défini sur Autorisé. Si ces paramètres sont désactivés, les lecteurs optiques ne sont pas mappés et les utilisateurs ne peuvent pas y accéder manuellement, quel que soit l'état du paramètre Lecteurs optiques clients.

Pour garantir la connexion automatique des lecteurs optiques lors de l'ouverture de session des utilisateurs, configurez le paramètre Connecter automatiquement les lecteurs clients.

Lecteurs amovibles clients

Ce paramètre autorise ou empêche les utilisateurs d'accéder à des fichiers ou d'en enregistrer sur les lecteurs USB de la machine utilisateur.

Par défaut, l'accès aux lecteurs amovibles clients est autorisé.

Lorsque que vous ajoutez ce paramètre à une stratégie, vérifiez que le paramètre Redirection de lecteur client est présent et défini sur Autorisé. Si ces paramètres sont désactivés, les lecteurs amovibles clients ne sont pas mappés et les utilisateurs ne peuvent pas y accéder manuellement, quel que soit l'état du paramètre Lecteurs amovibles clients.

Pour garantir la connexion automatique des lecteurs amovibles lors de l'ouverture de session des utilisateurs, configurez le paramètre Connecter automatiquement les lecteurs clients.

Redirection hôte vers client

Ce paramètre active ou désactive les associations de type de fichier pour les URL et le contenu de certains supports devant être ouverts sur la machine utilisateur. Lorsqu'elles sont désactivées, le contenu s'ouvre sur le serveur.

Par défaut, l'association de type de fichier est désactivée.

Ces types d'URL sont ouverts localement lorsque vous activez ce paramètre :

- HTTP (Hypertext Transfer Protocol) ;
- HTTPS (Secure Hypertext Transfer Protocol) ;
- Real Player et QuickTime (RTSP) ;
- Real Player et QuickTime (RTSPU) ;
- anciennes versions de Real Player (PNM) ;
- Microsoft Media Server (MMS).

Préserver les lettres de lecteurs clients

Ce paramètre active ou désactive le mappage des lecteurs client sur la même lettre de lecteur dans la session.

Par défaut, les lettres de lecteur client ne sont pas conservées.

Lorsque que vous ajoutez ce paramètre à une stratégie, vérifiez que le paramètre Redirection de lecteur client est présent et défini sur Autorisé.

Accès en lecture unique sur le lecteur client

Ce paramètre autorise les utilisateurs et les applications à créer ou modifier des fichiers sur les lecteurs clients mappés ou les en empêche.

Par défaut, les fichiers et les dossiers sur les lecteurs clients mappés peuvent être modifiés.

Si cette option est définie sur Activée, les fichiers et dossiers sont accessibles avec des permissions en lecture seule.

Lorsque que vous ajoutez ce paramètre à une stratégie, vérifiez que le paramètre Redirection de lecteur client est présent et défini sur Autorisé.

Redirection vers les dossiers spéciaux

Ce paramètre autorise ou empêche les utilisateurs Citrix Receiver et l'Interface Web de voir leurs dossiers spéciaux Documents et Bureau locaux à partir d'une session.

Par défaut, la redirection vers les dossiers spéciaux est autorisée.

Ce paramètre empêche les objets filtrés via une stratégie d'être redirigés vers les dossiers spéciaux, quels que soient les paramètres existant ailleurs. Lorsque ce paramètre est interdit, tous les paramètres connexes spécifiés pour StoreFront, l'Interface Web ou Citrix Receiver sont ignorés.

Pour déterminer les utilisateurs autorisés à disposer d'une redirection vers les dossiers spéciaux, sélectionnez Autorisé et incluez ce paramètre dans une stratégie filtrée sur les utilisateurs que vous souhaitez voir disposer de cette fonctionnalité. Ce paramètre remplace tous les autres paramètres de redirection vers les dossiers spéciaux.

Dans la mesure où la redirection vers les dossiers spéciaux doit interagir avec la machine utilisateur, les paramètres de stratégie qui empêchent les utilisateurs d'accéder à leurs lecteurs de disque fixe locaux et d'y enregistrer des fichiers empêchent également la redirection vers les dossiers spéciaux de fonctionner.

Lorsque que vous ajoutez ce paramètre à une stratégie, vérifiez que le paramètre Lecteurs fixes clients est présent et défini sur Autorisé.

Utiliser les écritures asynchrones

Ce paramètre active ou désactive les écritures asynchrones sur disque.

Par défaut, les écritures asynchrones sont désactivées.

Les écritures asynchrones sur disque peuvent accélérer la vitesse de transfert et d'écriture de fichiers sur les disques clients via des réseaux étendus, généralement caractérisés par une bande passante relativement élevée et une forte latence. Toutefois, en présence d'une erreur de connexion ou de disque,

il est possible que le ou les fichiers clients en cours d'écriture se retrouvent dans un état indéfini. Si cela se produit, une fenêtre contextuelle indique à l'utilisateur les fichiers affectés. L'utilisateur peut alors prendre une mesure corrective, par exemple en redémarrant un transfert de fichiers interrompu lors de la reconnexion ou une fois l'erreur de disque corrigée.

Citrix recommande de n'activer l'écriture asynchrone sur disque que pour les utilisateurs nécessitant une connexion distante dotée d'une rapidité d'accès aux fichiers satisfaisante et capables de réparer facilement la perte de fichiers ou de données causée par une erreur de connexion ou de disque.

Lorsque que vous ajoutez ce paramètre à une stratégie, vérifiez que le paramètre Redirection de lecteur client est présent et défini sur Autorisé. Si ce paramètre est désactivé, aucune écriture asynchrone n'aura lieu.

Paramètres de stratégie Redirection Flash

February 28, 2019

La section Redirection Flash contient les paramètres de stratégie permettant de gérer le contenu Flash dans les sessions utilisateur.

Accélération Flash

Ce paramètre permet d'activer ou de désactiver la restitution du contenu Flash sur les machines utilisateur plutôt que sur le serveur. Par défaut, la restitution du contenu Flash côté client est activée.

Remarque : ce paramètre est utilisé pour la redirection Flash d'ancienne génération avec Citrix Online Plug-in 12.1.

Lorsqu'il est activé, ce paramètre réduit la charge du réseau et du serveur en restituant le contenu Flash sur la machine utilisateur. De plus, le paramètre Liste de compatibilité d'adresses URL Flash force la restitution du contenu Flash de sites Web spécifiques sur le serveur.

Sur la machine utilisateur, le paramètre Activer HDX MediaStream pour Flash sur la machine cliente doit être également activé.

Lorsque ce paramètre est désactivé, le contenu Flash de tous les sites Web, quelle que soit leur adresse URL, est restitué sur le serveur. Pour ne permettre qu'à certains sites Web de restituer du contenu Flash sur la machine utilisateur, configurez le paramètre Liste de compatibilité d'adresses URL Flash.

Liste de couleur d'arrière-plan Flash

Ce paramètre vous permet de définir les couleurs clés pour certaines adresses URL.

Par défaut, aucune couleur clé n'est spécifiée.

Les couleurs clés s'affichent à l'arrière des contenus Flash restitués sur les clients et aident à offrir une détection de région visible. Les couleurs clés spécifiées doivent être rares ; sinon, la détection de région visible risque de ne pas fonctionner correctement.

Les entrées valides consistent en une adresse URL (avec des caractères génériques facultatifs situés au début et à la fin) suivie d'un code de couleur hexadécimal 24 bits RGB. Par exemple : `https://citrix.com 000003`.

Assurez-vous que l'adresse URL spécifiée est l'adresse URL du contenu Flash, qui peut être différente de l'adresse URL du site Web.

> **Avertissement**
>
> Une utilisation incorrecte de l'Éditeur du Registre peut occasionner de sérieux problèmes qui pourraient nécessiter l'installation du système d'exploitation. Citrix ne peut garantir la résolution des problèmes résultant d'une utilisation incorrecte de l'éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à effectuer une copie de sauvegarde avant de modifier le registre.

Sur les VDA exécutant Windows 8 ou Windows 2012, ce paramètre peut ne pas parvenir à définir des couleurs clés pour l'adresse URL. Si cela se produit, modifiez le registre sur le VDA.

Pour les machines 32 bits, utilisez ce paramètre de registre :

[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer] "ForceHDXFlashEnabled"=dword:00000001

Pour les machines 64 bits, utilisez ce paramètre de registre :

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer] "ForceHDXFlashEnabled"=dword:00000001

Compatibilité à effet rétroactif Flash

Ce paramètre active ou désactive l'utilisation des fonctionnalités de redirection Flash originales, d'ancienne génération avec d'anciennes versions de Citrix Receiver (anciennement appelé Citrix Online Plug-in).

Ce paramètre est activé par défaut.

Sur la machine utilisateur, le paramètre Activer HDX MediaStream pour Flash sur la machine cliente doit être également activé.

Les fonctionnalités de redirection Flash de seconde génération sont activées pour être utilisées avec Citrix Receiver 3.0. Les fonctionnalités de redirection d'ancienne génération sont prises en charge pour être utilisées avec Citrix Online Plug-in 12.1. Pour vous assurer que les fonctionnalités Flash de

seconde génération sont utilisées, la redirection Flash de seconde génération doit être activée à la fois sur le serveur et la machine utilisateur. Si la redirection d'ancienne génération est activée soit sur le serveur soit sur la machine utilisateur, les fonctionnalités de redirection d'ancienne génération sont utilisées.

Comportement Flash par défaut

Ce paramètre établit le comportement par défaut de l'accélération Flash de seconde génération.

Par défaut, l'accélération Flash est activée.

Pour contrôler ce paramètre, choisissez l'une des options suivantes :

- Activez la redirection Flash. La redirection Flash est utilisée.
- Bloquez le lecteur Flash. La redirection Flash et la restitution côté serveur ne sont pas utilisées. L'utilisateur ne peut visualiser aucun contenu Flash.
- Désactivez le lecteur Flash. La redirection Flash n'est pas utilisée. L'utilisateur peut visualiser le contenu Flash restitué côté serveur si une version du lecteur Adobe Flash Player compatible avec Windows Internet Explorer est installée sur le serveur.

Ce paramètre peut être remplacé pour des pages Web individuelles et des instances Flash basées sur la configuration du paramètre Liste de compatibilité d'adresses URL Flash. De plus, sur la machine utilisateur, le paramètre Activer HDX MediaStream pour Flash sur la machine cliente doit être également activé.

Journalisation d'événements Flash

Ce paramètre autorise l'enregistrement des événements Flash dans le journal d'événements d'application Windows.

Par défaut, la journalisation est autorisée.

Sur les ordinateurs exécutant Windows 7 ou Windows Vista, un journal spécifique à la redirection Flash s'affiche dans le nœud du journal Applications et services.

Retour intelligent Flash

Ce paramètre active et désactive les tentatives automatiques d'utiliser la restitution côté serveur des instances du lecteur Flash où la restitution côté client n'est soit pas nécessaire ou soit offre une expérience utilisateur appauvrie.

Ce paramètre est activé par défaut.

Seuil de latence Flash

Ce paramètre spécifie un seuil entre 0 et 30 millisecondes pour déterminer l'emplacement de restitution du contenu Adobe Flash.

Par défaut, le seuil est de 30 millisecondes.

Durant le démarrage, HDX MediaStream pour Flash mesure la latence actuelle entre le serveur et la machine utilisateur. Si la latence se trouve en dessous de ce seuil, HDX MediaStream pour Flash est utilisé pour restituer le contenu Adobe Flash sur la machine utilisateur. Si la latence se trouve au-dessus de ce seuil, le serveur réseau restitue le contenu si un lecteur Adobe Flash est disponible à cet endroit.

Lorsque vous activez ce paramètre, assurez-vous que le paramètre Compatibilité à effet rétroactif Flash est également présent et défini sur Activé.

Remarque : s'applique uniquement lors de l'utilisation de la redirection HDX MediaStream Flash en mode d'ancienne génération.

Prévention du retour à la vidéo Flash

Ce paramètre spécifie si et comment le contenu Flash « de petite taille » est restitué et affiché pour les utilisateurs.

Ce paramètre n'est pas configuré par défaut.

Pour contrôler ce paramètre, choisissez l'une des options suivantes :

- **Contenu de petite taille uniquement.** Seul le contenu de retour intelligent sera restitué sur le serveur ; tout autre contenu Flash sera remplacé par un fichier d'erreur *.swf.
- **Contenu de petite taille uniquement avec client pris en charge.** Seul le contenu de retour intelligent sera restitué sur le serveur si le client utilise la redirection Flash ; tout autre contenu sera remplacé par un fichier d'erreur *.swf.
- **Aucun contenu côté serveur.** Tout le contenu sur le serveur sera remplacé par une erreur *swf.

Pour utiliser ce paramètre de stratégie, vous devez spécifier un fichier d'erreur *.swf. Ce fichier d'erreur *.swf remplacera tout contenu que vous ne souhaitez pas restituer sur le VDA.

Erreur *.swf de prévention du retour à la vidéo Flash

Ce paramètre spécifie l'adresse URL du message d'erreur qui s'affiche pour les utilisateurs pour remplacer des instances Flash lorsque les stratégies de gestion de charge du serveur sont en cours d'utilisation. Par exemple :

```
http://domainName.tld/sample/path/error.swf
```


Liste d'adresses URL de récupération du contenu Flash côté serveur

Ce paramètre spécifie les sites Web pour lesquels le contenu Flash peut être téléchargé vers le serveur, puis transféré à la machine utilisateur pour restitution.

Par défaut, aucun site n'est spécifié.

Ce paramètre est utilisé lorsque la machine utilisateur n'ait pas accès direct à Internet ; le serveur offre cette connexion. De plus, sur la machine utilisateur, le paramètre Activer la récupération de contenu côté serveur doit être activé.

La redirection Flash de seconde génération comprend un retour vers la récupération de contenu côté serveur pour les fichiers .swf Flash. Si la machine utilisateur est incapable de restituer du contenu Flash depuis un site Web, et que le site Web est spécifié dans la liste d'adresses URL de récupération de contenu côté serveur, la récupération de contenu côté serveur se produit automatiquement.

Lors de l'ajout d'adresses URL à la liste :

- Ajoutez l'adresse URL de l'application Flash au lieu de la page HTML de niveau supérieur qui initie le lecteur Flash.
- Utilisez un astérisque (*) comme caractère générique au début ou à la fin de l'adresse URL.
- Utilisez un caractère générique de fin pour autoriser toutes les adresses URL enfant (`http://www.citrix.com/*`).
- Les préfixes `http://` et `https://` sont utilisés lorsqu'ils sont présents, mais ne sont pas requis pour des entrées de liste valides.

Liste de compatibilité d'adresses URL Flash

Ce paramètre spécifie les règles qui déterminent si le contenu Flash de certains sites Web est restitué sur la machine utilisateur, restitué sur le serveur ou si la restitution est bloquée.

Par défaut, aucune règle n'est spécifiée.

Lors de l'ajout d'adresses URL à la liste :

- Ordonnez la liste par ordre de priorité avec les adresses URL, les actions et l'emplacement de restitution les plus importants en haut de celle-ci.
- Utilisez un astérisque (*) comme caractère générique au début ou à la fin de l'adresse URL.
- Utilisez un caractère générique de fin pour faire référence à toutes les adresses URL enfant (`https://www.citrix.com/*`).
- Les préfixes `http://` et `https://` sont utilisés lorsqu'ils sont présents, mais ne sont pas requis pour des entrées de liste valides.
- Ajoutez à cette liste les sites Web dont le contenu Flash n'est pas restitué correctement sur la machine utilisateur et sélectionnez soit l'option Restituer sur le serveur soit l'option Bloquer.

Paramètres de stratégie Graphiques

January 23, 2019

La section Graphiques contient des paramètres de stratégie permettant de contrôler le traitement des images dans les sessions utilisateur.

Autoriser la compression visuelle sans perte

Ce paramètre permet d'utiliser une compression visuellement sans perte au lieu d'une compression vraie sans perte pour l'affichage des graphiques. La compression visuellement sans perte améliore les performances par rapport à la compression vraie sans perte, mais engendre une perte mineure qui ne peut être remarquée à l'œil nu. Ce paramètre change la manière dont les valeurs du paramètre « Qualité visuelle » sont utilisées.

Par défaut, ce paramètre est désactivé.

Limite de mémoire d'affichage

Ce paramètre spécifie la taille maximale de la mémoire tampon vidéo (en kilo-octets) pour la session.

Par défaut, la limite de mémoire d'affichage est de 65536 kilo-octets.

Spécifie la taille maximale de la mémoire tampon vidéo (en kilo-octets) pour la session. Spécifiez une taille en kilo-octets comprise entre 128 et 4 194 303. La valeur maximale de 4 194 303 ne limite pas la mémoire d'affichage. Par défaut, la mémoire d'affichage est de 65536 kilo-octets. Les connexions utilisant un nombre de couleurs et une résolution élevés nécessitent plus de mémoire. En mode graphique d'ancienne génération, si la limite de mémoire est atteinte, l'affichage se dégrade en fonction du paramètre « Préférence de dégradation du mode d'affichage ».

Pour les connexions nécessitant un nombre de couleurs et une résolution élevés, augmentez la limite. Calculez la mémoire maximale requise à l'aide de cette équation :

Quantité de mémoire en octets = (nombre-de-couleur-en-bits-par-pixel)/8) * (résolution-verticale-en-pixels) * (résolution-horizontale-en-pixels).

Par exemple, avec un nombre de couleurs de 32, une résolution verticale de 600 et une résolution horizontale de 800, la mémoire maximale nécessaire est (32 / 8) * (600) * (800) = 1920000 octets, qui fournit une limite de mémoire d'affichage de 1920 Ko.

Des nombres de couleurs autres que 32 bits sont uniquement disponibles si la stratégie de mode graphique d'ancienne génération est activée.

HDX alloue uniquement la quantité de mémoire d'affichage nécessaire pour chaque session. Donc, si seuls certains utilisateurs ont besoin de plus que la valeur par défaut, il n'existe aucun impact négatif sur la capacité à monter en charge par l'augmentation de la limite de mémoire d'affichage.

Préférence de dégradation du mode d'affichage

Remarque : pour Virtual Delivery Agent 7.x, ce paramètre de stratégie s'applique uniquement lorsque le paramètre de stratégie du Mode graphique d'ancienne génération est activé.

Ce paramètre spécifie que le nombre de couleurs ou la résolution se dégrade en premier lorsque la limite de mémoire d'affichage de la session est atteinte.

Par défaut, le nombre de couleurs se dégrade en premier.

Lorsque la limite de mémoire de la session est atteinte, vous pouvez réduire la qualité des images affichées en indiquant si le nombre de couleurs ou la résolution se dégrade en premier. Lorsque le nombre de couleurs se dégrade en premier, les images affichées utilisent moins de couleurs. Lorsque la résolution se dégrade en premier, les images affichées utilisent moins de pixels par pouce.

Pour avertir les utilisateurs lorsque le nombre de couleurs ou la résolution se dégrade, configurez le paramètre Notifier l'utilisateur lorsque le mode d'affichage se dégrade.

Aperçu de fenêtres dynamiques

Ce paramètre active ou désactive l'affichage de fenêtres transparentes en modes d'aperçu de fenêtres Flip, Flip 3D, Taskbar Preview et Peek.

Option d'aperçu de Windows Aéro	Description
Aperçu de la barre des tâches	Lorsque l'utilisateur place le pointeur de la souris sur l'icône de barre des tâches d'une fenêtre, une image de cette fenêtre s'affiche au-dessus de la barre des tâches.
Windows Peek	Lorsque l'utilisateur place le pointeur de la souris sur l'image d'un aperçu de la barre des tâches, une image plein écran de cette fenêtre s'affiche.
Flip	Lorsque l'utilisateur appuie sur ALT+TAB, des petites icônes d'aperçu s'affichent pour chaque fenêtre ouverte.

Option d'aperçu de Windows Aéro	Description
Flip 3D	Lorsque l'utilisateur appuie sur la touche Windows+TAB, des grandes images des fenêtres ouvertes s'affichent en cascade sur l'écran.

Ce paramètre est activé par défaut.

Cache d'image

Remarque : pour Virtual Delivery Agent 7.x, ce paramètre de stratégie s'applique uniquement lorsque le paramètre de stratégie du Mode graphique d'ancienne génération est activé.

Ce paramètre active ou désactive la mise en cache et la récupération de sections d'images dans les sessions. La mise en cache d'images dans des sections et la récupération de ces sections en cas de besoin facilite l'accès, réduit le volume de données transférées sur le réseau et réduit le traitement requis sur la machine utilisateur.

Le paramètre de mise en cache des images est activé par défaut.

Remarque : le paramètre de mise en cache des images contrôle la façon dont les images sont placées dans le cache et récupérées ; il ne contrôle pas si les images sont placées dans le cache. Les images sont placées dans le cache si le paramètre Mode graphique d'ancienne génération est activé.

Mode graphique d'ancienne génération

Ce paramètre désactive l'expérience graphique enrichie. Utilisez ce paramètre pour revenir à l'expérience graphique d'ancienne génération, ce qui réduit la consommation de bande passante sur un réseau étendu ou une connexion mobile. Les réductions apportées à la consommation de bande passante introduites dans XenApp et XenDesktop 7.13 rendent ce mode obsolète.

Par défaut, ce paramètre est désactivé et les utilisateurs se voient offrir une expérience graphique enrichie.

Le mode graphique d'ancienne génération est pris en charge avec les VDA Windows 7 et Windows Server 2008 R2.

Le mode graphique d'ancienne génération n'est pas pris en charge sur Windows 8.x, 10 ou Windows Server 2012, 2012 R2 et 2016.

Consultez l'article CTX202687 pour de plus amples informations sur l'optimisation des modes graphiques et sur les stratégies dans XenApp et XenDesktop 7.6 FP3 ou version supérieure.

Nombre de couleurs maximal autorisé

Remarque : pour Virtual Delivery Agent 7.x, ce paramètre de stratégie s'applique uniquement lorsque le paramètre de stratégie du Mode graphique d'ancienne génération est activé.

Ce paramètre spécifie le nombre maximal de couleurs autorisé pour une session.

Par défaut, le nombre maximal de couleurs autorisé est de 32 bits par pixel.

Ce paramètre s'applique uniquement aux pilotes et aux connexions ThinWire. Il ne s'applique pas aux VDA qui disposent d'un pilote non-ThinWire en tant que pilote d'écran principal, tels que les VDA qui utilisent un pilote Windows Display Driver Model (pilote WDDM) en tant que pilote d'écran principal. Pour les VDA avec OS de bureau utilisant un pilote WDDM en tant que pilote d'écran principal, tel que Windows 8, ce paramètre n'a aucun effet. Pour les VDA avec OS Windows Server utilisant un pilote WDDM, tel que Windows Server 2012 R2, ce paramètre peut empêcher les utilisateurs de se connecter au VDA.

Plus le nombre de couleurs est élevé, plus la mémoire requise est importante. Pour dégrader le nombre de couleurs lorsque la limite de mémoire est atteinte, configurez le paramètre Préférence de dégradation du mode d'affichage. Lorsque le nombre de couleurs se dégrade, les images affichées utilisent moins de couleurs.

Notifier l'utilisateur lorsque le mode d'affichage se dégrade

Remarque : pour Virtual Delivery Agent 7.x, ce paramètre de stratégie s'applique uniquement lorsque le paramètre de stratégie du Mode graphique d'ancienne génération est activé.

Ce paramètre permet d'afficher une brève explication pour l'utilisateur lorsque le nombre de couleurs ou la résolution se dégrade.

Par défaut, la notification des utilisateurs est désactivée.

Mise en file d'attente et ballotage

Remarque : pour Virtual Delivery Agent 7.x, ce paramètre de stratégie s'applique uniquement lorsque le paramètre de stratégie du Mode graphique d'ancienne génération est activé.

Ce paramètre permet d'ignorer toute image en file d'attente qui est remplacée par une autre image.

Par défaut, la mise en file d'attente et le ballotage sont activés.

Cela améliore le temps de réponse lorsque des graphiques sont envoyés à la machine utilisateur. La configuration de ce paramètre peut provoquer une animation hachée due à des trames ignorées.

Utiliser codec vidéo pour la compression

Permet d'utiliser un codec vidéo (H.264) pour compresser les graphiques lorsque le décodage vidéo est disponible sur le poste client. Lorsque **Pour l'écran entier** est sélectionné, le codec vidéo sera appliqué en tant que codec par défaut pour tout. Lorsque **Pour les zones changeant constamment** est sélectionné, le codec vidéo sera utilisé pour les zones changeant constamment sur l'écran, les autres données continueront à utiliser la compression d'image fixe et la mise en cache des bitmaps Si le décodage vidéo n'est pas disponible sur le poste client ou que vous avez spécifié **Ne pas utiliser**, une combinaison de compression d'image fixe et de mise en cache des bitmaps est utilisée. Lorsque l'option **Utiliser un codec vidéo au choix** est sélectionnée, le système se base sur plusieurs facteurs pour effectuer un choix. Les résultats peuvent varier en fonction des versions car la méthode de sélection est améliorée.

Sélectionnez l'option **Utiliser un codec vidéo au choix** pour permettre au système de choisir les paramètres qui conviennent le mieux au scénario actuel.

Sélectionnez l'option **Pour l'écran entier** pour optimiser l'expérience utilisateur et la bande passante, particulièrement dans les cas dans lesquels le rendu vidéo sur le serveur et les graphiques 3D sont fortement sollicités.

Sélectionnez l'option **Pour les zones changeant constamment** pour optimiser les performances vidéo, particulièrement en cas de faible bande passante, tout en conservant la capacité à monter en charge pour le contenu statique et changeant lentement. Ce paramètre est pris en charge dans les déploiements comportant plusieurs moniteurs.

Sélectionnez l'option **Ne pas utiliser de codec vidéo** pour optimiser la charge d'UC du serveur et pour les scénarios avec peu de rendu vidéo sur le serveur ou ne faisant pas appel à beaucoup d'applications exigeant d'importantes ressources graphiques.

La valeur par défaut est **Utiliser un codec vidéo au choix**.

Utiliser le codage matériel pour la vidéo

Ce paramètre permet d'utiliser du matériel graphique, si disponible, pour compresser les éléments d'écran avec un codec vidéo (H.264). Si ce matériel n'est pas disponible, le VDA utilisera le codage basé sur l'UC avec le codec vidéo logiciel.

L'option par défaut pour ce paramètre de stratégie est **Activé**.

Les moniteurs multiples sont pris en charge.

Tout Citrix Receiver qui prend en charge le décodage H.264 peut être utilisé avec le codage matériel NVENC.

La compression avec perte (4:2:0) et la compression visuelle sans perte (4:4:4) sont prises en charge. La compression visuelle sans perte (paramètre de stratégie graphique, Autoriser la compression visuelle sans perte) requiert Receiver pour Windows version 4.5 ou version supérieure.

NVIDIA

Pour les GPU NVIDIA GRID, le codage matériel est pris en charge avec les VDA pour OS de bureau en mode HDX 3D Pro.

Les GPU NVIDIA doivent prendre en charge le codage matériel NVENC. Voir SDK codec vidéo NVIDIA pour une liste des processeurs graphiques pris en charge.

NVIDIA GRID requiert une version de pilote 3.1 ou supérieure. NVIDIA Quadro requiert une version de pilote 362.56 ou supérieure. Citrix recommande des pilotes NVIDIA version R361.

Le texte sans perte, une fonctionnalité du VDA lorsqu'il est configuré en mode standard (et non HDX 3D Pro), n'est pas compatible avec le codage matériel NVENC. S'il a été activé en mode HDX 3D Pro, le texte sans perte a priorité sur le codage matériel NVENC.

L'utilisation sélective du codec de matériel H.264 pour les zones changeant constamment n'est pas prise en charge.

Intel

Pour les processeurs graphiques Intel Iris Pro, le codage matériel est pris en charge avec les VDA pour OS de bureau (en mode standard ou HDX 3D Pro) et les VDA pour OS de serveur.

Les processeurs graphiques Intel Iris Pro de la famille des processeurs Intel Broadwell et plus récents sont pris en charge. Le SDK du codeur matériel Intel Iris Pro est requis et peut être téléchargé depuis le site Web Intel : SDK affichages distants.

Le texte sans perte est pris en charge.

L'utilisation sélective du codec de matériel H.264 pour les zones changeant constamment est prise en charge.

Pris en charge avec Windows 10 et Windows Server 2012 et versions supérieures.

Sur les VDA en mode 3D Pro, le codeur Intel fournit une expérience utilisateur de bonne qualité pour jusqu'à huit sessions de codage (par exemple, un utilisateur utilisant huit moniteurs ou huit utilisateurs utilisant un moniteur). Si plus de huit sessions de codage sont requises, vérifiez le nombre de moniteurs auxquels la machine virtuelle se connecte. Afin de conserver une expérience utilisateur optimale, l'administrateur peut choisir de configurer ce paramètre de stratégie par utilisateur ou par machine.

Paramètres de stratégie Mise en cache

November 9, 2018

La section Mise en cache contient des paramètres de stratégie qui vous permettent de mettre en cache des données d'image sur les machines utilisateur lorsque les connexions clientes sont limitées en bande passante.

Seuil de cache permanent

Remarque : pour Virtual Delivery Agent 7.x, ce paramètre de stratégie s'applique uniquement lorsque le paramètre de stratégie du
Mode graphique d'ancienne génération est activé.

Ce paramètre met en cache les images bitmap sur le disque dur de la machine utilisateur. Ceci permet une réutilisation d'images de taille importante, fréquemment utilisées provenant de sessions précédentes.

Par défaut, le seuil est de 3000000 kilobits par seconde.

La valeur de seuil représente le point en dessous duquel la fonctionnalité de cache permanent prendra effet. Par exemple, concernant la valeur par défaut, les images bitmaps sont cachées sur le disque dur de la machine utilisateur lorsque la bande passante se trouve en dessous de 3000000 bps.

Paramètres de stratégie Framehawk

November 9, 2018

La section Framehawk contient des paramètres de stratégie permettant d'activer et de configurer le canal d'affichage Framehawk sur le serveur.

Canal d'affichage Framehawk

Lorsque cette option est activée, le serveur tente d'utiliser le canal d'affichage Framehawk pour les graphiques et la saisie à distance. Ce canal d'affichage utilise UDP pour offrir une meilleure expérience utilisateur sur les réseaux à perte et à latence élevées ; cependant, il peut également utiliser davantage de ressources serveur et de bande passante que les autres modes graphiques.

Par défaut, le canal d'affichage Framehawk est désactivé.

Plage de ports du canal d'affichage Framehawk

Ce paramètre spécifie la plage de numéros de ports UDP (sous la forme *numéro de port le plus bas,numéro de port le plus élevé*) que le VDA peut utiliser pour échanger des données de canal d'affichage Framehawk avec la machine utilisateur. Le VDA tente d'utiliser chaque port, en commençant par le numéro de port le plus bas et en remontant pour chaque tentative. Le port gère le trafic entrant et sortant.

Par défaut, la plage de ports est 3224,3324.

Paramètres de stratégie Persistance

November 9, 2018

La section Persistance contient les paramètres de stratégie pour gérer les messages de persistance ICA.

Délai d'expiration de persistance ICA

Ce paramètre spécifie le nombre de secondes entre les messages de persistance ICA successifs.

Par défaut, l'intervalle entre les messages de persistance est de 60 secondes.

Spécifiez l'intervalle (entre 1 et 3600 secondes) à utiliser pour envoyer des messages de persistance ICA. Ne configurez pas ce paramètre si votre logiciel de contrôle de réseau est responsable de la fermeture des connexions inactives.

Persistances ICA

Ce paramètre active ou désactive l'envoi périodique de messages de persistance ICA.

Par défaut, aucun message de persistance n'est envoyé.

L'activation de ce paramètre empêche la déconnexion des connexions interrompues. Si le serveur ne détecte pas d'activité, ce paramètre empêche les services Bureau à distance de déconnecter la session. Le serveur envoie des messages de persistance à quelques secondes d'intervalle pour détecter si la session est active. Si la session n'est plus active, le serveur marque la session en tant que déconnectée.

Cependant, la persistance ICA ne fonctionne pas si vous utilisez la fiabilité de session. Ne configurez la persistance ICA que pour les connexions qui n'utilisent pas la fiabilité de session.

Paramètres de stratégie liés : Connexions de fiabilité de session.

Paramètres de stratégie Local App Access

November 9, 2018

La section Local App Access contient des paramètres de stratégie qui gèrent l'intégration des applications des utilisateurs installées localement avec les applications hébergées dans un environnement de bureau hébergé.

Autoriser Local App Access

Ce paramètre autorise ou empêche l'intégration des applications installées localement avec les applications hébergées dans un environnement de bureau hébergé.

Lorsqu'un utilisateur lance une application installée localement, l'application semble être exécutée dans leur bureau virtuel, même si elle est exécutée localement.

Par défaut, l'accès à l'application locale est interdit.

Liste noire de redirection d'adresse URL

Ce paramètre spécifie les sites Web qui sont redirigés vers et lancés dans le navigateur Web local. Cela peut inclure les sites Web nécessitant des paramètres régionaux d'informations, tels que msn.com ou newsgoogle.com, ou des sites Web contenant du contenu multimédia enrichi qui sont mieux restitués sur la machine utilisateur.

Par défaut, aucun site n'est spécifié.

Liste blanche de redirection d'adresse URL

Ce paramètre spécifie les sites Web qui sont restitués dans l'environnement dans lequel elles sont lancées.

Par défaut, aucun site n'est spécifié.

Paramètres de stratégie Expérience mobile

November 9, 2018

La section Experience Mobile contient des paramètres de stratégie destinés à la gestion de Citrix Mobility Pack.

Affichage de clavier automatique

Ce paramètre active ou désactive l'affichage automatique du clavier sur les écrans des appareils mobiles.

Par défaut, l'affichage automatique du clavier est désactivé.

Démarrer le bureau tactile

Ce paramètre est désactivé et n'est pas disponible pour les machines Windows 10 ou Windows Server 2016.

Ce paramètre détermine le comportement général de l'interface du Citrix Receiver en autorisant ou en interdisant une interface tactile optimisée pour les tablettes.

Par défaut, une interface tactile est utilisée.

Pour n'utiliser que l'interface Windows, définissez cette stratégie sur Interdit.

Contrôler la zone combinée

Ce paramètre détermine les types de zones de liste déroulante que vous pouvez afficher dans les sessions sur les appareils mobiles. Pour afficher la commande de zone combinée d'appareil native, définissez ce paramètre de stratégie sur Autorisé. Lorsque ce paramètre est autorisé, un utilisateur peut modifier un paramètre de session Citrix Receiver pour iOS afin d'utiliser la zone combinée Windows.

Par défaut, la fonctionnalité Contrôler la zone combinée est interdite.

Paramètres de stratégie multimédia

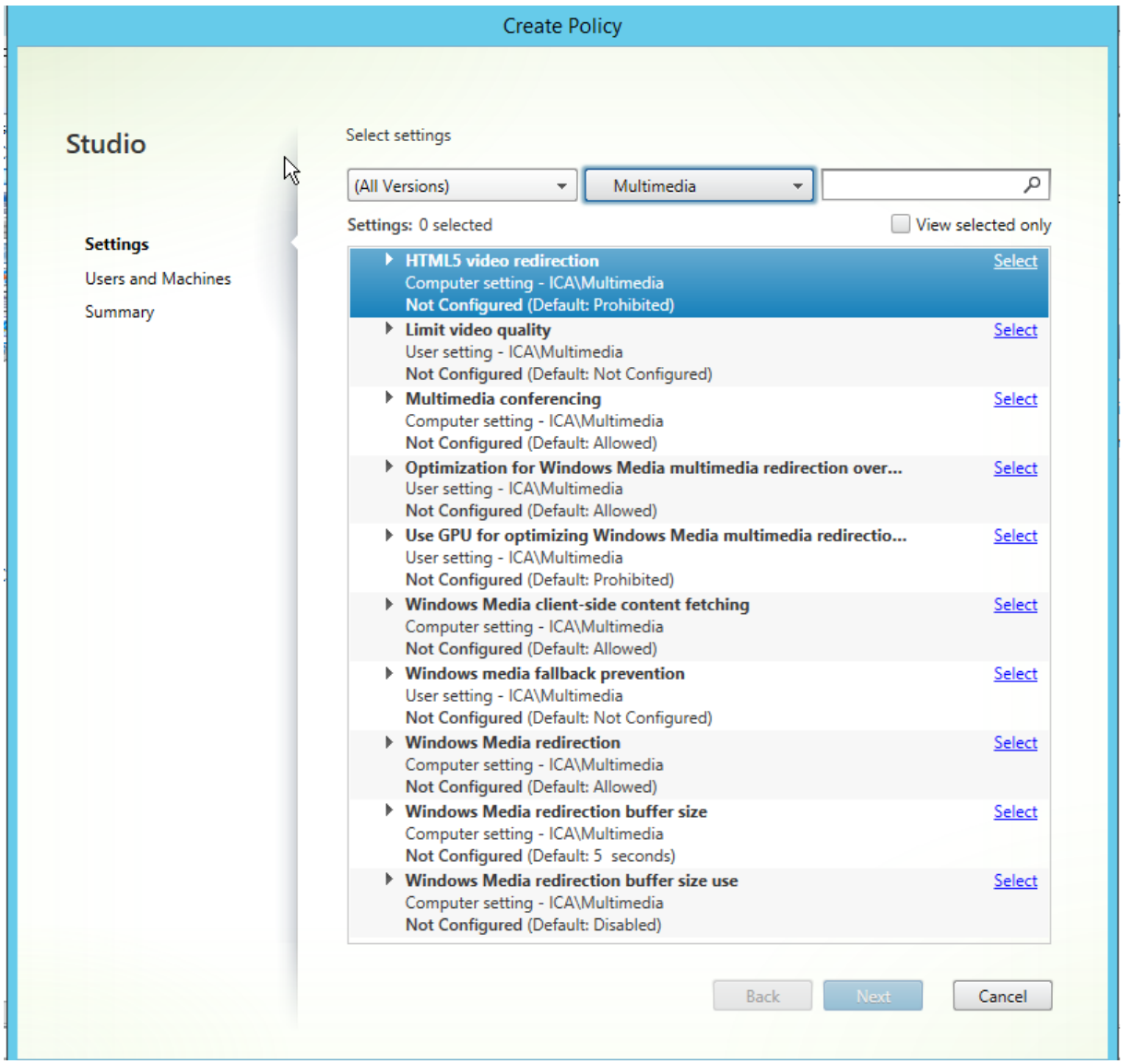
January 23, 2019

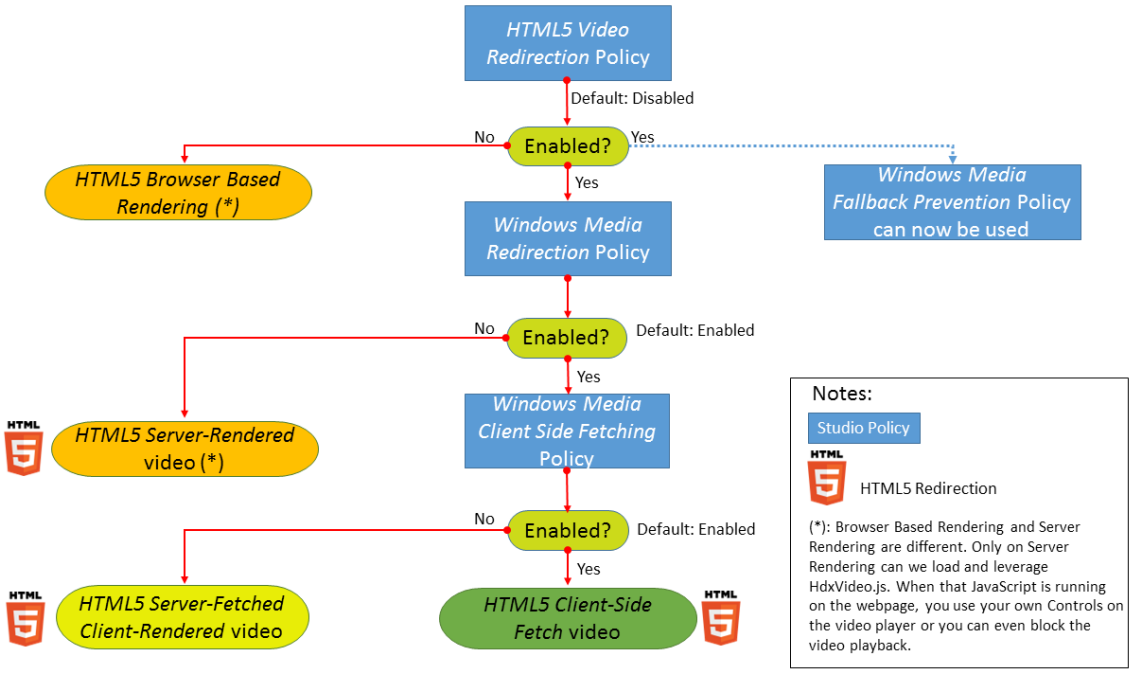
La section Multimédia contient les paramètres de stratégie permettant de gérer les données audio et vidéo HTML5 et Windows livrées en streaming dans les sessions utilisateur.

Redirection vidéo HTML5

Contrôle et optimise la manière dont les serveurs XenApp et XenDesktop mettent à disposition le contenu Web multimédia HTML5 pour les utilisateurs.

Par défaut, ce paramètre est désactivé.





Dans cette version, cette fonctionnalité est disponible pour les pages Web contrôlées uniquement. Elle requiert l'ajout de JavaScript dans les pages Web sur lesquelles le contenu multimédia HTML5 est disponible, par exemple, des vidéos sur un site de formation interne.

Pour configurer la redirection vidéo HTML5 :

1. Copiez le fichier **HdxVideo.js** depuis %Program Files%/Citrix/ICA Service/HTML5 Video Redirection sur l'installation du VDA vers votre page Web interne.
2. Insérez cette ligne dans votre page Web (si votre page Web dispose d'autres scripts, incluez **HdxVideo.js** avant ces scripts) :
   `<script src="HdxVideo.js"type="text/javascript"></script>`

Remarque : si HdxVideo.js ne figure pas dans le même emplacement que votre page Web, utilisez l'attribut **src** pour spécifier le chemin d'accès complet vers ce dernier.

Si la fonctionnalité JavaScript n'a pas été ajoutée à vos pages Web contrôlées et que l'utilisateur visionne une vidéo HTML5, XenApp et XenDesktop reviennent à la restitution côté serveur.

La ***redirection Windows Media*** doit être autorisée pour que la redirection vidéo HTML5 fonctionne. Cette stratégie est obligatoire pour Restitution client de récupération serveur et nécessaire pour Récupération côté client (qui nécessite également que *Récupération de contenu Windows Media côté client* soit autorisé).

Microsoft Edge ne prend pas en charge cette fonctionnalité.

HdxVideo.js remplace les contrôles du lecteur HTML5 du navigateur avec les siens. Pour vérifier que la stratégie de redirection vidéo HTML5 est appliquée sur un site Web donné, comparez les contrôles du lecteur à un scénario où la stratégie ***Redirection vidéo HTML5*** est interdite :

(Contrôles personnalisés Citrix lorsque la stratégie est autorisée)

(Contrôles de page Web natifs lorsque la stratégie est interdite ou non configurée)

Les commandes de vidéo suivantes sont prises en charge :

- lecture
- suspendre
- recherche
- répétition
- Audio
- plein écran

Vous pouvez afficher une page de test de redirection vidéo HTML5 sur https://www.citrix.com/virtualization/hdx/html5-redirect.html.

TLS et redirection vidéo HTML5

Vous pouvez utiliser la redirection vidéo HTML5 pour rediriger les sites Web HTTPS. Le code JavaScript injecté sur ces sites Web doit établir une connexion TLS avec le service de redirection vidéo Citrix HDX HTML5 (WebSocketService.exe) en cours d'exécution sur le VDA. Pour obtenir cette redirection et préserver l'intégrité TLS de la page Web, deux certificats personnalisés sont générés par le service de redirection vidéo Citrix HDX HTML5 dans le magasin de certificats sur le VDA.

HdxVideo.js utilise Secure WebSockets pour communiquer avec WebSocketService.exe en cours d'exécution sur le VDA. Ce processus s'exécute sur le système local et effectue le mappage de session utilisateur et d'arrêt SSL.

WebSocketService.exe écoute le port 9001 127.0.0.1.

Limiter la qualité de la vidéo

Ce paramètre s'applique uniquement à Windows Media et non à HTML5. Vous devez activer *Optimisation pour la redirection multimédia Windows Media sur un réseau étendu*.

Ce paramètre spécifie le niveau de qualité vidéo maximum autorisé pour une connexion HDX. Une fois configurée, la qualité vidéo maximale est limitée à la valeur spécifiée, en assurant que la qualité de service (QoS) multimédia est conservée dans un environnement.

Ce paramètre n'est pas configuré par défaut.

Pour limiter le niveau de qualité vidéo maximum autorisé, choisissez l'une des options suivantes :

- 1080p/8.5mbps
- 720p/4.0mbps
- 480p/720kbps
- 380p/400kbps
- 240p/200kbps

La lecture simultanée de plusieurs vidéos sur le même serveur utilise une quantité importante de ressources et peut avoir un impact sur l'extensibilité du serveur.

Conférences multimédia

Ce paramètre autorise ou empêche l'utilisation de la technologie de redirection de webcam optimisée par les applications de vidéoconférence.

Par défaut, la prise en charge de la visioconférence est activée.

Lors de l'ajout de ce paramètre à une stratégie, vérifiez que le paramètre Redirection Windows Media est présent et défini sur Autorisé.

Lorsque vous utilisez les fonctions de conférence multimédia, assurez-vous que les conditions suivantes sont remplies :

- Les pilotes fournis par le constructeur pour la webcam utilisée pour les conférences multimédia sont installés sur le client.
- Connectez la webcam à la machine cliente avant d'initier une session de visioconférence. Le serveur n'utilise qu'une seule webcam installée à la fois. Si plusieurs webcams sont installées sur la machine cliente, le serveur tente d'utiliser chacune d'elles successivement jusqu'à ce qu'il réussisse à créer une session de visioconférence.

Cette stratégie n'est pas nécessaire lors de la redirection de la webcam à l'aide de la redirection USB générique. Dans ce cas, installez les pilotes de webcam sur le VDA.

Optimisation de la redirection multimédia de Windows Media sur un réseau étendu

Ce paramètre s'applique uniquement à Windows Media et non à HTML5. Ce paramètre permet le transcodage multimédia en temps réel, ce qui permet la livraison en streaming audio et vidéo vers les appareils mobiles sur des réseaux dégradés, et l'amélioration de l'expérience utilisateur en améliorant la manière dont le contenu Windows Media est mis à disposition via un réseau étendu.

Par défaut, la mise à disposition du contenu Windows Media sur le réseau étendu est optimisée.

Lors de l'ajout de ce paramètre à une stratégie, vérifiez que le paramètre **Redirection Windows Media** est présent et défini sur **Autorisé**.

Lorsque ce paramètre est activé, le transcodage multimédia en temps réel est déployé automatiquement lorsque nécessaire pour activer la livraison en streaming de contenu multimédia, offrant une expérience utilisateur transparente, même dans des conditions réseau extrêmes.

Utiliser GPU pour l'optimisation de la redirection multimédia Windows Media sur un réseau étendu

Ce paramètre active le transcodage multimédia en temps réel qui doit être effectué dans l'unité de traitement graphique (GPU) sur le Virtual Delivery Agent (VDA). Il améliore l'extensibilité du serveur. Le transcodage sur l'unité de traitement graphique (GPU) n'est disponible que si le VDA possède une unité de traitement graphique pour l'accélération matérielle. Sinon, le transcodage retourne à l'UC.

Remarque : le transcodage GPU est pris en charge uniquement sur les GPU NVIDIA.

Par défaut, l'utilisation du GPU sur le VDA pour optimiser la mise à disposition de contenu Windows Media sur le réseau étendu est interdite.

Lorsque vous ajoutez ce paramètre à une stratégie, vérifiez que les paramètres Redirection Windows Media et Optimisation pour la redirection multimédia Windows Media sur un réseau étendu sont présent et définis sur Autorisé.

Prévention du retour à Windows Media

Ce paramètre s'applique à HTML5 et à Windows Media. Pour qu'il fonctionne avec HTML5, définissez la stratégie ***Redirection vidéo HTML*** sur **Autorisé**.

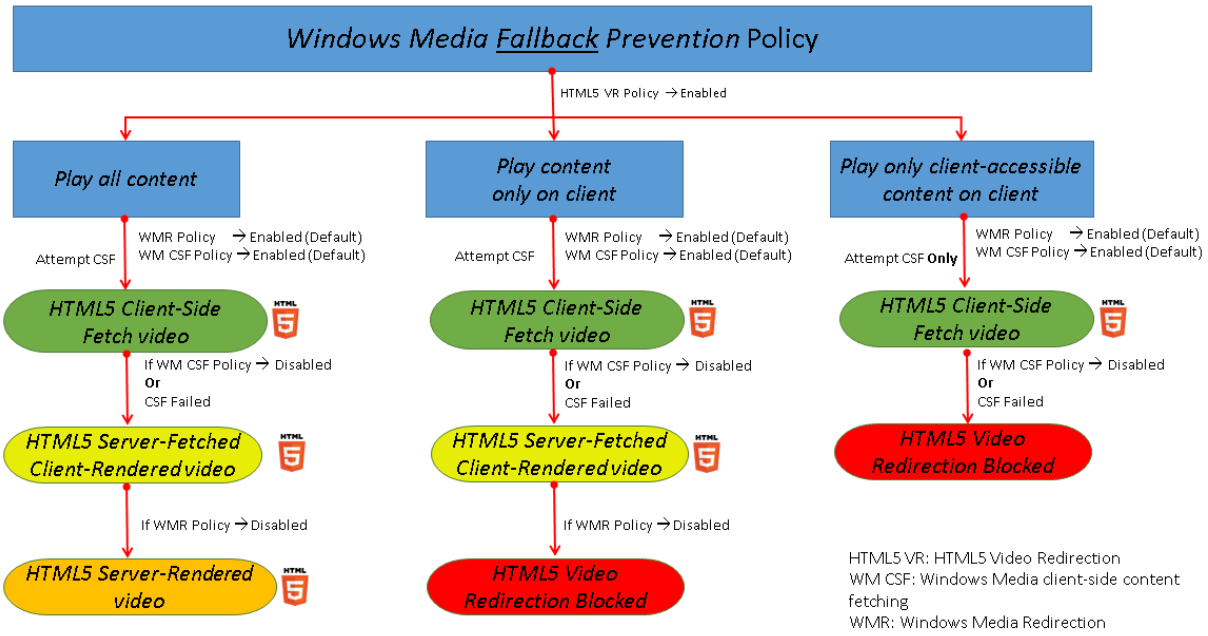
Les administrateurs peuvent utiliser le paramètre de prévention du retour à Windows Media pour spécifier la méthode qui sera utilisée pour livrer en streaming les contenus aux utilisateurs.

Ce paramètre n'est pas configuré par défaut. Lorsque le paramètre est défini sur Non configuré, le comportement est le même que **Lire tout le contenu**.

Pour contrôler ce paramètre, choisissez l'une des options suivantes :

- **Lire tout le contenu**. Tentative de récupération de contenu côté client, puis Redirection Windows Media. En cas d'échec, lit le contenu sur le serveur.
- **Lire tout le contenu uniquement sur le client**. Tentative de récupération côté client, puis Redirection Windows Media. En cas d'échec, le contenu n'est pas lu.
- **Lire uniquement le contenu accessible par le client sur le client**. Tentative de récupération côté client uniquement. En cas d'échec, le contenu n'est pas lu.

Lorsque le contenu ne fonctionne pas, le message d'erreur « Votre entreprise a bloqué la vidéo en raison d'un manque de ressources. » s'affiche (pendant 5 secondes) dans la fenêtre du lecteur.



La durée de ce message d'erreur peut être personnalisée avec la clé de registre suivante sur le VDA. Si l'entrée de registre n'existe pas, la durée par défaut est de 5 secondes.

> **Avertissement**
>
> Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Le chemin d'accès au Registre varie en fonction de l'architecture du VDA :

\HKLM\SOFTWARE\Wow6432Node\Citrix\HdxMediastream

ou

\HKLM\SOFTWARE\Citrix\HdxMediastream

Clé de registre :

Nom : VideoLoadManagementErrDuration

Type : DWORD

Plage : 1 - jusqu'à la limite DWORD (par défaut = 5)

Unité : secondes

Récupération de contenu côté client Windows Media

Ce paramètre s'applique à HTML5 et à Windows Media. Le paramètre permet aux machines utilisateur de livrer en streaming des fichiers multimédia directement à partir du fournisseur source sur Internet ou Intranet, plutôt qu'au travers du serveur hôte XenApp ou XenDesktop.

Par défaut, ce paramètre est **autorisé**. L'activation de ce paramètre améliore l'utilisation du réseau et l'extensibilité du serveur en déplaçant tout traitement sur le média du serveur hôte vers la machine utilisateur. Elle supprime également le besoin d'installer une infrastructure multimédia avancée tels que Microsoft DirectShow ou Media Foundation sur la machine utilisateur ; la machine utilisateur nécessite la possibilité de lire un fichier à partir d'une adresse URL

Lors de l'ajout de ce paramètre à une stratégie, vérifiez que le paramètre **Redirection Windows Media** est présent et défini sur **Autorisé**. Si **Redirection Windows Media** est désactivée, le streaming des fichiers multimédias vers la machine utilisateur directement à partir du fournisseur source est également désactivé.

Redirection Windows Media

Ce paramètre s'applique à HTML5 et Windows Media et permet de contrôler et d'optimiser la façon dont les serveurs livrent en streaming des données audio et vidéo auprès des utilisateurs.

Par défaut, ce paramètre est **autorisé**. Pour HTML5, ce paramètre ne prend pas effet si la stratégie ***Redirection vidéo HTML5*** est **Interdit**.

L'activation de ce paramètre améliore la qualité de l'audio et de la vidéo restitués depuis le serveur à un niveau comparable à celui obtenu avec de l'audio et de la vidéo exécutés localement sur une machine utilisateur. le serveur livre en streaming du contenu multimédia vers le client au format compressé d'origine et permet à la machine utilisateur de décompresser et de restituer le contenu multimédia.

La redirection Windows Media optimise les fichiers multimédia encodés à l'aide de codecs conformes aux normes DirectShow, DirectX Media Objects (DMO) et Media Foundation standard de Microsoft. Pour lire un fichier multimédia donné, la machine utilisateur doit disposer d'un codec compatible avec le format d'encodage du fichier multimédia.

par défaut, l'audio est désactivé sur Citrix Receiver. Pour permettre aux utilisateurs d'exécuter des applications multimédia dans les sessions ICA, activez l'audio ou accordez aux utilisateurs l'autorisation de l'activer dans leur interface Citrix Receiver.

Sélectionnez uniquement **Interdit** si la qualité obtenue avec la redirection Windows Media semble inférieure à celle obtenue à l'aide de la compression ICA de base et des réglages audio standard. Cette situation est rare mais possible dans le cas de conditions où la bande passante est faible, par exemple, si le contenu multimédia dispose d'une très faible fréquence de trames clés.

Taille de tampon de redirection Windows Media

Ce paramètre est hérité et ne s'applique pas à HTML5.

Ce paramètre spécifie une taille de tampon de 1 à 10 secondes pour l'accélération multimédia.

Par défaut, la taille du tampon est de 5 secondes.

Utilisation de la taille de tampon de redirection Windows Media

Ce paramètre est hérité et ne s'applique pas à HTML5.

Ce paramètre active ou désactive l'utilisation de la taille de tampon définie par le paramètre **Taille de tampon de redirection Windows Media**.

Par défaut, la taille du tampon spécifiée n'est pas utilisée.

Si ce paramètre est désactivé ou si le paramètre Taille de tampon de redirection Windows Media n'est pas configuré, le serveur utilise la valeur de taille de tampon par défaut (5 secondes).

Paramètres de stratégie Connexions Multi-Stream

February 28, 2019

La section Connexions Multi-Stream contient des paramètres de stratégie destinés à gérer la hiérarchisation de la qualité de service (QoS) pour les multiples connexions ICA dans une session.

Audio sur UDP

Ce paramètre autorise ou empêche l'audio via UDP sur le serveur.

Par défaut, l'audio sur UDP est autorisé sur le serveur.

Lorsqu'il est activé, ce paramètre s'ouvre un port UDP sur le serveur pour prendre en charge toutes les connexions configurées pour utiliser le transport en temps réel Audio sur UDP.

Plage de port UDP audio

Ce paramètre spécifie la plage de numéros de ports (sous la forme numéro de port le plus bas, numéro de port le plus élevé) utilisés par Virtual Delivery Agent(VDA) pour échanger des données de paquet audio avec la machine utilisateur. Le VDA tente d'utiliser chaque paire de ports UDP pour échanger des données avec la machine utilisateur, en commençant par le plus bas et en incrémentant de deux pour chaque tentative ultérieure. Chaque port gère le trafic entrant et sortant.

Par défaut, cette option est réglée sur 16500,16509.

Stratégie Multi-Port

Ce paramètre spécifie les ports TCP à utiliser pour le trafic ICA et établit la priorité réseau pour chaque port.

Par défaut, le port principal (2598) a une priorité élevée.

Lorsque vous configurez des ports, vous pouvez leur attribuer les priorités suivantes :

- Très élevée : réservée aux activités en temps réel, telles que les conférences Web (avec webcam).
- Élevée : réservée aux éléments interactifs, tels que l'écran, le clavier et la souris.
- Moyenne : réservée aux processus de masse, tels que le mappage des lecteurs clients.
- Faible : réservée aux activités d'arrière-plan, telles que l'impression.

Chaque port doit disposer d'une priorité unique. À titre d'exemple, vous ne pouvez pas attribuer une priorité Très élevé au port 1 CGP et au port 3 CGP.

Pour n'attribuer aucune priorité à un port, définissez le numéro de port sur 0. Vous ne pouvez ni supprimer le port principal, ni modifier son niveau de priorité.

Redémarrez le serveur après avoir configuré ce paramètre. Ce paramètre ne s'applique que lorsque le paramètre de stratégie Paramètre d'ordinateur Multi-Stream est activé.

Paramètre d'ordinateur Multi-Stream

Ce paramètre active ou désactive la fonctionnalité Multi-Stream sur le serveur.

Par défaut, Multi-Stream est désactivée.

Si vous utilisez Citrix NetScaler SD-WAN et que le Multi-Stream est pris en charge dans votre environnement, il n'est pas nécessaire de configurer ce paramètre. Configurez ce paramètre de stratégie lorsque vous utilisez des routeurs tiers ou des Branch Repeater d'ancienne génération pour réaliser la qualité de service désirée.

Une fois ce paramètre configuré, redémarrez le serveur pour que les modifications prennent effet.

Important : l'utilisation de ce paramètre de stratégie en conjonction avec les paramètres de stratégie de limite de bande passante Limite de bande passante de session générale peut produire des résultats inattendus. Lors de l'inclusion de ce paramètre dans une stratégie, assurez-vous que les paramètres de limite de bande passante ne sont pas inclus.

Paramètre utilisateur Multi-Stream

Ce paramètre active ou désactive la fonctionnalité Multi-Stream sur la machine utilisateur.

Par défaut, Multi-Stream est désactivé pour tous les utilisateurs.

Ce paramètre ne s'applique que sur les hôtes sur lesquels le paramètre de stratégie Paramètre d'ordinateur Multi-Stream est activé.

Important : l'utilisation de ce paramètre de stratégie en conjonction avec les paramètres de stratégie de limite de bande passante Limite de bande passante de session générale peut produire des résultats inattendus. Lors de l'inclusion de ce paramètre dans une stratégie, assurez-vous que les paramètres de limite de bande passante ne sont pas inclus.

Paramètres de stratégie de redirection de port

November 9, 2018

La section Redirection de port contient les paramètres de stratégie pour le mappage des ports LPT et COM clients.

Pour les versions du Virtual Delivery Agent **antérieures à la version 7.0**, utilisez les paramètres de stratégie suivants pour configurer la redirection de port. Pour les versions VDA de **7.0 à 7.8**, configurez ces paramètres à l'aide du registre ; consultez la section Configurer les paramètres de redirection du port COM et LPT à l'aide du Registre. Pour la version **7.9** du VDA, utilisez les paramètres de stratégie suivants.

Connecter automatiquement les ports COM du client

Ce paramètre active ou désactive la connexion automatique des ports COM sur les machines utilisateur lorsque les utilisateurs ouvrent une session sur un site.

Par défaut, les ports COM du client ne sont pas automatiquement connectés.

Connecter automatiquement les ports LPT du client

Ce paramètre active ou désactive la connexion automatique des ports LPT sur les machines utilisateur lorsque les utilisateurs ouvrent une session sur un site.

Par défaut, les ports LPT du client ne sont pas automatiquement connectés.

Redirection de port COM client

Ce paramètre autorise ou empêche l'accès aux ports COM sur la machine utilisateur.

Par défaut, la redirection des ports COM est interdite.

Les paramètres de stratégie suivants sont associés :

- Limite de bande passante pour la redirection du port COM
- Pourcentage de limite de bande passante de redirection du port COM

Redirection de port LPT client

Ce paramètre autorise ou empêche l'accès aux ports LPT sur la machine utilisateur.

Par défaut, la redirection des ports LPT est interdite.

Les ports LPT sont uniquement utilisés par les applications d'ancienne génération qui leur envoient les tâches d'impression plutôt que de les envoyer aux objets d'impression sur la machine utilisateur. La plupart des applications peuvent désormais envoyer des tâches d'impression aux objets d'imprimante. Ce paramètre de stratégie est uniquement nécessaire pour les serveurs hébergeant des applications d'ancienne génération qui impriment sur des ports LPT.

Veuillez noter que bien que la redirection des ports COM clients soit bi-directionnelle, la redirection des ports LPT est en sortie uniquement et limitée à \\client\LPT1 et \\client\LPT2 dans une session ICA.

Les paramètres de stratégie suivants sont associés :

- Limite de bande passante pour la redirection du port LPT
- Pourcentage de limite de bande passante de redirection du port LPT

Paramètres de stratégie Impression

November 9, 2018

La section Impression contient les paramètres de stratégie qui permettent de gérer l'impression cliente.

Redirection d'imprimante cliente

Ce paramètre contrôle si les imprimantes clientes sont mappées sur un serveur lorsqu'un utilisateur ouvre une session.

Par défaut, le mappage des imprimantes clientes est autorisé. Si ce paramètre est désactivé, l'imprimante PDF pour la session n'est pas créée automatiquement.

Paramètres de stratégie liés : créer automatiquement des imprimantes clientes

Imprimante par défaut

Ce paramètre spécifie la façon dont l'imprimante par défaut est définie sur la machine utilisateur dans une session.

Par défaut, l'imprimante actuelle de l'utilisateur est utilisée comme imprimante par défaut pour la session.

Pour utiliser le paramètre de profil utilisateur des services Bureau à distance ou Windows courant pour l'imprimante par défaut, sélectionnez
Ne pas ajuster l'imprimante par défaut de l'utilisateur. Si vous choisissez cette option, l'imprimante par défaut n'est pas enregistrée dans le profil et elle ne change pas selon les propriétés des autres sessions ou du client. L'imprimante par défaut d'une session sera la première imprimante créée automatiquement dans la session, à savoir :

- La première imprimante ajoutée localement au serveur Windows dans Panneau de configuration > Périphériques et imprimantes
- La première imprimante créée automatiquement, si aucune imprimante n'a été ajoutée localement sur le serveur.

Vous pouvez utiliser cette option pour présenter l'imprimante la plus proche aux utilisateurs par le biais des paramètres de profil (fonctionnalité connue sous le nom d'impression de proximité).

Attributions d'imprimantes

Ce paramètre permet d'offrir une alternative aux paramètres Imprimante par défaut et Imprimantes de session. Utilisez les paramètres Imprimante par défaut et Imprimantes de session pour configurer les comportements d'un site, d'un groupe important ou d'une unité d'organisation. Utilisez le paramètre Attributions d'imprimantes pour attribuer un groupe important d'imprimantes à plusieurs utilisateurs.

Ce paramètre spécifie la façon dont l'imprimante par défaut des machines utilisateur répertoriées est établie dans une session.

Par défaut, l'imprimante actuelle de l'utilisateur est utilisée comme imprimante par défaut pour la session.

Ce paramètre spécifie de créer automatiquement les imprimantes réseau dans une session pour chaque machine utilisateur. Par défaut, aucune imprimante n'est spécifiée.

- Lors de la définition de la valeur d'imprimante par défaut :

  Pour utiliser l'imprimante par défaut courante pour la machine utilisateur, sélectionnez Ne pas ajuster.

Pour utiliser le paramètre de profil utilisateur des services Bureau à distance ou Windows courant pour l'imprimante par défaut, sélectionnez Ne pas régler. Si vous choisissez cette option, l'imprimante par défaut n'est pas enregistrée dans le profil et elle ne change pas selon les propriétés des autres sessions ou du client. L'imprimante par défaut d'une session sera la première imprimante créée automatiquement dans la session, à savoir :

  - La première imprimante ajoutée localement au serveur Windows dans Panneau de configuration > Périphériques et imprimantes
  - La première imprimante créée automatiquement, si aucune imprimante n'a été ajoutée localement sur le serveur.

- Lors de la définition de la valeur des imprimantes de session : pour ajouter des imprimantes, entrez le chemin UNC de l'imprimante que vous souhaitez créer automatiquement. Après avoir ajouté l'imprimante, vous pouvez appliquer les paramètres personnalisés pour la session courante lors de chaque ouverture de session.

Préférence de journalisation des événements de création automatique des imprimantes

Ce paramètre spécifie les événements journalisés pendant le processus de création automatique de l'imprimante. Vous pouvez choisir de ne journaliser ni les erreurs ni les avertissements, uniquement les erreurs, ou les erreurs et les avertissements.

Par défaut, les erreurs et les avertissements sont journalisés.

Un exemple d'avertissement est un événement au cours duquel le pilote natif d'une imprimante n'a pas pu être installé, c'est le pilote d'impression universelle qui a été installé à la place. Pour utiliser le pilote d'impression universelle dans ce scénario, configurez le paramètre Utilisation du pilote d'impression universelle sur l'option Utiliser l'impression universelle uniquement ou Utiliser l'impression universelle uniquement si le pilote requis n'est pas disponible.

Imprimantes de session

Ce paramètre spécifie de créer automatiquement les imprimantes réseau dans une session.

Par défaut, aucune imprimante n'est spécifiée.

Pour ajouter des imprimantes, entrez le chemin UNC de l'imprimante que vous souhaitez créer automatiquement. Après avoir ajouté l'imprimante, vous pouvez appliquer les paramètres personnalisés pour la session courante lors de chaque ouverture de session.

Attendre la création d'imprimantes (bureau de serveur)

Ce paramètre autorise ou empêche l'application d'un délai lors de la connexion à une session de sorte à autoriser la création automatique des imprimantes de bureau de serveur.

Par défaut, aucun délai de connexion n'intervient.

Paramètres de stratégie d'imprimantes clientes

November 9, 2018

La section Imprimantes clientes contient les paramètres de stratégie des imprimantes clientes, notamment les paramètres relatifs à la création automatique d'imprimantes clientes, à la rétention des propriétés d'imprimante et à la connexion aux serveurs d'impression.

Créer automatiquement les imprimantes clientes

Ce paramètre spécifie les imprimantes clientes créées automatiquement. Il remplace les paramètres par défaut de création automatique d'imprimantes clientes.

Par défaut, toutes les imprimantes clientes sont créées automatiquement.

Ce paramètre n'entre en vigueur que si le paramètre Redirection d'imprimante cliente est présent et a la valeur Autorisé.

Lors de l'ajout de ce paramètre à une stratégie, sélectionnez une option :

- Créer automatiquement toutes les imprimantes clientes crée automatiquement toutes les imprimantes clientes sur une machine utilisateur.
- Ne créer automatiquement que l'imprimante par défaut du client ne crée automatiquement que l'imprimante sélectionnée comme imprimante par défaut sur la machine utilisateur.
- Ne créer automatiquement que les imprimantes clientes locales (non réseau) ne crée automatiquement que les imprimantes directement connectées à la machine utilisateur via un port LPT, COM, USB, TCP/IP ou un autre port local.
- Ne pas créer les imprimantes clientes automatiquement désactive la création automatique pour toutes les imprimantes clientes lorsque les utilisateurs ouvrent une session. De ce fait, les paramètres des services Bureau à distance (RDS) liés à la création automatique d'imprimantes clientes remplacent ce paramètre dans les stratégies de priorité inférieure.

Créer automatiquement l'imprimante universelle générique

Remarque : les corrections permettant de résoudre les problèmes relatifs à ce paramètre de stratégie sont disponibles dans les articles CTX141565 et CTX141566 du centre de connaissances.

Ce paramètre active ou désactive la création automatique de l'objet d'impression générique de l'imprimante universelle Citrix pour les sessions lorsqu'une machine utilisateur compatible avec l'impression universelle est en cours d'utilisation.

Par défaut, l'objet Imprimante universelle générique n'est pas créé automatiquement.

Les paramètres de stratégie suivants sont associés :

- Utilisation du pilote d'impression universelle
- Préférence de pilote universel

Noms des imprimantes clientes

Ce paramètre permet de sélectionner la convention d'appellation pour les imprimantes clientes créées automatiquement.

Par défaut, les noms d'imprimante standard sont utilisés.

Sélectionnez Noms d'imprimantes standards pour utiliser des noms d'imprimante tels que « HPLaserJet 4 sur nomClient dans la session 3 ».

Sélectionnez
Noms d'imprimantes d'ancienne génération pour utiliser les noms d'imprimantes clientes d'ancienne génération et préserver la rétrocompatibilité pour les utilisateurs et les groupes utilisant MetaFrame Presentation Server 3.0 ou une version antérieure. Un exemple de nom d'imprimante d'ancienne génération est « Client/nomclient#/HPLaserJet 4 ». Cette option est moins sécurisée.

Remarque : cette option est fournie uniquement à des fins de compatibilité à effet rétroactif avec les anciennes versions de XenApp et XenDesktop.

Diriger les connexions vers les serveurs d'impression

Ce paramètre permet d'activer ou de désactiver les connexions directes à partir du bureau virtuel ou du serveur hébergeant les applications vers un serveur d'impression pour les imprimantes clientes hébergées sur un partage réseau accessible.

Par défaut, les connexions directes sont activées.

Activez les connexions directes si le serveur d'impression réseau n'est pas sur un réseau étendu à partir du bureau virtuel ou du serveur hébergeant les applications. Les communications directes donnent lieu à des impressions plus rapides lorsque le serveur d'impression réseau et le bureau virtuel ou le serveur hébergeant les applications sont sur le même réseau local.

Vous pouvez désactiver les connexions directes si le réseau se trouve à l'autre extrémité d'un réseau étendu, s'il est soumis à une latence élevée ou s'il dispose d'une bande passante réduite. Les tâches

d'impression sont acheminées via la machine utilisateur, puis redirigées vers le serveur d'impression réseau. Les données envoyées à la machine utilisateur sont compressées. Les transmissions de données sur le réseau étendu nécessitent donc moins de bande passante.

Si deux imprimantes réseau ont le même nom, l'imprimante située sur le même réseau que la machine utilisateur est utilisée.

Mappage et compatibilité du pilote d'imprimante

Ce paramètre spécifie les règles de remplacement de pilotes pour les imprimantes créées automatiquement.

Ce paramètre est configuré pour exclure Microsoft OneNote et XPS Document Writer dans la liste d'imprimantes clientes créées automatiquement.

Lorsque vous définissez ces règles de remplacement, vous pouvez autoriser ou empêcher la création d'imprimantes avec le pilote spécifié. En outre, vous pouvez autoriser les imprimantes créées à utiliser uniquement les pilotes d'imprimantes universels. Le remplacement de pilote annule (ou mappe) le nom de pilote d'imprimante fourni par le client, en le remplaçant par un pilote équivalent sur le serveur. Cela permet à des applications exécutées sur le serveur d'accéder à des imprimantes clientes qui ont les mêmes pilotes que le serveur mais sous des noms de pilote différents.

Vous pouvez ajouter un mappage de pilote, modifier un mappage existant, remplacer les paramètres personnalisés d'un mappage, supprimer un mappage ou modifier l'ordre des entrées de pilote dans la liste. Lors de l'ajout d'un mappage, entrez le nom de pilote de l'imprimante cliente, puis sélectionnez le pilote serveur que vous souhaitez remplacer.

Rétention des propriétés d'imprimante

Ce paramètre indique si les propriétés d'imprimante sont ou non stockées et précise l'emplacement de stockage.

Par défaut, le système détermine si les propriétés d'imprimante doivent être stockées sur la machine utilisateur, le cas échéant, ou dans le profil utilisateur.

Lors de l'ajout de ce paramètre à une stratégie, sélectionnez une option :

- Enregistrées uniquement sur la machine cliente est une option destinée aux machines utilisateur qui possèdent un profil obligatoire ou itinérant qui n'est pas enregistré. Ne choisissez cette option que si tous les serveurs de votre batterie exécutent XenApp 5 et version ultérieure et si vos utilisateurs disposent de Citrix Online Plugin versions 9 à 12.x ou Citrix Receiver 3.x.
- Conservées uniquement dans le profil d'utilisateur est une option destinée aux machines utilisateur soumises à des contraintes de bande passante (cette option permet de réduire le trafic réseau) et de temps d'ouverture de session ou si des utilisateurs utilisent des plug-ins

d'ancienne génération. Cette option stocke les propriétés d'imprimante dans le profil utilisateur sur le serveur et empêche tout échange des propriétés avec la machine cliente. Cette option est disponible avec MetaFrame Presentation Server 3.0 (ou une version antérieure) et avec le Client MetaFrame Presentation Server 8.x (ou une version antérieure). Notez que cela ne s'applique qu'en cas d'utilisation d'un profil itinérant des services Bureau à distance (RDS).

- Le paramètre Contenu dans le profil uniquement si non enregistré sur le client permet au système de déterminer l'emplacement de stockage des propriétés d'imprimante. Les propriétés d'imprimante sont stockées sur la machine cliente, le cas échéant, ou dans le profil utilisateur. Bien que cette option soit la plus souple, elle peut aussi entraîner un ralentissement à l'ouverture de session et utiliser davantage de bande passante pour les vérifications du système.
- Ne pas conserver les propriétés des imprimantes empêche le stockage des propriétés de l'imprimante.

Imprimantes clientes conservées et restaurées

Ce paramètre permet d'activer ou de désactiver la rétention et la recréation d'imprimantes sur la machine utilisateur. Par défaut, les imprimantes clientes sont conservées automatiquement et restaurées automatiquement.

Les imprimantes conservées sont des imprimantes créées par l'utilisateur qui sont recréées, ou rappelées, au début de la session suivante. Lorsque XenApp recrée une imprimante conservée, il tient compte de tous les paramètres de stratégie, à l'exception du paramètre Créer automatiquement des imprimantes clientes.

Les imprimantes restaurées sont des imprimantes entièrement personnalisées par un administrateur, dans un état enregistré qui est connecté en permanence au port d'un client.

Paramètres de stratégie Pilotes

November 9, 2018

La section Pilotes contient des paramètres de stratégie relatifs aux pilotes d'imprimante.

Installation automatique de pilotes d'imprimante fournis par défaut

Ce paramètre active ou désactive l'installation automatique des pilotes d'imprimante fournis avec le jeu de pilotes Windows ou provenant de packs de pilotes sur l'hôte à l'aide de pnputil.exe /a.

Par défaut, ces pilotes sont installés selon vos besoins.

Préférence de pilote universel

Ce paramètre spécifie l'ordre dans lequel les pilotes d'imprimante universels sont utilisés, en commençant par la première entrée de la liste.

Par défaut, l'ordre de préférence est le suivant :

- EMF
- XPS
- PCL5c
- PCL4
- PS

Vous pouvez ajouter, modifier ou supprimer des pilotes et changer leur ordre dans la liste.

Utilisation du pilote d'impression universelle

Ce paramètre spécifie à quel moment utiliser l'impression universelle.

Par défaut, l'impression universelle n'est utilisée que si le pilote demandé n'est pas disponible.

L'impression universelle utilise des pilotes d'imprimante génériques au lieu de pilotes spécifiques au modèle standard, simplifiant potentiellement la charge de gestion des pilotes sur les ordinateurs hôtes. La disponibilité des pilotes d'impression universels dépend des capacités de la machine utilisateur, de l'hôte et du logiciel du serveur d'impression. Dans certaines configurations, il se peut que l'impression universelle ne soit pas disponible.

Lors de l'ajout de ce paramètre à une stratégie, sélectionnez une option :

- Utiliser uniquement les pilotes spécifiques au modèle de l'imprimante indique que l'imprimante cliente utilise uniquement les pilotes spécifiques au modèle standard qui sont créés automatiquement lors de l'ouverture de session. Si le pilote requis n'est pas disponible, l'imprimante cliente ne peut pas être créée automatiquement.
- Utiliser l'impression universelle uniquement spécifie qu'aucun pilote spécifique au modèle standard n'est utilisé. Seuls les pilotes d'impression universelle sont utilisés pour créer des imprimantes.
- Utiliser l'impression universelle uniquement si le pilote requis n'est pas disponible utilise les pilotes spécifiques au modèle standard pour la création des imprimantes s'ils sont disponibles. Si le pilote n'est pas disponible sur le serveur, l'imprimante cliente est automatiquement créée à l'aide du pilote d'imprimante universelle approprié.
- Utiliser les pilotes spécifiques au modèle d'imprimante uniquement si impression universelle non dispo utilise le pilote d'impression universelle s'il est disponible. Si le pilote n'est pas disponible sur le serveur, l'imprimante cliente est automatiquement créée à l'aide du pilote spécifique au modèle standard approprié.

Paramètres de stratégie Serveur d'impression universelle

November 9, 2018

La section Serveur d'impression universelle contient les paramètres de stratégie permettant de gérer le Serveur d'impression universelle.

Activer le serveur d'impression universelle

Ce paramètre active ou désactive la fonctionnalité Serveur d'impression universelle sur le bureau virtuel ou le serveur hébergeant les applications. Appliquez ce paramètre de stratégie aux unités d'organisation contenant le bureau virtuel ou le serveur hébergeant les applications.

Par défaut, le Serveur d'impression universelle est désactivé.

Lorsque vous ajoutez ce paramètre à une stratégie, sélectionnez l'une des options suivantes :

- **Activé avec retour à l'impression distante native de Windows**. Le service des connexions d'imprimante réseau est effectué par le serveur d'impression universelle, si possible. Si le serveur d'impression universelle n'est pas disponible, le fournisseur d'impression Windows est utilisé. Le fournisseur d'impression Windows continue de gérer toutes les imprimantes créées précédemment avec le fournisseur d'impression Windows.
- **Activé avec aucun retour à l'impression distante native de Windows**. Le service des connexions d'imprimante réseau est effectué par le serveur d'impression universelle, exclusivement. Si le serveur d'impression universelle n'est pas disponible, la connexion de l'imprimante réseau échoue. Ce paramètre désactive de manière effective l'impression réseau au travers du fournisseur d'impression Windows. Les imprimantes créées précédemment avec le fournisseur d'impression Windows ne sont pas créées tant qu'une stratégie contenant ce paramètre est active.
- **Désactivé**. La fonctionnalité Serveur d'impression universelle est désactivée. Aucune tentative de connexion avec le Serveur d'impression universelle n'est effectuée lors de la connexion à une imprimante réseau avec un nom UNC. Les connexions aux imprimantes distantes continuent d'utiliser l'outil d'impression à distance Windows natif.

Port (CGP) du flux de données d'impression du serveur d'impression universelle

Ce paramètre spécifie le numéro de port TCP utilisé par l'écouteur CGP (Common Gateway Protocol) du flux de données d'impression Serveur d'impression universelle. Appliquez ce paramètre de stratégie uniquement aux unités d'organisation contenant le serveur d'impression.

Le numéro port est défini par défaut sur 7229.

Les numéros de port valides doivent se trouver dans une plage de 1 à 65535.

Limite de bande passante d'entrée du flux d'impression du serveur d'impression universelle (kpbs)

Ce paramètre spécifie la limite supérieure (en kilobits par seconde) pour le taux de transfert des données d'impression mises à disposition depuis chaque tâche d'impression vers le Serveur d'impression universelle à l'aide de CGP. Appliquez ce paramètre de stratégie aux unités d'organisation contenant le bureau virtuel ou le serveur hébergeant les applications.

Par défaut, la valeur est 0, qui ne spécifie aucune limite supérieure.

Port (HTTP/SOAP) du service Web du serveur d'impression universelle

Ce paramètre spécifie le numéro de port TCP utilisé par l'écouteur du service Web Serveur d'impression universelle pour les requêtes (HTTP/SOAP). Le serveur d'impression universelle est un composant facultatif qui permet l'utilisation des pilotes d'impression universelle Citrix dans les scénarios d'impression réseau. Lorsque le serveur d'impression universelle est utilisé, les commandes d'impression sont envoyées depuis les hôtes XenApp et XenDesktop vers le serveur d'impression universelle via SOAP sur HTTP. Ce paramètre modifie le port TCP par défaut sur lequel le serveur d'impression universelle écoute les requêtes HTTP/SOAP entrantes.

Vous devez configurer le port HTTP du serveur d'impression et de l'hôte de façon identique. Si les ports ne sont pas configurés à l'identique, le logiciel de l'hôte ne se connectera pas au serveur d'impression universelle. Ce paramètre modifie le VDA sur XenApp et XenDesktop. Par ailleurs, vous devez modifier le port par défaut sur le serveur d'impression universelle.

Le numéro port est défini par défaut sur 8080.

Les numéros de port valides doivent se trouver dans une plage de 0 à 65535.

Serveurs d'impression universelle d'équilibrage de la charge

Ce paramètre dresse la liste des serveurs d'impression universelle à utiliser pour répartir la charge des connexions aux imprimantes établies lors du lancement de la session, après l'évaluation d'autres paramètres de stratégie d'impression Citrix. Pour optimiser la durée de création des imprimantes, Citrix recommande que les mêmes imprimantes partagées soient installées sur tous les serveurs d'impression. Il n'existe aucune limite au nombre de serveurs d'impression qui peuvent être ajoutés pour l'équilibrage de charge.

Ce paramètre s'applique également à la détection de basculement de serveur d'impression et à la récupération de connexion d'imprimante. Les serveurs d'impression contrôlent la disponibilité périodiquement. Si un serveur défaillant est détecté, ce serveur est supprimé du schéma d'équilibrage de charge, et les connexions d'imprimante sur ce serveur sont redistribuées sur d'autres serveurs

d'impression disponibles. Après reprise du serveur d'impression défaillant, il reprend sa place dans le schéma d'équilibrage de charge.

Cliquez sur **Valider les serveurs** pour vérifier que chaque serveur est un serveur d'impression et que tous les serveurs possèdent un ensemble identique d'imprimantes partagées. Cette opération peut prendre un certain temps.

Seuil au-delà duquel les serveurs d'impression universelle sont hors service

Ce paramètre indique la durée pendant laquelle l'équilibrage de charge attend le rétablissement de la connexion à un serveur d'impression universelle avant de considérer que le serveur est hors connexion et de répartir sa charge sur d'autres serveurs d'impression disponibles.

Par défaut, la valeur de seuil est de 180 (secondes).

Paramètres de stratégie Impression universelle

January 23, 2019

La section Impression universelle contient des paramètres de stratégie permettant de gérer l'impression universelle.

Mode de traitement de l'impression universelle EMF

Ce paramètre contrôle la méthode de traitement du fichier de spoule EMF sur la machine utilisateur Windows.

Par défaut, les enregistrements EMF sont spoulés directement sur l'imprimante.

Lors de l'ajout de ce paramètre à une stratégie, sélectionnez une option :

- Traiter à nouveau les EMF pour l'imprimante oblige le fichier de spoule EMF à être traité à nouveau et envoyé au travers du sous-système GDI sur la machine utilisateur. Vous pouvez utiliser ce paramètre pour les pilotes qui requièrent un nouveau traitement EMF mais qui peuvent ne pas être sélectionnés automatiquement dans une session.
- Spouler directement vers l'imprimante, lorsque utilisé avec le pilote d'impression universelle Citrix, assure que les données EMF sont spoulées et mises à disposition vers la machine utilisateur pour traitement. Généralement, ces fichiers de spoule EMF sont directement injectés dans la file d'attente du spoule du client. Pour les imprimantes et les pilotes qui sont compatibles avec le format EMF, ceci représente la méthode d'impression la plus rapide.

Limite de compression d'image de l'impression universelle

Ce paramètre définit la qualité maximale et le niveau de compression minimal disponibles pour les images imprimées avec le pilote d'impression universelle Citrix.

Par défaut, la limite de compression d'image est définie sur Meilleure qualité (compression sans perte).

Si Aucune compression est sélectionnée, la compression est désactivée uniquement pour l'impression EMF.

Lors de l'ajout de ce paramètre à une stratégie, sélectionnez une option :

- Aucune compression
- Meilleure qualité (compression sans perte)
- Qualité élevée
- Qualité standard
- Qualité réduite (compression maximale)

Lorsque vous ajoutez ce paramètre à une stratégie qui comprend le paramètre Valeurs par défaut de l'optimisation de l'impression universelle, assurez-vous des éléments suivants :

- Si le niveau de compression du paramètre Limite de compression d'image de l'impression universelle est inférieur au niveau défini dans le paramètre Valeurs par défaut de l'optimisation de l'impression universelle, les images sont compressées à l'aide du niveau défini dans le paramètre Limite de compression d'image de l'impression universelle.
- Si la compression est désactivée, les options Qualité d'image souhaitée et Activer la compression lourde du paramètre Valeurs par défaut de l'optimisation de l'impression universelle n'ont aucun effet sur la stratégie.

Valeur par défaut d'optimisation de l'impression universelle

Ce paramètre spécifie les valeurs par défaut de l'optimisation de l'impression lorsque le pilote d'impression universelle est créé pour une session.

- Qualité d'image souhaitée spécifie la limite de compression d'image par défaut appliquée à l'impression universelle. Par défaut, Qualité standard est activée, signifiant que les utilisateurs peuvent uniquement imprimer des images à l'aide des compressions standard ou de qualité réduite.
- Activer la compression lourde active ou désactive la réduction de la bande passante au-delà du niveau de compression défini par l'option Qualité d'image souhaitée, sans perte de qualité d'image. Par défaut, la compression intensive est désactivée.
- Les paramètres Cache d'image et de police spécifient si oui ou non vous pouvez cacher des images et des polices qui s'affichent plusieurs fois dans le flux d'impression, assurant ainsi que

chaque image ou police est envoyée à l'imprimante une seule fois. Par défaut, les images incorporées et les polices sont mises en cache. Notez que ces paramètres s'appliquent uniquement si la machine utilisateur prend ce comportement en charge.
- Autoriser les non-administrateurs à modifier ces paramètres spécifie si les utilisateurs peuvent ou non modifier les paramètres d'optimisation d'impression dans une session. Par défaut, les utilisateurs ne sont pas autorisés à modifier les paramètres par défaut d'optimisation de l'impression.

Remarque : toutes ces options sont prises en charge pour l'impression EMF. Pour l'impression XPS, seule l'option Qualité d'image souhaitée est prise en charge.

Lorsque vous ajoutez ce paramètre à une stratégie qui comprend le paramètre Limite de compression d'image de l'impression universelle, assurez-vous des éléments suivants :

- Si le niveau de compression du paramètre Limite de compression d'image de l'impression universelle est inférieur au niveau défini dans le paramètre Valeurs par défaut de l'optimisation de l'impression universelle, les images sont compressées à l'aide du niveau défini dans le paramètre Limite de compression d'image de l'impression universelle.
- Si la compression est désactivée, les options Qualité d'image souhaitée et Activer la compression lourde du paramètre Valeurs par défaut de l'optimisation de l'impression universelle n'ont aucun effet sur la stratégie.

Préférence d'aperçu d'impression universelle

Ce paramètre spécifie si la fonction d'aperçu d'impression doit ou non être utilisée pour les imprimantes créées automatiquement ou les imprimantes universelles génériques.

Par défaut, l'aperçu d'impression n'est pas utilisé pour les imprimantes créées automatiquement ou les imprimantes universelles génériques.

Lors de l'ajout de ce paramètre à une stratégie, sélectionnez une option :

- Ne pas utiliser l'aperçu pour les imprimantes créées automatiquement ou universelles génériques
- Utiliser l'aperçu d'impression pour les imprimantes créées automatiquement uniquement
- Utiliser l'aperçu d'impression pour les imprimantes universelles génériques uniquement
- Utiliser l'aperçu pour les imprimantes créées automatiquement et universelles génériques

Limite de qualité d'image de l'impression universelle

Ce paramètre spécifie le nombre maximal de points par pouce (ppp) disponible pour l'impression dans la session.

Par défaut, l'option Aucune limite est activée, signifiant que les utilisateurs peuvent sélectionner la qualité d'impression maximale autorisée par l'imprimante à laquelle ils se connectent.

Si ce paramètre est configuré, il limite la qualité d'impression maximale disponible auprès des utilisateurs en termes de résolution. À la fois la qualité d'impression elle-même et les capacités de qualité d'impression de l'imprimante à laquelle l'utilisateur se connecte sont restreintes au paramètre configuré. Par exemple, si la configuration est définie sur Moyenne résolution (600 PPP), les utilisateurs sont restreints à une impression d'une qualité maximale de 600 PPP et le paramètre Qualité d'impression de l'onglet Avancé de la boîte de dialogue Imprimante universelle affiche des paramètres de résolution jusqu'à Qualité moyenne (600 PPP).

Lors de l'ajout de ce paramètre à une stratégie, sélectionnez une option :

- Brouillon (150 PPP)
- Basse résolution (300 PPP)
- Moyenne résolution (600 PPP)
- Haute résolution (1200 PPP)
- Sans limite

Paramètres de stratégie Sécurité

February 28, 2019

La section Sécurité contient des paramètres de stratégie permettant de configurer le cryptage de session et des données d'ouverture de session.

Niveau de cryptage minimum SecureICA

Ce paramètre spécifie le niveau minimal auquel crypter les données de session envoyées entre le serveur et une machine utilisateur.

Important : pour Virtual Delivery Agent 7.x, ce paramètre de stratégie peut être utilisé uniquement pour activer le cryptage des données d'ouverture de session à l'aide du cryptage RC5 128 bits. Cette option est fournie uniquement à des fins de compatibilité à effet rétroactif avec les versions d'ancienne génération de XenApp et XenDesktop.

Pour VDA 7.x, le cryptage des données de session est défini à l'aide des paramètres de base du groupe de mise à disposition du VDA. Si l'option Activer Secure ICA est sélectionnée pour le groupe de mise à disposition, les données de session sont cryptées à l'aide du cryptage RC5 (128 bits). Si l'option Activer Secure ICA n'est pas sélectionnée pour le groupe de mise à disposition, les données de session sont cryptées à l'aide du cryptage de base.

Lors de l'ajout de ce paramètre à une stratégie, sélectionnez une option :

- De base crypte la connexion à l'aide d'un algorithme non RC5. Cet algorithme protège le flux de données d'une lecture directe, mais n'empêche pas le décryptage. Par défaut, le serveur utilise un cryptage de base pour le trafic client vers serveur.
- 128 bits - ouverture de session uniquement (RC5) crypte les données d'ouverture de session à l'aide du cryptage RC5 128 bits et la connexion cliente à l'aide du cryptage de base.
- 40 bits (RC5) crypte la connexion cliente à l'aide du cryptage RC5 40 bits.
- 56 bits (RC5) crypte la connexion cliente à l'aide du cryptage RC5 56 bits.
- 128 bits (RC5) crypte la connexion cliente à l'aide du cryptage RC5 128 bits.

Les paramètres que vous spécifiez pour le cryptage client-serveur peuvent interagir avec tout autre paramètre de cryptage de votre environnement et de votre système d'exploitation Windows. Si un niveau de cryptage supérieur est défini sur un serveur ou sur une machine cliente, les paramètres que vous spécifiez pour des ressources publiées peuvent être remplacés.

Vous pouvez augmenter les niveaux de cryptage afin de mieux sécuriser les communications et l'intégrité des messages pour certains utilisateurs. Si une stratégie requiert un niveau de cryptage plus élevé, les Citrix Receivers utilisant un niveau de cryptage inférieur se voient refuser la connexion.

SecureICA n'effectue pas d'authentification ni ne vérifie l'intégrité des données. Pour assurer un cryptage de bout en bout pour votre site, utilisez SecureICA avec le cryptage TLS.

SecureICA n'utilise pas d'algorithme conforme à la norme FIPS. Si cela pose un problème, configurez le serveur et Citrix Receiver pour éviter d'utiliser SecureICA.

SecureICA utilise le chiffrement par blocs RC5 décrit dans RFC 2040 pour assurer la confidentialité. La taille des blocs est 64 bits (un multiple d'unités de mots de 32 bits). La longueur de clé est 128 bits. Le nombre de boucles est 12.

Paramètres de stratégie Limites de serveur

February 28, 2019

La section Limites de serveur contient le paramètre de stratégie permettant de contrôler les connexions inactives.

Intervalle d'horloge inactive du serveur

Ce paramètre détermine la durée (en millisecondes) pendant laquelle une session utilisateur non interrompue pourra être maintenue si aucune entrée utilisateur n'est effectuée.

Par défaut, les connexions inactives ne sont pas déconnectées (Intervalle d'horloge inactive du serveur = 0). Citrix vous recommande de définir cette valeur sur un minimum de 60 000 millisecondes (60 secondes).

> **Remarque**
>
> Lorsque ce paramètre de stratégie est utilisé, une boîte de dialogue indiquant que le minuteur d'inactivité a expiré peut s'afficher lorsque la session a été inactive pendant la durée spécifiée. Il s'agit d'une boîte de dialogue Microsoft qui n'est pas contrôlée par les paramètres de stratégie Citrix. Pour plus d'informations, voir CTX118618.

Paramètres de stratégie des limites de session

January 23, 2019

La section Limites de session contient des paramètres de stratégie qui permettent de contrôler la durée pendant laquelle les sessions restent connectées avant que leur fermeture soit imposée.

> **Important :**
>
> Ces paramètres ne s'appliquent pas aux VDA de serveur Windows.

Horloge de session déconnectée

Ce paramètre active ou désactive une horloge permettant de déterminer la durée pendant laquelle un bureau déconnecté et verrouillé reste verrouillé avant fermeture de la session. Si cette horloge est activée, la session déconnectée est fermée à l'expiration de l'horloge.

Par défaut, les sessions déconnectées ne sont pas fermées.

Intervalle d'horloge de session déconnectée

Ce paramètre détermine la durée, en minutes, pendant laquelle un bureau déconnecté et verrouillé peut rester verrouillé avant que la session ne se ferme.

Par défaut, ce délai est de 1440 minutes (24 heures).

Horloge de connexion de session

Ce paramètre active ou désactive une horloge permettant de déterminer la durée maximale d'une connexion ininterrompue entre une machine utilisateur et un bureau. Si cette horloge est activée, la session est déconnectée ou fermée à l'expiration de l'horloge. Le paramètre Microsoft **Mettre fin à la session quand les délais d'expiration ont été atteints** détermine l'état suivant de la session.

Par défaut, cette horloge est désactivée.

Intervalle d'horloge de connexion de session

Ce paramètre spécifie le nombre maximal de minutes d'une connexion ininterrompue entre une machine utilisateur et un bureau.

Par défaut, la durée maximale est de 1440 minutes (24 heures).

Horloge inactive de session

Ce paramètre active ou désactive une horloge qui détermine la durée pendant laquelle une connexion ininterrompue entre une machine utilisateur et un bureau est maintenue si aucune entrée utilisateur n'est effectuée. Lorsque cette horloge expire, la session est placée dans l'état déconnecté et le paramètre **Horloge de session déconnectée** s'applique. Si le paramètre **Horloge de session déconnectée** est désactivé, la session est fermée.

Par défaut, cette horloge est activée.

Intervalle d'horloge inactive de session

Ce paramètre détermine la durée en minutes pour laquelle une connexion non interrompue d'une machine utilisateur vers un bureau peut être maintenue si aucune entrée utilisateur n'est effectuée.

Par défaut, les connexions inactives sont maintenues pendant 1440 minutes (24 heures).

Paramètres de stratégie Fiabilité de session

February 28, 2019

La section Fiabilité de session contient les paramètres de stratégie permettant de gérer les connexions de fiabilité de session.

Connexions de fiabilité de session

Ce paramètre autorise ou empêche les sessions de rester ouvertes en cas de perte de connexion réseau. La fiabilité de session, associée à la reconnexion automatique des clients, permet aux utilisateurs de se reconnecter automatiquement à leurs sessions Citrix Receiver suite au rétablissement de la connexion au réseau. Par défaut, la fiabilité de session est autorisée.

Sur Citrix Receiver pour Windows 4.7 et versions ultérieures, les paramètres de Studio sont appliqués sur le client. L'objet de stratégie de groupe Citrix Receiver sur les clients est remplacé par la stratégie Studio. Les mises à jour vers ces stratégies dans Studio synchronisent la fiabilité de session du serveur et du client.

> **Remarque :**
>
> - Citrix Receiver pour Windows 4.7 et versions ultérieures, et applications Citrix Workspace pour Windows – Définissez la stratégie dans Studio.
> - Citrix Receiver pour Windows, versions antérieures à 4.7 – Définissez les stratégies dans Studio et le modèle d'objet de stratégie de groupe Citrix Receiver sur le client pour un comportement cohérent.

La fiabilité de session maintient les sessions actives sur l'écran de l'utilisateur lorsque la connectivité au réseau est interrompue. L'utilisateur peut donc visualiser l'application jusqu'à ce que la connexion au réseau reprenne.

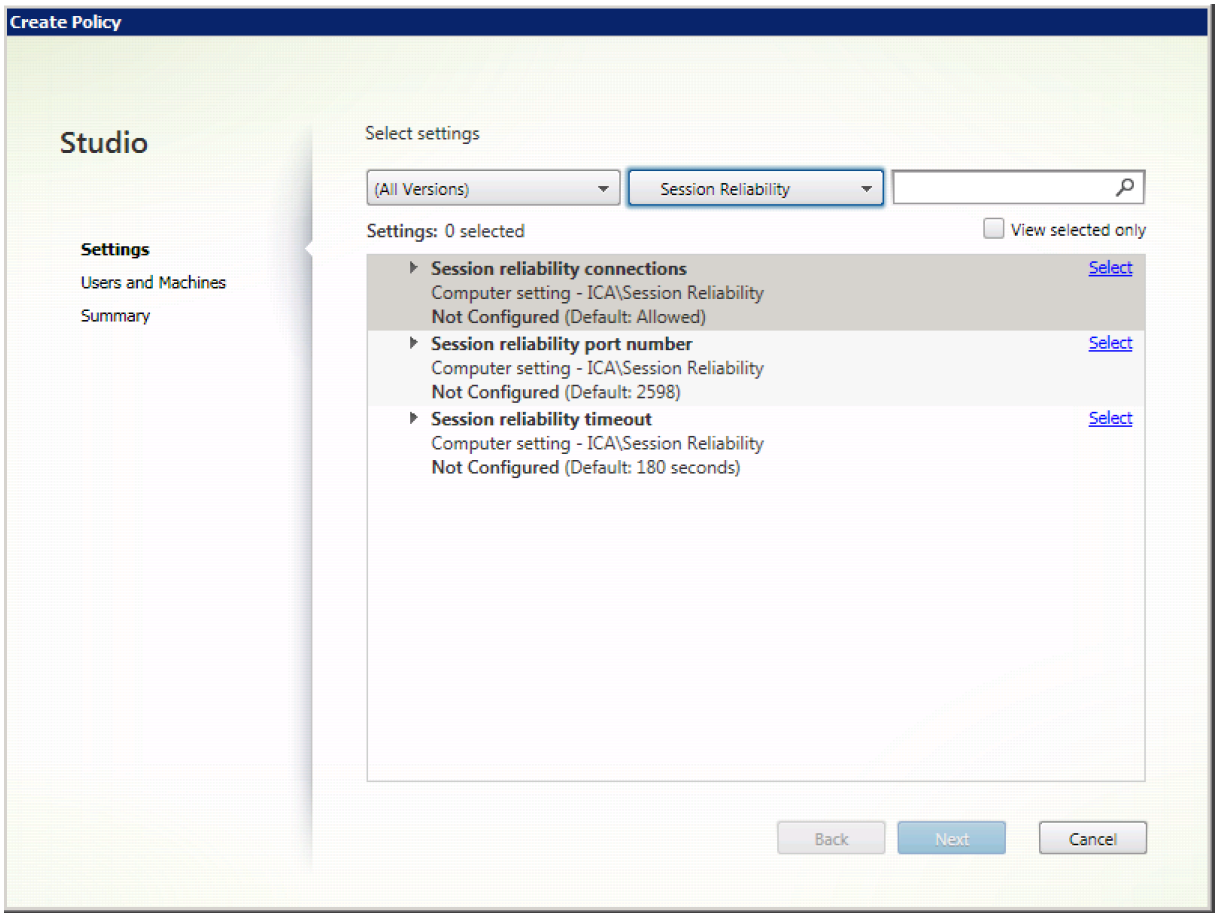
Grâce à la fiabilité de session, la session reste active sur le serveur. Pour indiquer que la connectivité est interrompue, l'affichage de l'utilisateur devient opaque. L'utilisateur peut observer une session bloquée durant l'interruption et peut reprendre l'interaction avec l'application lorsque la connexion réseau est rétablie. La fonction de fiabilité de session permet aux utilisateurs de se reconnecter sans invite de s'authentifier à nouveau.

Si vous utilisez la fonction de fiabilité de session et la fonction de reconnexion automatique des clients, ces fonctions agissent l'une après l'autre. La fonction de fiabilité de session ferme (ou déconnecte) la session utilisateur après l'expiration de la durée spécifiée dans le paramètre Expiration de délai de la fiabilité de session. Ensuite, les paramètres de reconnexion automatique des clients s'appliquent et la fonction tente d'opérer la reconnexion de l'utilisateur à la session déconnectée.

Par défaut, la fiabilité de session est autorisée.

Pour désactiver la fiabilité de session :

1. Démarrez Citrix Studio.
2. Ouvrez la stratégie **Connexions de fiabilité de session**.
3. Définissez la stratégie sur **Interdit**.



Numéro de port de la fiabilité de session

Ce paramètre spécifie le numéro de port TCP pour les connexions de fiabilité de session entrantes.

Le numéro port est défini par défaut sur 2598.

Pour modifier le numéro de port de la fiabilité de session :

1. Démarrez Citrix Studio.
2. Ouvrez la stratégie **Numéro de port de la fiabilité de session**.
3. Modifiez le numéro de port.
4. Cliquez sur **OK**.

Expiration de délai de la fiabilité de session

Ce paramètre indique la durée en secondes pendant lequel le proxy de fiabilité de session attend qu'un client se reconnecte avant d'autoriser la déconnexion de la session.

Bien que vous puissiez prolonger la durée pendant laquelle une session reste ouverte, mais le but de cette fonction consiste à éviter à l'utilisateur de devoir s'authentifier de nouveau. Plus une session

reste ouverte longtemps, et plus les chances qu'un utilisateur laisse l'appareil sans surveillance et que ce dernier soit potentiellement accessible par des utilisateurs non autorisés augmentent.

Par défaut, le délai d'expiration est défini sur 180 secondes, ou trois minutes.

Pour modifier l'expiration de délai de la fiabilité de session :

1. Démarrez Citrix Studio.
2. Ouvrez la stratégie **Expiration de délai de la fiabilité de session**.
3. Modifiez la valeur du délai d'expiration.
4. Cliquez sur **OK**.

Paramètres de stratégie Contrôle des fuseaux horaires

November 9, 2018

La section Contrôle de fuseau horaire contient des paramètres de stratégie liés à l'utilisation de l'heure locale dans les sessions.

Estimer l'heure locale pour les clients d'ancienne génération

Ce paramètre permet d'activer ou de désactiver l'estimation de l'heure locale des machines des utilisateurs qui envoient des informations de fuseau horaire au serveur.

Par défaut, le serveur estime le fuseau horaire local, si nécessaire.

Ce paramètre est conçu pour être utilisé avec les versions antérieures de Citrix Receiver ou clients ICA qui n'envoient pas d'informations de fuseau horaire au serveur. Lorsqu'il est utilisé avec des clients qui envoient des informations de fuseau horaire au serveur, telles que les versions prises en charge de Citrix Receiver pour Windows, ce paramètre n'a aucun effet.

Utilisation de l'heure locale du client

Ce paramètre permet de déterminer le fuseau horaire de la session utilisateur. Cela peut être soit le fuseau horaire de la session utilisateur soit le fuseau horaire de la machine utilisateur.

Par défaut, le fuseau horaire de la session de l'utilisateur est utilisé.

Pour que ce paramètre entre en vigueur, activez le paramètre Autoriser la redirection du fuseau horaire dans l'Éditeur de stratégie de groupe (Configuration Utilisateur > Modèles d'administration > Services Bureau à distance > Hôte de session Bureau à distance > Redirection de périphérique et de ressource).

Paramètres de stratégie Périphériques TWAIN

November 9, 2018

La section Périphériques TWAIN contient des paramètres de stratégie liés au mappage des périphériques TWAIN clients, tels qu'appareils photo numériques ou scanners, et à l'optimisation des transferts d'images du client au serveur.

> **Remarque**
>
> TWAIN 2.0 est pris en charge par Citrix Receiver pour Windows version 4.5.

Redirection de périphérique TWAIN client

Ce paramètre autorise ou empêche les utilisateurs d'accéder aux périphériques TWAIN sur la machine utilisateur à partir d'applications de traitement d'image hébergées sur les serveurs. Par défaut, la redirection de périphérique TWAIN est autorisée.

Les paramètres de stratégie suivants sont associés :

- Niveau de compression TWAIN
- Limite de bande passante de redirection du périphérique TWAIN
- Pourcentage de limite de bande passante de redirection du périphérique TWAIN

Niveau de compression TWAIN

Ce paramètre spécifie le niveau de compression des transferts d'images du client au serveur. Utilisez Basse pour une qualité d'image optimale, Moyenne pour une bonne qualité d'image ou Élevée pour une faible qualité d'image. Par défaut, la compression moyenne est appliquée.

Paramètres de stratégie Périphériques USB

February 28, 2019

La section Périphériques USB contient des paramètres de stratégie permettant de gérer la redirection de fichiers pour les périphériques USB.

Règles d'optimisation des périphériques USB clients

Les règles d'optimisation des périphériques USB clients peuvent être appliquées aux périphériques pour désactiver l'optimisation, ou pour modifier le mode d'optimisation.

Lorsqu'un utilisateur branche un périphérique USB, l'hôte vérifie si le périphérique est autorisé par les paramètres de stratégie USB. Si le périphérique est autorisé, l'hôte vérifie ensuite les **Règles d'optimisation de périphérique USB client** pour le périphérique. Si aucune règle n'est spécifiée, le périphérique n'est pas optimisé. Le mode capture (04) est la méthode recommandée pour les périphériques de signature. Pour les autres périphériques dont les performances se dégradent avec une latence élevée, les administrateurs peuvent activer le mode interactif (02). Consultez les descriptions ci-dessous pour connaître les modes disponibles.

À savoir

- Pour l'utilisation de tablettes et de dispositifs de signature numérique Wacom, Citrix recommande de désactiver l'écran de veille. Vous trouverez des procédures à cet effet à la fin de cette section.
- La prise en charge de l'optimisation des tablettes et des dispositifs de signature numérique Wacom STU a été préconfigurée dans l'installation de stratégies XenApp et XenDesktop.
- Les périphériques de signature fonctionnent sur XenApp et XenDesktop et ne requièrent pas de pilote pour être utilisés en tant que périphérique de signature. Wacom propose des logiciels supplémentaires qui peuvent être installés pour personnaliser le périphérique. Veuillez consulter la section https://www.wacom.com/.
- Tablettes graphiques. Certains périphériques de dessin peuvent être considérés comme périphérique HID sur des bus PCI/ACPI et ne sont pas pris en charge. Ces périphériques doivent être connectés sur un contrôleur d'hôte USB sur le client pour être redirigés dans une session XenDesktop.

Les règles de stratégies sont au format tag=value (balise=valeur) séparées par des espaces. Les balises suivantes sont prises en charge :

Nom de balise	Description
Mode	Le mode d'optimisation est pris en charge pour les périphériques d'entrée pour une classe=03. Les modes pris en charge sont : Aucune optimisation - valeur 01. Mode interactif - valeur 02. Recommandé pour les périphériques tels que des tablettes à stylet et des souris 3D Pro. Mode capture - valeur 04. Mode préféré pour les périphériques tels que les dispositifs de signature numérique.

Nom de balise	Description
VID	ID fournisseur du descripteur de périphérique, sous forme de nombre hexadécimal à quatre chiffres.
PID	ID produit du descripteur de périphérique, sous forme de nombre hexadécimal à quatre chiffres.
REV	ID de révision du descripteur de périphérique, sous forme de nombre hexadécimal à quatre chiffres.
Classe	Classe du descripteur de périphérique ou d'un descripteur d'interface.
Sous-classe	Sous-classe du descripteur de périphérique ou d'un descripteur d'interface.
Prot	Protocole à partir du descripteur de périphérique ou d'un descripteur d'interface.

Exemples

Mode=00000004 VID=067B PID=1230 class=03 #Périphérique fonctionnant en mode capture

Mode=00000002 VID=067B PID=1230 class=03 #Périphérique fonctionnant en mode interactif (valeur par défaut)

Mode=00000001 VID=067B PID=1230 class=03 #Périphérique fonctionnant sans optimisation

Mode=00000100 VID=067B PID=1230 #Optimisation de la configuration du périphérique désactivée (valeur par défaut)

Mode=00000200 VID=067B PID=1230 #Optimisation de la configuration du périphérique activée

Désactivation de l'écran de veille des dispositifs de signature numérique Wacom

Pour l'utilisation de tablettes et de dispositifs de signature numérique Wacom, Citrix recommande de désactiver l'écran de veille comme suit :

1. Installez **Wacom-STU-Driver** après la redirection du périphérique.
2. Installez **Wacom-STU-Display MSI** pour pouvoir accéder au panneau de configuration du dispositif de signature.

3. Accédez à **Control Panel > Wacom STU Display > STU430** ou **STU530** et sélectionnez l'onglet de votre modèle.
4. Cliquez sur **Change**, puis sélectionnez **Yes** lorsque la fenêtre de sécurité de compte utilisateur (UAC) s'affiche.
5. Sélectionnez **Disable slideshow**, puis **Apply**.

Une fois que le paramètre est défini pour un modèle de dispositif de signature numérique, il est appliqué à tous les modèles.

Redirection de périphérique USB client

Ce paramètre permet d'autoriser ou d'empêcher la redirection de périphériques USB vers et depuis la machine utilisateur.

Par défaut, les périphériques USB ne sont pas redirigés.

Règles de redirection des périphériques USB clients

Ce paramètre spécifie les règles de redirection des périphériques USB.

Par défaut, aucune règle n'est spécifiée.

Lorsqu'un utilisateur connecte un périphérique USB, la machine hôte vérifie celui-ci par rapport à chacune des règles de stratégie jusqu'à ce qu'une correspondance soit trouvée. La première correspondance trouvée pour un périphérique est considérée comme définitive. Si la première correspondance est une règle Autoriser, le périphérique est envoyé vers le bureau virtuel. Si la première correspondance est une règle Refuser, le périphérique n'est disponible que pour le bureau local. Si aucune correspondance n'est trouvée, les règles par défaut sont utilisées.

Les règles de stratégies sont au format {Allow:|Deny:} et sont suivies d'un ensemble d'expressions tag=value (balise=valeur) séparées par des espaces. Les balises suivantes sont prises en charge :

Nom de balise	Description
VID	ID fournisseur du descripteur de périphérique, sous forme de nombre hexadécimal à quatre chiffres.
PID	ID produit du descripteur de périphérique, sous forme de nombre hexadécimal à quatre chiffres.
REV	ID de révision du descripteur de périphérique, sous forme de nombre hexadécimal à quatre chiffres.

Nom de balise	Description
Classe	Classe du descripteur de périphérique ou d'un descripteur d'interface.
Sous-classe	Sous-classe du descripteur de périphérique ou d'un descripteur d'interface.
Prot	Protocole à partir du descripteur de périphérique ou d'un descripteur d'interface.

Lors de la création de nouvelles règles de stratégie, rappelez-vous ce qui suit :

- Les règles ne sont pas sensibles à la casse.
- Les règles peuvent éventuellement comporter un commentaire, introduit par #, à la fin.
- Les espaces vides et les lignes de commentaires pures sont ignorés.
- Les balises doivent utiliser l'opérateur de correspondance = (par exemple, VID=067B_).
- Chaque règle doit commencer sur une nouvelle ligne ou faire partie d'une liste séparée par des points-virgules.
- Reportez-vous aux codes de classe USB disponibles sur le site Web USB Implementers Forum.

Exemples de règles de stratégie USB définies par l'administrateur :

- Allow: VID=067B PID=0007 # Another Industries, Another Flash Drive
- Deny: Class=08 subclass=05 # Mass Storage
- Pour créer une règle qui refuse tous les périphériques USB, utilisez « DENY: » sans aucune autre balise.

Redirection de périphérique Plug and Play USB client

Ce paramètre permet d'autoriser ou d'empêcher l'utilisation de périphériques Plug and Play comme les appareils photo ou les périphériques de point de vente dans une session cliente.

Par défaut, la redirection de périphériques Plug and Play est autorisée. Lorsque l'option a la valeur Autorisé, tous les périphériques Plug and Play d'un utilisateur ou d'un groupe spécifique sont redirigés. Lorsque l'option a la valeur Interdit, aucun périphérique n'est redirigé.

Paramètres de stratégie Affichage visuel

February 28, 2019

La section Affichage visuel contient des paramètres de stratégie permettant de contrôler la qualité des images envoyées depuis des bureaux virtuels vers la machine utilisateur.

Nombre de couleurs préféré pour les graphiques simples

Ce paramètre de stratégie est disponible dans les versions VDA 7.6 FP3 et ultérieures. L'option 8 bits est disponible dans les versions VDA 7.12 et ultérieures.

Ce paramètre permet de réduire le nombre de couleurs à partir duquel les graphiques simples sont envoyés via le réseau. La réduction à 8 bits ou 16 bits par pixel améliore potentiellement le temps de réponse sur les connexions à faible bande passante, en contrepartie d'une légère dégradation de la qualité de l'image. Le nombre de couleurs 8 bits n'est pas pris en charge lorsque le paramètre de stratégie Utiliser codec vidéo pour la compression est réglé sur Pour l'écran entier.

Par défaut, le nombre de couleurs est de 24 bits par pixel.

Les VDA retourneront au nombre de couleurs 24 bits (valeur par défaut) si le paramètre 8 bits est appliqué sur le VDA 7.11 et versions antérieures.

Taux de trames cible

Ce paramètre spécifie le nombre maximal de trames par seconde envoyées depuis le bureau virtuel vers la machine utilisateur.

La valeur maximale par défaut est de 30 trames par seconde.

La définition d'un nombre élevé de trames par seconde (par exemple 30) améliore l'expérience utilisateur mais exige plus de bande passante. La réduction du nombre de trames par seconde (par exemple 10) augmente la capacité du serveur à monter en charge au détriment de l'expérience utilisateur. Pour les machines utilisateur possédant des UC plus lents, spécifiez une valeur inférieure pour améliorer l'expérience de l'utilisateur.

Le taux maximal pris en charge est 60 trames par seconde.

Qualité visuelle

Ce paramètre spécifie la qualité visuelle désirée pour les images affichées sur la machine utilisateur.

Par défaut, cette option est définie sur Moyenne.

Pour spécifier la qualité des images, choisissez l'une des options suivantes :

- **Faible :** recommandé pour les réseaux à bande passante limitée où la qualité visuelle peut être sacrifiée pour une meilleure interactivité
- **Moyen :** offre les meilleures performances et une bande passante optimale dans la plupart des cas d'utilisation
- **Élevée :** recommandé si vous avez besoin de qualité d'image visuelle sans perte

- **Sans perte si possible :** envoie des images avec perte à la machine utilisateur durant les périodes de forte activité réseau et des images sans perte après réduction de l'activité réseau ; ce paramètre améliore les performances des connexions réseau avec une bande passante réduite.
- **Toujours sans perte :** dans les cas où la préservation des données d'images est vitale (par exemple, lors de l'affichage de radiographies où la perte de qualité est inacceptable), sélectionnez Toujours sans perte pour vous assurer que les données avec perte ne sont jamais envoyées à la machine utilisateur.

Si le paramètre
Mode graphique d'ancienne génération est activé, le paramètre
Qualité visuelle n'a aucun effet dans cette stratégie.

Paramètres de stratégie des images en mouvement

January 23, 2019

La section Images en mouvement contient des paramètres qui vous permettent de supprimer ou de modifier la compression des images dynamiques.

Qualité d'image minimale

Remarque : pour Virtual Delivery Agent 7.x, ce paramètre de stratégie s'applique uniquement lorsque le paramètre de stratégie du Mode graphique d'ancienne génération est activé.

Ce paramètre spécifie la qualité d'image minimale acceptable pour l'affichage adaptatif. La qualité des images est d'autant plus élevée que la compression est faible. Choisissez entre les valeurs de compression Ultra élevée, Très élevée, Élevée, Normale et Basse.

Par défaut, cette option est définie sur Normale.

Compression d'images en mouvement

Ce paramètre spécifie si l'affichage adaptatif est activé ou non. L'affichage adaptatif ajuste automatiquement la qualité d'image des vidéos et des diapositives de transition des diaporamas en fonction de la bande passante disponible. Lorsque l'affichage adaptatif est activé, les utilisateurs doivent voir des présentations fluides sans réduction de qualité.

Par défaut, l'affichage adaptatif est activé.

Pour les versions VDA 7.0 à 7.6, ce paramètre s'applique uniquement lorsque le mode graphique d'ancienne génération est activé. Pour les versions VDA 7.6 FP1 et versions ultérieures, ce paramètre s'applique lorsque le mode graphique d'ancienne génération est activé, ou lorsque le mode

graphique d'ancienne génération est désactivé et qu'aucun codec vidéo n'est utilisé pour compresser les graphiques.

Lorsque le mode graphique d'ancienne génération est activé, la session doit être redémarrée pour que les modifications prennent effet. L'affichage adaptatif et l'affichage progressif sont mutuellement exclusifs ; l'activation de l'affichage adaptatif désactive l'affichage progressif et vice versa. Il est cependant possible de désactiver l'affichage progressif et l'affichage adaptatif en même temps. L'utilisation de l'affichage progressif en tant que fonctionnalité d'ancienne génération n'est pas recommandée avec XenApp ou XenDesktop. La définition du niveau de seuil de l'affichage progressif désactive l'affichage adaptatif.

Niveau de compression progressif

Remarque : pour Virtual Delivery Agent 7.x, ce paramètre de stratégie s'applique uniquement lorsque le paramètre de stratégie du Mode graphique d'ancienne génération est activé.

Ce paramètre permet un affichage initial d'images moins détaillé, mais plus rapide.

Par défaut, la compression progressive n'est pas appliquée.

L'image plus détaillée définie par le paramètre de compression avec perte normale, s'affiche lorsqu'elle devient disponible. Utilisez une compression très élevée ou extrêmement élevée pour un affichage optimal des images à utilisation intensive de la bande passante, telles que des photographies.

Pour que la compression progressive soit efficace, son niveau de compression doit être supérieur à celui du paramètre
Niveau de compression avec perte.

Remarque : le niveau amélioré de compression associé à la compression progressive optimise également l'interactivité des images dynamiques via les connexions clientes. La qualité d'une image dynamique, telle qu'un modèle pivotant à trois dimensions, est temporairement réduite jusqu'à ce que l'image devienne fixe, moment auquel le paramètre de compression avec perte normale est appliqué.

Les paramètres de stratégie suivants sont associés :

- Valeur de seuil de compression progressif
- Compression lourde progressive

Valeur de seuil de compression progressif

Remarque : pour Virtual Delivery Agent 7.x, ce paramètre de stratégie s'applique uniquement lorsque le paramètre de stratégie du Mode graphique d'ancienne génération est activé.

Ce paramètre représente la bande passante maximale, en kilobits par seconde, pour une connexion à laquelle la compression progressive est appliquée. Cela ne concerne que les connexions clientes liées à cette bande passante.

Par défaut, la valeur de seuil est de 2 147 483 647 kilobits par seconde.

Les paramètres de stratégie suivants sont associés :

- Valeur de seuil de compression progressif
- Compression lourde progressive

Taux de trame minimum cible

Ce paramètre spécifie le taux de trame minimum par seconde que le système tente de conserver, des images dynamiques, dans des conditions de bande passante faible.

Par défaut, cette option est définie sur 10fps.

Pour les versions VDA 7.0 à 7.6, ce paramètre s'applique uniquement lorsque le mode graphique d'ancienne génération est activé. Pour les versions VDA 7.6 FP1 et versions ultérieures, ce paramètre s'applique lorsque le mode graphique d'ancienne génération est activé ou désactivé.

Paramètres de stratégie Images immobiles

January 23, 2019

La section Images immobiles contient des paramètres qui vous permettent de supprimer ou de modifier la compression des images statiques.

Compression couleur supplémentaire

Ce paramètre active ou désactive l'utilisation d'une compression de couleur supplémentaire sur les images mises à disposition sur les connexions côté client qui sont limitées en bande passante, améliorant les temps de réponse en réduisant la qualité des images affichées.

Par défaut, la compression de couleur supplémentaire est désactivée.

Lorsqu'elle est activée, la compression de couleur supplémentaire est appliquée uniquement lorsque la bande passante de connexion cliente se trouve en dessous de la valeur du Seuil de compression de couleur supplémentaire. Lorsque la bande passante de connexion cliente se trouve en dessus de la valeur de seuil ou que Désactivé est sélectionné, la compression de couleur supplémentaire n'est pas appliquée.

Seuil de compression de couleur supplémentaire

Remarque : pour Virtual Delivery Agent 7.x, ce paramètre de stratégie s'applique uniquement lorsque le paramètre de stratégie du Mode graphique d'ancienne génération est activé.

Ce paramètre représente la bande passante maximale, en kilobits par seconde, pour une connexion en dessous de laquelle la compression de couleur supplémentaire est appliquée. Si la bande passante de connexion cliente tombe en dessous de la valeur définie, la compression de couleur supplémentaire, si activée, est appliquée.

Par défaut, la valeur de seuil est de 8 192 kilobits par seconde.

Compression lourde

Remarque : pour Virtual Delivery Agent 7.x, ce paramètre de stratégie s'applique uniquement lorsque le paramètre de stratégie du Mode graphique d'ancienne génération est activé.

Ce paramètre vous permet d'activer ou de désactiver la réduction de bande passante au-delà de la compression progressive sans perte de qualité d'image, en utilisant un algorithme graphique plus évolué, mais qui nécessite des ressources processeur importantes.

Par défaut, la compression intensive est désactivée.

Lorsqu'elle est activée, la compression intensive s'applique à tous les paramètres de compression avec perte. Elle est prise en charge sur Citrix Receiver, mais n'a aucun effet sur les autres plug-ins.

Les paramètres de stratégie suivants sont associés :

- Niveau de compression progressif
- Valeur de seuil de compression progressif

Niveau de compression avec perte

Remarque : pour Virtual Delivery Agent 7.x, ce paramètre de stratégie s'applique uniquement lorsque le paramètre de stratégie du Mode graphique d'ancienne génération est activé.

Ce paramètre permet de contrôler le niveau de compression avec perte utilisé sur des images fournies sur des connexions clientes à bande passante limitée. Le cas échéant, l'affichage des images sans compression risque d'être ralenti.

Par défaut, la compression moyenne est sélectionnée.

Pour améliorer la réactivité avec des images à utilisation intensive de la bande passante, utilisez une compression élevée. Si la conservation des données d'images est un élément essentiel, par exemple lors de l'affichage de radiographies où la perte de qualité ne peut pas être tolérée, il est préférable de ne pas utiliser une compression avec perte.

Paramètre de stratégie connexe : valeur de seuil de compression avec perte

Valeur de seuil de compression avec perte

Remarque : pour Virtual Delivery Agent 7.x, ce paramètre de stratégie s'applique uniquement lorsque le paramètre de stratégie du Mode graphique d'ancienne génération est activé.

Ce paramètre représente la bande passante maximale, en kilobits par seconde, pour une connexion à laquelle la compression avec perte est appliquée.

Par défaut, la valeur de seuil est de 2 147 483 647 kilobits par seconde.

L'ajout du paramètre Niveau de compression avec perte à une stratégie et l'inclusion d'un seuil non spécifié peut améliorer la vitesse d'affichage des bitmaps comprenant un nombre de détails élevés, tels que les photographies, dans un réseau local.

Paramètre de stratégie connexe : niveau de compression avec perte

Paramètres de stratégie WebSockets

November 9, 2018

La section WebSockets contient des paramètres de stratégie pour accéder aux bureaux virtuels et aux applications hébergées avec Citrix Receiver pour HTML5. La fonctionnalité WebSockets renforce la sécurité et réduit la charge en réalisant une communication bidirectionnelle entre les applications et les serveurs de navigateur sans ouvrir plusieurs connexions HTTP.

Connexions WebSockets

Ce paramètre autorise ou interdit les connexions WebSockets.

Par défaut, les connexions WebSockets sont interdites.

Numéro de port WebSockets

Ce paramètre identifie le port pour les connexions WebSockets entrantes.

Par défaut, la valeur est 8008.

Liste de serveurs d'origine approuvés WebSockets

Ce paramètre fournit une liste séparée par des virgules des serveurs d'origine de confiance, habituellement Citrix Receiver pour Web, exprimée sous la forme d'adresses URL. Seules les connexions WebSockets provenant de l'un de ces adresses est accepté par le serveur.

Par défaut, des caractères génériques sont utilisés pour faire confiance à toutes les adresses URL Citrix Receiver pour Web.

Si vous choisissez d'entrer une adresse dans la liste, utilisez la syntaxe suivante :

```
<protocol>://<Fully qualified domain name of host>:[port]
```

Le protocole doit être HTTP ou HTTPS. Si le port n'est pas spécifié, le port 80 pour HTTP et le port 443 est utilisé pour HTTPS.

Le caractère générique * peut être utilisé dans l'adresse URL, sauf dans le cadre d'une adresse IP (10.105. .).

Paramètres de stratégie Gestion de la charge

November 9, 2018

La section Gestion de la charge contient des paramètres de stratégie pour l'activation et la configuration de la gestion de la charge entre les serveurs mettant à disposition des machines avec OS Windows Server.

Pour de plus amples informations sur le calcul de l'index de calculateur de charge, consultez l'article CTX202150.

Tolérance d'ouvertures de session simultanée

Ce paramètre spécifie le nombre maximal d'ouvertures de session simultanées qu'un serveur peut accepter.

Par défaut, cette option est définie sur 2.

Lorsque ce paramètre est activé, l'équilibrage de charge fait en sorte de ne pas dépasser le nombre spécifié d'ouvertures de session actives en même temps sur un VDA serveur. Toutefois, la limite n'est pas strictement appliquée. Pour appliquer la limite (et entraîner l'échec des ouvertures de session simultanées qui dépassent le nombre spécifié), créez la clé de registre suivante :

HKLM\Software\Citrix\DesktopServer\LogonToleranceIsHardLimit
Type : DWORD
Valeur : 1

Utilisation UC

Ce paramètre spécifie le niveau d'utilisation de l'UC, sous la forme d'un pourcentage, à laquelle le serveur signale une pleine charge. Lorsque cette option est activée, la valeur par défaut à laquelle le serveur signale une pleine charge est 90%.

Par défaut, ce paramètre est désactivé et l'utilisation de l'UC est exclue du calcul de la charge.

Priorité de processus exclue de l'utilisation UC

Ce paramètre spécifie le niveau de priorité auquel l'utilisation de l'UC est exclue de l'index de charge de l'utilisation de l'UC.

Par défaut, cette option est définie sur Inférieure à la normale ou Basse.

Utilisation du disque

Ce paramètre spécifie la longueur de la file d'attente à laquelle le serveur signale une pleine charge 75%. Lorsque cette option est activée, la valeur par défaut de file d'attente du disque est de 8.

Par défaut, ce paramètre est désactivé et l'utilisation du disque est exclue du calcul des charges.

Nombre maximum de sessions

Ce paramètre spécifie le nombre maximal de sessions qu'un serveur peut héberger. Lorsqu'il est activé, le paramètre par défaut pour le nombre maximal de sessions qu'un serveur peut héberger est 250.

Ce paramètre est activé par défaut.

Utilisation de mémoire

Ce paramètre spécifie le niveau d'utilisation de la mémoire, sous la forme d'un pourcentage, à laquelle le serveur signale une pleine charge. Lorsque cette option est activée, la valeur par défaut à laquelle le serveur signale une pleine charge est 90%.

Par défaut, ce paramètre est désactivé et l'utilisation de mémoire est exclue du calcul de la charge.

Charge de base d'utilisation mémoire

Ce paramètre spécifie une approximation de l'utilisation de la mémoire du système d'exploitation de base et définit, en Mo, l'utilisation de la mémoire en dessous de laquelle un serveur est considéré comme ayant une charge de zéro.

Par défaut, cette option est définie sur 768 Mo.

Paramètres de stratégie Profile Management

November 9, 2018

La section Profile Management contient les paramètres de stratégie pour l'activation de Profile Management et la spécification des groupes à inclure et à exclure du traitement Profile Management.

D'autres informations (telles que les noms des paramètres du fichier .ini et la version de Profile Management requise pour un paramètre de stratégie spécifique) sont disponibles dans Stratégies de Profile Management.

Paramètres de stratégie Avancés

February 28, 2019

La section Paramètres avancés contient les paramètres de stratégie liés à la configuration avancée de Profile Management.

Désactiver la configuration automatique

Ce paramètre permet d'activer Profile Management pour examiner votre environnement ; par exemple, pour vérifier la présence de Personal vDisks, et configurer la stratégie de groupe en conséquence. Seules les stratégies Profile Management dans l'état Non configuré sont ajustées, de sorte que toutes les personnalisations effectuées précédemment sont conservées. Cette fonctionnalité accélère le déploiement et simplifie l'optimisation. Aucune configuration de la fonctionnalité n'est nécessaire, mais vous pouvez désactiver la configuration automatique lors de la mise à niveau (pour conserver les paramètres à partir de versions antérieures) ou lors de la résolution des problèmes. La configuration automatique ne fonctionne pas dans XenApp ou d'autres environnements.

Par défaut, la configuration automatique est autorisée.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, la configuration automatique est activée afin que les paramètres de Profile Management puissent être modifiés si votre environnement change.

Fermer la session de l'utilisateur si un problème se produit

Ce paramètre permet à Profile Management de fermer la session d'un utilisateur lorsqu'un problème est détecté, par exemple, si le magasin de l'utilisateur n'est pas disponible. Lorsqu'il est activé, un message d'erreur est affiché à l'utilisateur avant que sa session soit fermée. Lorsqu'il est désactivé, les utilisateurs se voient attribuer un profil temporaire.

Par défaut, ce paramètre est désactivé et un profil temporaire est attribué aux utilisateurs lorsqu'un problème est détecté.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici ou dans le fichier .ini, un profil temporaire est fourni.

Nombre de tentatives d'accès à des fichiers verrouillés

Ce paramètre spécifie le nombre de tentatives effectuées par Profile Management pour accéder à des fichiers verrouillés.

Par défaut, ce paramètre est défini sur 5 tentatives.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, la valeur par défaut est utilisée.

Traiter les cookies Internet à la fermeture de session

Ce paramètre permet d'activer Profile Management pour traiter le fichier index.dat lors de l'ouverture de session pour supprimer les cookies Internet dans le système de fichiers après la navigation intensive qui peuvent entraîner la saturation du profil. Étant donné que ce paramètre augmente la durée de fermeture de session, ne l'activez que si vous rencontrez ce problème.

Par défaut, ce paramètre est désactivé, Profile Management ne traite pas le fichier index.dat lors de la fermeture de session.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, index.dat n'est pas traité.

Paramètres de stratégie De base

November 9, 2018

La section Paramètres de base contient des paramètres de stratégie liés à la configuration de base de Profile Management.

Réécriture active

Ce paramètre permet de modifier les fichiers et dossiers (mais pas les paramètres de registre) devant être synchronisés avec le magasin utilisateur durant une session, avant la fermeture de session.

Par défaut, la synchronisation avec le magasin d'utilisateur durant une session est désactivée.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, il est activé.

Activer Profile Management

Ce paramètre permet d'activer Profile Management pour traiter les ouvertures et les fermetures de session.

Par défaut, ce paramètre est désactivé pour faciliter le déploiement.

Important : Citrix recommande d'activer Profile Management uniquement après avoir terminé toutes les autres tâches de configuration et testé le comportement des profils utilisateur Citrix dans votre environnement.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, Profile Management ne traite pas les profils utilisateur Windows.

Groupes exclus

Ce paramètre spécifie les groupes d'ordinateurs locaux et les groupes de domaines (locaux, globaux et universels) exclus du traitement Profile Management.

Lorsque cette option est activée, Profile Management ne traite pas les membres des groupes d'utilisateurs spécifiés.

Par défaut, ce paramètre est désactivé, les membres de tous les groupes d'utilisateurs sont traités.

Spécifiez les groupes de domaines au format : <NOM DE DOMAINE>\<NOM DE GROUPE>

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, les membres de tous les groupes d'utilisateurs sont traités.

Prise en charge des profils déconnectés

Ce paramètre permet d'activer la prise en charge de profil hors connexion, ce qui permet la synchronisation des profils avec le magasin de l'utilisateur à la première opportunité après une déconnexion du réseau.

Par défaut, la prise en charge des profils déconnectés est désactivée.

Ce paramètre s'applique à un ordinateur portable ou aux utilisateurs mobiles itinérants. Lorsque la connexion au réseau est interrompue, les profils restent inchangés sur l'ordinateur portable ou le périphérique même après redémarrage ou mise en veille prolongée. Au fur et à mesure que les utilisateurs mobiles travaillent, leurs profils sont mis à jour localement et synchronisés avec le magasin de l'utilisateur lorsque la connexion réseau est rétablie.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, la prise en charge des profils hors connexion est désactivée.

Chemin d'accès au magasin de l'utilisateur

Ce paramètre spécifie le chemin d'accès au répertoire (magasin de l'utilisateur) dans lequel les paramètres utilisateur, tels que les paramètres de registre et les fichiers synchronisés, sont enregistrés.

Par défaut, le répertoire Windows du lecteur de base est utilisé.

Si ce paramètre est désactivé, les paramètres utilisateur sont enregistrés dans le sous-répertoire Windows du répertoire de base.

Le chemin d'accès peut être :

- **Un chemin relatif**. Il doit être relatif au répertoire de base (qui est généralement configuré en tant qu'attribut #homeDirectory# pour un utilisateur dans Active Directory).
- **Un chemin UNC absolu**. Spécifie généralement un partage de serveurs ou un espace de noms DFS.
- **Désactivé ou non configuré**. Dans ce cas, la valeur #homeDirectory#\Windows est utilisée.

Utiliser les types de variables suivants lors de la configuration de ce paramètre de stratégie :

- Variables d'environnement système entourées de symboles pourcentage (par exemple, %ProfVer%). Veuillez noter que les variables d'environnement système requièrent généralement une configuration supplémentaire.
- Attributs de l'objet utilisateur Active Directory entourés de hachages (par exemple, #sAMAccountName#).

- Variables Profile Management. Pour plus d'informations, consultez la documentation relative à Profile Management.

Vous pouvez également utiliser les variables d'environnement utilisateur %username% et %userdomain% et créer des attributs personnalisés pour définir des variables d'organisation telles que l'emplacement ou les utilisateurs. Les attributs sont sensibles à la casse.

Exemples :

- \\server\share#sAMAccountName# stocke les paramètres utilisateur dans le chemin UNC \\server\share\JohnSmith (si #sAMAccountName# correspond à JohnSmith pour l'utilisateur actuel)
- \\server\profiles$%USERNAME%.%USERDOMAIN%\!CTX_PROFILEVER!!CTX_OSBITNESS! might expand to \\server\profiles$\JohnSmith.DOMAINCONTROLLER1\v2x64

Important : quels que soient les attributs ou variables que vous utilisez, vérifiez que ce paramètre est appliqué au dossier de niveau supérieur du dossier contenant NTUSER.DAT. Par exemple, si ce fichier figure dans \\serveur\profils$\JohnSmith.Finance\v2x64\UPM_Profile, définissez le chemin d'accès au magasin de l'utilisateur comme tel : \\serveur\profils$\JohnSmith.Finance\v2x64 (en n'incluant pas le sous-dossier \UPM_Profile).

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, le répertoire Windows du lecteur de base est utilisé.

Traiter les connexions des administrateurs locaux

ce paramètre spécifie si les ouvertures de session des membres du groupe BUILTIN\Administrators sont traitées. Cela permet aux utilisateurs de domaine avec des droits d'administrateur local, généralement utilisateurs XenDesktop avec des bureaux virtuels attribués d'ignorer le traitement, d'ouvrir une session et de résoudre les problèmes liés à un bureau avec Profile Management.

Si ce paramètre est désactivé ou qu'il n'est pas configuré sur les systèmes d'exploitation serveur, Profile Management suppose que les ouvertures de session des utilisateurs du domaine doivent être traitées, mais pas celles des administrateurs locaux. Sur les systèmes d'exploitation de bureau, les ouvertures de session des administrateurs locaux sont traitées.

Par défaut, ce paramètre est désactivé, et les ouvertures de session des administrateurs locaux ne sont pas traitées.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, les ouvertures de session des administrateurs locaux ne sont pas traitées.

Groupes traités

Ce paramètre spécifie les groupes d'ordinateurs locaux et les groupes de domaines (locaux, globaux et universels) qui sont inclus dans le traitement Profile Management.

Lorsque cette option est activée, Profile Management traite uniquement les membres des groupes d'utilisateurs spécifiés.

Par défaut, ce paramètre est désactivé, les membres de tous les groupes d'utilisateurs sont traités.

Spécifiez les groupes de domaines au format : <NOM DE DOMAINE><NOM DE GROUPE>

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, les membres de tous les groupes d'utilisateurs sont traités.

Paramètres de stratégie Multi-plateformes

November 9, 2018

La section Multi-plateformes contient des paramètres de stratégie liés à la configuration de la fonctionnalité de paramètres multi-plateformes de Profile Management.

Paramètres multi-plateformes des groupes d'utilisateurs

Ce paramètre spécifie les groupes d'utilisateurs Windows dont les profils sont traités lorsque la fonctionnalité de paramètres multi-plateformes est activée.

Par défaut, ce paramètre est désactivé et tous les groupes d'utilisateurs traités spécifiés dans le paramètre de stratégie Groupes traités sont traités.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, tous les groupes d'utilisateurs sont traités.

Activer les paramètres multi-plateformes

Ce paramètre active ou désactive la fonctionnalité de paramètres au travers des plates-formes, qui vous permet de migrer les profils des utilisateurs et d'assurer leur itinérance lorsque l'utilisateur se connecte à la même application exécutée sur de multiples systèmes d'exploitation.

Cette fonctionnalité de paramètres au travers des plates-formes est désactivée par défaut.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, aucun paramètre multi-plateforme n'est appliqué.

Chemin d'accès aux définitions multi-plateformes

Ce paramètre spécifie l'emplacement réseau, sous la forme d'un chemin d'accès UNC, de la définition des fichiers copiés à partir du pack de téléchargement.

Remarque : les utilisateurs doivent posséder un accès en lecture, et les administrateurs un accès en écriture à cet emplacement et il doit être un partage de fichiers SMB (Server Message Block) ou CIFS (Common Internet File System).

Par défaut, aucun chemin n'est spécifié.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, aucun paramètre multi-plateforme n'est appliqué.

Chemin d'accès au magasin des paramètres multi-plateformes

Ce paramètre spécifie le chemin d'accès au magasin multi-plateformes, le dossier dans lequel les paramètres multi-plateformes des utilisateurs sont enregistrés. Le chemin peut être soit un chemin UNC vers le répertoire de base ou relatif à celui-ci.

Remarque : les utilisateurs doivent posséder un accès en écriture à ce magasin.

Par défaut, ce paramètre est désactivé et le chemin d'accès Windows\PM_CP est utilisé.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, la valeur par défaut est utilisée.

Source utilisée pour créer les paramètres multi-plateformes

Ce paramètre spécifie une plate-forme en tant que plate-forme de base si ce paramètre est activé pour l'unité d'organisation de cette plate-forme. Les données provenant des profils de la plate-forme de base sont migrées vers le magasin de paramètres multi-plateformes.

Le jeu de profils de chaque plate-forme est stocké dans une unité d'organisation distincte. Ceci signifie que vous devez décider quelles données de profil de la plate-forme utiliser pour amorcer le magasin de paramètres multi-plateformes. On parle de plate-forme de base.

Lorsque cette option est activée, Profile Management fait migrer les données du profil à plate-forme unique vers le magasin si le magasin des paramètres multi-plateformes contient un fichier de définition sans aucune donnée, ou que les données cachées dans un profil à plate-forme unique sont plus récentes que les données de définition du magasin.

Important : si ce paramètre est activé dans plusieurs unités d'organisation, ou plusieurs objets d'utilisateur ou de machine, la plate-forme sur laquelle le premier utilisateur ouvre une session devient le profil de base.

Par défaut, ce paramètre est désactivé, et Profile Management ne fait pas migrer les données depuis le profil à plate-forme unique vers le magasin.

Paramètres de stratégie Système de fichiers

November 9, 2018

La section Système de fichiers contient des paramètres de stratégie permettant de configurer les fichiers et les répertoires dans le profil utilisateur qui sont synchronisés entre le système sur lequel le profil est installé et le magasin de l'utilisateur.

Paramètres de stratégie Exclusions

November 9, 2018

La section Exclusions contient des paramètres de stratégie permettant de configurer les fichiers et les répertoires dans un profil utilisateur sont exclus du processus de synchronisation.

Liste d'exclusion - répertoires

Ce paramètre spécifie une liste de dossiers dans le profil d'utilisateur qui sont ignorées durant la synchronisation.

Spécifiez les noms de dossier en tant que chemins d'accès relatifs au profil utilisateur (USERPROFILE%%).

Par défaut, ce paramètre est désactivé et tous les dossiers du profil utilisateur sont synchronisés.

Exemple : Desktop ignore le dossier Desktop dans le profil utilisateur.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, tous les dossiers du profil utilisateur sont synchronisés.

Liste d'exclusion - fichiers

Ce paramètre spécifie une liste de fichiers dans le profil d'utilisateur qui sont ignorées durant la synchronisation.

Par défaut, ce paramètre est désactivé et tous les fichiers du profil utilisateur sont synchronisés.

Spécifiez les noms de fichiers en tant que chemins d'accès relatifs au profil utilisateur (USERPROFILE%%). Notez que les caractères génériques sont autorisés et sont appliqués de manière récursive.

Exemple : Desktop\Desktop.ini ignore le fichier Desktop.ini dans le dossier Bureau.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, tous les fichiers du profil utilisateur sont synchronisés.

Paramètres de stratégie Synchronisation

November 9, 2018

La section Synchronisation contient des paramètres de stratégie pour spécifier les fichiers et les dossiers dans un profil utilisateur qui sont synchronisés entre le système sur lequel le profil est installé et le magasin de l'utilisateur.

Répertoires à synchroniser

Ce paramètre spécifie tous les fichiers, qui figurent dans des dossiers exclus, que vous voulez que Profile Management inclue dans le processus de synchronisation. Par défaut, Profile Management synchronise tout ce qui se trouve dans le profil utilisateur. Il n'est pas nécessaire d'inclure de sous-dossiers dans le profil utilisateur en les ajoutant à cette liste. Pour plus d'informations, veuillez consulter information la section Inclure et exclure des éléments.

Les chemins d'accès de cette liste doivent être relatifs au profil utilisateur.

Exemple : Desktop\exclude\include s'assure que le sous-dossier appelé include est synchronisé même si le dossier appelé Desktop\exclude ne l'est pas.

Par défaut, ce paramètre est désactivé et aucun dossier n'est spécifié.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, seuls les dossiers non exclus dans le profil utilisateur sont synchronisés.

Fichiers à synchroniser

Ce paramètre spécifie tous les fichiers, qui figurent dans des dossiers exclus, que vous voulez que Profile Management inclue dans le processus de synchronisation. Par défaut, Profile Management synchronise tout ce qui se trouve dans le profil utilisateur. Il n'est pas nécessaire d'inclure de fichiers dans le profil utilisateur en les ajoutant à cette liste. Pour plus d'informations, veuillez consulter information la section Inclure et exclure des éléments.

Les chemins d'accès de cette liste doivent être relatifs au profil utilisateur. Les chemins relatifs sont interprétés comme étant relatifs au profil utilisateur. Les caractères génériques peuvent être utilisés mais sont uniquement autorisés pour les noms de fichiers. Les caractères génériques ne peuvent pas être imbriqués et sont appliqués de manière récursive.

Exemples :

- AppData\Local\Microsoft\Office\Access.qat spécifie un fichier sous un dossier exclus dans la configuration par défaut.
- AppData\Local\MyApp*.cfg spécifie tous les fichiers avec l'extension .cfg dans le dossier de profil AppData\Local\MyApp et ses sous-dossiers.

Par défaut, ce paramètre est désactivé et aucun fichier n'est spécifié.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, seuls les fichiers non exclus dans le profil utilisateur sont synchronisés.

Dossiers en miroir

Ce paramètre spécifie les dossiers relatifs au profil de l'utilisateur par rapport à un dossier racine de l'utilisateur à mettre en miroir. La configuration de cette stratégie permet de faciliter la résolution des problèmes rencontrés avec tout dossier transactionnel (également appelé dossier référentiel), un dossier contenant des fichiers interdépendants, dans lequel un fichier fait référence aux autres.

La mise en miroir de dossiers permet à Profile Management de traiter un dossier transactionnel et son contenu en tant qu'entité unique, ce qui évite l'engorgement du profil. Dans ces cas de figure, tenez compte du fait que le modèle « Last Write Wins » s'applique, ce qui veut dire que les fichiers présents dans les dossiers mis en miroir qui ont été modifiés dans plus d'une session seront écrasés par la dernière mise à jour, ce qui se traduit par la perte des modifications apportées au profil.

Vous pouvez par exemple mettre en miroir le dossier cookies d'Internet Explorer de manière à ce que le fichier Index.dat soit synchronisé avec les cookies qu'il indexe.

Si l'utilisateur a ouvert deux sessions Internet Explorer, chacune sur un serveur différent, et qu'il visite des sites différents dans chaque session, les cookies de chaque site sont ajoutés au serveur approprié.

Lorsque l'utilisateur se déconnecte de la première session (ou au milieu d'une session, si la fonctionnalité de réécriture active est configurée), les cookies de la seconde session devraient remplacer ceux de la première session. Au lieu de cela, ils sont fusionnés et les références aux cookies dans index.dat deviennent obsolètes. Lorsque l'utilisateur accède de nouveau à des sites dans les nouvelles sessions, cela entraîne davantage de fusionnements et l'engorgement du dossier de cookies.

La mise en miroir du dossier permet de résoudre ce problème en remplaçant les cookies avec ceux de la dernière session chaque fois que l'utilisateur ferme une session, ce qui fait que index.dat reste constamment à jour.

Par défaut, ce paramètre est désactivé et aucun dossier n'est mis en miroir.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si cette stratégie n'est pas configurée ici ou dans le fichier .ini, aucun dossier n'est mis en miroir.

Paramètres de stratégie Redirection de dossiers

November 9, 2018

La section Redirection de dossier contient des paramètres de stratégie permettant de spécifier si vous souhaitez rediriger les dossiers qui apparaissent communément dans des profils vers un emplacement réseau partagé.

Accorder l'accès administrateur

Ce paramètre permet à un administrateur d'accéder au contenu des dossiers redirigés des utilisateurs.

Par défaut, ce paramètre est désactivé et les utilisateurs disposent d'un accès exclusif au contenu de leurs dossiers redirigés.

Inclure le nom de domaine

Ce paramètre permet d'activer l'inclusion de la variable d'environnement %userdomain% dans le chemin d'accès UNC spécifié pour la redirection de dossiers.

Par défaut, ce paramètre est désactivé et la variable d'environnement %userdomain% n'est pas incluse dans le chemin d'accès UNC spécifié pour la redirection de dossiers.

Paramètres de stratégie AppData(Roaming)

November 9, 2018

La section AppData(Roaming) contient des paramètres de stratégie pour spécifier si vous souhaitez rediriger le contenu du dossier AppData(Roaming) vers un emplacement réseau partagé.

Chemins d'accès au dossier AppData(Roaming)

Ce paramètre spécifie l'emplacement réseau vers lequel le contenu du dossier AppData(Roaming) est redirigé.

Par défaut, ce paramètre est désactivé et aucun emplacement n'est spécifié.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

Paramètres de redirection du dossier AppData(Roaming)

Ce paramètre spécifie comment rediriger le contenu du dossier AppData(Roaming).

Par défaut, le contenu est redirigé vers un chemin d'accès UNC.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

Paramètres de stratégie Contacts

November 9, 2018

La section Contacts contient les paramètres de stratégie destinés à spécifier si vous souhaitez rediriger le contenu du dossier Contacts vers un emplacement réseau partagé.

Chemin d'accès au dossier Contacts

Ce paramètre spécifie l'emplacement réseau vers lequel le contenu du dossier Contacts est redirigé.

Par défaut, ce paramètre est désactivé et aucun emplacement n'est spécifié.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

Paramètres de redirection du dossier Contacts

Ce paramètre spécifie comment rediriger le contenu du dossier Contacts.

Par défaut, le contenu est redirigé vers un chemin d'accès UNC.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

Paramètres de stratégie Bureau

November 9, 2018

La section Bureau contient des paramètres de stratégie destinés à spécifier si vous souhaitez rediriger le contenu du dossier Bureau vers un emplacement réseau partagé.

Chemin d'accès au dossier Bureau

Ce paramètre spécifie l'emplacement réseau vers lequel le contenu du dossier Desktop est redirigé.

Par défaut, ce paramètre est désactivé et aucun emplacement n'est spécifié.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

Paramètres de redirection du dossier Bureau

Ce paramètre spécifie comment rediriger le contenu du dossier Bureau.

Par défaut, le contenu est redirigé vers un chemin d'accès UNC.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

Paramètres de stratégie Documents

November 9, 2018

La section Documents contient des paramètres de stratégie pour spécifier si vous souhaitez rediriger le contenu du dossier Documents vers un emplacement réseau partagé.

Chemin d'accès au dossier Mes documents

Ce paramètre spécifie l'emplacement réseau vers lequel les fichiers du dossier Documents sont redirigés.

Par défaut, ce paramètre est désactivé et aucun emplacement n'est spécifié.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

Le paramètre Chemin d'accès au dossier Documents doit être activé non seulement pour rediriger les fichiers vers le dossier Documents, mais aussi pour rediriger les fichiers vers les dossiers Musique, Images et Vidéos.

Paramètres de redirection du dossier Mes documents

Ce paramètre spécifie la manière de rediriger le contenu du dossier Documents.

Par défaut, le contenu est redirigé vers un chemin d'accès UNC.

Pour contrôler la manière de rediriger le contenu du dossier Documents, choisissez l'une des options suivantes :

- Rediriger vers le chemin UNC suivant. Redirections de contenu pour le chemin d'accès UNC spécifié dans le paramètre de stratégie Chemin d'accès au dossier Documents.
- Rediriger vers le répertoire de base de l'utilisateur. Redirections de contenu pour le répertoire de base utilisateur, généralement configuré en tant qu'attribut #homeDirectory# pour un utilisateur dans Active Directory.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

Télécharge les stratégies de groupe

January 23, 2019

La section Téléchargements contient les paramètres de stratégie destinés à spécifier si vous souhaitez rediriger le contenu du dossier Téléchargements vers un emplacement réseau partagé.

Chemin d'accès au dossier Téléchargements

Ce paramètre spécifie l'emplacement réseau vers lequel les fichiers du dossier Documents sont redirigés.

Par défaut, ce paramètre est désactivé et aucun emplacement n'est spécifié.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

Paramètres de redirection du dossier Téléchargements

Ce paramètre spécifie la redirection du contenu du dossier Téléchargements.

Par défaut, le contenu est redirigé vers un chemin d'accès UNC.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

Paramètres de stratégie Favoris

January 23, 2019

La section Favoris contient des paramètres de stratégie destinés à spécifier si vous souhaitez rediriger le contenu du dossier Favoris vers un emplacement réseau partagé.

Chemin d'accès au dossier Favoris

Ce paramètre spécifie l'emplacement réseau vers lequel le contenu du dossier Favoris est redirigé.

Par défaut, ce paramètre est désactivé et aucun emplacement n'est spécifié.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

Paramètres de redirection du dossier Favoris

Ce paramètre spécifie la façon de rediriger le contenu du dossier Favoris.

Par défaut, le contenu est redirigé vers un chemin d'accès UNC.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

Paramètres de stratégie Liens

November 9, 2018

La section Liens contient des paramètres de stratégie pour spécifier si vous souhaitez rediriger le contenu du dossier Liens vers un emplacement réseau partagé.

Chemin d'accès au dossier Liens

Ce paramètre spécifie l'emplacement réseau vers lequel le contenu du dossier Liens est redirigé.

Par défaut, ce paramètre est désactivé et aucun emplacement n'est spécifié.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

Paramètres de redirection du dossier Liens

Ce paramètre spécifie comment rediriger le contenu du dossier Liens.

Par défaut, le contenu est redirigé vers un chemin d'accès UNC.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

Paramètres de stratégie Musique

November 9, 2018

La section Musique contient les paramètres de stratégie pour spécifier si vous souhaitez rediriger le contenu du dossier Musique vers un emplacement réseau partagé.

Chemin d'accès au dossier Ma musique

Ce paramètre spécifie l'emplacement réseau vers lequel le contenu du dossier Musique est redirigé.

Par défaut, ce paramètre est désactivé et aucun emplacement n'est spécifié.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

Paramètres de redirection du dossier Ma musique

Ce paramètre spécifie comment rediriger le contenu du dossier Musique.

Par défaut, le contenu est redirigé vers un chemin d'accès UNC.

Pour contrôler comment rediriger le contenu du dossier Musique, choisissez l'une des options suivantes :

- Rediriger vers le chemin UNC suivant. Permet de rediriger du contenu vers le chemin d'accès UNC spécifié dans le paramètre de stratégie Chemin d'accès au dossier Musique.
- Rediriger en fonction du dossier Documents. Permet de rediriger du contenu vers un dossier relatif au dossier Documents.

Pour rediriger du contenu vers un dossier relatif au dossier Documents, le paramètre Chemin d'accès au dossier Documents doit être activé.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

Paramètres de stratégie Images

November 9, 2018

La section Images contient des paramètres de stratégie pour spécifier si vous souhaitez rediriger le contenu du dossier Images vers un emplacement réseau partagé.

Chemin d'accès au dossier Mes images

Ce paramètre spécifie l'emplacement réseau vers lequel le contenu du dossier Images est redirigé.

Par défaut, ce paramètre est désactivé et aucun emplacement n'est spécifié.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

Paramètres de redirection du dossier Mes images

Ce paramètre spécifie la façon de rediriger le contenu du dossier Images.

Par défaut, le contenu est redirigé vers un chemin d'accès UNC.

Pour contrôler la manière dont le contenu du dossier Images est redirigé, choisissez l'une des options suivantes :

- Rediriger vers le chemin UNC suivant. Permet de rediriger du contenu vers le chemin d'accès UNC spécifié dans le paramètre de stratégie Chemin d'accès au dossier Images.
- Rediriger en fonction du dossier Documents. Permet de rediriger du contenu vers un dossier relatif au dossier Documents.

Pour rediriger du contenu vers un dossier relatif au dossier Documents, le paramètre Chemin d'accès au dossier Documents doit être activé.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

Paramètres de stratégie Parties enregistrées

November 9, 2018

La section Parties enregistrées contient des paramètres de stratégie pour spécifier si vous souhaitez rediriger le contenu du dossier Parties enregistrées vers un emplacement réseau partagé.

Paramètres de redirection du dossier Parties enregistrées

Ce paramètre spécifie comment rediriger le contenu du dossier Parties enregistrées.

Par défaut, le contenu est redirigé vers un chemin d'accès UNC.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

Chemin d'accès au dossier Parties enregistrées

Ce paramètre spécifie l'emplacement réseau vers lequel le contenu du dossier Parties enregistrées est redirigé.

Par défaut, ce paramètre est désactivé et aucun emplacement n'est spécifié.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

Paramètres de stratégie Menu Démarrer

November 9, 2018

La section Menu Démarrer contient des paramètres de stratégie pour spécifier si vous souhaitez rediriger le contenu du dossier Menu Démarrer vers un emplacement réseau partagé.

Paramètres de redirection du menu Démarrer

Ce paramètre spécifie comment rediriger le contenu du dossier Menu Démarrer.

Par défaut, le contenu est redirigé vers un chemin d'accès UNC.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

Chemin d'accès au menu Démarrer

Ce paramètre spécifie l'emplacement réseau vers lequel le contenu du dossier Menu Démarrer est redirigé.

Par défaut, ce paramètre est désactivé et aucun emplacement n'est spécifié.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

Paramètres de stratégie Recherches

November 9, 2018

La section Recherches contient des paramètres de stratégie destinées à spécifier si vous souhaitez rediriger le contenu du dossier Recherches vers un emplacement réseau partagé.

Paramètres de redirection du dossier Recherches

Ce paramètre spécifie comment rediriger le contenu du dossier Recherches.

Par défaut, le contenu est redirigé vers un chemin d'accès UNC.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

Chemin d'accès au dossier Recherches

Ce paramètre spécifie l'emplacement réseau vers lequel le contenu du dossier Recherches est redirigé.

Par défaut, ce paramètre est désactivé et aucun emplacement n'est spécifié.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

Paramètres de stratégie Vidéo

November 9, 2018

La section Vidéo contient des paramètres de stratégie pour spécifier si vous souhaitez rediriger le contenu du dossier Vidéo vers un emplacement réseau partagé.

Paramètres de redirection pour la vidéo

Ce paramètre spécifie comment rediriger le contenu du dossier Vidéo.

Par défaut, le contenu est redirigé vers un chemin d'accès UNC.

Pour contrôler comment rediriger le contenu du dossier Vidéo, choisissez l'une des options suivantes :

- Rediriger vers le chemin UNC suivant. Permet de rediriger du contenu vers le chemin d'accès UNC spécifié dans le paramètre de stratégie Chemin d'accès au dossier Vidéo.
- Rediriger en fonction du dossier Documents. Permet de rediriger du contenu vers un dossier relatif au dossier Documents.

Pour rediriger du contenu vers un dossier relatif au dossier Documents, le paramètre Chemin d'accès au dossier Documents doit être activé.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

Chemin d'accès au dossier Vidéo

Ce paramètre spécifie l'emplacement réseau vers lequel le contenu du dossier Vidéo est redirigé.

Par défaut, ce paramètre est désactivé et aucun emplacement n'est spécifié.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

Paramètres de stratégie Journal

November 9, 2018

La section Journal contient des paramètres de stratégie permettant de configurer la journalisation Profile Management.

Actions Active Directory

Ce paramètre active ou désactive la journalisation détaillée des actions effectuées dans Active Directory.

Par défaut, ce paramètre est désactivé.

Lorsque vous activez ce paramètre, assurez-vous que le paramètre Activer la journalisation est également activé.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, les erreurs et les informations générales sont consignées.

Informations courantes

Ce paramètre active ou désactive la journalisation détaillée des informations courantes.

Par défaut, ce paramètre est désactivé.

Lorsque vous activez ce paramètre, assurez-vous que le paramètre Activer la journalisation est également activé.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, les erreurs et les informations générales sont consignées.

Avertissements courants

Ce paramètre active ou désactive la journalisation détaillée des avertissements courants.

Par défaut, ce paramètre est désactivé.

Lorsque vous activez ce paramètre, assurez-vous que le paramètre Activer la journalisation est également activé.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, les erreurs et les informations générales sont consignées.

Activer la journalisation

Ce paramètre active ou désactive la journalisation de Profile Management en mode (journalisation détaillée) de débogage. En mode de débogage, les informations d'état complètes sont journalisées dans les fichiers journaux situées dans "%SystemRoot%\System32\Logfiles\UserProfileManager".

Par défaut, ce paramètre est désactivé et seules les erreurs sont journalisées.

Citrix vous recommande d'activer ce paramètre uniquement si vous effectuez la résolution des problèmes de Profile Management.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, seules les erreurs sont consignées.

Actions du système de fichiers

Ce paramètre active ou désactive la journalisation détaillée des actions effectuées dans le système de fichiers.

Par défaut, ce paramètre est désactivé.

Lorsque vous activez ce paramètre, assurez-vous que le paramètre Activer la journalisation est également activé.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, les erreurs et les informations générales sont consignées.

Notifications du système de fichiers

Ce paramètre active ou désactive la journalisation détaillée des notifications des systèmes de fichiers.

Par défaut, ce paramètre est désactivé.

Lorsque vous activez ce paramètre, assurez-vous que le paramètre Activer la journalisation est également activé.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, les erreurs et les informations générales sont consignées.

Fermeture de session

Ce paramètre active ou désactive la journalisation détaillée des fermetures de session de l'utilisateur.

Par défaut, ce paramètre est désactivé.

Lorsque vous activez ce paramètre, assurez-vous que le paramètre Activer la journalisation est également activé.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, les erreurs et les informations générales sont consignées.

Ouverture de session

Ce paramètre active ou désactive la journalisation détaillée des ouvertures de session d'utilisateur.

Par défaut, ce paramètre est désactivé.

Lorsque vous activez ce paramètre, assurez-vous que le paramètre Activer la journalisation est également activé.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, les erreurs et les informations générales sont consignées.

Taille maximale du fichier journal

Ce paramètre spécifie la taille maximale autorisée pour le fichier journal de Profile Management, en octets.

Par défaut, ce paramètre est défini sur 1048576 octets (1Mo).

Citrix recommande d'augmenter la taille de ce fichier à 5 Mo ou plus, si vous disposez de suffisamment d'espace disque. Si le fichier journal dépasse la taille maximale, le fichier de sauvegarde existant (.bak) est supprimé, le fichier journal est renommé .bak et un nouveau fichier journal est créé.

Le fichier journal est créé dans %SystemRoot%\System32\Logfiles\UserProfileManager.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, la valeur par défaut est utilisée.

Chemin vers le fichier journal

Ce paramètre spécifie un chemin alternatif sur lequel enregistrer le fichier journal de Profile Management.

Par défaut, ce paramètre est désactivé et les fichiers journaux sont enregistrés à l'emplacement par défaut : %SystemRoot%\System32\Logfiles\UserProfileManager.

Le chemin peut pointer vers un lecteur local ou un lecteur réseau distant (chemin d'accès UNC). Les chemins d'accès distants peuvent s'avérer utiles dans les environnements de grande taille distribués, mais ils peuvent engendrer un volume important de trafic réseau, ce qui ne convient pas aux fichiers journaux. Pour les machines virtuelles pré-configurées dotées d'un disque dur persistant, définissez un chemin d'accès local à ce lecteur. Cela garantit la préservation des fichiers journaux lorsque la machine redémarre. Pour les machines virtuelles qui ne sont pas équipées d'un disque dur persistant, la définition d'un chemin d'accès UNC vous permet de conserver les fichiers journaux mais le compte système des machines doit disposer d'un accès en écriture au partage UNC. Utilisez un chemin d'accès local pour les ordinateurs portables gérés par la fonctionnalité de profils déconnectés.

Si un chemin d'accès UNC est utilisé pour les fichiers journaux, Citrix recommande d'appliquer une liste de contrôle d'accès appropriée au dossier du fichier journal de manière à ce que seuls les comptes d'ordinateur ou d'utilisateur autorisés puissent accéder aux fichiers stockés.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, l'emplacement par défaut %SystemRoot%\System32\Logfiles\UserProfileManager est utilisé.

Informations utilisateur personnalisées

Ce paramètre active ou désactive la journalisation détaillée des informations utilisateur personnalisées.

Par défaut, ce paramètre est désactivé.

Lorsque vous activez ce paramètre, assurez-vous que le paramètre Activer la journalisation est également activé.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, les erreurs et les informations générales sont consignées.

Valeurs de stratégie à l'ouverture et fermeture de session

Ce paramètre active ou désactive la journalisation détaillée des valeurs de stratégie lorsqu'un utilisateur ouvre ou ferme une session.

Par défaut, ce paramètre est désactivé.

Lorsque vous activez ce paramètre, assurez-vous que le paramètre Activer la journalisation est également activé.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, les erreurs et les informations générales sont consignées.

Actions du registre

Ce paramètre active ou désactive la journalisation détaillée des actions effectuées dans le Registre.

Par défaut, ce paramètre est désactivé.

Lorsque vous activez ce paramètre, assurez-vous que le paramètre Activer la journalisation est également activé.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, les erreurs et les informations générales sont consignées.

Différences de registre à la fermeture de session

Ce paramètre active ou désactive la journalisation détaillée des différences dans le registre lorsqu'un utilisateur ferme sa session.

Par défaut, ce paramètre est désactivé.

Lorsque vous activez ce paramètre, assurez-vous que le paramètre Activer la journalisation est également activé.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, les erreurs et les informations générales sont consignées.

Paramètres de stratégie Gestion des profils

February 28, 2019

La section Traitement des profils contient des paramètres de stratégie qui spécifient la manière dont Profile Management gère les profils utilisateur.

Délai avant la suppression des profils du cache

Ce paramètre spécifie une extension facultative pour le délai, en minutes, avant que Profile Management supprime les profils mis en cache localement à la fermeture de session.

Une valeur de 0 supprime les profils immédiatement, à la fin du processus de fermeture de session. Profile Management vérifie les fermetures de session toutes les minutes, ainsi une valeur de 60 garantit que les profils sont supprimés entre une et deux minutes après que les utilisateurs aient fermé leur session (en fonction du moment où la dernière vérification a été effectué). L'extension du délai est utile si vous savez qu'un processus conserve les fichiers ou que la ruche du Registre de l'utilisateur est ouverte durant la fermeture de session. Avec des profils importants, cela peut également accélérer la fermeture de session.

Par défaut, cette option est définie sur 0 et Profile Management supprime les profils mis en cache localement immédiatement.

Lorsque vous activez ce paramètre, assurez-vous que l'option Supprimer les profils mis en cache localement à la fermeture de session est également activée.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, les profils sont immédiatement supprimés.

Supprimer les profils mis en cache localement à la fermeture de session

Ce paramètre spécifie si les profils mis en cache localement sont supprimés après qu'un utilisateur ferme sa session.

Si ce paramètre est activé, le cache de profil local d'un utilisateur est supprimé après fermeture de leur session. Citrix vous recommande d'activer ce paramètre pour les serveurs Terminal Server.

Par défaut, ce paramètre est désactivé, le cache de profil local d'un utilisateur est conservé après la fermeture de session.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, les profils mis en cache ne sont pas supprimés.

Gestion des conflits de profils locaux

Ce paramètre configure le comportement de Profile Management si un profil utilisateur existe dans le magasin de l'utilisateur et en tant que profil utilisateur Windows local (pas un profil utilisateur Citrix).

Par défaut, Profile Management utilise le profil Windows local mais n'y apporte aucune modification.

Pour contrôler le comportement de Profile Management, choisissez l'une des options suivantes :

- Utiliser profil local. Profile Management utilise le profil local, mais n'y apporte aucune modification.
- Supprimer profil local. Profile Management supprime le profil utilisateur Windows local, puis importe le profil utilisateur Citrix à partir du magasin de l'utilisateur.
- Renommer profil local. Profile Management renomme le profil utilisateur Windows local (à des fins de sauvegarde) et importe le profil utilisateur Citrix à partir du magasin de l'utilisateur.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, les profils locaux existants sont utilisés.

Migration des profils existants

Ce paramètre spécifie les types de profil migrés vers le magasin de l'utilisateur lors de l'ouverture de session si un utilisateur ne dispose d'aucun profil courant dans le magasin de l'utilisateur.

Profile Management peut effectuer la migration des profils existants « à la volée » durant l'ouverture de session si l'utilisateur ne dispose d'aucun profil dans le magasin de l'utilisateur. Une fois ce processus terminé, le profil du magasin de l'utilisateur est utilisé par Profile Management dans la session en cours et toute autre session configurée avec le chemin d'accès au même magasin de l'utilisateur.

Par défaut, les profils locaux et itinérants sont migrés vers le magasin de l'utilisateur lors de l'ouverture de session.

Pour spécifier les types de profil migrés vers le magasin de l'utilisateur lors de l'ouverture de session, choisissez l'une des options suivantes :

- Profils locaux et itinérants
- Locaux

- Itinérance
- Aucun (désactivé)

Si vous sélectionnez Aucun, le système utilise le mécanisme Windows existant de création de nouveaux profils, comme dans un environnement dans lequel Profile Management n'est pas installé.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, les profils locaux et itinérants existants sont migrés.

Chemin d'accès au profil modèle

Ce paramètre spécifie le chemin d'accès au profil que vous souhaitez que Profile Management utilise comme modèle pour la création de nouveaux profils utilisateur.

Le chemin d'accès spécifié doit être le chemin d'accès complet au dossier contenant le fichier de registre NTUSER.DAT ainsi que tout autre dossier et fichier requis pour le profil modèle.

Remarque : n'incluez pas NTUSER.DAT dans le chemin d'accès. Par exemple, avec le fichier \\nomserveur\mesprofils\modèle\ntuser.dat, définissez l'emplacement en tant que \\nomserveur\mesprofils\mo

Utilisez des chemins d'accès absolus. Il peut s'agir de chemins UNC où de chemins sur la machine locale. Vous pouvez utiliser ces derniers pour spécifier, par exemple, un profil modèle de manière permanente sur une image Citrix Provisioning Services. les chemins d'accès relatifs ne sont pas pris en charge.

Remarque : ce paramètre ne prend pas en charge l'expansion d'attributs Active Directory, de variables d'environnement système ou des variables %USERNAME% et %USERDOMAIN%.

Par défaut, ce paramètre est désactivé et les nouveaux profils utilisateur sont créés à partir du profil utilisateur par défaut sur la machine sur laquelle un utilisateur ouvre une session.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, aucun modèle n'est utilisé.

Le profil modèle remplace le profil local

Ce paramètre active le profil modèle pour remplacer le profil local lors de la création de nouveaux profils utilisateur.

Si un utilisateur ne dispose d'aucun profil utilisateur Citrix, mais qu'un profil utilisateur Windows local existe, le profil local est utilisé par défaut (et migré vers le magasin de l'utilisateur, si ce paramètre n'est pas désactivé). L'activation de cette stratégie permet au profil modèle de remplacer le profil local utilisé lors de la création de nouveaux profils utilisateur.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, aucun modèle n'est utilisé.

Le profil modèle remplace le profil itinérant

Ce paramètre active le profil modèle pour remplacer un profil itinérant lors de la création de nouveaux profils utilisateur.

Si un utilisateur ne dispose d'aucun profil utilisateur Citrix, mais qu'un profil utilisateur Windows itinérant existe, le profil itinérant est utilisé par défaut (et migré vers le magasin de l'utilisateur, si ce paramètre n'est pas désactivé). L'activation de ce paramètre de stratégie permet au profil modèle de remplacer le profil itinérant utilisé lors de la création de nouveaux profils utilisateur.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, aucun modèle n'est utilisé.

Profil modèle utilisé en tant que profil Citrix obligatoire pour toutes les ouvertures de session

Ce paramètre permet d'activer Profile Management de manière à utiliser le profil modèle comme profil par défaut pour la création de tous les nouveaux profils utilisateur.

Par défaut, ce paramètre est désactivé et les nouveaux profils utilisateur sont créés à partir du profil utilisateur par défaut sur la machine sur laquelle un utilisateur ouvre une session.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, aucun modèle n'est utilisé.

Paramètres de stratégie Registre

November 9, 2018

La section Registre contient des paramètres de stratégie permettant de spécifier les clés de Registre qui sont inclues et exclues du traitement Profile Management.

Liste d'exclusion

Ce paramètre spécifie la liste des clés de registre dans la ruche HKCU exclues du traitement Profile Management lorsqu'un utilisateur ferme sa session.

Lorsque cette option est activée, des clés spécifiées dans cette liste sont exclues du traitement lorsqu'un utilisateur ferme sa session.

Par défaut, ce paramètre est désactivé, et toutes les clés de registre dans la ruche HKCU sont traitées lorsqu'un utilisateur ferme sa session.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, aucune clé de registre n'est exclue du traitement.

Liste d'inclusion

Ce paramètre spécifie la liste des clés de registre dans la ruche HKCU inclues dans le traitement Profile Management lorsqu'un utilisateur ferme sa session.

Lorsqu'il est activé, seules les clés spécifiées dans cette liste sont traitées lorsqu'un utilisateur ferme sa session.

Par défaut, ce paramètre est désactivé, et toutes les clés de registre dans la ruche HKCU sont traitées lorsqu'un utilisateur ferme sa session.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, toutes les entrées de HKCU sont traitées.

Paramètres de stratégie Profils utilisateur streamés

November 9, 2018

La section Profils utilisateur streamés contient des paramètres de stratégie spécifiant la manière dont Profile Management traite les profils utilisateur livrés en streaming.

Toujours mettre en cache

Ce paramètre spécifie si Profile Management met en cache les fichiers streamés dès que possible après qu'un utilisateur ouvre une session. La mise en cache de fichiers après qu'un utilisateur ouvre une session économise de la bande passante réseau, améliorant ainsi l'expérience utilisateur.

Utilisez ce paramètre avec le paramètre Streaming des profils.

Par défaut, ce paramètre est désactivé et les fichiers streamés ne sont pas mis en cache dès que possible après qu'un utilisateur ouvre une session.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, il est désactivé.

Toujours mettre en cache la taille

Ce paramètre spécifie une limite inférieure, en méga-octets, à la taille des fichiers streamés. Profile Management met en cache les fichiers de taille égale ou supérieure dès que possible après qu'un utilisateur ouvre une session.

Par défaut, cette option est définie sur 0 (zéro) et la fonctionnalité de mise en cache du profil entier est utilisée. Lorsque la fonctionnalité de mise en cache du profil entier est activée, Profile Management récupère le contenu des profils dans le magasin de l'utilisateur, lorsqu'un utilisateur ouvre une session, en arrière-plan.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, il est désactivé.

Streaming des profils

Ce paramètre active ou désactive la fonctionnalité de profils utilisateur streamés Citrix. Lorsqu'il est activé, les fichiers et les dossiers contenus dans un profil sont récupérés depuis le magasin de l'utilisateur sur l'ordinateur local uniquement lorsque les utilisateurs y accèdent après avoir ouvert une session. Les entrées de registre et les fichiers dans la zone d'attente sont récupérés immédiatement.

Par défaut, le streaming des profils est désactivé.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, il est désactivé.

Groupes des profils utilisateurs streamés

Ce paramètre spécifie les profils utilisateur qui sont livrés en streaming au sein d'une unité d'organisation, en fonction des groupes d'utilisateurs Windows.

Lorsque ce paramètre est activé, seuls les profils utilisateur dans les groupes d'utilisateurs spécifiés sont livrés en streaming. Tous les autres profils utilisateur sont traités normalement.

Par défaut, ce paramètre est désactivé et tous les profils utilisateur au sein d'une unité d'organisation sont traités normalement.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, tous les profils utilisateur sont traités.

Pour activer l'exclusion du streaming des profils

Lorsque l'exclusion du streaming des profils est activée, Profile Management ne livre pas en streaming les dossiers spécifiés dans la liste d'exclusion et tous les dossiers sont récupérés immédiatement depuis le magasin de l'utilisateur vers l'ordinateur local lorsqu'un utilisateur ouvre une session.

Pour plus d'informations, consultez la section Pour activer l'exclusion du streaming des profils.

Délai d'expiration des fichiers de verrous de la zone d'attente

Ce paramètre spécifie la période (en jours) après laquelle les fichiers des utilisateurs sont écrits dans le magasin de l'utilisateur à partir de la zone d'attente au cas où le magasin de l'utilisateur reste verrouillé lorsqu'un serveur ne répond plus. Cela évite l'engorgement dans la zone d'attente et garantit que le magasin de l'utilisateur contient toujours la dernière version des fichiers.

Par défaut, ce paramètre est défini sur 1 (un) jour.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, la valeur par défaut est utilisée.

Paramètres de stratégie Receiver

November 9, 2018

Remarque : sauf spécification contraire, « Receiver » fait référence à Citrix Receiver.

La section Receiver contient des paramètres de stratégie qui spécifient une liste d'adresses StoreFront à distribuer vers Citrix Receiver pour Windows exécuté sur le bureau virtuel.

Liste de comptes StoreFront

Ce paramètre spécifie une liste d'administrateurs de magasins StoreFront qui peuvent choisir de distribuer Citrix Receiver pour Windows exécuté sur le bureau virtuel. Lors de la création d'un groupe de mise à disposition, les administrateurs peuvent sélectionner les magasins pour distribuer Citrix Receiver pour Windows exécuté sur des bureaux virtuels dans ce groupe.

Par défaut, aucun magasin n'est spécifié.

Pour chaque magasin, spécifiez les informations suivantes en tant qu'entrée séparés par des points-virgules :

- Nom du magasin. Le nom affiché pour les utilisateurs du magasin.
- Adresse URL du magasin. L'adresse URL du magasin.

- État activé du magasin. Indique si le magasin est disponible ou non pour les utilisateurs. Ceci est activé ou désactivé.
- Description du magasin. La description affichée pour les utilisateurs du magasin.

Par exemple : Magasin des ventes;`https:`//sales.mycompany.com/Citrix/Store/discovery;On;Store Personnel des ventes

Paramètres de stratégie Virtual Delivery Agent

November 9, 2018

La section Virtual Delivery Agent (VDA) contient des paramètres de stratégie qui contrôlent les communications entre le VDA et les contrôleurs d'un site.

Important : le VDA requiert des informations fournies par ces paramètres pour s'enregistrer auprès d'un Delivery Controller, si vous n'utilisez pas la fonctionnalité de mise à jour automatique. Comme ces informations sont requises pour l'enregistrement, vous devez configurer les paramètres suivants avec l'éditeur de stratégie de groupe, à moins que vous ne fournissiez ces informations pendant l'installation du VDA :

- Masque réseau IPv6 d'enregistrement du contrôleur
- Port d'enregistrement du contrôleur
- SID de contrôleur
- Controller
- Uniquement utiliser l'enregistrement du contrôleur IPv6
- GUID de site

Masque réseau IPv6 d'enregistrement du contrôleur

Ce paramètre de stratégie permet aux administrateurs de restreindre le VDA uniquement à un sous-réseau favori (plutôt qu'une adresse IP globale, si elle est enregistrée). Ce paramètre spécifie l'adresse IPv6 et le réseau où le VDA s'enregistrera. Le VDA s'enregistre uniquement sur la première adresse qui correspond au masque de sous-réseau spécifié. Ce paramètre est uniquement valide si le paramètre de stratégie Uniquement utiliser l'enregistrement du contrôleur IPv6 est activé.

Par défaut, ce paramètre est vide.

Port d'enregistrement du contrôleur

Utilisez ce paramètre uniquement si le paramètre de stratégie Activer la mise à jour automatique des contrôleurs est désactivé.

Ce paramètre spécifie le numéro de port TCP/IP que le VDA utilise pour s'enregistrer auprès d'un Controller, en cas d'utilisation de l'enregistrement basé sur le registre.

Le numéro port est défini par défaut sur 80.

SID de contrôleur

Utilisez ce paramètre uniquement si le paramètre de stratégie Activer la mise à jour automatique des contrôleurs est désactivé.

Ce paramètre spécifie une liste d'identificateurs de sécurité (SID) de Controller séparés par des espaces que le VDA utilise pour s'enregistrer auprès d'un Controller, en cas d'utilisation de l'enregistrement basé sur le registre. Il s'agit d'un paramètre facultatif, qui peut être utilisé avec le paramètre Contrôleurs pour limiter la liste des contrôleurs utilisés pour l'enregistrement.

Par défaut, ce paramètre est vide.

Controller

Utilisez ce paramètre uniquement si le paramètre de stratégie Activer la mise à jour automatique des contrôleurs est désactivé.

Ce paramètre spécifie une liste de noms de domaines complets (FQDN) de contrôleurs séparés par des espaces que le VDA utilise pour s'enregistrer auprès d'un Controller, en cas d'utilisation de l'enregistrement basé sur le registre. Il s'agit d'un paramètre facultatif, qui peut être utilisé avec le paramètre SID de Controller.

Par défaut, ce paramètre est vide.

Activer la mise à jour automatique des contrôleurs

Ce paramètre permet d'activer le VDA pour s'enregistrer auprès d'un Controller automatiquement après l'installation.

Après l'enregistrement du VDA, le Controller auquel il s'enregistre envoie une liste des domaines complets (FQDN) et le SID de ce contrôleur au VDA Le VDA inscrit cette liste dans le stockage permanent. Chaque Controller vérifie également la base de données du site toutes les 90 minutes pour des informations sur le Controller ; si un Controller a été ajouté ou supprimé depuis la dernière vérification ou, si une modification de stratégie s'est produite, le Controller envoie les listes mises à jour vers les VDA enregistrés. Le VDA acceptera les connexions provenant de tous les Controller figurant dans la dernière liste reçue.

Ce paramètre est activé par défaut.

Uniquement utiliser l'enregistrement du contrôleur IPv6

Ce paramètre détermine le format d'adresse utilisé par le VDA pour s'enregistrer avec le Controller :

- lorsque cette option est activée, le VDA s'enregistre auprès du Controller à l'aide de l'adresse IPv6 de la machine. Lorsque le VDA communique avec le Controller, il utilise l'ordre d'adresse suivant : adresse IP globale, adresse locale unique (ULA), adresse locale au lien (si aucune autre adresse IPv6 n'est disponible).
- Lorsque cette stratégie est désactivée, le VDA s'enregistre et communique avec le Controller à l'aide de l'adresse IPv4 de la machine.

Par défaut, ce paramètre est désactivé.

GUID de site

Utilisez ce paramètre uniquement si le paramètre de stratégie Activer la mise à jour automatique des contrôleurs est désactivé.

Ce paramètre spécifie le GUID (Globally Unique Identifier) du site que le VDA utilise pour s'enregistrer auprès d'un Controller en cas d'utilisation de l'enregistrement à partir d'Active Directory.

Par défaut, ce paramètre est vide.

Paramètres de stratégie HDX 3D Pro

November 9, 2018

La section HDX 3D Pro contient des paramètres de stratégie permettant d'activer et de configurer l'outil de configuration de la qualité d'image pour vos utilisateurs. Cet outil permet aux utilisateurs d'optimiser l'utilisation de la bande passante disponible en ajustant en temps réel l'équilibre entre la qualité d'image et le temps de réponse.

Activer sans perte

Ce paramètre détermine si les utilisateurs peuvent ou non activer ou désactiver la compression sans perte à l'aide de l'outil de configuration de la qualité d'image. Par défaut, les utilisateurs n'ont pas la possibilité d'activer la compression sans perte.

Lorsqu'un utilisateur active la compression sans perte, la qualité d'image est automatiquement définie sur la valeur maximale disponible dans l'outil de configuration de la qualité d'image. Par défaut, il est possible d'utiliser la compression basée sur le processeur graphique ou sur l'UC, en fonction des possibilités de la machine utilisateur et de l'ordinateur hôte.

Paramètres de qualité HDX 3D Pro

Ce paramètre spécifie les valeurs maximale et minimale qui déterminent la plage de réglages de la qualité d'image accessible aux utilisateurs dans l'outil de configuration de la qualité d'image.

Indiquez des valeurs de qualité entre 0 et 100 (inclus). La valeur maximale doit être supérieure ou égale à la valeur minimale.

Paramètres de stratégie Surveillance

November 9, 2018

La section Surveillance contient des paramètres de stratégie pour la surveillance des processus, des ressources et des échecs d'application.

L'étendue de ces stratégies peut être définie en fonction du site, du groupe de mise à disposition, du type de groupe de mise à disposition, de l'unité d'organisation et de balises.

Stratégies pour la surveillance des processus et des ressources

Chaque point de données pour l'UC, la mémoire et les processus est collecté depuis le VDA et stocké dans la base de données de surveillance. L'envoi de points de données depuis le VDA consomme de la bande passante réseau et leur stockage occupe énormément d'espace sur la base de données de surveillance. Si vous ne souhaitez pas surveiller les données de ressources ou de processus ou les deux pour une étendue spécifique (par exemple, un groupe de mise à disposition ou une unité d'organisation), il est recommandé de désactiver la stratégie.

Activer le suivi des processus

Activez ce paramètre pour autoriser le suivi des processus en cours d'exécution sur des machines avec VDA. Les statistiques telles que l'utilisation d'UC et de mémoire sont envoyées au service de surveillance. Les statistiques sont utilisées à des fins de notification en temps réel et pour générer des rapports historiques dans Director.

Par défaut, ce paramètre est désactivé.

Activer le suivi des ressources

Activez ce paramètre pour permettre le suivi des compteurs de performance critiques sur les machines équipées de VDA. Les statistiques (telles que l'utilisation d'UC et de mémoire, les données de nombre d'E/S par seconde et de latence de disque) sont envoyées au service de surveillance. Les statistiques

sont utilisées à des fins de notification en temps réel et pour générer des rapports historiques dans Director.

Par défaut, ce paramètre est activé.

Capacité à monter en charge

Les données d'UC et de mémoire sont transmises à la base de données à partir de chaque VDA à des intervalles de 5 minutes ; les données de processus (si activées) sont transmises à la base de données à des intervalles de 10 minutes. Les données d'E/S par seconde et de latence de disque sont transmises à la base de données à intervalles réguliers d'1 heure.

Données d'UC et de mémoire

Les données d'UC et de mémoire sont **activées** par défaut. Les valeurs de rétention des données sont les suivantes (licence Platinum) :

Granularité des données	Nombre de jours
5 minutes	1 jour
10 minutes	7 jours
1 heure	30 jours
1 jour	90 jours

Données E/S par seconde et latence de disque

Les données E/S par seconde et latence de disque sont **activées** par défaut. Les valeurs de rétention des données sont les suivantes (licence Platinum) :

Granularité des données	Nombre de jours
1 heure	3 jours
1 jour	90 jours

Avec les paramètres de rétention des données ci-dessus, environ 276 Ko d'espace disque est nécessaire pour stocker les données d'UC, de mémoire, d'E/S par seconde et de latence de disque pour un VDA sur une période d'un an.

Nombre de machines	Stockage requis (valeur approximative)
1	276 Ko
1 K	270 Mo
40 K	10,6 Go

Données de processus

Les données de processus sont **désactivées** par défaut. Il est recommandé d'activer les données de processus sur un sous-ensemble de machines si nécessaire. Les paramètres de rétention des données par défaut sont les suivants :

Granularité des données	Nombre de jours
10 minutes	1 jour
1 heure	7 jours

Si les données de processus sont activées, avec les paramètres de rétention par défaut, les données de processus pourraient utiliser environ 1,5 Mo par VDA et 3 Mo par VDA Terminal Services (VDA TS) sur une période d'un an.

Nombre de machines	Stockage requis pour VDA (valeur approximative)	Stockage requis pour VDA TS (valeur approximative)
1	1.5 Mo	3 Mo
1 000	1.5 Go	3 Go

> **Remarque**
>
> Les chiffres ci-dessus n'incluent pas l'espace d'index. Et tous les calculs ci-dessus sont approximatifs et peuvent varier en fonction du déploiement.

Configurations facultatives

Vous pouvez modifier les paramètres de rétention par défaut en fonction de vos besoins. Toutefois, cela consomme davantage de stockage. En activant les paramètres ci-dessous, vous pouvez obtenir plus de précision dans les données d'utilisation des processus. Les configurations pouvant être activées sont les suivantes :

EnableMinuteLevelGranularityProcessUtilization

EnableDayLevelGranularityProcessUtilization

Ces configurations peuvent être activées à partir de l'applet de commande PowerShell : Set-MonitorConfiguration

Stratégies pour la détection des défaillances applicatives

Par défaut, l'onglet **Échec applicatifs** affiche uniquement les échecs applicatifs de VDA avec OS de serveur. Les paramètres de détection des défaillances applicatives peuvent être modifiés avec les stratégies de surveillance suivantes :

Activer la détection des défaillances applicatives

Utilisez ce paramètre pour configurer la surveillance d'échecs applicatifs pour détecter les erreurs ou les défaillances d'application (plantages et exceptions non prises en charge) ou les deux.
Désactivez la détection des défaillances applicatives en définissant la **valeur** sur **Aucun**.
La valeur par défaut pour ce paramètre est Défaillances applicatives uniquement.

Activer la détection des défaillances applicatives sur les VDA d'OS de bureau

Par défaut, seuls les échecs d'applications hébergées sur des VDA avec OS de serveur sont détectés. Pour contrôler les VDA avec OS de bureau, définissez la stratégie sur **Autorisé**.
La valeur par défaut est **Interdit**.

Liste des applications exclues de la détection des défaillances

Spécifiez une liste des applications qui ne doivent pas être contrôlées.
Par défaut, cette liste est vide.

Conseils pour la planification du stockage

Stratégie de groupe. Si vous ne souhaitez pas surveiller les données de ressources ou de processus, vous pouvez les désactiver à l'aide de la stratégie de groupe. Pour de plus amples informations, consultez la section Créer des stratégies.

Nettoyage des données. Les paramètres de rétention des données par défaut peuvent être modifiés pour nettoyer les données et libérer de l'espace de stockage. Pour de plus amples informations sur

les paramètres de nettoyage, consultez la section Granularité de données et rétention dans Accès aux données à l'aide de l'API.

Paramètres de stratégie Adresse IP virtuelle

November 9, 2018

La section Adresse IP virtuelle contient des paramètres de stratégie permettant de contrôler si les sessions ont leur propre adresse virtuelle de bouclage.

Prise en charge du bouclage d'adresse IP virtuelle

Lorsque ce paramètre est activé, chaque session possède sa propre adresse virtuelle de bouclage. Lorsqu'il est désactivé, les sessions n'ont pas d'adresses de bouclage individuelles.

Par défaut, ce paramètre est désactivé.

Liste de programmes de bouclage virtuel d'adresse IP virtuelle

Ce paramètre spécifie les exécutables d'application susceptibles d'utiliser les adresses de bouclage virtuelles. Lorsque vous ajoutez des programmes à la liste, spécifiez uniquement le nom de l'exécutable, vous ne devez pas spécifier le chemin d'accès complet.

Par défaut, aucun exécutable n'est spécifié.

Configurer les paramètres de redirection du port COM et LPT à l'aide du Registre

November 9, 2018

Dans les versions VDA 7.0 à 7.8, les paramètres du port COM et LPT sont uniquement configurables à l'aide du Registre. Pour les versions VDA antérieures à la version 7.0 et les VDA 7.9 et versions ultérieures, ces paramètres sont configurables dans Studio. Pour de plus amples informations, consultez la section Paramètres de stratégie de redirection de port et Paramètres de stratégie de bande passante.

Les paramètres de stratégie pour la redirection du port COM et du port LPT sont situés sous HKLM\Software\Citrix\GroupPolicy\Defaults\Deprecated sur l'image ou la machine VDA.

Pour activer la redirection des ports COM et LPT, ajoutez de nouvelles clés de Registre de type REG_DWORD, comme suit :

Avertissement : toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Clé de Registre	Description	Valeurs autorisées
AllowComPortRedirection	Autoriser ou interdire la redirection de port COM	1 (Autoriser) ou 0 (Interdire)
LimitComBw	Limite de bande passante pour le canal de redirection du port COM	Valeur numérique
LimitComBWPercent	Limite de bande passante pour le canal de redirection du port COM sous forme de pourcentage de la bande passante totale de session	Valeur numérique comprise entre 0 et 100
AutoConnectClientComPorts	Connecter automatiquement les ports COM de la machine utilisateur	1 (Autoriser) ou 0 (Interdire)
AllowLptPortRedirection	Autoriser ou interdire la redirection de port LPT	1 (Autoriser) ou 0 (Interdire)
LimitLptBw	Limite de bande passante pour le canal de redirection du port LPT	Valeur numérique
LimitLptBwPercent	Limite de bande passante pour le canal de redirection du port LPT sous forme de pourcentage de la bande passante totale de session	Valeur numérique comprise entre 0 et 100
AutoConnectClientLptPorts	Connecter automatiquement les ports LPT de la machine utilisateur	1 (Autoriser) ou 0 (Interdire)

Après la configuration de ces paramètres, modifiez les catalogues de machines pour utiliser la nouvelle image principale ou la machine physique mise à jour. Les bureaux sont mis à jour avec les nouveaux paramètres lors de la fermeture de session suivante.

Paramètres de stratégie de Connector pour Configuration Manager 2012

November 9, 2018

La section Connector pour Configuration Manager 2012 contient des paramètres de stratégie pour la configuration de l'agent Citrix Connector 7.5.

Important : les stratégies d'avertissement, de fermeture de session et de message de redémarrage s'appliquent uniquement aux déploiements de catalogues de machines avec OS de serveur qui sont gérés manuellement ou par Provisioning Services Pour ces catalogues de machines, le service Connector alerte les utilisateurs lorsqu'ils sont en attente d'une installation d'application ou de mises à jour logicielles.

Pour les catalogues gérés par MCS, utilisez Studio pour avertir les utilisateurs. Pour gérer des catalogues avec OS de bureau manuellement, utilisez le gestionnaire de configuration pour avertir les utilisateurs. Pour des catalogues avec OS de bureau gérés par Provisioning Services, utilisez Provisioning Services pour avertir les utilisateurs.

Intervalle de fréquence de notification préalable

Ce paramètre définit l'intervalle entre les apparitions du message d'avertissement avancé auprès des utilisateurs.

Les intervalles sont définis selon le format jjj.hh:mm:ss, où :

- jjj représente les jours, un paramètre facultatif, avec une plage de 0 à 999.
- hh représente les heure avec une plage de 0 à 23.
- mm représente les minutes avec une plage de 0 à 59.
- ss représente les secondes avec une plage de 0 à 59.

Par défaut, le paramètre d'intervalle est de 1 heure (01:00:00).

Texte du corps de la zone de message de notification préalable

Ce paramètre contient le texte modifiable du message qui s'affiche aux utilisateurs pour les notifier de mises à jour logicielles ou de tâches de maintenance à venir nécessitant qu'ils ferment leur session.

Par défaut, le message est : {TIMESTAMP} Please save your work. Le serveur sera placé en mode déconnecté à des fins de maintenance dans {TIMELEFT}.

Titre de la zone de message de notification préalable

Ce paramètre contient le texte modifiable de la barre de titre du message d'avertissement avancé pour les utilisateurs.

Par défaut, le titre est Upcoming Maintenance.

Période de notification préalable

Ce paramètre définit combien de temps avant la maintenance où le premier message d'avertissement avancé s'affiche.

Le temps est défini selon le format jjj.hh:mm:ss, où :

- jjj représente les jours, un paramètre facultatif, avec une plage de 0 à 999.
- hh représente les heure avec une plage de 0 à 23.
- mm représente les minutes avec une plage de 0 à 59.
- ss représente les secondes avec une plage de 0 à 59.

Par défaut, le paramètre est de 16 heures (16:00:00), ce qui indique que le premier message d'avertissement avancé s'affiche approximativement 16 heures avant la maintenance.

Texte du corps de la zone de message de fermeture de session forcée finale

Ce paramètre contient le texte modifiable du message alertant les utilisateurs qu'une ouverture de session forcée a commencé.

Par défaut, le message est : The server is currently going offline for maintenance (Le serveur est actuellement en mode déconnecté pour maintenance).

Titre de la zone de message de fermeture de session forcée finale

Ce paramètre contient le texte modifiable de la barre de titre du message final de fermeture de session forcée.

Par défaut, le titre est : Notification From IT Staff (Notification du personnel informatique).

Obliger la fermeture de session de la période de grâce

Ce paramètre définit la période de temps entre la notification de fermer leur session aux utilisateurs et l'implémentation de la fermeture de session forcée pour traiter la maintenance en attente.

Le temps est défini selon le format jjj.hh:mm:ss, où :

- jjj représente les jours, un paramètre facultatif, avec une plage de 0 à 999.
- hh représente les heure avec une plage de 0 à 23.
- mm représente les minutes avec une plage de 0 à 59.
- ss représente les secondes avec une plage de 0 à 59.

Par défaut, le paramètre force logoff grace period est de 5 minutes (00:05:00).

Texte du corps de la zone de message de fermeture de session forcée

Ce paramètre contient le texte modifiable du message demandant aux utilisateurs d'enregistrer leur travail et de fermer leur session avant le début d'une fermeture de session forcée.

Par défaut, le message contient ce qui suit : {TIMESTAMP}Please save your work and log off (Veuillez enregistrer votre travail et fermer votre session). Le serveur sera placé en mode déconnecté à des fins de maintenance dans {TIMELEFT}.

Titre de la zone de message de fermeture de session forcée

Ce paramètre contient le texte modifiable de la barre de titre du message de fermeture de session forcée.

Par défaut, le titre est : Notification From IT Staff (Notification du personnel informatique).

Mode d'image gérée

L'agent Connector détecte automatiquement s'il est en cours d'exécution sur une machine clone gérée par Provisioning Services ou MCS. L'agent bloque de l'agent les mises à jour Configuration Manager sur les clones dont l'image est gérée et installe automatiquement les mises à jour sur l'image principale du catalogue.

Après mise à jour d'une image principale, utilisez Studio pour orchestrer le redémarrage des clones de catalogue MCS. L'Agent du Connector orchestre automatiquement le redémarrage des clones du catalogue PVS lors des fenêtres de maintenance Configuration Manager. Pour remplacer ce comportement afin que le logiciel soit installé sur des clones de catalogue par Configuration Manager, changez le mode Image gérée en Désactivé.

Texte du corps de la zone de message de redémarrage

Ce paramètre contient le texte modifiable du message notifiant les utilisateurs lorsque le serveur est sur le point d'être redémarré.

Par défaut, le message est : The server is currently going offline for maintenance (Le serveur est actuellement en mode déconnecté pour maintenance).

Intervalle de temps régulier durant lequel la tâche d'agent doit être exécutée

Ce paramètre détermine la fréquence d'exécution de la tâche d'agent Citrix Connector.

Le temps est défini selon le format jjj.hh:mm:ss, où :

- jjj représente les jours, un paramètre facultatif, avec une plage de 0 à 999.
- hh représente les heure avec une plage de 0 à 23.
- mm représente les minutes avec une plage de 0 à 59.
- ss représente les secondes avec une plage de 0 à 59.

Par défaut, le paramètre d'intervalle de temps régulier est de 5 minutes (00:05:00).

Gérer

February 28, 2019

La gestion d'un site XenApp ou XenDesktop couvre un grand nombre d'éléments et de tâches.

Licences

Une connexion valide avec le serveur de licences Citrix est requise lorsque vous créez un site. Plus tard, vous pourrez effectuer plusieurs opérations de gestion de licences à partir de Studio, y compris l'ajout de licences, la modification des types ou modèles de licences et la gestion des administrateurs de licences. Vous pourrez également accéder à la console License Administration Console à partir de Studio.

Applications

Permet de gérer les applications dans les groupes de mise à disposition et éventuellement, les groupes d'applications.

Zones

Dans un déploiement réparti sur différents sites géographiques, vous pouvez utiliser des zones pour que les applications et les bureaux se trouvent à proximité des utilisateurs finaux, ce qui peut améliorer les performances. Lorsque vous installez et configurez un site, tous les Controller, les catalogues de machines et les connexions hôtes se trouvent dans une zone principale. Plus tard, vous pourrez utiliser Studio pour créer des zones satellite contenant ces éléments. Une fois que votre site comporte plusieurs zones, vous pouvez indiquer dans quelle zone les catalogues de machines et les connexions hôtes créés ou les Controller ajoutés doivent être placés. Vous pouvez aussi déplacer les éléments entre les zones.

Connexions et ressources

Si vous utilisez un hyperviseur ou un service de cloud pour héberger les machines qui mettront à disposition les applications et les bureaux auprès des utilisateurs, vous devez créer votre première

connexion à l'hyperviseur ou au service de cloud lorsque vous créez un site. Les détails de stockage et de réseau constituent les *ressources* de cette connexion. Plus tard, vous pourrez modifier la connexion et ses ressources, et créer de nouvelles connexions. Vous pourrez également gérer les machines qui utilisent une connexion configurée.

Cache d'hôte local

Le cache d'hôte local permet aux opérations de négociation de connexion d'un site de se poursuivre lorsque la connexion entre un Delivery Controller et la base de données du site échoue. Il s'agit de la fonctionnalité de haute disponibilité la plus complète proposée par Citrix pour XenApp et XenDesktop.

Location de connexion

Citrix vous recommande d'utiliser le cache d'hôte local à la place de la location de connexion. Le cache d'hôte local est une solution plus puissante.

Adresse IP virtuelle et bouclage virtuel

La fonctionnalité d'adresse IP virtuelle Microsoft fournit une application publiée avec une adresse IP unique attribuée dynamiquement à chaque session. La fonctionnalité de bouclage virtuel Citrix vous permet également de configurer des applications qui dépendent des communications avec localhost (127.0.0.1 par défaut) pour utiliser une adresse de bouclage virtuel unique dans la plage localhost (127.*).

Delivery Controller

Cet article décrit les considérations et procédures lors de l'ajout et de la suppression de Controller à partir d'un site. Il décrit également comment déplacer des Controller vers une autre zone ou un autre site et comment déplacer un VDA vers un autre site.

Enregistrement d'un VDA auprès d'un Controller

Avant qu'un VDA puisse effectuer la mise à disposition d'applications et de bureaux, il doit s'enregistrer (établir la communication) auprès d'un Controller. Les adresses de Controller peuvent être spécifiées de plusieurs façons, lesquelles sont décrites dans cet article. Il est d'une importance critique que les VDA obtiennent des informations actualisées au fur et à mesure que des Controller sont ajoutés, déplacés et supprimés sur le site.

Sessions

La gestion de l'activité de session est critique pour offrir la meilleure expérience utilisateur possible. Plusieurs fonctionnalités peuvent optimiser la fiabilité des sessions, réduire les désagréments, les temps d'arrêt et la perte de productivité.

- Fiabilité de session
- Reconnexion automatique des clients
- Persistance ICA
- Le contrôle de l'espace de travail

- Itinérance de session

Utilisation de la fonction de recherche dans Studio

Lorsque vous souhaitez afficher des informations sur les machines, sessions, catalogues de machines, applications ou groupes de mise à disposition dans Studio, vous pouvez utiliser la fonctionnalité de recherche flexible.

Balises

Utilisez des balises pour identifier des éléments tels que des machines, applications, groupes et stratégies. Vous pouvez ensuite configurer certaines opérations pour qu'elles s'appliquent aux éléments avec une balise spécifique.

IPv4/IPv6

XenApp et XenDesktop prend en charge les déploiements IPv4 purs, IPv6 purs et double pile qui utilisent des réseaux IPv4 et IPv6 qui se chevauchent. Cet article décrit et illustre ces déploiements. Il décrit également les paramètres de stratégie Citrix qui contrôlent l'utilisation de IPv4 ou IPv6.

Profils utilisateur

Par défaut, Citrix Profile Management est installé automatiquement lorsque vous installez un VDA. Si vous utilisez cette solution de gestion des profils, consultez cet article pour des informations générales et reportez-vous à la documentation relative à Profile Management pour plus de détails.

Accéder à Citrix Insight Services

Citrix Insight Services (CIS) est une plate-forme Citrix depuis laquelle vous pouvez générer des informations d'instrumentation, de télémétrie et autres données stratégiques.

Licences

January 23, 2019

> **Remarque**
>
> Studio et Director ne prennent pas en charge le serveur de licences Citrix VPX. Pour de plus amples informations sur le serveur de licences Citrix VPX, consultez la documentation relative au système de licences Citrix.

Vous pouvez utiliser Studio pour gérer et suivre les licences, à condition que le serveur de licences se trouve dans le même domaine que Studio, ou dans un domaine approuvé. Pour de plus amples informations sur les autres tâches liées aux licences, consultez la documentation relative au système de licences et Licences multitypes.

Vous devez être un administrateur de licence complet pour effectuer les tâches décrites ci-dessous, à l'exception de l'affichage des informations de licence. Pour afficher les informations de licence dans

Studio, un administrateur doit avoir au moins l'autorisation d'administration déléguée de licence en lecture ; l'Administrateur complet intégré et des rôles d'administrateur en lecture seule ont cette autorisation.

Le tableau suivant dresse la liste des versions prises en charge et les modèles de licences :

Produits	Éditions	Modèles de licence
XenApp	Platinum, Enterprise, Advanced	Simultanée
XenDesktop	Platinum, Enterprise, App, VDI	Utilisateur/machine, Utilisateurs simultanés

Pour afficher les informations de licence, sélectionnez **Configuration > Licences** dans le panneau de navigation de Studio. Un récapitulatif de l'utilisation des licences et des paramètres du site est affiché, ainsi qu'une liste de toutes les licences actuellement installées sur le serveur de licences spécifié.

Pour télécharger une licence Citrix :

1. Sélectionnez **Configuration > Licences** dans le volet de navigation de Studio.
2. Sélectionnez **Allouer des licences** dans le volet Actions.
3. Entrez le code d'accès aux licences que Citrix vous a envoyé par e-mail.
4. Sélectionnez un produit et cliquez sur **Allouer des licences**. Toutes les licences disponibles pour ce produit sont allouées et téléchargées. Veuillez noter qu'après avoir alloué et téléchargé toutes les licences pour un code d'accès aux licences spécifique, vous ne pouvez plus utiliser ce code. Si vous devez effectuer d'autres transactions avec ce code, ouvrez une session sur My Account.

Pour ajouter des licences qui sont stockées sur votre ordinateur local ou sur le réseau :

1. Sélectionnez **Configuration > Licences** dans le volet de navigation de Studio.
2. Sélectionnez **Ajouter des licences** dans le volet Actions.
3. Accédez à un fichier de licences et ajoutez-le au serveur de licences.

Pour changer de serveur de licences

1. Sélectionnez **Configuration > Licences** dans le volet de navigation de Studio.
2. Sélectionnez **Changer le serveur de licences** dans le volet Actions.
3. Tapez l'adresse du serveur de licences sous la forme nom:port, où nom est une adresse DNS, NetBIOS ou IP. Si vous n'indiquez pas de numéro de port, le port par défaut (27000) est utilisé.

Pour sélectionner le type de licence à utiliser :

- Lors de la configuration du site, après avoir spécifié le serveur de licences, vous êtes invité à sélectionner le type de licence à utiliser. S'il n'y a aucune licence sur le serveur, l'option

d'utilisation du produit pour une période d'évaluation de 30 jours est automatiquement sélectionnée.
- Si le serveur comporte des licences, leurs détails sont affichés et vous pouvez sélectionner l'une d'elles. Vous pouvez également ajouter un fichier de licences au serveur et le sélectionner.

Pour changer l'édition du produit et le modèle de licence :

1. Sélectionnez **Configuration > Licences** dans le volet de navigation de Studio.
2. Sélectionnez **Modifier l'édition du produit** dans le volet Actions.
3. Mettez à jour les options appropriées.

Pour accéder à la console License Administration Console, dans le volet Actions, sélectionnez **License Administration Console**. La console soit apparaît immédiatement soit, si le tableau de bord est configuré comme protégé par un mot de passe, vous êtes invité à entrer les informations d'identification de la console License Administration Console. Pour plus de détails sur l'utilisation de la console, veuillez consulter la documentation concernant les licences.

Pour ajouter un administrateur de licences :

1. Sélectionnez **Configuration > Licences** dans le volet de navigation de Studio.
2. Dans le panneau du milieu, choisissez l'onglet Administrateurs de licences.
3. Sélectionnez **Ajouter un administrateur de licences** dans le volet Actions.
4. Recherchez le nom de l'utilisateur que vous souhaitez ajouter en tant qu'administrateur et choisissez les autorisations.

Pour modifier les autorisations d'un administrateur de licences ou supprimer un administrateur de licences :

1. Sélectionnez **Configuration > Licences** dans le volet de navigation de Studio.
2. Dans le panneau du milieu, choisissez l'onglet Administrateurs de licences et sélectionnez l'administrateur.
3. Sélectionnez **Modifier l'administrateur de licences** ou **Supprimer l'administrateur de licences** dans le volet Actions.

Pour ajouter un groupe d'administrateurs de licences :

1. Sélectionnez **Configuration > Licences** dans le volet de navigation de Studio.
2. Dans le panneau du milieu, choisissez l'onglet Administrateurs de licences.
3. Sélectionnez **Ajouter un groupe d'administrateurs de licences** dans le volet Actions.
4. Recherchez le groupe que vous souhaitez voir opérer en tant qu'administrateur de licences et choisissez les autorisations. L'ajout d'un groupe Active Directory donne à l'administrateur de licences des autorisations d'accès aux utilisateurs dans ce groupe.

Pour modifier les autorisations d'un groupe d'administrateurs de licences ou supprimer un groupe d'administrateurs de licences :

1. Sélectionnez **Configuration > Licences** dans le volet de navigation de Studio.

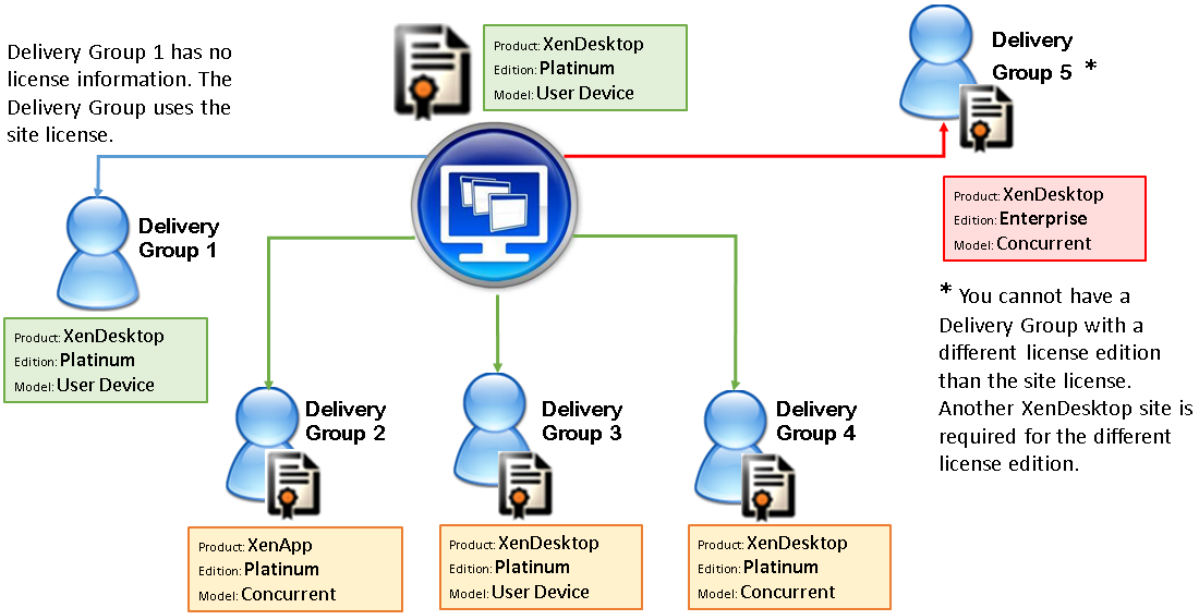
2. Dans le panneau du milieu, choisissez l'onglet Administrateurs de licences et sélectionnez le groupe d'administrateurs.
3. Sélectionnez **Modifier le groupe d'administrateurs de licences** ou **Supprimer le groupe d'administrateurs de licences** dans le volet Actions.

Licences multitypes

February 28, 2019

La fonction Licences multitypes prend en charge la consommation de différents types de licence pour les groupes de mise à disposition sur un seul site XenApp ou XenDesktop. Le **Type** est une combinaison unique de l'ID du produit (XDT, MPS) et du modèle (UserDevice, Concurrent). Les groupes de mise à disposition doivent utiliser l'édition du produit définie pour le site.

Si la fonction Licences multitypes n'est pas configurée, il est possible d'utiliser différents types de licences uniquement s'ils sont configurés sur des sites distincts. Les groupes de mise à disposition utilisent la licence de site.



Pour déterminer les groupes de mise à disposition qui consomment différents types de licence, utilisez ces applets de commande PowerShell de Broker :

- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup
- Get-BrokerDesktopGroup

Pour installer des licences, utilisez :

- Citrix Studio

- Citrix Licensing Manager
- License Administration Console
- citrix.com

Les dates de Subscription Advantage sont spécifiques à chaque fichier de licence et à chaque produit et modèle. Les groupes de mise à disposition définis différemment peuvent avoir différentes dates de Subscription Advantage.

SDK PowerShell de Broker

L'objet **DesktopGroup** a ces deux propriétés que vous pouvez manipuler à l'aide des applets de commande New-BrokerDesktopGroup et Set-BrokerDesktopGroup.

Name	Valeur	Restriction
LicenseModel	Enum (Concurrent ou UserDevice) spécifiant le modèle de licence pour le groupe.	Si la fonctionnalité est désactivée, la définition des propriétés échoue.
ProductCode	Chaîne de texte XDT (pour XenDesktop) ou MPS (pour XenApp) spécifiant l'ID de produit de licence pour le groupe.	Si la fonctionnalité est désactivée, la définition des propriétés échoue.

New-BrokerDesktopGroup

Crée un groupe de bureaux pour gérer la négociation des groupes de bureaux. Pour plus d'informations sur cette applet de commande, voir https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerDesktopGroup/.

Set-BrokerDesktopGroup

Désactive ou active un groupe de bureaux broker existant ou modifie ses paramètres. Pour plus d'informations sur cette applet de commande, voir https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/

Get-BrokerDesktopGroup

Récupère les groupes de bureaux correspondant aux critères spécifiés. Le résultat de l'applet de commande Get-BrokerDesktopGroup inclut les propriétés ProductCode et LicenseModel du groupe. Si les propriétés n'ont pas été définies à l'aide de New-BrokerDesktopGroup ou Set- BrokerDesktop-Group, des valeurs null sont renvoyées. Si la valeur est null, le code de produit et le modèle de licence de l'ensemble du site sont utilisés. Pour plus d'informations sur cette applet de commande, voir https://citrix.github.io/delivery-controller-sdk/Broker/Get-BrokerDesktopGroup/.

Configurer différents produits et modèles de licence par groupe de mise à disposition

1. Ouvrez PowerShell avec des droits d'administration et ajoutez le composant logiciel enfichable Citrix.
2. Exécutez la commande **Get-BrokerDesktopGroup –Name "DeliveryGroupName"** pour afficher la configuration de licence actuelle. Recherchez les paramètres **LicenseModel** et **ProductCode**. Si vous n'avez pas configuré ces paramètres auparavant, ils peuvent être vides.

   > Remarque :
   >
   > Si un groupe de mise à disposition ne dispose pas d'informations sur les licences, appliquez la **licence du site au niveau du site**.

3. Pour modifier le modèle de licence, exécutez la commande **Set-BrokerDesktopGroup –Name "DeliveryGroupName" –LicenseModel LicenseModel**.
4. Pour modifier le produit de licence, exécutez la commande **Set-BrokerDesktopGroup –Name "DeliveryGroupName" –ProductCode ProductCode**.
5. Entrez la commande **Get-BrokerDesktopGroup –Name "DeliveryGroupName"** pour valider les modifications.

   > Remarque :
   >
   > Vous ne pouvez pas combiner les éditions, par exemple les licences Premium et Advanced.

6. Pour supprimer la configuration de licence, exécutez les mêmes commandes **Set-BrokerDesktopGroup** décrites ci-dessus et définissez la valeur sur **$null**.

   > Remarque :
   >
   > Studio n'affiche pas la configuration de licence pour chaque groupe de mise à disposition. Utilisez PowerShell pour afficher la configuration actuelle.

Exemple

Cet exemple d'applet de commande PowerShell illustre la définition d'une licence multitypes pour deux groupes de mise à disposition existants et crée et définit un troisième groupe de mise à disposition.

Pour voir le produit sous licence et le modèle de licence associés à un groupe de mise à disposition, utilisez l'applet de commande PowerShell **Get-BrokerDesktopGroup**.

1. Nous définissons le premier groupe de mise à disposition pour XenApp et Concurrent.
   Set-BrokerDesktopGroup -Name "Delivery Group for XenApp Platinum Concurrent" -ProductCode MPS -LicenseModel Concurrent
2. Nous définissons le deuxième groupe de mise à disposition pour XenDesktop et Concurrent.
   Set-BrokerDesktopGroup -Name "Delivery Group for XenDesktop Platinum Concurrent" -ProductCode XDT -LicenseModel Concurrent
3. Nous créons et définissons le troisième groupe de mise à disposition pour XenDesktop et UserDevice.
   New-BrokerDesktopGroup -Name "Delivery Group for XenDesktop Platinum UserDevice" -PublishedName "MyDesktop" -DesktopKind Private -ProductCode XDT -LicenseModel UserDevice

Considérations spéciales

Les licences multitypes proposent des fonctionnalités différentes des licences XenApp et XenDesktop standard.

Director et Studio n'envoient pas d'alertes ni de notifications :

- Aucune notification lors de l'approche des limites de la licence ou du déclencheur ou de l'expiration de la période de grâce supplémentaire.
- Aucune notification lorsqu'un groupe spécifique a un problème.

Applications

February 28, 2019

Introduction

Si votre déploiement utilise uniquement des groupes de mise à disposition (et aucun groupe d'applications), vous devez ajouter des applications aux groupes de mise à disposition. Si vous

disposez également de groupes d'application, vous devez, en règle générale, ajouter des applications aux groupes d'applications. Ces recommandations permettent de faciliter l'administration. Une application doit toujours appartenir à au moins un groupe de mise à disposition ou groupe d'applications.

Dans l'assistant Ajouter des applications, vous pouvez sélectionner un ou plusieurs groupes de mise à disposition, ou un ou plusieurs groupes d'applications, mais pas les deux. Bien que vous puissiez par la suite modifier l'association à un groupe d'applications (par exemple, transférer une application d'un groupe d'applications sur un groupe de mise à disposition), cela n'est pas recommandé pour des raisons de complexité. Gardez vos applications dans un type de groupe.

Lorsque vous associez une application à plusieurs groupes de mise à disposition ou groupes d'applications, vous risquez de rencontrer un problème de visibilité si vous ne disposez pas d'autorisations suffisantes pour afficher l'application dans tous ces groupes. Dans de tels cas, consultez un administrateur disposant des autorisations appropriées ou demandez une extension de vos autorisations à tous les groupes auxquels l'application est associée.

Si vous publiez deux applications du même nom (provenant de groupes différents) vers les mêmes utilisateurs, modifiez la propriété Nom de l'application (pour l'utilisateur) dans Studio ; sinon, les utilisateurs verront des noms en double s'afficher dans Citrix Receiver.

Vous pouvez modifier les propriétés d'une application (paramètres) lorsque vous l'ajoutez ou ultérieurement. Vous pouvez également modifier le dossier dans lequel l'application est placée, lorsque vous ajoutez l'application, ou ultérieurement.

Pour de plus amples informations sur :

- Groupes de mise à disposition, consultez l'article Créer des groupes de mise à disposition.
- Groupes d'applications, consultez l'article Créer des groupes d'applications.
- Balises, que vous pouvez ajouter aux applications ; consultez l'article Balises.

Ajouter des applications

Vous pouvez ajouter des applications lorsque vous créez un groupe de mise à disposition ou un groupe d'applications ; ces procédures sont détaillées dans les articles Créer des groupes de mise à disposition et Créer des groupes d'applications. La procédure suivante explique comment ajouter des applications après la création d'un groupe.

À savoir

- vous ne pouvez pas ajouter d'applications aux groupes de mise à disposition Remote PC Access.
- Vous ne pouvez pas utiliser l'assistant Ajouter une application pour supprimer des applications de groupes de mise à disposition ou de groupes d'applications. Il s'agit d'une opération distincte.

Pour ajouter une ou plusieurs applications :

1. Sélectionnez **Applications** dans le panneau de navigation de Studio, puis sélectionnez **Ajouter des applications** dans le volet Actions.
2. L'assistant Ajouter des applications s'ouvre avec une page **Introduction**, que vous pouvez supprimer des lancements ultérieurs de cet assistant.
3. L'assistant vous guide à travers les pages Groupes, Applications, et Résumé décrites ci-dessous. Lorsque vous avez terminé chaque page, cliquez sur **Suivant** jusqu'à la page finale.

Alternatives à l'étape 1 si vous souhaitez ajouter des applications à un seul groupe de mise à disposition ou groupe d'applications :

- Pour ajouter des applications à un seul groupe de mise à disposition, à l'étape 1, sélectionnez **Groupes de mise à disposition** dans le volet de navigation Studio, sélectionnez un groupe de mise à disposition dans le volet du milieu, puis sélectionnez **Ajouter des applications** dans le volet Actions. L'assistant n'affichera pas la page **Groupes**.
- Pour ajouter des applications à un seul groupe d'applications, à l'étape 1, sélectionnez **Groupes d'applications** dans le volet de navigation Studio, sélectionnez un **groupe d'applications** dans le volet du milieu, puis sélectionnez **Ajouter des applications** sous le nom du groupe dans le volet Actions. L'assistant n'affichera pas la page **Groupes**.

Groupes

Cette page dresse la liste de tous les groupes de mise à disposition dans le site. Si vous avez également créé des groupes d'applications, la page dresse la liste des groupes d'applications et des groupes de mise à disposition. Vous pouvez choisir dans l'un ou l'autre des groupes, mais pas dans les deux groupes. En d'autres termes, vous ne pouvez pas ajouter d'applications à un groupe d'applications et à un groupe de mise à disposition. En général, si vous utilisez des groupes d'application, les applications doivent être ajoutées à des groupes d'applications plutôt qu'à des groupes de mise à disposition.

Lorsque vous ajoutez une application, vous devez sélectionner la case à cocher en regard d'au moins un groupe de mise à disposition (ou groupe d'applications, le cas échéant), car chaque application doit toujours être associée à au moins un groupe.

Applications

Cliquez sur la liste déroulante **Ajouter** pour afficher les sources des applications.

- **À partir du menu Démarrer :** applications qui sont découvertes sur une machine dans les groupes de mise à disposition sélectionnés. Lorsque vous sélectionnez cette source, une nouvelle page se lance avec une liste des applications découvertes. Sélectionnez les cases à cocher des applications à ajouter, puis cliquez sur OK.

Cette source ne peut pas être sélectionnée si vous avez (1) sélectionné des groupes d'applications qui ne sont associés à aucun groupe de mise à disposition, (2) sélectionné des groupes d'applications avec des groupes de mise à disposition associés qui ne contiennent aucune machine, ou (3) sélectionné un groupe de mise à disposition ne contenant aucune machine.

- **Manuellement définies :** applications qui se trouvent dans le site ou ailleurs dans votre réseau. Lorsque vous sélectionnez cette source, une nouvelle page s'affiche dans laquelle vous pouvez taper le chemin d'accès de l'exécutable, le répertoire de travail, les arguments de la ligne de commande (facultatifs), et les noms affichés des administrateurs et des utilisateurs. Après avoir entré ces informations, cliquez sur OK.
- **Existantes :** applications déjà ajoutées au site. Lorsque vous sélectionnez cette source, une nouvelle page se lance avec une liste des applications découvertes. Sélectionnez les cases à cocher des applications à ajouter, puis cliquez sur OK.

Cette source ne peut pas être sélectionnée si le site ne dispose d'aucune application.

- **App-V :** applications dans des packages App-V. Lorsque vous sélectionnez cette source, une nouvelle page s'affiche dans laquelle vous pouvez sélectionner le serveur App-V ou la bibliothèque d'applications. À partir de l'écran qui s'affiche, sélectionnez les cases à cocher des applications à ajouter, puis cliquez sur OK. Pour plus d'informations, veuillez consulter l'article App-V.

Cette source ne peut pas être sélectionnée lorsque App-V n'est pas configuré pour le site.

- **Groupe d'applications :** groupes d'applications. Lorsque vous sélectionnez cette source, une nouvelle page se lance avec une liste des groupes d'applications. (Bien que l'affichage dresse également la liste des applications de chaque groupe, vous ne pouvez sélectionner que le groupe, et non pas des applications individuelles.) Toutes les applications actuelles et futures dans les groupes sélectionnés seront ajoutées. Sélectionnez les cases à cocher des groupes d'applications à ajouter, puis cliquez sur OK.

Cette source ne peut pas être sélectionnée s'il (1) n'existe aucun groupe d'applications, ou (2) si les groupes de mise à disposition sélectionnés ne prennent pas en charge les groupes d'applications (par exemple, les groupes de mise à disposition avec des machines attribuées de manière statique).

Comme indiqué dans le tableau, certaines sources dans la liste déroulante Ajouter ne peuvent pas être sélectionnées s'il n'existe source valide de ce type. Les sources qui ne sont pas compatibles (par exemple, vous ne pouvez pas ajouter des groupes d'applications à des groupes d'applications) ne sont pas incluses dans la liste déroulante. Les applications qui ont déjà été ajoutées aux groupes que vous avez choisis ne peuvent pas être sélectionnées.

Pour ajouter une application à partir d'un AppDisk affecté, sélectionnez **Depuis le menu Démarrer**. Si l'application n'est pas disponible, sélectionnez **Manuellement définies** et fournissez les détails. En cas d'erreur d'accès au dossier, configurez le dossier comme « partagé » et réessayez d'ajouter l'application par le biais de l'option **Manuellement définies**.

Vous pouvez modifier les propriétés d'une application (paramètres) sur cette page ou ultérieurement.

Par défaut, les applications que vous ajoutez sont placées dans le dossier appelé Applications. Vous pouvez modifier l'application sur cette page ou ultérieurement. Si vous essayez d'ajouter une application et qu'une application avec le même nom existe déjà dans le même dossier, vous êtes invité à renommer l'application que vous ajoutez. Vous pouvez accepter le nouveau nom proposé ou refuser et renommer l'application, ou sélectionner un autre dossier. Par exemple, si « application » existe déjà dans le dossier Applications, et que vous essayez d'ajouter une autre application appelée « application » à ce dossier, le nouveau nom proposé sera « application_1 ».

Synthèse

Si vous ajoutez 10 applications ou moins, leurs noms sont répertoriés dans **Applications à ajouter**. Si vous ajoutez plus de 10 applications, le nombre total est spécifié.

Consultez les informations récapitulatives, puis cliquez sur **Terminer**.

Modifier l'association d'un groupe d'applications

Après l'ajout d'une application, vous pouvez modifier les groupes de mise à disposition et groupes d'applications auxquels l'application est associée.

Vous pouvez utiliser le glisser-déplacer pour associer une application à un autre groupe. Ceci est une alternative à l'utilisation des commandes dans le volet Actions.

Si une application est associée à plus d'un groupe de mise à disposition ou plus d'un groupe d'applications, la priorité attribuée au groupe est utilisée pour spécifier l'ordre dans lequel plusieurs groupes sont vérifiés afin de trouver des applications. Par défaut, tous les groupes ont la priorité 0 (priorité la plus élevée). La charge des groupes ayant le même niveau de priorité est équilibrée.

Une application peut être associée à des groupes de mise à disposition contenant des machines partagées (non privées) qui peuvent mettre à disposition des applications. Vous pouvez également sélectionner des groupes de mise à disposition contenant des machines partagées qui mettent uniquement à disposition des bureaux, si (1) le groupe de mise à disposition contient des machines partagées et a été créé avec une version antérieure de XenDesktop 7.x, et (2) vous disposez de l'autorisation Modifier le groupe de mise à disposition. Le type de groupe de mise à disposition est automatiquement converti en « bureaux et applications » lorsque la boîte de dialogue des propriétés est validée.

1. Sélectionnez **Applications** dans le volet de navigation de Studio, puis sélectionnez l'application dans le panneau central.
2. Sélectionnez **Propriétés** dans le volet Actions.
3. Sélectionnez la page **Groupes**.

4. Pour ajouter un groupe, cliquez sur la liste déroulante **Ajouter** et sélectionnez **Groupes d'applications** ou **Groupes de mise à disposition**. (Si vous n'avez pas créé de groupes d'applications, la seule entrée sera Groupes de mise à disposition). Puis sélectionnez un ou plusieurs groupes disponibles. Les groupes qui ne sont pas compatibles avec l'application, ou qui sont déjà associés à l'application ne peuvent pas être sélectionnés.
5. Pour supprimer un groupe, sélectionnez un ou plusieurs groupes, puis cliquez sur **Supprimer**. Si la suppression de l'association de groupe a pour conséquence que l'application n'est plus être associée à un groupe d'applications ou groupe de mise à disposition, vous serez averti que l'application va être supprimée.
6. Pour modifier la priorité des groupes de mise à disposition, sélectionnez le groupe, puis cliquez sur **Modifier la priorité**. Sélectionnez une valeur de priorité puis cliquez sur **OK**.
7. Lorsque vous avez terminé, cliquez sur **Appliquer** pour appliquer les modifications et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Dupliquer, activer/désactiver, renommer ou supprimer une application

Utilisation de ces actions :

- **Dupliquer :** il se peut que vous souhaitiez dupliquer une application pour créer une version différente avec des propriétés ou paramètres différents. Lorsque vous dupliquez une application, elle est automatiquement renommée avec un suffixe unique et placée de manière adjacente à l'original. Vous pouvez également vouloir dupliquer une application et l'ajouter à un autre groupe. (Après la duplication, la manière la plus facile de déplacer une application est de la glisser-déposer.)
- **Activer ou désactiver :** activer/désactiver une application ne signifie pas activer/désactiver un groupe de mise à disposition ou groupe d'applications.
- **Renommer :** vous ne pouvez renommer qu'une seule application à la fois. Si vous essayez de renommer une application et qu'une application avec le même nom existe déjà dans le même dossier ou groupe, vous êtes invité à spécifier un nom différent.
- **Supprimer :** la suppression d'une application la supprime des groupes de mise à disposition et des groupes d'applications auxquels elle était associée, mais pas de la source utilisée pour ajouter l'application à l'origine. Supprimer une application ne signifie pas supprimer une application d'un groupe de mise à disposition ou groupe d'applications.

Pour dupliquer, activer/désactiver, renommer ou supprimer une application :

1. Sélectionnez **Applications** dans le volet de navigation de Studio.
2. Sélectionnez une ou plusieurs applications dans le panneau du milieu, puis sélectionnez la tâche appropriée dans le volet Actions.
3. Confirmez l'action lorsque vous y êtes invité.

Supprimer des applications d'un groupe de mise à disposition

Une application doit être associée (appartenir) à au moins un groupe de mise à disposition ou groupe d'applications. Si vous tentez de supprimer une application d'un groupe de mise à disposition qui supprimerait l'association de cette application avec un groupe de mise à disposition ou groupe d'applications, vous êtes averti que l'application va être supprimée si vous continuez. Lorsque cela se produit, si vous souhaitez mettre à disposition cette application, vous devez l'ajouter à nouveau à partir d'une source valide.

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe de mise à disposition. Dans le panneau central inférieur, sélectionnez l'onglet **Applications**, puis sélectionnez l'application à supprimer.
3. Sélectionnez **Retirer application** dans le panneau Actions.
4. Confirmez la suppression.

Supprimer des applications d'un groupe d'applications

Une application doit appartenir à au moins un groupe de mise à disposition ou groupe d'applications. Si vous tentez de supprimer une application d'un groupe d'applications qui aurait pour conséquence que cette application n'appartiendrait plus à aucun groupe de mise à disposition ou groupe d'applications, vous êtes averti que l'application va être supprimée si vous continuez. Lorsque cela se produit, si vous souhaitez mettre à disposition cette application, vous devez l'ajouter à nouveau à partir d'une source valide.

1. Sélectionnez **Applications** dans le volet de navigation de Studio.
2. Sélectionnez le groupe d'applications dans le volet central, puis sélectionnez une ou plusieurs applications dans le panneau central.
3. Sélectionnez **Retirer application du groupe d'applications** dans le panneau Actions.
4. Confirmez la suppression.

Modifier les propriétés de l'application

Vous pouvez modifier les propriétés d'une seule application à la fois.

Pour modifier les propriétés d'une application :

1. Sélectionnez **Applications** dans le volet de navigation de Studio.
2. Sélectionnez une application, puis sélectionnez **Modifier les propriétés d'application** dans le volet Actions.
3. Sélectionnez la page contenant la propriété que vous souhaitez modifier.

4. Lorsque vous avez terminé, cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Dans la liste suivante, la page est indiquée entre parenthèses.

- Catégorie/dossier dans lequel l'application s'affiche dans Receiver (Mise à disposition)
- Arguments de ligne de commande ; voir la section Passer des paramètres aux applications publiées (Emplacement)
- Les groupes de mise à disposition et groupes d'applications dans lesquels l'application est disponible (Groupes)
- Description (Identification)
- Extensions de fichier et association de type de fichier : extensions que l'application ouvre automatiquement (Association de type de fichier)
- Icône (Mise à disposition)
- Mots-clés pour StoreFront (Identification)
- Limites ; consultez la section Configurer les limites d'application (Mise à disposition)
- Nom : noms que l'utilisateur et l'administrateur voient (Identification)
- Chemin d'accès au fichier exécutable ; voir la section Passer des paramètres aux applications publiées (Emplacement)
- Raccourci sur le bureau de l'utilisateur : activer ou désactiver (Mise à disposition)
- Visibilité : limite les utilisateurs autorisés à voir l'application dans Citrix Receiver ; une application non visible peut toujours être démarrée ; pour la rendre non disponible ainsi qu'invisible, ajoutez-la à un groupe différent (Limiter la visibilité)
- Répertoire de travail (Emplacement)

Les modifications apportées aux applications peuvent ne pas prendre effet pour les utilisateurs d'applications courantes tant qu'ils n'ont pas fermé leur session.

Configurer les limites d'application

Configurez les limites d'application pour vous aider à gérer l'utilisation des applications. Par exemple, vous pouvez utiliser les limites d'application pour gérer le nombre d'utilisateurs pouvant accéder à une application simultanément. De même, les limites d'application peuvent être utilisées pour gérer le nombre d'instances simultanées d'applications très consommatrices de ressources, ce qui peut vous aider à gérer les performances des serveurs et à empêcher la détérioration du service.

Cette fonctionnalité limite le nombre de démarrages d'application qui sont négociés par le Controller (par exemple, à partir de Citrix Receiver et StoreFront), et non pas le nombre d'applications qui peuvent être lancées par d'autres méthodes. Par conséquent, les limites d'application aident les administrateurs à gérer l'utilisation simultanée, mais ne peuvent pas être appliquées de force dans tous les

scénarios. Par exemple, les limites d'application ne peuvent pas être appliquées lorsque le Controller se trouve en mode de location de connexion.

Par défaut, il n'existe aucune limite sur le nombre d'instances d'application qui peuvent être exécutées simultanément. Il existe deux paramètres de limite d'application ; vous pouvez en configurer un ou les deux :

- Le nombre maximal d'instances simultanées d'une application par tous les utilisateurs du groupe de mise à disposition.
- Une instance de l'application par utilisateur dans le groupe de mise à disposition

Si une limite est configurée, un message d'erreur est généré lorsqu'un utilisateur tente de démarrer une instance de l'application qui dépasse la limite configurée.

Exemples d'utilisation des limites d'application :

- **Nombre maximal d'instances simultanées.** Dans un groupe de mise à disposition, vous configurez le nombre maximal d'instances d'applications simultanées Alpha sur 15. Plus tard, les utilisateurs de ce groupe de mise à disposition ont 15 instances de cette application en cours d'exécution en même temps. Si un utilisateur de ce groupe de mise à disposition tente de lancer Alpha, un message d'erreur est généré et l'application Alpha n'est pas lancée car la limite d'instances d'applications simultanées (15) aurait été dépassée.
- **Une instance d'application par utilisateur.** Dans un autre groupe de mise à disposition, vous activez l'option une instance par utilisateur pour l'application Beta. L'utilisateur Tony lance l'application Beta avec succès. Plus tard, alors que l'application est toujours en cours d'exécution dans la session de Tony, il tente de démarrer une autre instance de Beta. Un message d'erreur est généré et Beta n'est pas lancé car la limite d'une instance par utilisateur aurait été dépassée.
- **Nombre maximal d'instances simultanées et une instance par utilisateur.** Dans un autre groupe de mise à disposition, vous configurez un nombre maximal d'instances simultanées de 10 et activez l'option une instance par utilisateur pour l'application Delta. Plus tard, lorsque dix utilisateurs de ce groupe de mise à disposition exécutent chacun une instance de Delta, les autres utilisateurs de ce groupe de mise à disposition qui tentent de lancer Delta reçoivent un message d'erreur et Delta n'est pas démarré. Si un des dix utilisateurs de Delta tente de démarrer une seconde instance de cette application, il reçoit un message d'erreur et la deuxième instance ne peut pas être démarrée.

Si des instances de l'application sont également lancées par d'autres méthodes que la négociation Controller (par exemple, lorsqu'un Controller se trouve en mode de location de connexion) et que les limites configurées sont dépassées, les utilisateurs ne pourront pas lancer d'instances supplémentaires jusqu'à ce qu'ils ferment suffisamment d'instances pour ne plus dépasser la limite. Les instances qui ont dépassé la limite ne sont pas arrêtées ; elles peuvent continuer jusqu'à ce que les utilisateurs les ferment.

Si vous désactivez l'itinérance de session, désactivez la limite d'application « Une seule instance par utilisateur ». Si vous activez la limite d'application « Une seule instance par utilisateur », ne configurez pas les deux valeurs qui permettent de nouvelles sessions sur de nouvelles machines. Pour de plus amples informations sur l'itinérance, consultez l'article Sessions.

Pour configurer les limites d'application :

1. Sélectionnez **Applications** dans le volet de navigation de Studio, puis sélectionnez une application.
2. Sélectionnez **Modifier les propriétés d'application** dans le volet Actions.
3. Sur la page **Mise à disposition**, choisissez l'une des options ci-dessous. Lorsque vous avez terminé, cliquez sur **OK** ou **Appliquer**. (**OK** applique la modification et ferme la boîte de dialogue Modifier les propriétés d'application ; **Appliquer** applique la modification et laisse la boîte de dialogue ouverte.)

- Autoriser l'utilisation illimitée de l'application. Il n'existe aucune limite au nombre d'instances exécutées en même temps. Il s'agit de l'option par défaut.
- Définir des limites pour l'application. Il existe deux types de limite ; spécifiez-en une ou les deux.
  - Spécifier le nombre maximal d'instances pouvant être exécutées simultanément
  - Limiter à une instance d'application par utilisateur

Passer des paramètres aux applications publiées

Utilisez la page Emplacement des propriétés d'une application pour entrer la ligne de commande et les paramètres à transmettre aux applications publiées.

Lorsque vous associez des types de fichier à une application publiée, les symboles"%*" (pourcentage et étoile entre guillemets) sont ajoutés à la fin de la ligne de commande de l'application. Ces symboles réservent l'emplacement des paramètres transmis aux machines utilisateur.

Si une application publiée ne démarre pas, vérifiez que la ligne de commande contient les symboles appropriés. Par défaut, les paramètres fournis par les machines utilisateur sont validés lorsque les symboles « %* » sont ajoutés. Pour les applications publiées qui utilisent des paramètres personnalisés fournis par la machine utilisateur, les symboles "%**" sont ajoutés à la ligne de commande pour éviter la validation de ligne de commande. Si ces symboles n'apparaissent pas dans la ligne de commande d'une application, vous pouvez les ajouter manuellement.

Si le chemin d'accès du fichier exécutable comprend des noms de répertoire avec des espaces, (« C:\Program Files », par exemple), mettez la ligne de commande de l'application entre guillemets afin d'indiquer que l'espace fait partie de la ligne de commande. Pour ce faire, ajoutez des guillemets autour du chemin d'accès et des guillemets autour des symboles %*. Veillez à inclure un espace entre le guillemet final du chemin d'accès et le guillemet initial des symboles %*.

Par exemple, la ligne de commande pour l'application publiée Lecteur Windows Media est :

“C:\Program Files\Windows Media Player\mplayer1.exe” “%*”

Gérer les dossiers d’applications

Par défaut, les applications que vous ajoutez aux groupes de mise à disposition sont placées dans un dossier nommé **Applications**. Vous pouvez spécifier un dossier différent lorsque vous créez le groupe de mise à disposition, lorsque vous ajoutez une application ou plus tard.

À savoir

- Vous ne pouvez pas renommer ou supprimer le dossier Applications, mais vous pouvez déplacer toutes les applications qu’il contient vers d’autres dossiers que vous créez.
- Un nom de dossier peut contenir entre 1 et 64 caractères. Les espaces sont autorisés.
- Les dossiers peuvent être imbriqués jusqu’à cinq niveaux.
- Les dossiers n’ont pas à contenir d’applications, des dossiers vides sont autorisés.
- Les dossiers sont répertoriés par ordre alphabétique dans Studio, sauf si vous les déplacer ou spécifiez un emplacement différent lorsque vous les créez.
- Vous pouvez posséder plus d’un dossier du même nom, tant que chacun possède un dossier parent différent. De même, vous pouvez posséder plus d’une application du même nom, tant que chacune se trouve dans un dossier différent.
- Vous devez disposer de l’autorisation Afficher l’application pour voir les applications dans des dossiers, et vous devez posséder l’autorisation Modifier les propriétés d’application pour toutes les applications dans le dossier pour déplacer, renommer ou supprimer un dossier qui contient des applications.
- La plupart des procédures suivantes requièrent des actions depuis le panneau Actions de Studio. Éventuellement, vous pouvez utiliser les menus du bouton droit de la souris ou le glisser-déplacer. Par exemple, si vous créez ou déplacez un dossier dans un emplacement indésirable, vous pouvez le faire glisser et le déposer à l’emplacement approprié.

Pour gérer les dossiers d’applications, sélectionnez **Applications** dans le volet de navigation de Studio. Utilisez la liste ci-dessous pour plus d’informations.

- Pour afficher tous les dossiers (mis à part les dossiers incorporés), cliquez sur **Afficher tout** au-dessus de la liste de dossiers.
- Pour afficher un dossier au niveau le plus élevé (non imbriqué), sélectionnez le dossier Applications. Pour placer le nouveau dossier sous un dossier existant autre que le dossier Applications, sélectionnez ce dossier. Sélectionnez ensuite **Créer un dossier** dans le volet Actions. Entrez un nom.
- Pour déplacer un dossier, sélectionnez le dossier, puis sélectionnez **Déplacer le dossier** dans le volet Actions. Vous pouvez déplacer un seul dossier à la fois, à moins que le dossier contienne des dossiers incorporés. Conseil : la manière la plus facile de déplacer un dossier est d’utiliser le glisser-déplacer.

- Pour renommer un dossier, sélectionnez le dossier, puis sélectionnez **Renommer le dossier** dans le volet Actions. Entrez un nom.
- Pour supprimer un dossier, sélectionnez le dossier, puis sélectionnez **Supprimer le dossier** dans le volet Actions. Lorsque vous supprimez un dossier qui contient des applications et d'autres dossiers, ces objets sont également supprimés. La suppression de l'application supprime l'attribution de l'application depuis le groupe de mise à disposition, elle ne supprime pas l'application de la machine.
- Pour déplacer des applications dans un dossier, sélectionnez une ou plusieurs applications. Sélectionnez ensuite **Déplacer l'application** dans le panneau Actions. Sélectionnez le dossier.

Vous pouvez également placer des applications que vous ajoutez dans un dossier spécifique (même un nouveau) sur la page **Application** des assistants Créer un groupe de mise à disposition et Créer un groupe d'applications. Par défaut, les applications ajoutées sont placées dans le dossier Applications ; cliquez sur **Modifier** pour sélectionner ou créer un dossier.

Applications de la plate-forme Windows universelle

February 28, 2019

XenApp et XenDesktop prennent en charge l'utilisation d'applications de la plate-forme Windows universelle (UWP) avec des VDA sur machines Windows 10 et Windows Server 2016. Pour de plus amples informations sur les applications UWP, veuillez consulter la documentation Microsoft suivante.

- Qu'est-ce qu'une application de plate-forme Windows universelle (UWP) ?
- Distribuer des applications en mode déconnecté
- Guide des applications de la plate-forme Windows universelle (UWP)

Le terme « applications universelles » est utilisé dans cet article pour faire référence aux applications UWP.

Configuration requise et limitations

Les applications universelles sont prises en charge pour les VDA sur machines Windows 10 et Windows Server 2016.

Les VDA doivent être à la version minimale 7.11.

Les fonctionnalités suivantes de XenApp et XenDesktop ne sont pas prises en charge ou sont limitées lors de l'utilisation d'applications universelles :

- L'association de type de fichier n'est pas prise en charge.
- Local App Access n'est pas pris en charge.

- Aperçu dynamique : si les applications exécutées dans la session se chevauchent, l'aperçu affiche l'icône par défaut. Les API Win32 utilisées pour l'aperçu dynamique ne sont pas prises en charge dans les applications universelles.
- Centre de maintenance à distance : les applications universelles peuvent utiliser le Centre de maintenance pour afficher les messages dans la session. Redirigez ces messages vers le point de terminaison afin de les afficher pour l'utilisateur.

Le lancement d'applications universelles et non universelles à partir du même serveur n'est pas pris en charge pour les VDA Windows 10. Pour Windows Server 2016, les applications universelles et non universelles doivent être dans des groupes de mise à disposition ou groupe d'applications distincts.

Toutes les applications universelles installées sur la machine sont énumérées ; par conséquent, Citrix vous recommande de désactiver l'accès utilisateur au Windows Store. Ceci empêche les applications universelles installées par un utilisateur d'être accessibles par un autre utilisateur.

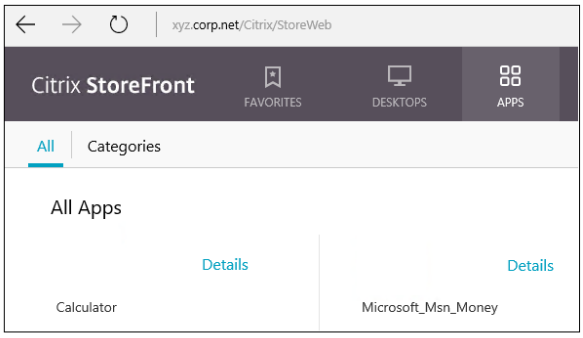
Durant le chargement de version test, l'application universelle est installée sur la machine et elle est disponible pour d'autres utilisateurs. Lorsqu'un autre utilisateur lance l'application, l'application est installée. Le système d'exploitation met ensuite à jour sa base de données AppX pour marquer l'application comme installée pour l'utilisateur qui lance l'application.

En cas de fermeture de session normale à partir d'une application universelle publiée qui a été lancée dans une fenêtre transparente ou fixe, la session peut ne pas se fermer et l'utilisateur être déconnecté. Plusieurs processus restant dans la session empêchent alors la session de se fermer correctement. Pour résoudre ce problème, déterminez le processus qui empêche la fermeture de session et ajoutez-le à la valeur de la clé de registre « LogoffCheckSysModules », en suivant les instructions de la section CTX891671.

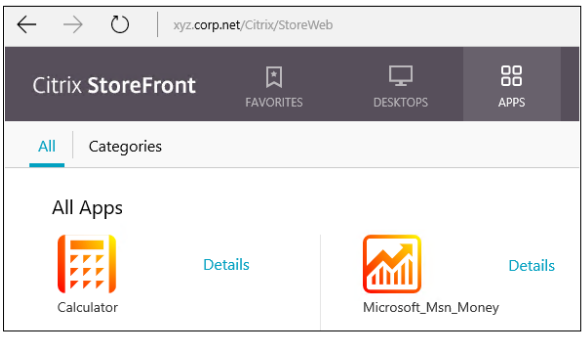
Les noms d'affichage des applications et les descriptions des applications universelles peuvent ne pas porter le nom correct. Modifiez et corrigez ces propriétés lors de l'ajout des applications au groupe de mise à disposition.

Consultez les Problèmes connus afin de prendre connaissance de problèmes supplémentaires.

Actuellement, plusieurs applications universelles ont des icônes blanches avec transparence activée, et par conséquent l'icône n'est pas visible sur l'arrière-plan blanc de StoreFront. Pour éviter ce problème, vous pouvez modifier l'arrière-plan. Par exemple, sur la machine StoreFront, modifiez le fichier C:\inetpub\wwwroot\Citrix\StoreWeb\custom\style.css. À la fin du fichier, ajoutez **.storeapp-icon {background-image: radial-gradient(circle at top right, yellow, red); }**. L'image ci-dessous illustre l'arrière-plan avant et après pour cet exemple.



Before



After

Sur Windows Server 2016, le Gestionnaire de serveur peut également démarrer lorsqu'une application universelle est lancée. Pour éviter ce problème, vous pouvez désactiver le démarrage automatique du Gestionnaire de serveur lors de l'ouverture de session avec la clé de registre HKLM\Software\Microsoft\ServerManager\DoNotOpenServerManagerAtLogon. Pour plus de détails, consultez https://blogs.technet.microsoft.com/rmilne/2014/05/30/how-to-hide-server-manager-at-logon/.

Installer et publier des applications universelles

La prise en charge des applications universelles est activée par défaut.

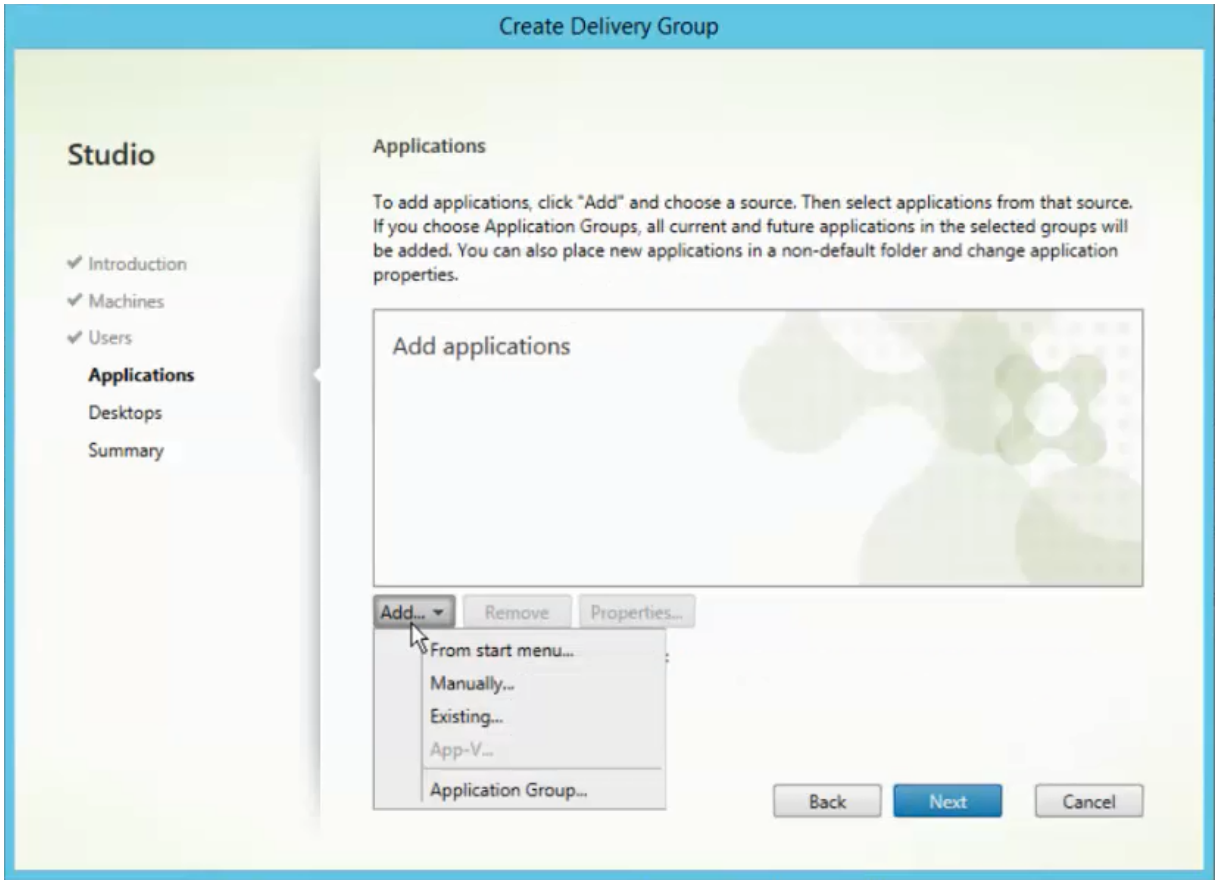
Pour désactiver l'utilisation des applications universelles sur un VDA, ajoutez le paramètre de registre **EnableUWASeamlessSupport** dans HKLM\Software\Citrix\VirtualDesktopAgent\FeatureToggle et définissez-le sur **0**.

Pour installer une ou plusieurs applications universelles sur des VDA (ou une image principale), utilisez l'une des méthodes suivantes :

- Effectuez une installation en mode déconnecté à partir du Windows Store d'entreprise, à l'aide d'un outil tel que Deployment Image Servicing and Management (DISM) pour déployer les applications sur l'image de bureau. Pour plus d'informations, veuillez consulter l'article https://technet.microsoft.com/en-us/itpro/windows/manage/distribute-offline-apps.
- Chargez la version test des applications. Pour plus d'informations, veuillez consulter l'article https://technet.microsoft.com/en-us/itpro/windows/deploy/sideload-apps-in-windows-10.

Pour ajouter (publier) une ou plusieurs applications universelles dans XenApp ou XenDesktop :

Une fois que les applications universelles sont installées sur la machine, ajoutez les applications universelles à un groupe de mise à disposition ou un groupe d'applications. Vous pouvez le faire lorsque vous créez un groupe ou ultérieurement. Sur la page Applications de l'assistant, sélectionnez la source **Depuis le menu Démarrer**.



Lorsque la liste des applications s'affiche, sélectionnez les cases à cocher des applications universelles que vous souhaitez publier. Cliquez ensuite sur **Suivant**.

Désinstaller des applications universelles

Lorsque vous désinstallez des applications universelles avec une commande telle que Remove-AppXPackage, l'élément est désinstallé uniquement pour les administrateurs. Pour supprimer l'application sur les machines des utilisateurs qui ont lancé et utilisé l'application, vous devez exécuter la commande de suppression sur chaque machine. Vous ne pouvez pas désinstaller le package AppX de toutes les machines des utilisateurs à l'aide d'une seule commande.

Zones

February 28, 2019

Les déploiements répartis sur différents emplacements géographiques et connectés à un réseau étendu peuvent rencontrer des problèmes de latence réseau et de fiabilité. Il existe deux options pour pallier ces problèmes :

- Déployer plusieurs sites, chacun avec sa propre base de données de site SQL Server.

Cette option est recommandée pour les déploiements de grande taille. Plusieurs sites sont gérés séparément et chacun requiert sa propre base de données de site SQL Server. Chaque site est un déploiement XenApp distinct.

- Configurer plusieurs zones au sein d'un seul site.

La configuration de zones peut aider les utilisateurs situés dans des régions éloignées à se connecter à des ressources sans que leurs connexions soient obligées de traverser des segments importants de réseau étendu. L'utilisation de zones permet une gestion efficace de site à partir d'une seule console Citrix Studio, de Citrix Director et de la base de données du site. Vous économisez ainsi les coûts liés au déploiement, au personnel, aux licences et à l'exploitation de sites contenant des bases de données distinctes dans des emplacements distants.

Les zones peuvent s'avérer utiles dans les déploiements de toutes tailles. Vous pouvez utiliser des zones pour que les applications et les bureaux se trouvent à proximité des utilisateurs finaux, ce qui améliore les performances. Une zone peut disposer d'un ou de plusieurs Controller installés localement pour assurer la redondance et la résilience, mais cette configuration n'est pas obligatoire.

Le nombre de Controller configurés sur le site peut affecter les performances de certaines opérations, telles que l'ajout de nouveaux Controller au site lui-même. Pour éviter ce problème, nous vous recommandons de limiter le nombre de zones de votre site XenDesktop ou XenApp à un maximum de 50.

> **Remarque :**
>
> Lorsque la latence du réseau de vos zones est supérieure à 250 ms (RTT), nous vous recommandons de déployer plusieurs sites plutôt que des zones.

Dans cet article, le terme « local » fait référence à la zone dont il est question. Par exemple, « Un VDA s'enregistre auprès d'un Controller local » signifie qu'un VDA s'enregistre auprès d'un Controller dans la zone dans laquelle le VDA est situé.

Les zones de cette version sont semblables, mais pas identiques aux zones de XenApp 6.5 et versions antérieures. Par exemple, dans cette implémentation de zones, il n'existe aucun collecteur de données. Tous les Controller du site communiquent avec une seule base de données du site dans la zone principale. En outre, les zones de basculement et les zones préférées fonctionnent différemment dans cette version.

Types de zone

Un site dispose toujours d'une zone principale. Il peut également disposer d'une ou de plusieurs zones satellite. Les zones satellite peuvent être utilisées pour la récupération d'urgence, des centres de données distants, des succursales, un cloud ou une zone de disponibilité dans un cloud.

Zone principale

La zone principale est appelée « Principale » par défaut et contient la base de données du site SQL Server (et des serveurs SQL haute disponibilité, le cas échéant), Studio, Director, StoreFront, le serveur de licences Citrix et NetScaler Gateway. La base de données du site doit toujours se trouver dans la zone principale.

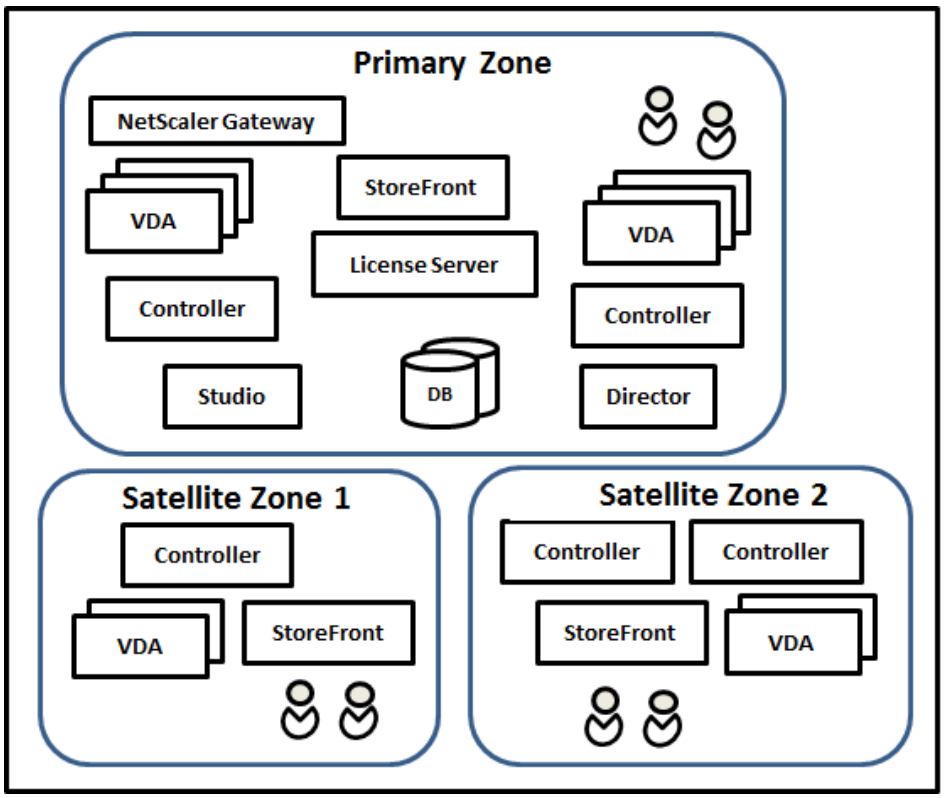
La zone principale doit également disposer d'au moins deux Controller pour assurer la redondance et peut disposer d'un ou de plusieurs VDA avec des applications qui sont étroitement liées avec la base de données et l'infrastructure.

Zone satellite

Une zone satellite contient un ou plusieurs VDA, Controller, serveurs StoreFront et serveurs NetScaler Gateway. Dans des conditions de fonctionnement normales, les Controller d'une zone satellite communiquent directement avec la base de données située dans la zone principale.

Une zone satellite, en particulier une zone de grande taille, peut également contenir un hyperviseur qui est utilisé pour provisionner et/ou stocker des machines pour cette zone. Lorsque vous configurez une zone satellite, vous pouvez lui associer une connexion à un hyperviseur ou à un service de cloud (Assurez-vous que les catalogues de machines qui utilisent cette connexion se trouvent dans la même zone).

Un site peut contenir différentes configurations de zones satellite, en fonction de vos besoins et de votre environnement. La figure suivante illustre une zone principale et des exemples de zones satellite.



- La zone principale contient deux Controller, Studio, Director, StoreFront, le serveur de licences et la base de données du site (plus des déploiements SQL Server haute disponibilité). La zone principale contient également plusieurs VDA et un boîtier NetScaler Gateway.
- Zone satellite 1 - VDA avec Controller

La zone satellite 1 contient un Controller, des VDA et un serveur StoreFront. Les VDA de cette zone satellite s'enregistrent auprès du Controller local. Le Controller local communique avec la base de données du site et le serveur de licences de la zone principale.

Si le réseau étendu échoue, la fonctionnalité de location de connexion permet au Controller de la zone satellite de continuer la négociation des connexions avec les VDA de cette zone. Un tel déploiement peut être efficace dans un bureau où les utilisateurs utilisent un site StoreFront local et le Controller local pour accéder à leurs ressources locales, même si la liaison WAN connectant leur bureau au réseau d'entreprise échoue.

- Zone satellite 2 - VDA avec Controller redondants

La zone satellite 2 contient deux Controller, des VDA et un serveur StoreFront. Il s'agit du type de zone le plus robuste, offrant une protection contre un échec simultané du réseau étendu et de l'un des Controller locaux.

Enregistrement des VDA et basculement des Controller

Dans un site contenant des zones principale et satellite, avec des VDA à la version 7.7 au minimum :

- Un VDA de la zone principale s'enregistre auprès d'un Controller de la zone principale. Un VDA de la zone principale ne tentera jamais de s'enregistrer auprès d'un Controller situé dans une zone satellite.
- Un VDA situé dans une zone satellite s'enregistre auprès d'un Controller local, si possible (Il est considéré comme Controller préféré). Si aucun Controller local n'est disponible (par exemple, lorsque les Controller locaux ne peuvent pas accepter d'enregistrements VDA supplémentaires ou si les Controller locaux ont échoué), le VDA tente de s'enregistrer auprès d'un Controller de la zone principale. Dans ce cas, le VDA reste dans la zone principale sans être enregistré, même si un Controller de la zone satellite devient de nouveau disponible. Un VDA situé dans une zone satellite ne tentera jamais de s'enregistrer auprès d'un Controller situé dans une autre zone satellite.
- Lorsque la mise à jour automatique est activée pour la découverte VDA de Controller, et que vous spécifiez une liste d'adresses de Controller lors de l'installation du VDA, un Controller est sélectionné de façon aléatoire à partir de cette liste pour l'enregistrement initial (quelle que soit la zone dans laquelle le Controller réside). Une fois que la machine avec ce VDA est redémarrée, le VDA s'enregistre de préférence auprès d'un Controller de sa zone locale.
- Si un Controller d'une zone satellite échoue, il bascule vers un autre Controller local, si possible. Si aucun Controller local n'est disponible, il bascule vers un Controller de la zone principale.
- Si vous déplacez un Controller dans ou hors d'une zone, et que la mise à jour automatique est activée, les VDA des deux zones reçoivent des listes mises à jour qui indiquent quels Controller sont locaux et lesquels se trouvent dans la zone principale, de façon à ce qu'ils sachent avec lesquels ils peuvent s'enregistrer et accepter des connexions.
- Si vous déplacez un catalogue de machines vers une autre zone, les VDA de ce catalogue s'enregistrent auprès des Controller situés dans la zone dans laquelle vous avez déplacé le catalogue (Lorsque vous déplacez un catalogue vers une zone qui est mal connectée à la zone actuelle (par exemple, via un réseau à latence élevée ou à faible bande passante), veillez également à déplacer toute connexion hôte associée vers la même zone.)
- Les Controller de la zone principale conservent les données de location de connexion pour toutes les zones. Les Controller situés dans des zones satellite conservent les données de location de connexion pour leur propre zone et la zone principale, mais pas les données des autres zones satellite.

Si tous les Controller de la zone principale échouent :

- Studio ne peut pas se connecter au site.
- Impossible de se connecter aux VDA de la zone principale.
- Les performances du site vont se dégrader de plus en plus jusqu'à ce que les Controller de la zone principale deviennent disponibles.

Pour les sites contenant des VDA de versions antérieures à la version 7.7 :

- Un VDA situé dans une zone satellite accepte les requêtes de Controller situés dans sa zone locale et la zone principale (Les VDA à partir de la version 7.7 peuvent accepter les demandes de Controller d'autres zones satellite).
- Un VDA situé dans une zone satellite s'enregistre auprès d'un Controller situé dans la zone principale ou la zone locale de façon aléatoire. (Les VDA à partir de la version 7.7 préfèrent la zone locale).

Préférence de zone

> **Important :**
>
> Pour utiliser la fonctionnalité de préférence de zone, vous devez utiliser StoreFront 3.7 et NetScaler Gateway 11.0-65.x au minimum.

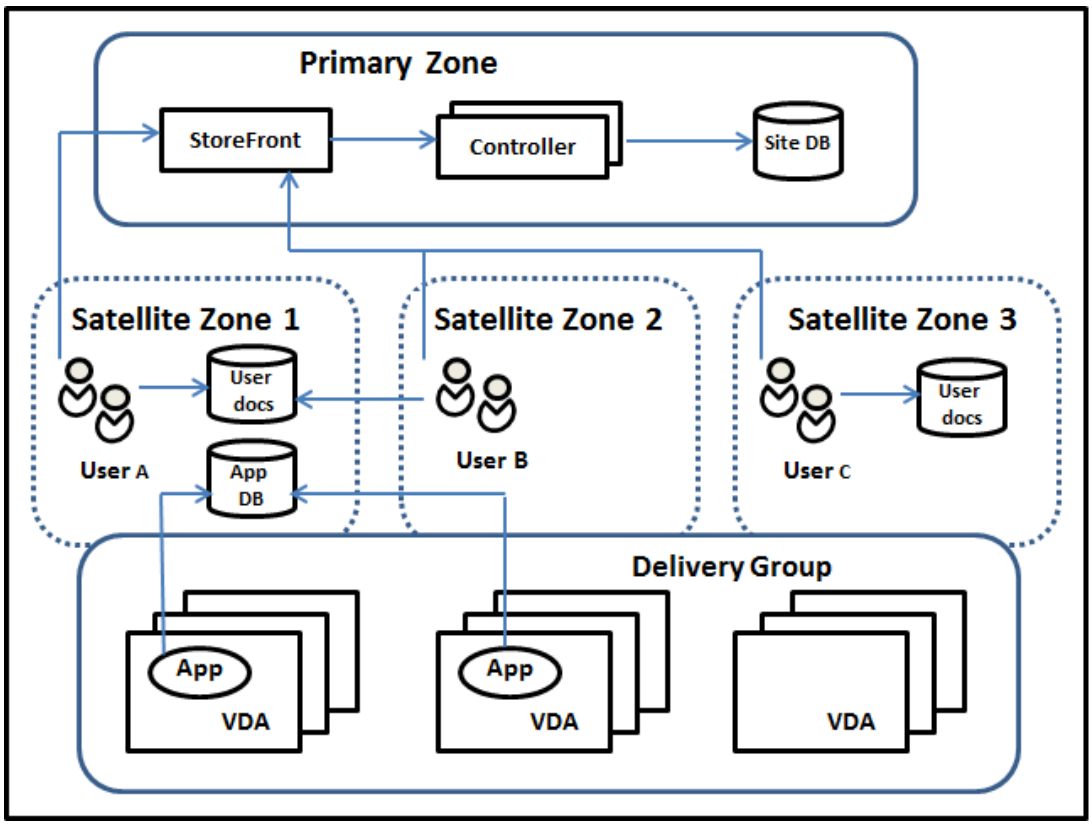
Dans un site multi-zone, la fonctionnalité de préférence de zone permet à l'administrateur de mieux contrôler les VDA utilisés pour lancer une application ou un bureau.

Comment fonctionne la préférence de zone

Il existe trois formes de préférence de zone. Il est possible d'utiliser un VDA situé dans une zone spécifique, en fonction des éléments suivants :

- Emplacement où les données de l'application sont stockées. Il s'agit de la zone d'accueil de l'application.
- Emplacement de base des données de l'utilisateur, comme un profil ou un partage. Il s'agit de la zone d'accueil de l'utilisateur.
- Emplacement actuel de l'utilisateur (où Citrix Receiver est exécuté). Il s'agit de l'emplacement de l'utilisateur.

Le graphique suivant illustre un exemple de configuration multi-zone.



Dans cet exemple, les VDA sont répartis entre trois zones satellite, mais ils sont tous dans le même groupe de mise à disposition. Par conséquent, le broker peut choisir le VDA à utiliser pour une demande de lancement d'un utilisateur. Cet exemple montre qu'il existe plusieurs emplacements où les utilisateurs peuvent exécuter leurs points de terminaison Citrix Receiver : l'utilisateur A utilise une machine avec Citrix Receiver dans la zone satellite 1 ; l'utilisateur B utilise une machine dans la zone satellite 2. Les documents d'un utilisateur peuvent être stockés dans plusieurs emplacements : les utilisateurs A et B utilisent un partage basé dans la zone satellite 1 ; l'utilisateur C utilise un partage de la zone satellite C. De plus, l'une des applications publiées utilise une base de données qui se trouve dans la zone satellite 1.

Vous pouvez associer un utilisateur ou une application avec une zone en configurant une zone d'accueil pour l'utilisateur ou l'application. Le broker du Delivery Controller utilise ces associations pour sélectionner la zone dans laquelle une session est lancée, si les ressources sont disponibles. Vous pouvez :

- Configurer la zone d'accueil d'un utilisateur en ajoutant un utilisateur à une zone.
- Configurer la zone d'accueil d'une application en modifiant les propriétés de l'application.

Un utilisateur ou une application ne peut avoir qu'une seule zone d'accueil à la fois (Il peut exister une exception pour les utilisateurs qui peuvent être associés à plusieurs zones s'ils sont membres de plusieurs groupes d'utilisateurs ; veuillez consulter la section « Autres considérations ». Toutefois, même dans ce cas, le broker utilise une seule zone d'accueil).

Bien que les préférences de zone pour les utilisateurs et les applications puissent être configurées, le broker sélectionne une seule zone préférée pour le lancement. L'ordre de priorité par défaut pour sélectionner la zone préférée est : accueil application > accueil utilisateur > emplacement utilisateur. (vous pouvez limiter la séquence, comme décrit dans la section suivante). Lorsqu'un utilisateur lance une application :

- Si l'application est associée à une zone (accueil application), la zone préférée est la zone d'accueil de cette application.
- Si l'application n'est pas associée à une zone, mais si l'utilisateur est associé à une zone (accueil utilisateur), la zone préférée est la zone d'accueil de cet utilisateur.
- Si ni l'application ni l'utilisateur n'est associé à une zone, la zone préférée est la zone dans laquelle l'utilisateur exécute une instance de Citrix Receiver (emplacement utilisateur). Si cette zone n'est pas définie, le VDA et la zone sont sélectionnés de façon aléatoire. L'équilibrage de charge est appliqué à tous les VDA dans la zone préférée. S'il n'existe aucune zone préférée, l'équilibrage de charge est appliqué à tous les VDA du groupe de mise à disposition.

Configuration de la préférence de zone

Lorsque vous configurez (ou supprimez) une zone d'accueil pour un utilisateur ou une application, vous pouvez restreindre la façon dont la préférence de zone sera (ou ne sera pas) utilisée.

- **Utilisation obligatoire de la zone d'accueil utilisateur :** dans un groupe de mise à disposition, vous pouvez spécifier qu'une session devrait être lancée dans la zone d'accueil de l'utilisateur (si l'utilisateur dispose d'une zone d'accueil), sans basculement vers une autre zone si les ressources ne sont pas disponibles dans la zone d'accueil. Cette restriction est utile lorsque vous souhaitez éviter les risques de copie de profils ou de fichiers de données importants entre les zones. En d'autres termes, vous souhaitez plutôt interdire le lancement d'une session plutôt que de lancer une session dans une zone différente.
- **Utilisation obligatoire de la zone d'accueil de l'application :** de même, lorsque vous configurez une zone d'accueil pour une application, vous pouvez indiquer que l'application doit être lancée uniquement dans cette zone, sans basculement vers une autre zone si les ressources ne sont pas disponibles dans la zone d'accueil de l'application.
- **Aucune zone d'accueil de l'application et ignorer la zone d'accueil utilisateur configurée :** si vous ne spécifiez pas de zone d'accueil pour une application, vous pouvez également spécifier qu'aucune des zones utilisateur ne devrait être considérée lors du lancement de cette application. Par exemple, vous pouvez préférer que les utilisateurs exécutent une application spécifique sur un VDA proche de la machine qu'ils utilisent (où Citrix Receiver est exécuté), utilisant alors l'emplacement de l'utilisateur comme préférence de zone, même si certains utilisateurs peuvent disposer d'une zone d'accueil différente.

Comment les zones préférées affectent les sessions

Lorsqu'un utilisateur lance une application ou un bureau, le broker préfère utiliser la zone préférée, plutôt que d'utiliser une session existante.

Si l'utilisateur qui démarre une application ou un bureau est déjà dans une session qui est appropriée pour la ressource en cours de démarrage (par exemple, qui peut utiliser le partage de session pour une application, ou une session qui exécute déjà la ressource en cours de démarrage), mais que la session s'exécute sur un VDA situé dans une zone différente de la zone préférée pour l'utilisateur/application, le système peut créer une nouvelle session. Cela permet de démarrer dans la zone appropriée (si elle dispose d'une capacité disponible), plutôt que de se reconnecter à une session dans une zone moins adaptée aux besoins de cette session.

Pour éviter une session orpheline ne pouvant plus être contactée, la reconnexion est autorisée à des sessions déconnectées existantes, même si elles ne se trouvent pas dans une zone préférée.

L'ordre de préférence pour un démarrage réussi des sessions est le suivant :

1. Se reconnecter à une session existante dans la zone préférée.
2. Se reconnecter à une session déconnectée existante dans une zone différente de la zone préférée.
3. Démarrer une nouvelle session dans la zone préférée.
4. Se reconnecter à une session connectée existante dans une zone différente de la zone préférée.
5. Démarrer une nouvelle session dans une zone différente de la zone préférée.

Autres considérations pour les préférences de zone

- Si vous configurez une zone d'accueil pour un groupe d'utilisateurs (par exemple, un groupe de sécurité), les utilisateurs de ce groupe (via une appartenance directe ou indirecte) sont associés à la zone spécifiée. Toutefois, un utilisateur peut appartenir à plusieurs groupes de sécurité, et, par conséquent, être associé à une autre zone d'accueil configurée via d'autres appartenances à un groupe. Dans de tels cas, déterminer la zone d'accueil de l'utilisateur peut être aléatoire.

Si un utilisateur est associé à une zone d'accueil qui n'a pas été acquise par l'appartenance à un groupe, cette zone est utilisée pour la préférence de zone. Toute association de zone acquise par l'appartenance à un groupe est ignorée.

Si l'utilisateur est associé à plusieurs zones acquises uniquement via l'appartenance à un groupe, le broker choisit entre les zones de manière aléatoire. Une fois que le broker a effectué ce choix, cette zone est utilisée pour chaque démarrage de session suivant, jusqu'à ce que l'appartenance de l'utilisateur à ce groupe change.

- Si la préférence de zone est l'emplacement utilisateur, Citrix Receiver sur la machine de point de terminaison doit être détecté par le boîtier Citrix NetScaler Gateway par le biais duquel la

machine est connectée. NetScaler doit être configuré pour associer des plages d'adresses IP avec certaines zones et l'identité de la zone découverte doit être transmise via StoreFront au Controller.

Pour plus d'informations sur les préférences de zone, consultez la section Fonctionnement des préférences de zone.

Considérations, configurations requises et recommandations

- Vous pouvez placer les éléments suivants dans une zone : Controller, catalogues de machines, connexions hôtes, utilisateurs et applications. Si un catalogue de machines utilise une connexion hôte, le catalogue et la connexion doivent se trouver dans la même zone pour une connexion à faible latence et à bande passante élevée.
- Lorsque vous placez des éléments dans une zone satellite, cette opération affecte la façon dont le site interagit avec eux et avec d'autres objets qui leur sont liés.
  - Lorsque des machines Controller sont placées dans une zone satellite, il est supposé que ces machines disposent d'une bonne connectivité (locale) aux hyperviseurs et aux machines VDA dans la même zone satellite. Les Controller dans cette zone satellite sont ensuite préférés aux Controller de la zone principale pour gérer ces hyperviseurs et machines VDA.
  - Lorsqu'une connexion d'hyperviseur est placée dans une zone satellite, il est supposé que tous les hyperviseurs gérés via cette connexion d'hyperviseur résident également dans cette zone satellite. Les Controller dans cette zone satellite sont alors préférés aux Controller de la zone principale lors de la communication avec cette connexion d'hyperviseur.
  - Lorsqu'un catalogue de machines est placé dans une zone satellite, il est supposé que toutes les machines VDA de ce catalogue se trouvent dans la zone satellite. Les Controller locaux sont préférés aux Controller de la zone principale lors de la tentative d'enregistrement auprès du site, une fois que le mécanisme de mise à jour automatique de liste des Controller a été activé après le premier enregistrement de chaque VDA.
  - Des instances de NetScaler Gateway peuvent également être associées à des zones. Cela se fait dans le cadre de la configuration du routage HDX optimal de StoreFront plutôt que, comme pour les autres éléments décrits ici, dans le cadre de la configuration du site XenApp ou XenDesktop. Lorsqu'une passerelle NetScaler Gateway est associée à une zone, elle est utilisée de préférence lorsque des connexions HDX à des machines VDA dans cette zone sont utilisées.
- Lorsque vous créez un site de production, puis créez le premier catalogue de machines et le premier groupe de mise à disposition, tous les éléments se trouvent dans la zone principale ; vous ne pouvez pas créer de zones satellite tant que cette configuration initiale n'a pas été effectuée (Si vous créez un site vide, la zone principale contient initialement un seul Controller ; vous pouvez créer des zones satellite avant ou après la création d'un catalogue de machines

et d'un groupe de mise à disposition).

- Lorsque vous créez la première zone satellite contenant un ou plusieurs éléments, tous les autres éléments de votre site restent dans la zone principale.
- La zone principale est appelée « Principale » par défaut ; vous pouvez changer ce nom. Bien que Studio indique quelle zone est la zone principale, il est recommandé d'utiliser un nom facile à identifier pour la zone principale. Vous pouvez réaffecter la zone principale (c'est-à-dire définir une autre zone comme zone principale), mais elle doit toujours contenir la base de données du site et les serveurs haute disponibilité.
- La base de données du site doit toujours se trouver dans la zone principale.
- Après avoir créé une zone, vous pouvez déplacer les éléments d'une zone à une autre. Veuillez noter que cette flexibilité vous permet de potentiellement séparer les éléments qui fonctionnent mieux lorsqu'ils sont à proximité ; par exemple, le déplacement d'un catalogue de machines vers une autre zone que la connexion (hôte) qui crée les machines dans le catalogue peut affecter les performances. Par conséquent, prenez en compte les effets potentiels du déplacement d'éléments entre les zones. Gardez un catalogue et la connexion hôte qu'il utilise dans la même zone ou dans des zones bien connectées (par exemple, via un réseau à faible latence et à bande passante élevée).
- Pour des performances optimales, installez Studio et Director uniquement dans la zone principale. Si vous souhaitez utiliser une autre instance de Studio dans une zone satellite (par exemple, si une zone satellite contenant des Controller est utilisée pour le basculement au cas où la zone principale serait inaccessible), exécutez Studio en tant qu'application publiée localement. Vous pouvez également accéder à Director à partir d'une zone satellite car il s'agit d'une application Web.
- Dans l'idéal, NetScaler Gateway situé dans une zone satellite doit être utilisé pour les connexions utilisateur entrant dans cette zone depuis d'autres zones ou des emplacements externes, mais vous pouvez l'utiliser pour les connexions à l'intérieur de la zone.
- **Rappel :** pour utiliser la fonctionnalité de préférence de zone, vous devez utiliser StoreFront 3.7 et NetScaler Gateway 11.0-65.x au minimum
- Pour plus de détails techniques et des informations sur les performances, consultez l'article Zones Deep Dive.

Limites de la qualité des connexions

Les Controller de la zone satellite effectuent les interactions SQL directement avec la base de données du site. Cela impose certaines limites sur la qualité de la liaison entre la zone satellite et la zone principale qui contient la base de données du site. Les limites spécifiques sont relatives au nombre de VDA et de sessions utilisateur sur ces VDA qui sont déployés dans la zone satellite. Ainsi, des zones satellite avec uniquement quelques VDA et sessions peuvent fonctionner avec une connexion à la base de données de qualité plus faible que des zones satellite avec un grand nombre de sessions et de VDA.

Pour plus d'informations, consultez la section Latency and SQL Blocking Query Improvements.

Impact de la latence sur les performances de négociation

Bien que les zones permettent aux utilisateurs de se trouver sur des liaisons à latence plus élevée, à condition qu'il y ait un broker local, la latence supplémentaire a un impact inévitable sur l'utilisateur final. La plupart du temps, les utilisateurs observeront une certaine lenteur causée par l'aller-retour entre les Controller de la zone satellite et la base de données du site.

Avec le lancement d'applications, il est possible de rencontrer des délais supplémentaires pendant que le processus de négociation de session identifie les VDA appropriés auxquels envoyer des demandes de lancement de session.

Créer et gérer des zones

Un administrateur complet peut effectuer toutes les tâches de création et de gestion de zone. Toutefois, vous pouvez également créer un rôle personnalisé qui vous permet de créer, modifier ou supprimer une zone. Le déplacement d'éléments entre les zones ne nécessite pas d'autorisations liées à la zone (à l'exception des autorisations en lecture) ; cependant, vous devez disposer d'une autorisation de modification pour les éléments que vous déplacez. Par exemple, pour déplacer un catalogue de machines d'une zone vers une autre, vous devez disposer d'une autorisation de modification pour ce catalogue de machines. Pour plus d'informations, veuillez consulter l'article Administration déléguée.

Si vous utilisez Provisioning Services : étant donné que la console Provisioning Services fournie avec cette version ne sait pas identifier les zones, Citrix vous recommande d'utiliser Studio pour créer des catalogues de machines que vous souhaitez placer dans des zones satellite. Utilisez l'assistant Studio pour créer le catalogue, et spécifiez la zone satellite appropriée. Puis, utilisez la console Provisioning Services pour provisionner des machines dans ce catalogue (Si vous créez le catalogue à l'aide de l'assistant Provisioning Services, il sera placé dans la zone principale et vous devrez utiliser Studio pour le déplacer vers la zone satellite ultérieurement).

Créer une zone

1. Sélectionnez **Configuration > Zones** dans le volet de navigation Studio.
2. Sélectionnez **Créer une zone** dans le volet Actions.
3. Entrez un nom pour la zone et une description (facultatif). Le nom doit être unique dans le site.
4. Sélectionnez les éléments à placer dans la nouvelle zone. Vous pouvez filtrer ou effectuer une recherche dans la liste des éléments à partir de laquelle vous sélectionnez. Vous pouvez également créer une zone vide ; dans ce cas, ne sélectionnez pas d'éléments.
5. Cliquez sur **Enregistrer**.

Au lieu de cette méthode, vous pouvez sélectionner un ou plusieurs éléments dans Studio, puis sélectionner **Créer une zone** dans le volet Actions.

Modifier le nom ou la description d'une zone

1. Sélectionnez **Configuration > Zones** dans le volet de navigation Studio.
2. Sélectionnez une zone dans le volet central, puis sélectionnez **Modifier la zone** dans le volet Actions.
3. Modifiez le nom et/ou la description de la zone. Si vous modifiez le nom de la zone principale, assurez-vous que la zone reste facile à identifier comme zone principale.
4. Cliquez sur **OK** ou **Appliquer**.

Déplacer des éléments d'une zone à une autre

1. Sélectionnez **Configuration > Zones** dans le volet de navigation Studio.
2. Sélectionnez une zone dans le volet central, puis sélectionnez un ou plusieurs éléments.
3. Faites glisser les éléments vers la zone de destination, ou sélectionnez **Déplacer des éléments** dans le panneau Actions et spécifiez la zone vers laquelle les déplacer.

Un message de confirmation dresse la liste des éléments que vous avez sélectionnés et demande si vous êtes sûr de vouloir déplacer tous ces éléments.

Rappel : si un catalogue de machines utilise une connexion hôte vers un hyperviseur ou un service de cloud, le catalogue et la connexion doivent se trouver dans la même zone. Sinon, les performances peuvent être affectées. Si vous déplacez un élément, déplacez l'autre.

Supprimer une zone

Une zone doit être vide pour pouvoir être supprimée. Vous ne pouvez pas supprimer la zone principale.

1. Sélectionnez **Configuration > Zones** dans le volet de navigation Studio.
2. Sélectionnez une zone dans le volet central.
3. Sélectionnez **Supprimer la zone** dans le volet Actions. Si la zone n'est pas vide (elle contient des éléments), vous êtes invité à choisir la zone vers laquelle ces éléments seront déplacés.
4. Confirmez la suppression.

Ajouter une zone d'accueil pour un utilisateur

La configuration d'une zone d'accueil pour un utilisateur consiste à *ajouter un utilisateur à une zone*.

1. Sélectionnez **Configuration > Zones** dans le volet de navigation Studio et sélectionnez une zone dans le volet central.
2. Sélectionnez **Ajouter des utilisateurs à la zone** dans le volet Actions.
3. Dans la boîte de dialogue **Ajouter des utilisateurs à la zone**, cliquez sur **Ajouter**, puis sélectionnez les utilisateurs et les groupes d'utilisateurs à ajouter à la zone. Si vous spécifiez des utilisateurs qui disposent déjà d'une zone d'accueil, un message offre deux options : **Oui** = ajouter uniquement les utilisateurs que vous avez spécifiés qui ne disposent pas d'une zone d'accueil ; **Non** = retourner à la boîte de dialogue de sélection des utilisateurs.
4. Cliquez sur **OK**.

Pour les utilisateurs associés à une zone d'accueil, vous pouvez demander à ce que les sessions démarrent uniquement à partir de leur zone d'accueil :

1. Créez ou modifiez un groupe de mise à disposition.
2. Sur la page **Utilisateurs**, sélectionnez la case **Les sessions doivent être lancées dans la zone d'accueil d'un utilisateur, si une zone a été configurée**.

Toutes les sessions lancées par un utilisateur dans ce groupe de mise à disposition doivent être lancées à partir de machines se trouvant dans la zone d'accueil de l'utilisateur. Si un utilisateur du groupe de mise à disposition n'est pas associé à une zone d'accueil, ce paramètre n'a aucun effet.

Supprimer une zone d'accueil pour un utilisateur

Cette procédure consiste à supprimer un utilisateur d'une zone.

1. Sélectionnez **Configuration > Zones** dans le volet de navigation Studio et sélectionnez une zone dans le volet central.
2. Sélectionnez **Supprimer des utilisateurs de la zone** dans le volet Actions.
3. Dans la boîte de dialogue **Supprimer des utilisateurs de la zone**, cliquez sur **Supprimer**, puis sélectionnez les utilisateurs et les groupes d'utilisateurs à supprimer de la zone. Notez que cette action supprime les utilisateurs de la zone uniquement ; ces utilisateurs restent dans les groupes de mise à disposition et les groupes d'applications auxquels ils appartiennent.
4. Confirmez la suppression lorsque vous y êtes invité.

Gérer les zones d'accueil pour les applications

La configuration d'une zone d'accueil pour une application consiste à ajouter une application à une zone. Par défaut, dans un environnement multi-zone, une application ne dispose pas de zone d'accueil.

La zone d'accueil d'une application est spécifiée dans les propriétés de l'application. Vous pouvez configurer les propriétés de l'application lorsque vous ajoutez l'application à un groupe ou ultérieurement, en sélectionnant l'application dans Studio et en modifiant ses propriétés.

- Lors de la création d'un groupe de mise à disposition, la création d'un groupe d'applications ou l'ajout d'applications à des groupes existants, sélectionnez **Propriétés** sur la page **Applications** de l'assistant.
- Pour modifier les propriétés d'une application lorsque l'application est ajoutée, sélectionnez **Applications** dans le volet de navigation de Studio. Sélectionnez une application, puis sélectionnez **Modifier les propriétés d'application** dans le volet Actions.

Sur la page **Zones** des propriétés/paramètres de l'application :

- Si vous souhaitez que l'application soit associée à une zone d'accueil :
  - Sélectionnez le bouton radio **Utiliser la zone sélectionnée pour déterminer**, puis sélectionnez la zone dans le menu déroulant.
  - Si vous souhaitez que l'application démarre uniquement depuis la zone sélectionnée (et non pas à partir d'une autre zone), sélectionnez la case à cocher sous la sélection de zone.
- Si vous ne souhaitez pas que l'application soit associée à une zone d'accueil :
  - Sélectionnez le bouton radio **Ne pas configurer de zone d'accueil**.
  - Si vous ne souhaitez pas que le broker prenne en compte les zones utilisateur configurées lors du lancement de cette application, sélectionnez la case à cocher sous le bouton radio. Dans ce cas, ni la zone d'accueil de l'application ni la zone d'accueil de l'utilisateur ne sera utilisée pour déterminer l'emplacement du lancement de cette application.

Autres actions impliquant la spécification de zones

Lorsque vous ajoutez une connexion hôte ou que vous créez un catalogue de machines (à un autre moment que lors de la création du site), vous pouvez spécifier une zone à laquelle l'élément sera attribué, si vous avez déjà créé au moins une zone satellite.

Dans la plupart des cas, la zone principale est la valeur par défaut. Lors de l'utilisation de Machine Creation Services pour créer un catalogue de machines, la zone qui est configurée pour la connexion hôte est sélectionnée automatiquement.

Si le site ne contient aucune zone satellite, il est supposé que la zone principale sera utilisée et la sélection de zone ne s'affiche pas.

Connexions et ressources

February 28, 2019

Introduction

Vous pouvez éventuellement créer votre première connexion pour héberger des ressources lorsque vous créez un site. Plus tard, vous pouvez modifier cette connexion et en créer de nouvelles. La configuration d'une connexion implique de sélectionner le type de connexion parmi les hyperviseurs et les services de cloud pris en charge. Le stockage et le réseau que vous sélectionnez constituent les ressources de cette connexion.

Les administrateurs en lecture seule peuvent afficher les détails de connexion et de ressources ; vous devez être un administrateur complet pour effectuer la connexion et des tâches de gestion des ressources. Consultez l'article Administration déléguée pour plus de détails.

Où trouver des informations sur les types de connexion

Vous pouvez utiliser les plates-formes de virtualisation prises en charge pour héberger et gérer des machines dans votre environnement XenApp ou XenDesktop. L'article Configuration système requise répertorie les types pris en charge. Vous pouvez utiliser les solutions de déploiement cloud prises en charge pour héberger les composants du produit et provisionner des machines virtuelles. Ces ressources informatiques de pool de solutions destinées à créer des clouds d'infrastructure as a service (IaaS) publics, privés et hybrides.

Pour de plus amples informations, consultez les sources d'informations suivantes.

Microsoft Hyper-V

- Article Environnements de virtualisation Microsoft System Center Virtual Machine Manager.
- Documentation Microsoft.

Microsoft Azure

- Article Environnements de virtualisation Microsoft Azure.
- Documentation Microsoft.

Microsoft Azure Resource Manager

- Article Environnements de virtualisation Microsoft Azure Resource Manager.
- Documentation Microsoft.

services Web Amazon (AWS)

- Citrix XenDesktop sur AWS.
- Documentation AWS.
- Lorsque vous créez une connexion dans Studio, vous devez fournir la clé API et la clé secrète. Vous pouvez exporter le fichier de clé contenant ces valeurs à partir d'AWS, puis les importer. Vous devez également fournir la région, la zone de disponibilité, le nom du VPC, les adresses

de sous-réseau, le nom du domaine, les noms de groupe de sécurité et les informations d'identification.
- Le fichier d'informations d'identification pour le compte AWS de racine, (récupéré à partir de la console AWS) n'est pas au même format que les fichiers d'informations d'identification téléchargés pour les utilisateurs standard AWS. Par conséquent, Studio ne peut pas utiliser le fichier pour remplir les champs de clé API et de clé secrète. Vérifiez que vous utilisez les fichiers d'informations d'identification AWS IAM.

CloudPlatform

- Documentation CloudPlatform.
- Lorsque vous créez une connexion dans Studio, vous devez fournir la clé API et la clé secrète. Vous pouvez exporter le fichier de clé contenant ces valeurs à partir de CloudPlatform, puis importer ces valeurs dans Studio.

Citrix XenServer

- Documentation Citrix XenServer.
- Lorsque vous créez une connexion, vous devez fournir les informations d'identification d'un administrateur avancé de VM ou d'un utilisateur de niveau plus élevé.
- Citrix vous recommande d'utiliser HTTPS pour sécuriser les communications avec XenServer. Pour utiliser HTTPS, vous devez remplacer le certificat SSL par défaut installé sur XenServer ; consultez l'article CTX128656.
- Vous pouvez configurer la haute disponibilité si elle est activée sur XenServer. Citrix vous recommande de sélectionner tous les serveurs du pool (dans Modifier les serveurs HA) pour permettre la communication avec XenServer au cas où le pool principal échoue.
- Vous pouvez sélectionner un type et un groupe de processeur graphique, ou de pass-through, si XenServer prend en charge vGPU. La vue indique si la sélection possède des ressources GPU dédiées.

Nutanix Acropolis

- Article Environnements de virtualisation Nutanix.
- Documentation Nutanix.

VMware

- Article Environnement de virtualisation VMware.
- Documentation du produit VMware.

Stockage hôte

Lors du provisioning de machines, les données sont classées par type :

- Données du système d'exploitation, ce qui comprend les images principales.

- Données temporaires, ce qui comprend toutes les données non persistantes écrites sur les machines provisionnées avec MCS, les fichiers de pages Windows, les données du profil utilisateur et les données qui sont synchronisées avec ShareFile. Ces données sont supprimées chaque fois qu'une machine redémarre.
- Données stockées sur les Personal vDisks.

La mise à disposition d'espaces de stockage distincts pour chaque type de données peut réduire la charge et améliorer les performances IOPS (opérations E/S par seconde) sur chaque périphérique de stockage, ce qui permet d'utiliser les ressources disponibles de l'hôte de manière optimale. Cela permet également d'utiliser un stockage approprié pour les différents types de données : la persistance et la résilience sont des facteurs plus importants pour certaines données que pour d'autres.

Le stockage peut être partagé (centralisé, séparé de l'hôte, utilisé par tous les hôtes) ou local sur un hyperviseur. Par exemple, un stockage partagé central peut être un ou plusieurs volumes de stockage en cluster Windows Server 2012 (avec ou sans stockage attaché), ou l'appliance d'un fournisseur de stockage. Le stockage central peut également fournir ses propres optimisations telles que des chemins de contrôle de stockage de l'hyperviseur et un accès direct au travers de plug-ins de partenaires.

Le stockage des données temporaires localement évite d'avoir à traverser le réseau pour accéder à un espace de partagé. Cela permet également de réduire la charge ((opérations E/S par seconde) sur le périphérique de stockage partagé. Le stockage partagé peut être plus coûteux, par conséquent le stockage des données localement peut réduire les dépenses. Ces avantages doivent être pondérés par rapport à la disponibilité d'un stockage suffisant sur les serveurs hyperviseur.

Lorsque vous créez une connexion, vous devez choisir l'une des deux méthodes de gestion du stockage : stockage partagé par les hyperviseurs, ou stockage local sur l'hyperviseur.

> **Remarque :**
>
> Lorsque vous utilisez le stockage local sur un ou plusieurs hôtes XenServer pour le stockage des données temporaires, assurez-vous que chaque emplacement de stockage du pool a un nom unique. (Pour modifier un nom dans XenCenter, cliquez avec le bouton droit sur le stockage et modifiez le nom de la propriété.)

Stockage partagé par les hyperviseurs

La méthode de stockage partagé par les hyperviseurs stocke centralement les données qui doivent être archivées à long terme, ce qui offre une gestion et une sauvegarde centralisées. Ce stockage contient les disques de système d'exploitation et les disques Personal vDisk.

Lorsque vous sélectionnez cette méthode, vous pouvez choisir d'utiliser le stockage local (sur les serveurs dans le même pool d'hyperviseurs) pour les données temporaires qui ne nécessitent pas d'être archivées ou d'autant de résilience que les données dans le stockage partagé. Ceci s'appelle la *mise en cache des données temporaires*. Le disque local permet de réduire le trafic vers le stockage

du système d'exploitation principal. Ce disque est effacé après chaque redémarrage de machine. Le disque est accessible via un cache mémoire en écriture continue. Gardez à l'esprit que si vous utilisez le stockage local pour les données temporaires, le VDA provisionné est associé à un hyperviseur hôte spécifique ; si cet hôte échoue, la VM ne peut pas démarrer.

Exception : si vous utilisez des volumes de stockage en cluster (CSV), Microsoft System Center Virtual Machine Manager n'autorise pas la création de disques de mise en cache des données temporaires sur le stockage local.

Lorsque vous créez une connexion, si vous activez l'option permettant de stocker les données temporaires localement, vous pouvez activer et configurer des valeurs autres que les valeurs par défaut pour la taille de disque et de mémoire pour chaque VM lorsque vous créez un catalogue de machines qui utilise cette connexion. Toutefois, les valeurs par défaut sont adaptées au type de connexion, et sont suffisantes pour la plupart des cas. Pour de plus amples informations, consultez l'article Créer des catalogues de machines.

L'hyperviseur peut également fournir des technologies d'optimisation par le biais d'une mise en cache de lecture locale des images de disque ; par exemple, XenServer offre IntelliCache. Cela peut également réduire le trafic réseau vers le stockage central.

Stockage local sur l'hyperviseur

La méthode de stockage local sur l'hyperviseur stocke les données localement sur l'hyperviseur. Avec cette méthode, les images principales et les autres données d'OS sont transférées vers tous les hyperviseurs utilisés dans le site, aussi bien pour la création initiale d'une machine que pour les mises à jour futures des images. Cela se traduit par un trafic important sur le réseau de gestion. Les transferts d'images sont également chronophages, et les images deviennent disponibles auprès de chaque hôte à un moment différent.

Lorsque vous sélectionnez cette méthode, vous pouvez choisir d'utiliser un stockage partagé pour les Personal vDisks, afin de fournir la résilience et la prise en charge de systèmes de sauvegarde et de récupération d'urgence.

Créer une connexion et des ressources

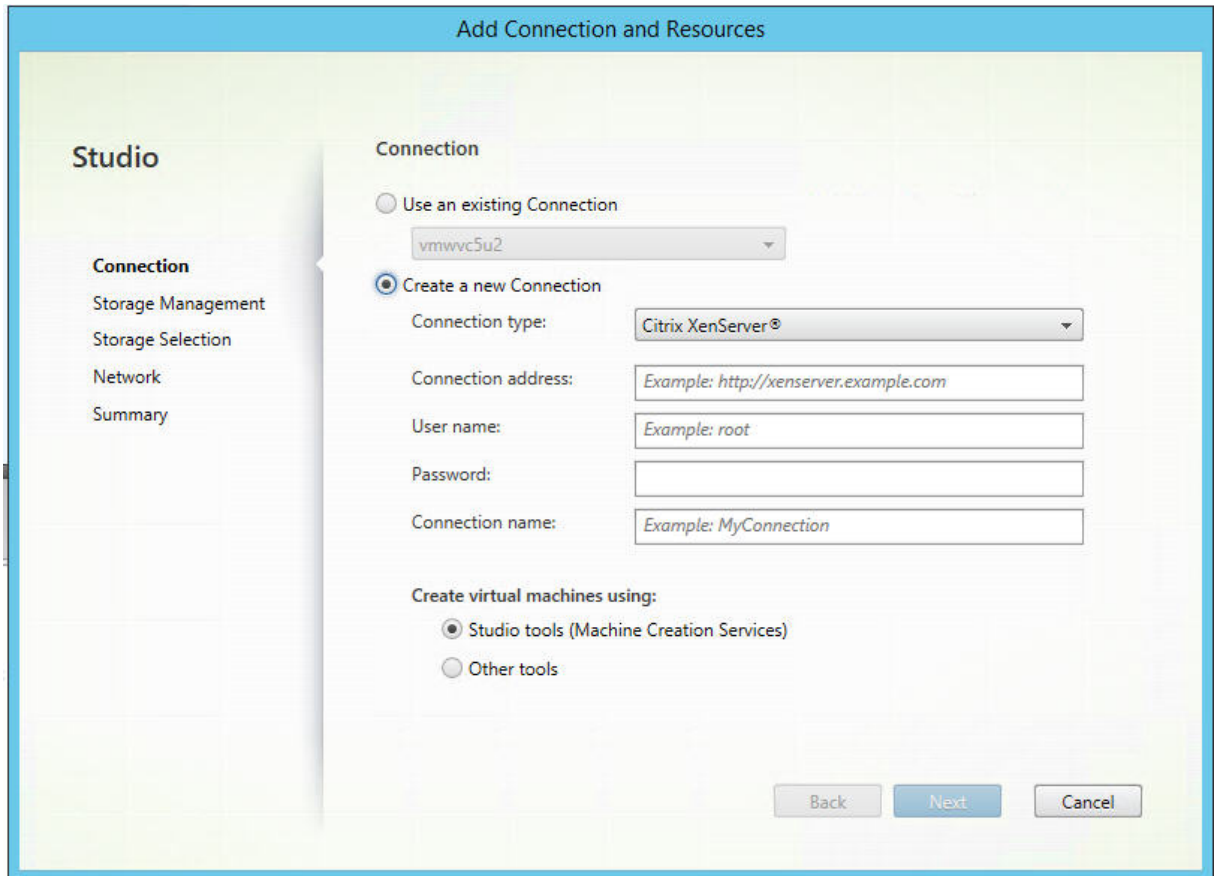
Vous pouvez éventuellement créer la première connexion lorsque vous créez le site. L'Assistant de création de site contient les pages de connexion décrites ci-dessous : connexion, gestion du stockage, sélection du stockage et le réseau.

Si vous créez une connexion après la création du site, commencez à l'étape 1 ci-dessous.

> **Important :**
>
> Les ressources hôte (stockage et réseau) doivent être disponibles avant de créer une connexion.

- Sélectionnez **Configuration > Hébergement** dans le volet de navigation de Studio.
- Sélectionnez **Ajouter une connexion et des ressources** dans le volet Actions.
- L'assistant vous guide à travers les pages suivantes (le contenu des pages dépend du type de connexion sélectionné). Après avoir complété chaque page, cliquez sur **Suivant** jusqu'à la page **Résumé**.

Connexion

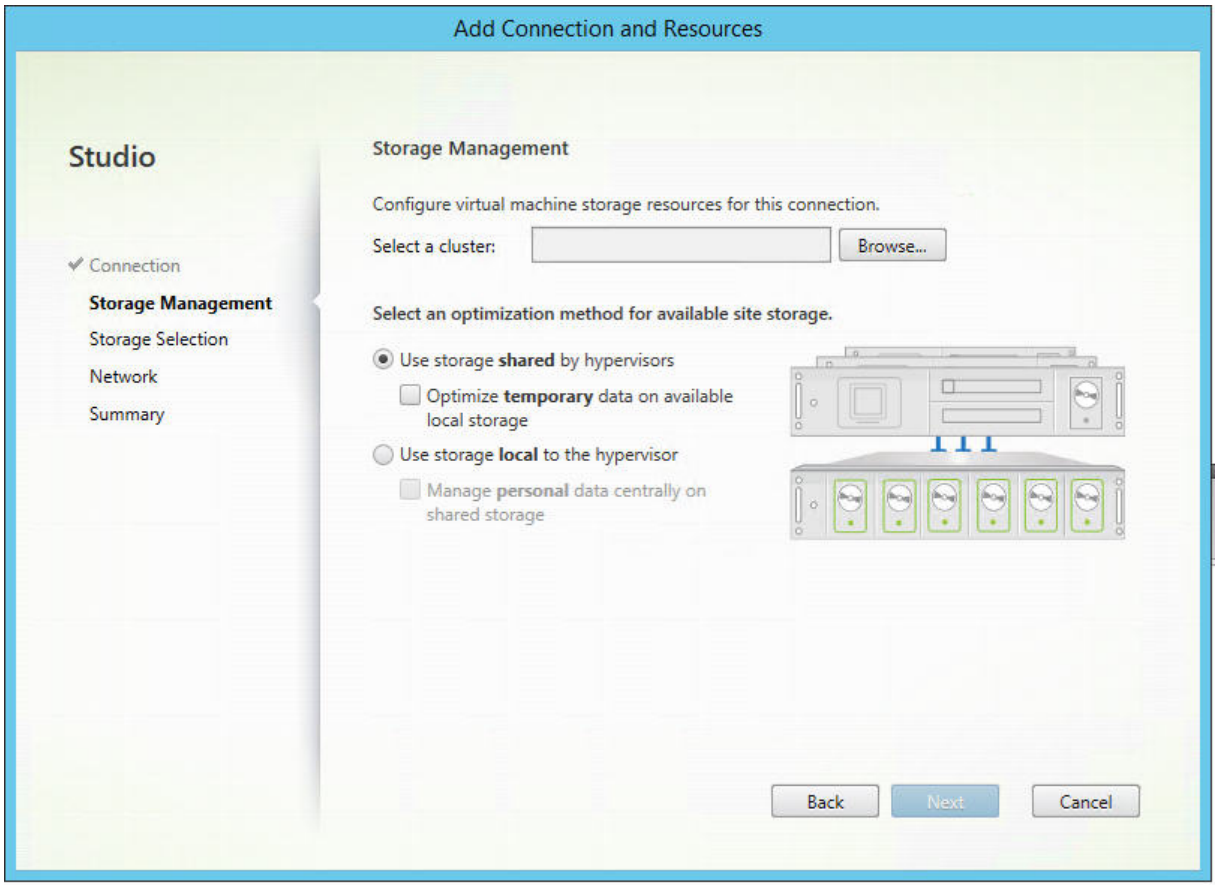


Sur la page **Connexion** :

- Pour créer une nouvelle connexion, sélectionnez **Créer une nouvelle connexion**. Pour créer une connexion basée sur la même configuration d'hôte qu'une connexion existante, sélectionnez **Utiliser une connexion existante**, puis choisissez la connexion appropriée
- Sélectionnez l'hyperviseur ou le service de cloud que vous utilisez dans le champ **Type de connexion**.
- Les champs relatifs à l'adresse de connexion et aux informations d'identification diffèrent en fonction du type de connexion sélectionné. Entrez les informations requises.

- Entrez un nom pour la connexion. Ce nom apparaît dans Studio.
- Choisissez l'outil que vous utilisez pour créer des machines virtuelles : les outils Studio (Machine Creation Services ou Provisioning Services) ou d'autres outils.

Gestion du stockage



Pour de plus amples informations sur les types et méthodes de gestion du stockage, consultez la section Stockage hôte.

Si vous configurez une connexion à un hôte Hyper-V ou VMware, sélectionnez un nom de cluster. D'autres types de connexion ne nécessitent pas de nom de cluster.

Sélectionnez une méthode de gestion du stockage : stockage partagé par les hyperviseurs ou stockage local sur l'hyperviseur.

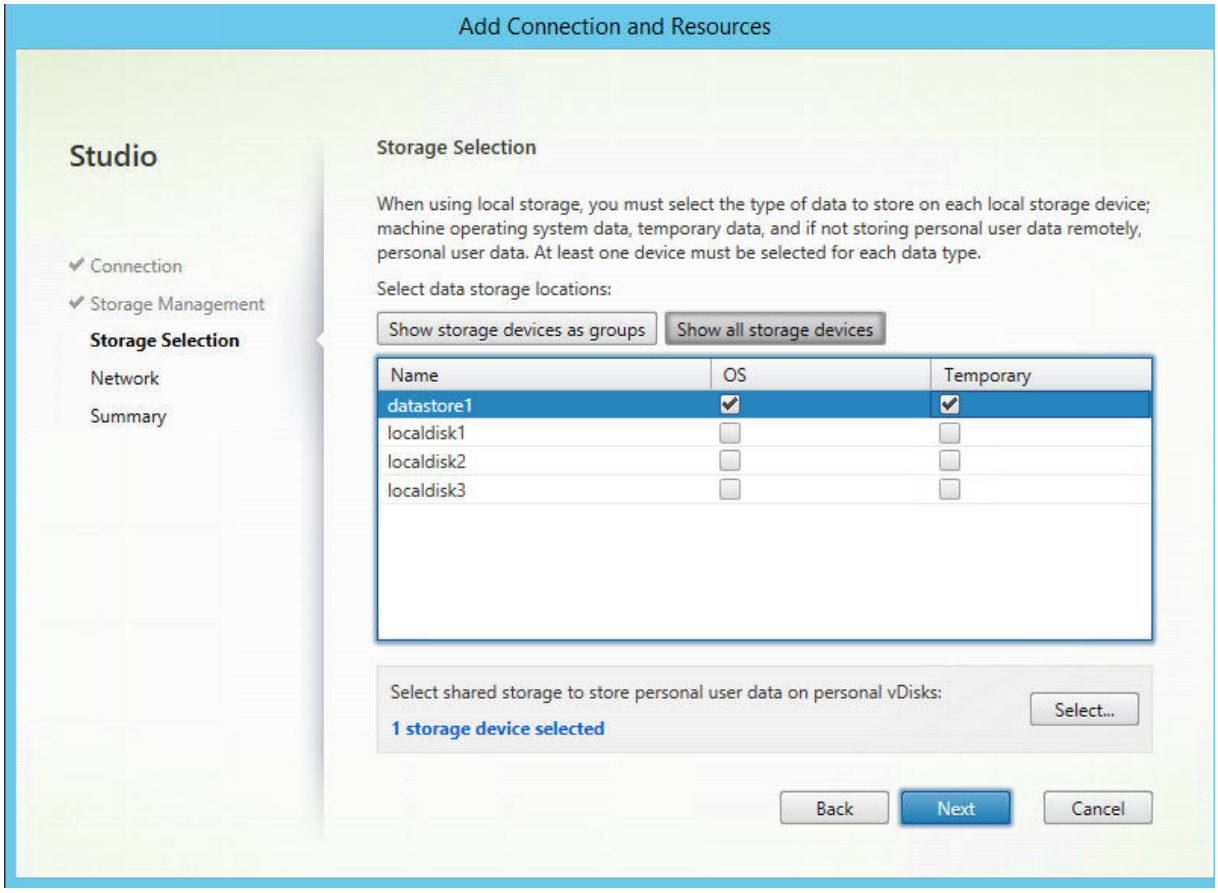
- Si vous choisissez le stockage partagé par les hyperviseurs, indiquez si vous souhaitez conserver les données temporaires sur l'espace de stockage local disponible. (Vous pouvez spécifier des tailles de stockage temporaire autres que les valeurs par défaut dans les catalogues de machines qui utilisent cette connexion.) **Exception :** lors de l'utilisation de volumes de stockage en cluster (CSV), Microsoft System Center Virtual Machine Manager n'autorise pas la création de disques de

mise en cache des données temporaires sur le stockage local, par conséquent la configuration de la gestion du stockage échouera dans Studio.

- Si vous choisissez le stockage local sur l'hyperviseur, indiquez si vous souhaitez gérer des données personnelles (Personal vDisk) sur l'espace de stockage partagé.

Si vous utilisez un espace de stockage partagé sur un hyperviseur XenServer, indiquez si vous souhaitez utiliser IntelliCache pour réduire la charge sur le périphérique de stockage partagé. Consultez la section Utiliser les connexions IntelliCache pour XenServer.

Sélection du stockage



Pour de plus amples informations sur la sélection du stockage, consultez la section Stockage hôte.

Sélectionnez au moins un périphérique de stockage hôte pour chaque type de données disponible. La méthode de gestion du stockage que vous avez sélectionnée sur la page précédente affecte les types de données disponibles sur cette page. Vous devez sélectionner au moins un périphérique de stockage pour chaque type de données pris en charge avant de pouvoir passer à la page suivante de l'assistant.

La partie inférieure de la page **Sélectionner un stockage** contient des options de configuration supplémentaires si vous avez sélectionné l'une des options suivantes sur la page précédente.

- Si vous avez choisi le stockage partagé par les hyperviseurs, et activé la case **Optimiser les données temporaires sur le stockage local disponible**, vous pouvez sélectionner les périphériques de stockage local (dans le même pool d'hyperviseurs) à utiliser pour des données temporaires.
- Si vous avez choisi le stockage local sur l'hyperviseur et activé la case **Gérer les données personnelles centralement sur le stockage partagé**, vous pouvez sélectionner les périphériques partagés à utiliser pour les données personnelles (PvD).

Le nombre de périphériques de stockage actuellement sélectionnés est affiché (dans le diagramme ci-dessus, « 1 périphérique de stockage sélectionné »). Lorsque vous placez le curseur sur cette entrée, les noms des périphériques sélectionnés s'affichent (sauf si aucun périphérique n'est configuré).

1. Cliquez sur **Sélectionner** pour modifier les périphériques de stockage à utiliser.
2. Dans la boîte de dialogue **Sélectionner un stockage**, activez ou désactivez les cases de périphérique de stockage, puis cliquez sur **OK**.

Réseau

Entrez un nom pour les ressources ; ce nom apparaît dans Studio pour identifier la combinaison stockage et réseau associée à la connexion.

Sélectionnez un ou plusieurs réseaux que les machines virtuelles utiliseront.

Synthèse

Vérifiez vos sélections ; si vous souhaitez apporter des modifications, revenez sur les pages précédentes de l'assistant. Une fois que vous avez terminé avec votre évaluation, cliquez sur **Terminer**.

Rappel : si vous avez choisi de stocker les données temporaires localement, vous pouvez configurer des valeurs autres que les valeurs par défaut pour le stockage des données temporaires lorsque vous créez le catalogue de machines contenant les machines utilisant cette connexion. Pour de plus amples informations, consultez l'article Créer des catalogues de machines.

Modifier les paramètres de connexion

N'utilisez pas cette procédure pour renommer une connexion ou pour créer une nouvelle connexion. Ces opérations sont différentes. Modifiez l'adresse uniquement si la machine hôte actuelle possède une nouvelle adresse ; si vous entrez l'adresse d'une autre machine, cela mettra fin à la connexion avec les catalogues de machines.

Vous ne pouvez pas modifier les paramètres GPU d'une connexion, car les catalogues de machines qui accèdent à cette ressource doivent utiliser une image principale appropriée spécifique au GPU. Créez une nouvelle connexion.

1. Sélectionnez **Configuration > Hébergement** dans le volet de navigation de Studio.
2. Sélectionnez la connexion, puis sélectionnez **Modifier la connexion** dans le volet Actions.
3. Vous trouverez ci-dessous les paramètres disponibles lorsque vous modifiez une connexion.
4. Lorsque vous avez terminé, cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Page **Propriétés de la connexion** :

- Pour modifier l'adresse et les informations d'identification de connexion, sélectionnez **Modifier les paramètres** et entrez de nouvelles informations.
- Pour spécifier les serveurs haute disponibilité pour une connexion XenServer, sélectionnez **Modifier les serveurs HA**. Citrix vous recommande de sélectionner tous les serveurs du pool pour permettre la communication avec XenServer au cas où le pool principal échoue.

Page **Avancé** :

Pour un type de connexion Microsoft System Center Configuration Manager (ConfMgr) Wake on LAN, qui est utilisé avec Remote PC Access, entrez les informations ConfMgr Wake Proxy, des paquets magiques et des transmissions de paquets.

Les paramètres de seuil de limitation vous permettent de spécifier un nombre maximal d'actions d'alimentation autorisées sur une connexion. Ces paramètres peuvent aider lorsque les paramètres de gestion de l'alimentation autorisent trop ou trop peu de machines à démarrer en même temps. Chaque type de connexion possède des valeurs par défaut qui sont appropriées pour la plupart des cas et ne doivent généralement pas être modifiées.

Les paramètres **Actions simultanées (tous types)** et **Mises à jour d'inventaire Personal vDisk simultanées** définissent deux valeurs : le nombre maximal absolu pouvant se produire simultanément sur cette connexion, et un pourcentage maximal de toutes les machines utilisant cette connexion. Vous devez spécifier les deux valeurs, absolue et pourcentage ; la limite réelle appliquée est la plus faible des valeurs.

Par exemple, dans un déploiement de 34 machines, si **Actions simultanées (tous types)** sont définies sur une valeur absolue de 10 et une valeur de pourcentage de 10, la limite réelle appliquée est de 3 (10 pour cent de 34 arrondis au nombre entier le plus proche, qui est inférieure à la valeur absolue de 10 machines).

Le **nombre maximal de nouvelles actions par minute** est un nombre absolu ; il n'existe pas de valeur de pourcentage.

Remarque : entrez les informations dans le champ **Options de connexion**uniquement selon les directives d'un représentant de l'assistance Citrix.

Activer ou désactiver le mode maintenance pour une connexion

Le fait d'activer le mode de maintenance pour une connexion empêche toute nouvelle action d'alimentation d'affecter les machines stockées sur cette connexion. Les utilisateurs ne peuvent pas se connecter à une machine lorsqu'elle est en mode de maintenance. Si les utilisateurs sont déjà connectés, le mode maintenance prend effet lorsqu'ils ferment leur session.

1. Sélectionnez **Configuration > Hébergement** dans le volet de navigation de Studio.
2. Sélectionnez la connexion. Pour activer le mode de maintenance, sélectionnez **Activer le mode de maintenance** dans le volet Actions. Pour désactiver le mode de maintenance, sélectionnez **Désactiver le mode de maintenance**.

Vous pouvez également activer ou désactiver le mode de maintenance pour des machines individuelles. De plus, vous pouvez activer ou désactiver le mode de maintenance sur les machines dans les catalogues de machines ou les groupes de mise à disposition.

Supprimer une connexion

> **Attention :**
>
> La suppression d'une connexion peut entraîner la suppression de nombreuses machines et la perte de données. Assurez-vous que les données utilisateur sur les machines affectées sont sauvegardées ou ne sont plus nécessaires.

Avant de supprimer une connexion, assurez-vous que :

- Tous les utilisateurs ont fermé leur session sur les machines stockées sur la connexion.
- Aucune session utilisateur déconnectée n'est en cours d'exécution.
- Le mode de maintenance est activé pour les machines regroupées et dédiées.
- Toutes les machines des catalogues de machines utilisées par la connexion sont hors tension.

Un catalogue de machines devient inutilisable lorsque vous supprimez une connexion référencée par ce catalogue. Si cette connexion est référencée par un catalogue, vous avez la possibilité de supprimer le catalogue. Avant de supprimer un catalogue, assurez-vous qu'il n'est pas utilisé par d'autres connexions.

1. Sélectionnez **Configuration > Hébergement** dans le volet de navigation de Studio.
2. Sélectionnez la connexion, puis sélectionnez **Supprimer la connexion** dans le volet Actions.
3. Si cette connexion possède des machines stockées sur celle-ci, vous êtes invité à indiquer si elles doivent être supprimées. Si elles doivent être supprimées, spécifiez la procédure à suivre pour les comptes d'ordinateurs Active Directory associés.

Renommer ou tester une connexion

1. Sélectionnez **Configuration > Hébergement** dans le volet de navigation de Studio.
2. Sélectionnez la connexion puis sélectionnez **Renommer la connexion** ou **Tester la connexion** dans le volet Actions.

Afficher les détails des machines sur une connexion

1. Sélectionnez **Configuration > Hébergement** dans le volet de navigation de Studio.
2. Sélectionnez la connexion, puis sélectionnez **Afficher les machines** dans le volet Actions.

Le volet supérieur dresse la liste des machines accessibles via la connexion. Sélectionnez une machine pour afficher les détails correspondants dans le volet inférieur. Les détails de session sont également fournis pour les sessions ouvertes.

Utilisez la fonctionnalité de recherche pour trouver des machines rapidement. Soit sélectionnez une recherche enregistrée dans la liste en haut de la fenêtre, soit créez une nouvelle recherche. Vous pouvez effectuer la recherche en tapant le nom de la machine ou une partie de celui-ci, ou créer une expression que vous utiliserez ensuite dans une recherche avancée. Pour créer une expression, cliquez sur le bouton de **développement**, puis sélectionnez dans les listes de propriétés et d'opérateurs.

Gérer les machines sur une connexion

1. Sélectionnez **Configuration > Hébergement** dans le volet de navigation de Studio.
2. Sélectionnez une connexion, puis sélectionnez **Afficher les machines** dans le volet Actions.
3. Sélectionnez l'une des options suivantes dans le volet Actions. Certaines actions risquent de ne pas être disponibles, en fonction de l'état de la machine et le type d'hôte de la connexion.

- **Démarrer :** démarre la machine si celle-ci est hors tension ou suspendue.
- **Suspendre :** pause la machine sans la fermer et actualise la liste de machines.
- **Arrêter :** requiert la fermeture du système d'exploitation.
- **Forcer l'arrêt :** force l'arrêt de la machine et actualise la liste des machines.
- **Redémarrer :** requiert la fermeture du système d'exploitation de la machine, puis redémarrage de la machine. Si le système d'exploitation ne peut pas répondre, le bureau reste dans son état actuel.
- **Activer le mode de maintenance :** arrête temporairement les connexions à une machine. Les utilisateurs ne peuvent pas se connecter à une machine dans cet état. Si les utilisateurs sont connectés, le mode maintenance prend effet lorsqu'ils ferment leur session. (Vous pouvez aussi activer ou désactiver le mode de maintenance sur toutes les machines accessibles via une connexion, comme décrit ci-dessus.)

- **Supprimer du groupe de mise à disposition :** la suppression d'une machine d'un groupe de mise à disposition n'est pas supprimée du catalogue de machines que le groupe de mise à disposition utilise. Vous pouvez supprimer une machine uniquement si aucun utilisateur n'y est connecté ; activez le mode de maintenance pour empêcher temporairement les utilisateurs de se connecter lors de la suppression de la machine.
- **Supprimer :** lorsque vous supprimez une machine, les utilisateurs n'y ont plus accès et la machine disparaît du catalogue de machines. Avant de supprimer une machine, assurez-vous que toutes les données utilisateur sont sauvegardées ou ne sont plus nécessaires. Vous pouvez supprimer une machine uniquement si aucun utilisateur n'y est connecté ; activez le mode de maintenance pour empêcher temporairement les utilisateurs de se connecter lors de la suppression de la machine.

Pour les actions qui impliquent la fermeture de la machine, si la machine ne se ferme pas dans les 10 minutes, elle est mise hors tension. Si Windows tente d'installer des mises à jour durant la fermeture, il y a un risque que la machine soit mise hors tension avant la fin des mises à jour.

Modifier un espace de stockage

Vous pouvez afficher l'état des serveurs utilisés pour stocker les données du système d'exploitation, les données temporaires et les données personnelles (PvD) des machines virtuelles qui utilisent une connexion. Vous pouvez également spécifier les serveurs que vous souhaitez utiliser pour le stockage de chaque type de données.

1. Sélectionnez Configuration > Hébergement dans le volet de navigation de Studio.
2. Sélectionnez la connexion, puis sélectionnez Modifier le stockage dans le volet Actions.
3. Dans le panneau de gauche, sélectionnez le type de données : système d'exploitation, Personal vDisk, ou temporaires.
4. Cochez ou décochez les cases à cocher d'un ou plusieurs périphériques de stockage pour le type de données sélectionné.
5. Cliquez sur OK.

Chaque périphérique de stockage dans la liste inclut son nom et l'état du stockage. Les valeurs d'état du stockage valides sont les suivantes :

- **En cours d'utilisation :** le stockage est utilisée pour la création de nouvelles machines.
- **Remplacé :** le stockage est utilisé uniquement pour des machines existantes. Aucune nouvelle machine ne sera ajoutée à ce stockage.
- **Non utilisé :** le stockage n'est pas utilisé pour la création de machines.

Si vous désactivez la case à cocher d'un périphérique qui est actuellement **en cours d'utilisation**, son état passera à **Remplacé**. Les machines existantes continueront à utiliser ce périphérique de stockage (et peuvent écrire des données dessus), par conséquent, il est possible que cet emplacement atteigne sa pleine capacité même après qu'il cesse d'être utilisé pour la création de nouvelles machines.

Supprimer, renommer ou test des ressources

1. Sélectionnez **Configuration > Hébergement** dans le volet de navigation de Studio.
2. Sélectionnez la ressource puis sélectionnez l'entrée appropriée dans le volet Actions : **Supprimer les ressources**, **Renommer les ressources** ou **Tester les ressources**.

Utiliser les connexions IntelliCache pour XenServer

À l'aide d'IntelliCache, les déploiements VDI hébergés sont plus rentables car ils vous permettent d'utiliser une combinaison de stockage partagé et de stockage local. Cela améliore les performances et réduit le trafic réseau. Le stockage local met en cache l'image principale depuis le stockage partagé ; cela réduit le nombre de lectures sur le stockage partagé. Pour les bureaux partagés, les écritures sur les disques de différenciation s'effectuent sur le stockage local sur l'hôte et non sur le stockage partagé.

- Le stockage partagé doit être de type NFS si vous utilisez IntelliCache.
- Citrix vous recommande d'utiliser un périphérique de stockage local à hautes performances pour assurer un transfert de données optimal.

Pour utiliser IntelliCache, vous devez l'activer dans ce produit et XenServer.

- Lors de l'installation de XenServer, sélectionnez**Enable thin provisioning (Optimized storage for XenDesktop)**. Citrix ne prend pas en charge les regroupements mixtes de serveurs avec IntelliCache activé et de serveurs sans IntelliCache activé. Pour plus d'informations, veuillez consulter la documentation de XenServer.
- Dans XenApp et XenDesktop, IntelliCache est désactivé par défaut. Vous pouvez modifier le paramètre uniquement lors de la création d'une connexion XenServer ; vous ne pouvez pas désactiver IntelliCache ultérieurement. Lorsque vous ajoutez une connexion XenServer depuis Studio :
  - Sélectionnez**Partagé**en tant que type de stockage.
  - Sélectionnez la case à cocher **Utiliser IntelliCache**.

Horloges de connexion

Vous pouvez utiliser des paramètres de stratégie permettant de configurer trois horloges de connexion :

- **Minuteur de connexion maximal :** détermine la durée maximale d'une connexion non interrompue entre une machine utilisateur et un bureau virtuel. Utilisez les paramètres de stratégies **Horloge de connexion de session** et **Intervalle d'horloge de connexion de session**.

- **Minuteur de connexion inactif :** détermine la durée pendant laquelle une connexion non interrompue d'une machine utilisateur à un bureau virtuel sera maintenue si aucune entrée utilisateur n'est effectuée. Utilisez les paramètres de stratégie **Horloge inactive de session** et **Intervalle d'horloge inactive de session**.
- **Horloge de déconnexion :** détermine la durée pendant laquelle un bureau virtuel déconnecté et verrouillé peut rester verrouillé avant que la session ne se ferme. Utilisez les paramètres de stratégie **Horloge de session déconnectée** et **Intervalle d'horloge de session déconnectée**.

Lorsque vous mettez à jour l'un de ces paramètres, vous devez vous assurer qu'ils sont cohérents sur votre déploiement.

Consultez la documentation sur les paramètres de stratégie pour plus d'informations.

Cache d'hôte local

February 28, 2019

Pour vous assurer que la base de données du site XenApp et XenDesktop est toujours disponible, Citrix recommande de commencer par un déploiement SQL Server ayant une tolérance aux pannes en suivant la haute disponibilité des meilleures pratiques de Microsoft. (La section Bases de données dans l'article Configuration système requise répertorie les fonctionnalités de haute disponibilité de SQL Server prises en charge dans XenApp et XenDesktop). Toutefois, les utilisateurs peuvent ne pas être en mesure de se connecter à leurs applications ou bureaux à cause de problèmes et d'interruptions réseau.

La fonctionnalité Cache d'hôte local (LHC) permet aux opérations de négociation de connexions sur un site XenApp ou XenDesktop de se poursuivre en cas de panne. Une panne se produit lorsque la connexion entre un Delivery Controller et la base de données du site échoue. Le cache de l'hôte local est activé lorsque la base de données du site est inaccessible pendant 90 secondes.

Le cache d'hôte local est la fonctionnalité de haute disponibilité la plus complète dans XenApp et XenDesktop. Il s'agit de la plus puissante solution alternative à la fonctionnalité de location de connexion, qui a été introduite dans XenApp 7.6.

Bien que cette implémentation du cache d'hôte local porte le même nom que la fonctionnalité de cache d'hôte local dans XenApp 6.5 et les versions antérieures de XenApp, d'importantes améliorations y ont été apportées. Cette implémentation est plus solide et plus résistante à la corruption des données. Les besoins de maintenance ont été réduits, par exemple le besoin de commandes dsmaint périodiques a été éliminé. Ce cache d'hôte local est une implémentation complètement différente sur le plan technique ; lisez la section suivante pour savoir comment il fonctionne.

> **Remarque :**
>
> Bien que la location de connexions soit prise en charge dans la version 7.15 LTSR, elle sera supprimée dans la version suivante.

Contenu des données

Le cache d'hôte local inclut les informations suivantes, qui constituent un sous-ensemble des informations de la base de données principale :

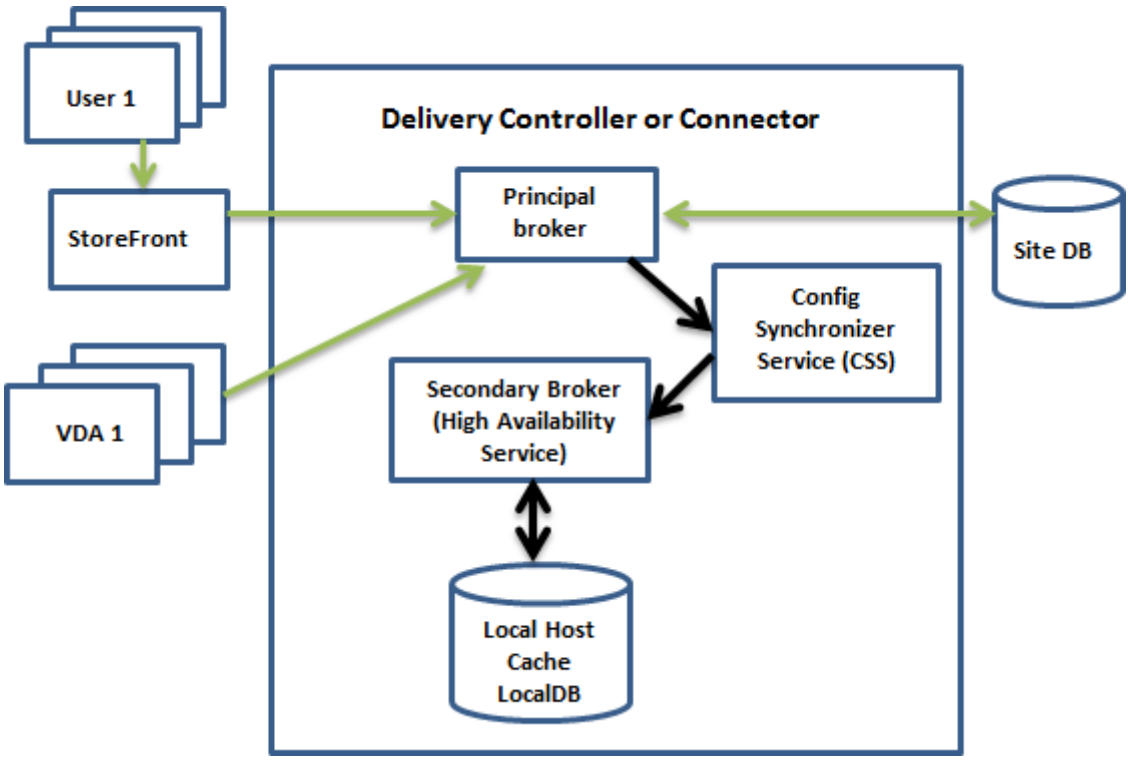
- Identités des utilisateurs et des groupes auxquels sont spécifiquement attribués des droits sur les ressources publiées à partir du site.
- Identités des utilisateurs qui utilisent actuellement ou ont récemment utilisé des ressources publiées à partir du site.
- Identités des machines VDA (y compris les machines Remote PC Access) configurées sur le site.
- Identités (noms et adresses IP) des machines Citrix Receiver utilisées activement pour se connecter aux ressources publiées.

Il contient également des informations sur les connexions actuellement actives qui ont été établies alors que la base de données principale était indisponible :

- Résultats de toute analyse de point de terminaison de machine client réalisée par Citrix Receiver.
- Identités des machines d'infrastructure (telles que les serveurs NetScaler Gateway et StoreFront) impliquées dans le site.
- Dates/heures et types d'activités récentes des utilisateurs.

Fonctionnement

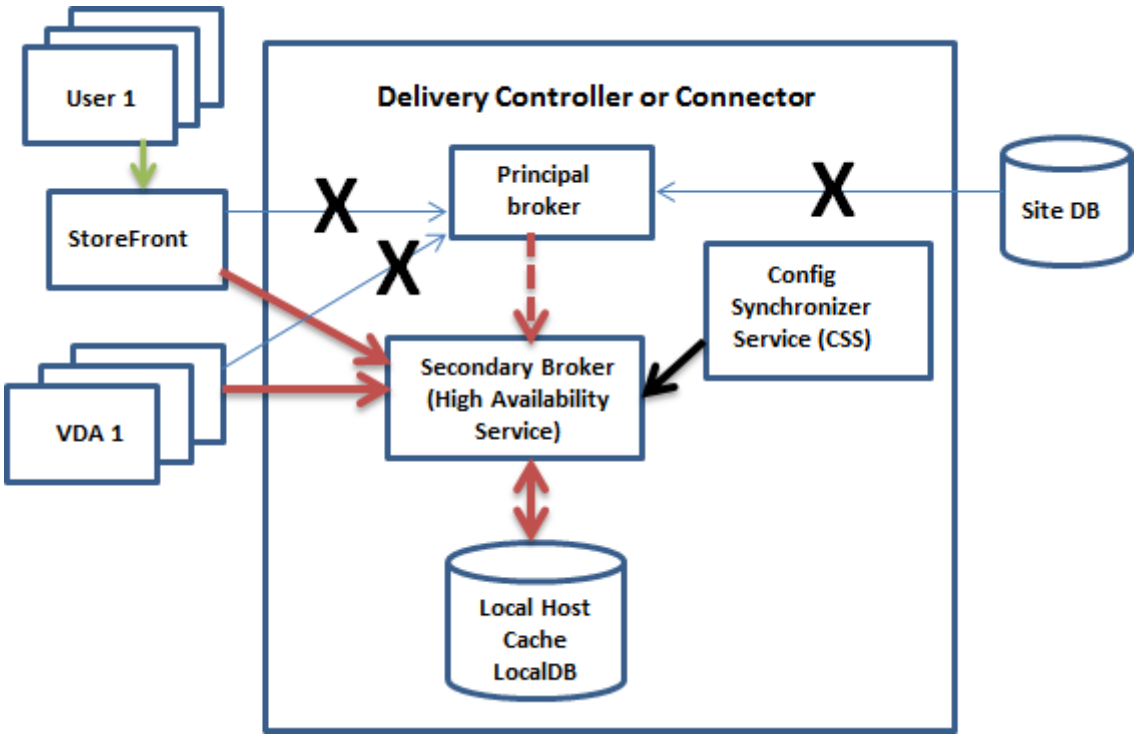
Le graphique suivant illustre les composants et les chemins de communication du cache d'hôte local en fonctionnement normal.



En mode de fonctionnement normal :

- Le *broker principal* (Citrix Broker Service) sur un Controller accepte des requêtes de connexion provenant de StoreFront, et communique avec la base de données du site pour connecter les utilisateurs avec des VDA qui sont enregistrés avec le Controller.
- Une vérification est effectuée toutes les deux minutes pour déterminer si des modifications ont été apportées à la configuration du broker principal. Ces modifications peuvent avoir été initiées par des actions PowerShell/Studio (telles que la modification d'une propriété de groupe de mise à disposition) ou des actions du système (telles que les attributions de machine).
- Si une modification a été apportée depuis la dernière vérification, le broker principal utilise le service Citrix Config Synchronizer Service (CSS) pour synchroniser (copier) les informations sur un *broker secondaire* (service Citrix High Availability Service) du Controller. Toutes les données de configuration du broker sont copiées, et pas seulement les éléments qui ont été modifiés depuis la dernière vérification. Le broker secondaire importe les données dans une base de données Microsoft SQL Server Express LocalDB sur le Controller. Le service CSS garantit que les informations de la base de données LocalDB du broker secondaire correspondent aux informations de la base de données du site. La base de données LocalDB est recréée chaque fois que la synchronisation se produit.
- Si aucune modification n'a été apportée depuis la dernière vérification, aucune donnée n'est copiée.

Le graphique suivant illustre les modifications apportées aux chemins de communication si le broker principal perd le contact avec la base de données du site (une panne commence) :



Lorsqu'une panne commence :

- Le broker principal ne peut plus communiquer avec la base de données du site, et arrête d'écouter les informations StoreFront et VDA (marque X dans le diagramme). Le broker principal demande ensuite au broker secondaire (High Availability Service) de démarrer l'écoute et le traitement des demandes de connexion (ligne en pointillés rouge dans le diagramme).
- Lorsque la panne commence, le broker secondaire ne dispose d'aucune donnée d'enregistrement de VDA, mais dès qu'un VDA communique avec lui, un processus de ré-enregistrement est déclenché. Au cours de ce processus, le broker secondaire obtient également des informations de session sur ce VDA.
- Bien que ce soit le broker secondaire qui gère les connexions, le broker principal continue à surveiller la connexion à la base de données du site. Lorsque la connexion est rétablie, le broker principal demande au broker secondaire d'arrêter l'écoute des informations de connexion, et le broker principal reprend les opérations de négociation de connexion. La prochaine fois qu'un VDA communique avec le broker principal, un processus de ré-enregistrement est déclenché. Le broker secondaire supprime les enregistrements de VDA de la panne précédente, et reprend la mise à jour de la base de données LocalDB avec les modifications de configuration reçues depuis CSS.

Dans le cas peu probable où une panne démarre pendant une synchronisation, l'importation en cours est annulée et la dernière configuration connue est utilisée.

Le journal d'événements contient des informations sur les synchronisations et les pannes. Consultez la section « Contrôle » ci-dessous pour plus de détails.

Vous pouvez également déclencher une panne volontairement ; veuillez consulter la section « Forcer une panne » ci-dessous pour plus de détails sur cette procédure.

Sites disposant de plusieurs Controller

Parmi ses différentes tâches, le service CSS fournit régulièrement au broker secondaire des informations sur tous les Controller de la zone (si votre déploiement ne contient pas plusieurs zones, cette action affecte tous les Controller du site). Ces informations permettent à chaque broker secondaire de connaître tous les brokers secondaires homologues.

Les brokers secondaires communiquent entre eux sur un canal distinct. Ils utilisent une liste alphabétique des noms de domaine complet (FQDN) des machines qu'ils exécutent pour déterminer (sélectionner) le broker secondaire qui sera en charge des opérations de négociation dans la zone si une panne se produit. Durant la panne, tous les VDA se ré-enregistrent auprès du broker secondaire sélectionné. Les brokers secondaires non sélectionnés dans la zone rejettent activement les requêtes de connexion et d'enregistrement de VDA entrantes.

Si un broker secondaire sélectionné échoue lors d'une panne, un autre broker secondaire est sélectionné pour prendre le relais et les VDA se ré-enregistrent auprès du broker secondaire qui vient d'être sélectionné.

Durant une panne, si un Controller est redémarré :

- Si ce Controller n'est pas le broker principal sélectionné, le redémarrage n'a aucun impact.
- Si ce Controller est le broker principal sélectionné, un autre Controller est sélectionné, et par conséquent le VDA s'enregistre à nouveau. Une fois que le Controller redémarré est sous tension, il reprend automatiquement la négociation des connexions, et le VDA s'enregistre à nouveau. Dans ce scénario, les performances peuvent être affectées lors des ré-enregistrements.

Si vous mettez un Controller hors tension en fonctionnement normal et le remettez sous tension durant une panne, le cache d'hôte local ne peut pas être utilisé sur ce Controller s'il est sélectionné en tant que broker principal.

Le journal d'événements contient des informations sur les sélections. Consultez la section « Contrôle » ci-dessous.

Considérations relatives à la conception et configuration requise

Le cache d'hôte local est pris en charge pour les applications et les bureaux hébergés sur le serveur, et les bureaux statiques (attribués) ; il n'est pas pris en charge pour les bureaux VDI regroupés (créés par MCS ou PVS).

Aucun délai n'est imposé pour le fonctionnement en mode panne. Toutefois, restaurez le site pour un fonctionnement normal le plus rapidement possible.

Disponibilités ou changements au cours d'une panne :

- Vous ne pouvez pas utiliser Studio ou exécuter des applets de commande PowerShell.
- Les informations d'identification de l'hyperviseur ne peuvent pas être obtenues depuis Host Service. Toutes les machines se trouvent dans un état d'alimentation inconnu et aucune opération d'alimentation ne peut être émise. Toutefois, les VM de l'hôte qui sont sous tension peuvent être utilisées pour les demandes de connexion.
- Une machine attribuée peut uniquement être utilisée si l'attribution s'est produite lors d'un fonctionnement normal. De nouvelles attributions ne peuvent pas être effectuées lors d'une panne.
- L'inscription et la configuration automatiques de machines Remote PC Access ne sont pas possibles. Toutefois, les machines qui ont été inscrites et configurées lors du fonctionnement normal peuvent être utilisées.
- Les utilisateurs d'applications et de bureaux hébergés sur le serveur peuvent utiliser plus de sessions que leurs limites de session configurées, si les ressources se trouvent dans des zones différentes.
- Les utilisateurs peuvent lancer des applications et bureaux uniquement à partir de VDA enregistrés dans la zone contenant le broker (secondaire) actuellement actif/sélectionné. Les lancements entre zones (depuis un broker dans une zone vers un VDA situé dans une autre zone) ne sont pas pris en charge durant une panne.

Par défaut, les VDA de bureau avec alimentation gérée dans des groupes de mise à disposition regroupés dont la propriété ShutdownDesktopsAfterUse est activée sont placés en mode maintenance lorsqu'une panne se produit. Vous pouvez modifier ce comportement par défaut pour autoriser ces bureaux à être utilisés lors d'une panne. Toutefois, vous ne pouvez pas compter sur la gestion de l'alimentation durant la panne. (La gestion de l'alimentation reprend une fois que les opérations normales reprennent.) En outre, ces bureaux peuvent contenir des données de l'utilisateur précédent, car ils n'ont pas été redémarrés.

Pour modifier le comportement par défaut, vous devez l'activer au niveau du site et pour chaque groupe de mise à disposition affecté. Exécutez les applets de commande PowerShell suivants.

Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true
Set-BrokerDesktopGroup -Name "<*name*>" -ReuseMachinesWithoutShutdownInOutage $true

L'activation de cette fonctionnalité dans le site et les groupes de mise à disposition n'affecte pas le fonctionnement de la propriété « ShutdownDesktopsAfterUse » configurée en fonctionnement normal.

Taille de RAM :

Le service LocalDB peut utiliser environ 1,2 Go de RAM (jusqu'à 1 Go pour le cache de base de données, plus 200 Mo pour l'exécution de SQL Server Express LocalDB). High Availability Service peut utiliser jusqu'à 1 Go de RAM si une panne dure longtemps avec un grand nombre d'ouvertures de session (par

exemple, 12 heures avec 10 000 utilisateurs). Ces exigences de mémoire s'ajoutent aux exigences de RAM requises normalement pour le Controller, il se peut donc que vous deviez augmenter la quantité totale de capacité RAM.

Notez que si vous utilisez une installation SQL Server Express pour la base de données du site, le serveur aura deux processus sqlserver.exe.

Configuration des sockets et des cœurs d'UC :

Une configuration d'UC de Controller, notamment le nombre de cœurs disponibles pour SQL Server Express LocalDB, affecte directement les performances de cache d'hôte local, encore plus que l'allocation de mémoire. Cette charge de l'UC est observée uniquement au cours de la période de panne lorsque la base de données ne peut pas être contactée et que le service High Availability Service est actif.

Bien que la base de données LocalDB puisse utiliser plusieurs cœurs (jusqu'à 4), elle est limitée à un seul socket. L'ajout de sockets ne permet pas d'améliorer les performances (par exemple, 4 sockets avec 1 cœur chacun). Citrix vous recommande plutôt d'utiliser plusieurs sockets avec plusieurs cœurs. Au cours des tests Citrix, une configuration 2x3 (2 sockets, 3 cœurs) a fourni de meilleures performances que les configurations 4x1 et 6x1.

Stockage :

Lorsque les utilisateurs accèdent à des ressources pendant une panne, la taille de la base de données LocalDB augmente. Par exemple, lors d'un test d'ouverture/fermeture de session avec 10 ouvertures de session par seconde, la base de données a augmenté d'1 Mo toutes les 2-3 minutes. Lorsque le fonctionnement normal reprend, la base de données locale est recréée et l'espace disque est rétabli. Toutefois, le broker doit avoir suffisamment d'espace sur le disque sur lequel la base de données LocalDB est installée pour permettre à la taille de la base de données d'augmenter durant une panne. Le cache d'hôte local entraîne également des E/S supplémentaires pendant une panne : environ 3 Mo d'écritures par seconde, avec plusieurs centaines de milliers de lectures.

Performances :

Durant une panne, un seul broker gère toutes les connexions ; dans les sites (ou zones) qui équilibrent la charge entre plusieurs Controller en fonctionnement normal, le broker sélectionné peut être amené à prendre en charge beaucoup plus de requêtes que d'habitude durant une panne. Par conséquent, les demandes d'UC seront plus nombreuses. Chaque broker du site (ou de la zone) doit être en mesure de gérer la charge supplémentaire imposée par la base de données LocalDB et tous les VDA, concernés car le broker sélectionné lors d'une panne peut changer.

Limites de VDI :

- Dans un déploiement VDI à zone unique, jusqu'à 10 000 VDA peuvent être gérés efficacement au cours d'une panne.

- Dans un déploiement VDI multizone, jusqu'à 10 000 VDA par zone peuvent être gérés au cours d'une panne, avec un maximum de 40 000 VDA sur le site. Par exemple, chacun des sites suivants peut être géré de manière efficace durant une panne :
  - Un site avec quatre zones, chacune contenant 10 000 VDA.
  - Un site avec sept zones, une contenant 10 000 VDA et six contenant 5 000 VDA chacune.

Durant une panne, la gestion de la charge pour l'ensemble du site peut être affectée. Les calculateurs de charge (et plus particulièrement les règles du nombre de sessions) risquent d'être dépassés.

Pendant que tous les VDA s'enregistrent à nouveau avec un broker, il est possible que ce broker ne dispose pas d'informations complètes sur les sessions en cours. Par conséquent, une demande de connexion d'un utilisateur pendant cet intervalle peut entraîner le démarrage d'une nouvelle session, même si la reconnexion à une session existante est possible. Cet intervalle (pendant lequel le nouveau broker reçoit les informations de session depuis tous les VDA dans le cadre du ré-enregistrement) est inévitable. Notez que les sessions qui sont connectées lorsqu'une panne démarre ne sont pas affectées lors de l'intervalle de transition, mais les nouvelles sessions et les reconnexions de session peuvent l'être.

Cet intervalle se produit lorsque les VDA doivent se ré-enregistrer auprès d'un autre broker :

- Une panne démarre : lors de la migration depuis un broker principal vers un broker secondaire.
- Défaillance du broker durant une panne : lors de la migration depuis un broker secondaire qui a échoué vers un nouveau broker secondaire.
- Reprise après une panne : lorsque les opérations normales reprennent, et que le broker principal reprend le contrôle.

Vous pouvez réduire cet intervalle en réduisant la valeur de registre HeartbeatPeriodMs de Citrix Broker Protocol (valeur par défaut=600000 ms, c'est-à-dire 10 minutes). Cette valeur de pulsation est le double de l'intervalle que le VDA utilise pour les pings, donc la valeur par défaut entraîne un ping toutes les 5 minutes.

Par exemple, la commande suivante règle la pulsation sur cinq minutes (300000 millisecondes), ce qui entraîne un ping toutes les 2,5 minutes :

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer -Name HeartbeatPeriodMs
-PropertyType DWORD –Value 300000
```

L'intervalle ne peut pas être entièrement éliminé, quelle que soit la rapidité avec laquelle les VDA s'enregistrent.

Le temps nécessaire à la synchronisation entre les brokers augmente avec le nombre d'objets (VDA, applications, groupes) Par exemple, la synchronisation de 5000 VDA peut prendre plus de dix minutes. Consultez la section « Contrôle » ci-dessous pour de plus amples informations sur les entrées de synchronisation dans le journal d'événements.

Gérer le cache d'hôte local

Pour que le cache d'hôte local fonctionne correctement, la stratégie d'exécution de PowerShell sur chaque Controller doit être définie sur RemoteSigned, Unrestricted ou Bypass.

SQL Server Express LocalDB

La base de données Microsoft SQL Server Express LocalDB que le cache d'hôte local utilise est installée automatiquement lorsque vous installez un Controller ou mettez à niveau un Controller à partir d'une version antérieure à la version 7.9. Aucune maintenance administrateur n'est requise pour LocalDB. Seul le broker secondaire communique avec cette base de données ; vous ne pouvez pas utiliser les applets de commande PowerShell pour modifier quoi que ce soit sur cette base de données. La base de données LocalDB ne peut pas être partagée entre les Controller.

Le logiciel de la base de données SQL Server Express LocalDB est installé que le cache d'hôte local soit activé ou non.

Pour empêcher son installation, installez ou mettez à niveau le Delivery Controller à l'aide de la commande XenDesktopServerSetup.exe et ajoutez l'option /exclude "Local Host Cache Storage (LocalDB)". Cependant, n'oubliez pas que la fonctionnalité de cache d'hôte local ne fonctionnera pas sans la base de données, et vous ne pouvez pas utiliser une autre base de données avec le broker secondaire.

L'installation de cette base de données LocalDB ne détermine pas si vous devez installer SQL Server Express ou non pour l'utiliser en tant que base de données du site.

Paramètres par défaut après l'installation ou la mise à niveau de XenApp ou XenDesktop

Lors d'une nouvelle installation de XenApp et XenDesktop, le cache d'hôte local est désactivé par défaut. (La location de connexions est activée par défaut.)

Après une mise à niveau, le paramètre de cache d'hôte local est inchangé. Par exemple, si le cache d'hôte local a été activé dans la version antérieure, il reste activé dans la version mise à niveau. Si le cache d'hôte local a été désactivé (ou qu'il n'est pas pris en charge) dans la version antérieure, il reste désactivé dans la version mise à niveau.

Activer/désactiver le cache d'hôte local

Pour activer le cache d'hôte local, entrez :


```
Set-BrokerSite -LocalHostCacheEnabled $true -ConnectionLeasingEnabled
$false
```

Cette applet de commande désactive également la fonctionnalité de location de connexion. N'activez pas le cache d'hôte local et la location de connexion en même temps.

Pour déterminer si le cache d'hôte local est activé, entrez :

```
Get-BrokerSite
```

Vérifiez que la propriété LocalHostCacheEnabled est True, et que la propriété ConnectionLeasingEnabled est False.

Pour désactiver le cache d'hôte local (et activer la location de connexion), entrez :

```
Set-BrokerSite -LocalHostCacheEnabled $false -ConnectionLeasingEnabled
$true
```

Forcer une interruption

Vous pouvez souhaiter délibérément forcer une interruption de la base de données.

- Si votre réseau s'interrompt et reprend de manière répétée. Forcer une panne jusqu'à la résolution des problèmes réseau empêche le basculement en continu entre les modes de fonctionnement normal et de panne.
- Pour tester un plan de récupération d'urgence.
- Lorsque vous remplacez ou effectuez une maintenance sur le serveur de base de données du site.

Pour forcer une panne, modifiez le registre de chaque serveur contenant un Delivery Controller.

- Dans HKLM\Software\Citrix\DesktopServer\LHC, définissez OutageModeForced sur 1. Ce réglage demande au broker d'entrer en mode panne, quel que soit l'état de la base de données (si vous définissez la valeur sur 0, le serveur sort du mode panne).
- Dans un scénario Citrix Cloud, le connecteur entre en mode panne quel que soit l'état de la connexion avec le plan de contrôle ou la zone principale.

Analyse

Les journaux d'événements consignent les synchronisations et les pannes.

Config Synchronizer Service :

Lors du fonctionnement normal, les événements suivants peuvent se produire lorsque le service CSS copie et exporte la configuration du broker puis l'importe dans la base de données LocalDB à l'aide du High Availability Service (broker secondaire).

- 503 : une modification a été trouvée dans la configuration du broker principal et une importation démarre.
- 504 : la configuration du broker a été copiée, exportée, puis importée avec succès dans LocalDB.
- 505 : une 'importation dans LocalDB a échoué ; consultez la section ci-dessous pour plus d'informations.

High Availability Service :

- 3502 : une panne s'est produite et le broker secondaire (High Availability Service) effectue les opérations de négociation.
- 3503 : une panne a été résolue et le fonctionnement normal est rétabli.
- 3504 : indique le broker secondaire qui a été sélectionné, ainsi que les autres brokers impliqués dans la sélection.

Dépannage

Plusieurs outils de dépannage sont disponibles lorsque l'importation de la synchronisation dans LocalDB échoue et qu'un événement 505 est signalé.

Traçage CDF : contient les options des modules ConfigSyncServer et BrokerLHC. Ces options, ainsi que d'autres modules de broker, sont susceptibles d'identifier le problème.

Rapport : vous pouvez générer et fournir un rapport détaillant le point d'échec. Cette fonctionnalité de rapport affecte la vitesse de synchronisation, Citrix vous recommande donc de la désactiver lorsqu'elle n'est pas utilisée.

Pour activer et générer un rapport de traçage CSS, entrez :

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name
EnableCssTraceMode -PropertyType DWORD -Value 1
```

Le rapport HTML est publié sous C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\CitrixBrokerC
(Si le rapport n'est pas généré correctement, créez la clé de registre sous WOW6432Node et réessayez.)

Une fois le rapport généré, désactivez la fonctionnalité de rapport :

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name
EnableCssTraceMode -Value 0
```

Exporter la configuration du broker : fournit la configuration exacte à des fins de débogage.

```
Export-BrokerConfiguration | Out-File file-pathname
```

Par exemple, `Export-BrokerConfiguration | Out-File C:\\BrokerConfig.xml`.

Location de connexion

February 28, 2019

> **Important :**
>
> LHC (cache d'hôte local) est la solution haute disponibilité XenApp et XenDesktop recommandée, plutôt que la location de connexion. Pour plus d'informations, veuillez consulter Cache d'hôte local.

- Dans cette version, lors d'une nouvelle installation de XenApp et XenDesktop, la location de connexion est désactivée par défaut.
- La location de connexion ne sera plus fournie, à compter de la version suivant cette version XenDesktop et XenApp 7.15 Long Term Service Release.

Pour vous assurer que la base de données du site est toujours disponible, Citrix recommande de commencer par un déploiement SQL Server ayant une tolérance aux pannes en suivant la haute disponibilité des meilleures pratiques de Microsoft. Cependant, les problèmes et les interruptions réseau peuvent empêcher les Delivery Controller d'accéder à la base de données, ce qui fait que des utilisateurs ne vont pas pouvoir se connecter à leurs applications ou bureaux.

La fonctionnalité de location de connexion complète les meilleures pratiques de la haute disponibilité du serveur SQL Server en permettant aux utilisateurs de se connecter et de se reconnecter à leurs applications et bureaux les plus récemment utilisés, même lorsque la base de données du site n'est pas disponible.

Bien que les utilisateurs puissent posséder un nombre important de ressources publiées disponibles, ils n'utilisent souvent que quelques-unes régulièrement. Lorsque vous activez la location de connexion, chaque Controller met en cache les connexions utilisateur vers les applications et bureaux utilisés récemment lors d'opérations normales (lorsque la base de données est disponible).

Les baux générés sur chaque Controller sont téléchargées vers la base de données du site pour la synchronisation périodique vers d'autres Controller du site. Outre le bail, chaque Controller du cache contient l'application, le bureau, l'icône et les informations du travailleur. Le bail et les informations associées sont stockés sur le disque local de chaque Controller. Si la base de données devient indisponible, le Controller entre en mode de connexion de location et « relit » les opérations de mise en cache lorsqu'un utilisateur tente de se connecter ou se reconnecter à une application ou d'un bureau récemment utilisé(e) depuis StoreFront.

Les connexions sont mises en cache pour une période de bail de deux semaines. Par conséquent, si la base de données devient non disponible, les bureaux et les applications qui ont été lancés par l'utilisateur dans les deux semaines précédentes restent accessibles pour cet utilisateur via StoreFront. Toutefois, des bureaux et des applications qui n'ont pas été lancés pendant la dernière période de bail de deux semaines ne sont pas accessibles lorsque la base de données n'est pas disponible. Par exemple, si une application a été lancée par un utilisateur il y a trois semaines, son bail a expiré

et l'application ne peut pas être lancée par cet utilisateur si la base de données devient désormais indisponible. Les baux de sessions actives de longue durée, ou d'application de déconnexion ou de sessions de bureaux sont étendus afin de ne pas être considérés comme expiré.

Par défaut, la location de connexion affecte l'ensemble du site ; cependant, vous pouvez révoquer tous les baux pour certains utilisateurs, ce qui leur évite d'accéder à des applications ou des bureaux lorsque le Controller se trouve en mode de connexion louée. Plusieurs autres paramètres du Registre s'appliquent sur une base de Controller.

Considérations et limitations

Tandis que la location de connexion peut améliorer la résilience de connexion et la productivité des utilisateurs, il existe des considérations relatives à la disponibilité, opération, et performances d'autres fonctionnalités.

La location de connexion est prise en charge pour les applications et les bureaux hébergés sur le serveur et les bureaux statiques (attribués) ; elle n'est pas prise en charge pour les bureaux VDI regroupés ou pour les utilisateurs qui n'ont pas été attribués à un bureau lorsque la base de données devient indisponible.

Lorsque le Controller se trouve en mode de connexion loué :

- Les administrateurs ne peuvent pas utiliser Studio, Director, ou la console PowerShell.
- Le contrôle de l'espace de travail n'est pas disponible. Lorsqu'un utilisateur ouvre une session sur Citrix Receiver, les sessions ne sont pas automatiquement reconnectées, l'utilisateur doit redémarrer l'application.
- Si un nouveau bail est créé avant que la base de données ne devienne indisponible, mais que les informations de bail n'ont pas encore été synchronisées entre les Controller, l'utilisateur peut ne pas être en mesure de démarrer cette ressource après que la base de données soit devenue indisponible.
- Les utilisateurs d'applications et de bureaux hébergés sur le serveur peuvent utiliser plus de sessions que leurs limites de session configurées. Par exemple :
  - Une session ne peut pas itinérer lorsqu'un utilisateur la démarre à partir d'une machine (connexion au travers de NetScaler Gateway) lorsque le Controller ne se trouve pas en mode de connexion loué puis se connecte à partir d'une autre machine sur le réseau local où le contrôleur se trouve en mode de connexion loué.
  - La reconnexion de session peut échouer si une application démarre juste avant que la base de données ne devienne indisponible ; dans ce cas, une nouvelle session et instance d'application sont lancées.

- L'alimentation des bureaux statiques (attribués) n'est pas gérée. Les VDA qui sont mis hors tension lorsque le Controller entre en mode de connexion loué restent indisponibles tant que la connexion à la base de données n'est pas restaurée, sauf si l'administrateur les place manuellement sous tension.
- Si le pré-lancement de session et la persistance de session sont activés, les nouvelles sessions de pré-lancement ne sont pas démarrés. Le pré-lancement de session et la persistance de session ne seront pas terminés selon les seuils configurés alors que la base de données n'est pas disponible.
- La gestion de la charge dans le site peut être affectée. Les connexions de serveur sont routées vers le VDA le plus récemment utilisé. Les calculateurs de charge (et plus particulièrement les règles du nombre de sessions) risquent d'être dépassés.
- Le Controller n'entrera pas en mode de connexion louée si vous utilisez SQL Server Management Studio pour mettre la base de données hors connexion. Au lieu de cela, utilisez l'une des instructions Transact-SQL suivantes :
  - ALTER DATABASE SET OFFLINE WITH ROLLBACK IMMEDIATE
  - ALTER DATABASE <nom-base-de-données> SET OFFLINE WITH ROLLBACK AFTER <secondes>

  Les deux instructions annulent toutes les transactions en attente et provoquent la perte de sa connexion à la base de données par le Controller. Le Controller entre alors en mode de connexion louée.

Lorsque la location de connexion est activée, il existe deux brefs intervalles de temps pendant lesquels les utilisateurs ne peuvent pas se connecter ou se reconnecter : (1) du moment où la base de données devient indisponible au moment où le Controller entre en mode de connexion louée, et (2) du moment où le Controller change d'un mode de connexion louée au moment où l'accès à la base de données est entièrement restauré et les VDA ont se sont réinscrits.

Si vous configurez une valeur autre que la valeur par défaut d'itinérance de session, la reconnexion de session retourne à sa valeur par défaut lorsqu'un Controller entre en mode de location de connexion. Pour plus d'informations, veuillez consulter Location de connexion et itinérance de session.

Consultez l'article Zones pour savoir où les données de location de connexion sont conservées.

Pour de plus amples informations, consultez la rubrique Considérations à prendre en compte lors de la conception d'une location de connexion XenDesktop 7.6.

Configurer et déployer

Lors de la configuration de votre déploiement pour prendre en charge la location de connexion :

- La version des VDA doit être de 7.6 au minimum et les catalogues de machines et groupes de mise à disposition qui utilisent ces machines doivent être à ce niveau minimum (ou une version ultérieure prise en charge).
- La taille de la base de données du site augmentera.
- Chaque Controller a besoin de plus d'espace disque pour la mise en cache des fichiers du bail.

Vous pouvez activer ou désactiver la location de connexion à partir du kit de développement PowerShell ou du Registre. Depuis le kit de développement PowerShell, vous pouvez également supprimer des baux d'en cours. Les applets de commande PowerShell suivantes affectent la location des connexions ; voir l'aide de l'applet de commande pour plus de détails.

- Set-BrokerSite -ConnectionLeasingEnabled $true | $false - Active ou désactive la fonction de location de connexion. Valeur par défaut = $true
- Get-BrokerServiceAddedCapability - Place « ConnectionLeasing » à l'emplacement spécifié pour le Controller local.
- Get-BrokerLease - Récupère l'ensemble (ou une série filtrée) des baux actuels.
- Remove-BrokerLease - Marque un bail ou une série filtrée de baux pour suppression.
- Update-BrokerLocalLeaseCache – Met à jour le cache de location de connexion sur le Controller local. Les données sont resynchronisées lors de la prochaine opération de synchronisation.

Adresse IP virtuelle et bouclage virtuel

February 28, 2019

Remarque : ces fonctionnalités ne sont valides que pour les machines de serveur Windows prises en charge. Elles ne s'appliquent pas aux machines avec OS de bureau Windows.

La fonctionnalité d'adresse IP virtuelle Microsoft fournit une application publiée avec une adresse IP unique attribuée dynamiquement à chaque session. La fonctionnalité de bouclage virtuel Citrix vous permet également de configurer des applications qui dépendent des communications avec localhost (127.0.0.1 par défaut) pour utiliser une adresse de bouclage virtuel unique dans la plage localhost (127.*).

Certaines applications, telles que les applications de type CRM ou CTI (Computer Telephony Integration), utilisent une adresse IP pour l'adressage, l'identification, les licences, ou à d'autres fins. Elles nécessitent par conséquent des sessions à adresse IP unique ou adresse de bouclage. D'autres applications peuvent se lier à un port statique, c'est pourquoi les tentatives de démarrage des instances d'une application dans un environnement multi-utilisateur échoueront car le port est déjà utilisé. Pour assurer un fonctionnement correct de ces applications dans l'environnement XenApp, chaque machine nécessite une adresse IP unique.

Les adresses IP virtuelles et le bouclage virtuel sont des fonctionnalités indépendantes. Vous pouvez sélectionnez ces deux options ou l'une ou l'autre.

Résumé des actions de l'administrateur :

- Pour utiliser l'adresse IP virtuelle Microsoft, activez et configurez-la sur le serveur Windows. (Les paramètres de stratégie Citrix ne sont pas nécessaires).
- Pour utiliser le bouclage virtuel Citrix, configurez deux paramètres dans une stratégie Citrix.

IP virtuelle

Lorsque l'adresse IP virtuelle est activée et configurée sur le serveur Windows, chaque application configurée en cours d'exécution dans une session dispose d'une adresse unique. Les utilisateurs peuvent accéder à ces applications sur un serveur XenApp comme ils accèdent à toute autre application publiée. Un processus nécessite une adresse IP virtuelle dans les cas suivants :

- Le processus utilise un numéro de port TCP fixe
- Le processus utilise des sockets Windows et nécessite une adresse IP unique ou un numéro de port TCP spécifié

Pour déterminer si une application doit utiliser des adresses IP virtuelles :

1. Obtenez l'outil TCP View auprès de Microsoft. Cet outil répertorie toutes les applications liées à des adresses IP et ports spécifiques.
2. Désactivez la fonction Résoudre les adresses IP afin de visualiser les adresses au lieu des noms d'hôtes.
3. Lancez l'application et utilisez l'outil TCPView pour voir quelles adresses IP et ports sont ouverts par celle-ci ainsi que les noms des processus qui ouvrent ces ports.
4. Configurez tous les processus qui ouvrent l'adresse IP du serveur, 0.0.0.0 ou 127.0.0.1.
5. Lancez une autre instance de l'application afin de vous assurer qu'elle n'ouvre pas la même adresse IP sur un port différent.

Fonctionnement de la virtualisation IP Microsoft Remote Desktop (RD)

- L'adressage IP virtuel doit être activé sur le serveur Microsoft.

  Par exemple, dans un environnement Windows Server 2008 R2, à partir du Gestionnaire de serveur, développez Services Bureau à distance > Connexions hôtes de session Bureau à distance pour activer la fonctionnalité de virtualisation IP des services Bureau à distance et configurer les paramètres pour attribuer dynamiquement des adresses IP à l'aide du serveur DHCP (Dynamic Host Configuration Protocol) par session ou par programme. Consultez la documentation Microsoft pour obtenir des instructions.

- Lorsque cette fonctionnalité est activée, au démarrage de la session, le serveur demande des adresses IP attribuées dynamiquement auprès du serveur DHCP.

- La fonctionnalité de virtualisation IP des services Bureau à distance attribue les adresses IP aux connexions Bureau à distance par session ou par programme. Si vous attribuez des adresses IP à de multiples programmes, ces derniers partagent une adresse IP par session.
- Après attribution d'une adresse à une session, celle-ci utilise cette adresse virtuelle plutôt que l'adresse IP principale du système en présence des appels suivants : bind ¸ closesocket ¸ connect, WSAConnect, WSAAccept, getpeername, getsockname, sendto, WSASendTo, WSASocketW, gethostbyaddr, getnameinfo, getaddrinfo

Lors de l'utilisation de la fonctionnalité de virtualisation d'adresses IP de Microsoft dans la configuration d'hôte de session Bureau à distance, les applications sont liées à des adresses IP spécifiques par l'insertion d'un composant « filtre » entre l'application et les appels de fonction Winsock. L'application ne voit ensuite que l'adresse IP qu'elle doit utiliser. Toute tentative d'écoute de communications TCP ou UDP par l'application est liée à l'adresse IP virtuelle (ou adresse de bouclage) qui lui est attribuée automatiquement. Toutes les connexions ouvertes par l'application sont établies au départ par l'adresse IP liée à l'application.

Pour les fonctions qui renvoient une adresse, telle que GetAddrInfo() (contrôlée par une stratégie Windows) si l'adresse IP de l'hôte local est demandée, la fonctionnalité d'adresse IP virtuelle intercepte l'adresse IP retournée et la remplace par l'adresse IP virtuelle de la session. Les applications qui tentent d'obtenir l'adresse IP du serveur local à travers ce type de fonctions de nom n'obtiennent que l'adresse IP virtuelle unique attribuée à la session. Cette adresse IP est souvent utilisée dans les appels de socket suivants, tels que bind ou connect.

Une application demande souvent à se lier à un port pour procéder à une écoute de l'adresse « 0.0.0.0 ». Lorsque c'est le cas et qu'une application utilise un port statique, vous ne pouvez pas ouvrir plus d'une instance de celle-ci. La fonction d'adresse IP virtuelle recherche également 0.0.0.0 dans ces types d'appels et modifie l'appel en écoute sur l'adresse IP virtuelle spécifique, ce qui permet à plusieurs applications d'écouter sur le même port sur le même ordinateur, car ils effectuent l'écoute sur des adresses différentes. Cette écoute est uniquement modifiée si une session ICA et la fonction d'adresse IP virtuelle sont activées. Par exemple, si deux instances d'une application exécutée dans des sessions différentes tentent toutes deux de se lier à toutes les interfaces (0.0.0.0) et à un port spécifique (comme 9000), elles sont liées à VIPAddress1:9000 et VIPAddress2:9000, sans aucun conflit.

Bouclage virtuel

L'activation des paramètres de stratégie d'adresse IP virtuelle Citrix permettent à chaque session de disposer de sa propre adresse de bouclage pour les communications. Lorsqu'une application utilise l'adresse localhost (valeur par défaut = 127.0.0.1) dans un appel Winsock, la fonctionnalité de bouclage virtuel remplace simplement 127.0.0.1 par 127.X.X.X, où X.X.X représente l'ID de session + 1. Par exemple, 127.0.0.8. pour un ID session de 7. Dans le cas peu probable où l'ID session dépasse le quatrième

octet (plus de 255), l'adresse passe à l'octet suivant (127.0.1.0), jusqu'à 127.255.255.255 maximum.

Un processus nécessite le bouclage virtuel dans l'un des cas suivants :

- Le processus utilise l'adresse de bouclage de socket Windows 127.0.0.1 (localhost)
- Le processus utilise un numéro de port TCP fixe

Utilisez les
paramètres de stratégie de bouclage virtuel pour les applications qui utilisent une adresse de bouclage pour la communication entre les processus. Aucune configuration supplémentaire n'est requise. Le bouclage virtuel n'a pas de dépendance à l'égard des adresses IP virtuelles, de sorte que vous n'avez pas à configurer le serveur Microsoft.

- Prise en charge du bouclage d'adresse IP virtuelle. Lorsqu'il est activé, ce paramètre de stratégie permet à chaque session de disposer de sa propre adresse de bouclage virtuel. Cette option est désactivée par défaut. Cette fonctionnalité ne s'applique qu'aux applications spécifiées avec le paramètre de stratégie Liste de programmes de bouclage virtuel d'adresse IP virtuelle.
- Liste de programmes de bouclage virtuel d'adresse IP virtuelle. Ce paramètre de stratégie spécifie les applications qui utilisent la fonctionnalité de bouclage d'adresse IP virtuelle. Ce paramètre ne s'applique que lorsque le paramètre de stratégie de prise en charge du bouclage d'adresse IP virtuelle est activé.

Fonction connexe

Vous pouvez utiliser les paramètres de registre suivants pour vous assurer que le bouclage virtuel est préféré aux adresses IP virtuelles ; cela s'appelle un bouclage par défaut. Soyez, toutefois, prudent :

- Le bouclage par défaut est pris en charge sur Windows Server 2008 R2 et Windows Server 2012 R2 uniquement.
- Utilisez le bouclage par défaut uniquement si les adresses IP virtuelles et le bouclage virtuel sont activés ; sinon, vous risquez d'obtenir des résultats inattendus.
- Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Exécutez regedit sur les serveurs sur lesquels les applications résident.

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\VIP (HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\V pour machines 32 bits)
- Nom : PreferLoopback, Type : REG_DWORD, Données : 1
- Nom : PreferLoopbackProcesses, Type : REG_MULTI_SZ, Données :<liste des processus>

Delivery Controller

February 28, 2019

Le Delivery Controller est le composant côté serveur qui est responsable de la gestion de l'accès utilisateur, ainsi que de la négociation et de l'optimisation des connexions. Les Controller fournissent également les services Machine Creation qui créent des images de bureau et de serveur.

Un site doit avoir au moins un Controller. Après avoir installé le Controller initial, vous pouvez ajouter des Controller supplémentaires lorsque vous créez un site, ou plus tard. Avoir plus d'un Controller dans un site présente deux avantages.

- Redondance : il est recommandé qu'un site de production dispose toujours d'au moins deux Controller sur des serveurs physiques différents. Si un Controller échoue, les autres peuvent gérer les connexions et administrer le site.
- Évolutivité : au fur et à mesure que l'activité du site augmente, il en va de même pour l'utilisation de l'UC sur le Controller et l'activité de la base de données. Les Controller supplémentaires permettent de gérer plus d'utilisateurs et plus de demandes d'applications et de bureaux, et peuvent améliorer la réactivité générale.

Chaque Controller communique directement avec la base de données du site. Dans un site avec plusieurs zones, les Controller de chaque zone communiquent avec la base de données du site dans la zone principale.

> **Important :**
>
> Ne modifiez pas le nom de l'ordinateur ou l'appartenance à un domaine d'un Controller une fois que le site est configuré.

Comment les VDA s'enregistrent auprès d'un Controller

Avant qu'un VDA puisse être utilisé, il doit s'enregistrer (établir la communication) auprès d'un Delivery Controller sur le site. Pour plus d'informations sur l'enregistrement de VDA, voir Enregistrement d'un VDA auprès d'un Delivery Controller.

(Dans la documentation pour les versions XenApp et XenDesktop 7.x antérieures, les informations sur l'enregistrement de VDA apparaissaient dans cet article. Ces informations ont été améliorées et se trouvent maintenant dans l'article connexe ci-dessus.)

Ajouter, supprimer ou déplacer des Delivery Controller

Pour ajouter, supprimer ou déplacer un Controller, vous devez disposer des autorisations de rôle de serveur et de rôle de base de données répertoriées dans l'article *Bases de données*.

> **Remarque :**
>
> L'installation d'un Controller sur un nœud dans une installation de mise en cluster SQL ou mise en miroir SQL n'est pas prise en charge.

Si votre déploiement utilise la mise en miroir de base de données :

- Avant l'ajout, la suppression ou le déplacement d'un Controller, assurez-vous que les bases de données principale et en miroir sont en cours d'exécution. En outre, si vous utilisez les scripts avec SQL Server Management Studio, activez le mode SQLCMD avant d'exécuter les scripts.
- Pour vérifier la mise en miroir après ajout, suppression ou déplacement d'un Delivery Controller, exécutez l'applet de commande PowerShell **get-configdbconnection** pour vous assurer que le partenaire de basculement a été défini dans la chaîne de connexion sur le miroir.

Après avoir ajouté, supprimé ou déplacé un Delivery Controller :

- Si la mise à jour automatique est activée, les VDA recevront une liste actualisée des Delivery Controller dans les 90 minutes qui suivent.
- Si la mise à jour automatique n'est pas activée, vérifiez que le paramètre de stratégie du Delivery Controller ou la clé de registre ListOfDDCs sont mis à jour pour tous les VDA. Après déplacement d'un Delivery Controller vers un autre site, mettez à jour le paramètre de stratégie ou la clé de registre sur les deux sites.

Ajouter un Controller

Vous pouvez ajouter des Controller lorsque vous créez un site et ultérieurement. Vous ne pouvez pas ajouter des Controller installés avec une version antérieure de ce logiciel à un site qui a été créé avec cette version.

1. Exécutez le programme d'installation sur un serveur contenant un système d'exploitation pris en charge. Installez le composant Delivery Controller et les autres composants principaux requis. Suivez les instructions de l'assistant d'installation.
2. Si vous n'avez pas encore créé de site, démarrez Studio ; vous êtes invité à créer un site. Sur la page Bases de données de l'Assistant de création de site, cliquez sur le bouton Sélectionner et ajoutez l'adresse du serveur sur lequel vous avez installé le Controller supplémentaire. **Important :** si vous souhaitez générer des scripts qui initialiseront les bases de données, ajoutez les Controller avant de générer les scripts.
3. Si vous avez déjà créé un site, pointez Studio vers le serveur sur lequel vous avez installé le Controller supplémentaire. Cliquez sur **Adapter votre déploiement** et entrez l'adresse du site.

Supprimer un Controller

La suppression d'un Delivery Controller d'un site n'entraîne pas la désinstallation du logiciel Citrix ou de tout autre composant ; elle supprime le Delivery Controller de la base de données afin qu'il ne puisse plus être utilisé pour les connexions du broker et pour effectuer d'autres tâches. Si vous supprimez un Delivery Controller, vous pouvez le rajouter par la suite au même site ou à un autre site. Un site a besoin d'au moins un Delivery Controller ; vous ne pouvez donc pas supprimer le dernier Delivery Controller répertorié dans Studio.

Lorsque vous supprimez un Controller d'un site, l'ouverture de session Controller sur le serveur de base de données n'est pas supprimée. Cela évite potentiellement la suppression d'une ouverture de session utilisée par des services d'autres produits sur la même machine. L'ouverture de session doit être supprimée manuellement si elle n'est plus requise ; l'autorisation de rôle de serveur securityadmin est nécessaire pour la supprimer.

> **Important :**
>
> Ne supprimez pas le Controller depuis Active Directory tant que vous ne l'avez pas supprimé du site.

1. Assurez-vous que le Controller est sous tension afin que Studio puisse se charger en moins d'une heure. Une fois que Studio charge le Controller que vous souhaitez supprimer, placez le Controller hors tension lorsque vous y êtes invité.
2. Sélectionnez **Configuration > Delivery Controller** dans le panneau de navigation Studio, puis sélectionnez le Controller que vous voulez supprimer.
3. Cliquez sur **Supprimer le Controller** dans le volet Actions. Si vous ne possédez pas les droits et les rôles de base de données appropriés, vous pouvez générer un script qui permet à votre administrateur de base de données de supprimer le Delivery Controller à votre place.
4. Vous devrez peut-être supprimer le compte machine du Delivery Controller du serveur de base de données. Avant de procéder de la sorte, vérifiez qu'aucun autre service n'utilise le compte.

Après utilisation de Studio pour supprimer un Controller, le trafic vers ce Controller peut rester affiché pour un laps de temps pour assurer le bon d'achèvement des tâches courantes. Si vous souhaitez forcer la suppression d'un Controller dans un bref délai, Citrix vous recommande de fermer le serveur sur lequel il a été installé, ou de supprimer ce serveur à partir d'Active Directory. Ensuite, redémarrez les autres Controller du site pour vous assurer qu'aucune autre communication avec le Controller supprimé n'est réalisée.

Déplacer un Controller vers une autre zone

Si votre site contient plusieurs zones, vous pouvez déplacer un Controller vers une autre zone. Consultez l'article *Zones* pour savoir comment cela peut affecter l'enregistrement de VDA et d'autres opérations.

1. Sélectionnez **Configuration > Delivery Controller** dans le panneau de navigation Studio, puis sélectionnez le Controller que vous voulez déplacer.
2. Sélectionnez **Déplacer** dans le volet Actions.
3. Spécifiez la zone vers laquelle vous souhaitez déplacer le Controller.

Pour déplacer un Controller vers un autre site

Vous ne pouvez pas déplacer un Delivery Controller vers un site qui a été créé avec une version antérieure de ce logiciel.

1. Sur le site dans lequel figure le Controller (l'ancien site), sélectionnez **Configuration > Delivery Controller** dans le panneau de navigation de Studio, puis sélectionnez le Controller que vous souhaitez déplacer.
2. Cliquez sur **Supprimer le Controller** dans le volet Actions. Si vous ne possédez pas les droits et les rôles de base de données appropriés, vous pouvez générer un script qui permet à un utilisateur disposant de ces autorisations (tel qu'un administrateur de base de données) de supprimer le Delivery Controller à votre place. Un site a besoin d'au moins un Delivery Controller ; vous ne pouvez donc pas supprimer le dernier Delivery Controller répertorié dans Studio.
3. Sur le Controller que vous déplacez, ouvrez Studio, réinitialisez les services lorsque vous y êtes invité, cliquez sur **Joindre un site existant** et saisissez l'adresse du nouveau site.

Déplacer un VDA vers un autre site

Si un VDA a été provisionné à l'aide de Provisioning Services ou qu'il est une image existante, vous pouvez déplacer un VDA vers un autre site (d'un site 1 au site 2) lors de la mise à niveau, ou lors du déplacement d'une image de VDA qui a été créée dans un site test vers un site de production. Les VDA provisionnés à l'aide de Machine Creation Services (MCS) ne peuvent pas être déplacés d'un site à un autre car MCS ne prend pas en charge la modification des listes ListOfDDC que VDA vérifie pour s'enregistrer auprès d'un Controller ; les VDA provisionnés à l'aide de MCS vérifient toujours les listes ListOfDDC associées au site dans lequel ils ont été créés.

Il existe deux façons de déplacer un VDA vers un autre site : à l'aide du programme d'installation ou de stratégies Citrix.

Programme d'installation : exécutez le programme d'installation et ajoutez un Controller, en spécifiant le nom complet (entrée DNS) d'un Controller du site 2. **Important :** ne spécifiez les Controller dans le programme d'installation que lorsque le paramètre de stratégie des Controller n'est pas utilisé.

Éditeur de stratégie de groupe : l'exemple suivant déplace plusieurs VDA entre sites.

1. Créez une stratégie dans le site 1 qui contient les paramètres suivants, puis filtrez la stratégie au niveau du groupe de mise à disposition pour initier une migration VDA échelonnée entre les

sites.
Controller : contenant les noms complets (entrées DNS) d'un ou de plusieurs Controller dans le site 2.
Activer la mise à jour automatique des Controller : défini sur désactivé.

2. Chaque VDA dans le groupe de mise à disposition reçoit une alerte dans les 90 minutes qui suivent la création de la nouvelle stratégie. Le VDA ignore la liste de Controller qu'il reçoit (car la mise à jour automatique est désactivée) : il sélectionne l'un des Controller spécifiés dans la stratégie, qui répertorie les Controller du site 2.
3. Lorsque le VDA s'enregistre avec succès auprès d'un Controller du site 2, il reçoit la liste ListOfDDCs du site 2 et les informations de stratégie, dans laquelle la mise à jour automatique est activée par défaut. Étant donné que le Controller auquel duquel le VDA s'est enregistré dans le site 1 ne figure pas sur la liste envoyée par le Controller du site 2, le VDA se réenregistre, en choisissant parmi les Controller de la liste du site 2. Dès lors, le VDA est automatiquement mis à jour avec les informations du site 2.

Enregistrement de VDA

February 28, 2019

Introduction

Avant qu'un VDA puisse être utilisé, il doit s'enregistrer (établir la communication) auprès d'un ou de plusieurs Controller ou Cloud Connector sur le site. (Dans un déploiement de XenApp et XenDesktop sur site, les VDA s'enregistrent auprès des Controller. Dans un déploiement de XenApp et XenDesktop Service, les VDA s'enregistrent auprès de Cloud Connector.) Le VDA trouve un Controller ou Connector en vérifiant une liste appelée ListofDDCs. La liste ListOfDDCs sur un VDA se compose d'une ou plusieurs entrées DNS qui pointent le VDA vers des Controller ou Cloud Connector sur le site. Pour assurer l'équilibrage de charge, le VDA répartit automatiquement les connexions de manière équitable entre les Controller ou Cloud Connector dans la liste.

Pourquoi l'enregistrement de VDA est-il si important ?

- Du point de vue de la sécurité, l'enregistrement est une opération délicate : vous établissez une connexion entre le Controller ou le Cloud Connector et le VDA. Pour une telle opération délicate, le comportement attendu est le rejet de la connexion si toutes les conditions requises ne sont pas remplies. Vous établissez en fait deux canaux de communication distincts : VDA vers Controller ou Cloud Connector et Controller ou Cloud Connector vers VDA. La connexion utilise Kerberos, donc les problèmes de synchronisation de l'heure et d'appartenance de domaine bloqueront le processus. Kerberos utilise les noms principaux de service (SPN), donc vous ne pouvez pas utiliser d'adresse IP ou de nom d'hôte avec équilibrage de charge.

- Si un VDA ne dispose pas d'informations précises et à jour sur le Controller ou Cloud Connector lorsque vous ajoutez et supprimez des Controller ou Cloud Connector, le VDA peut rejeter les lancements de session qui ont été négociés par un Controller ou Cloud Connector non répertorié. La présence d'entrées non valides peut retarder le démarrage du logiciel système du bureau virtuel. Un VDA n'accepte pas de connexion à partir d'un Controller ou Cloud Connector inconnu et non fiable.

En plus de la ListOfDDCs, la ListOfSIDs (ID de sécurité) indique les machines de ListOfDDCs qui sont fiables. La liste ListOfSIDs peut être utilisée pour réduire la charge sur Active Directory ou pour éviter des menaces de sécurité provenant d'un serveur DNS non fiable. Pour plus d'informations, consultez la section *ListOfSIDs* ci-dessous.

Si une liste ListOfDDCs spécifie plusieurs Controller ou Cloud Connector, le VDA tente de s'y connecter aléatoirement. Dans un déploiement sur site, la liste ListOfDDCs peut également contenir des groupes de Controller. Le VDA tente de se connecter à chaque Controller dans un groupe avant de passer à d'autres entrées dans la liste ListOfDDCs.

XenApp et XenDesktop testent automatiquement la connectivité avec les Controller ou Cloud Connector configurés lors de l'installation de VDA. Les erreurs sont affichées si un Controller ou Cloud Connector n'est pas accessible. Si vous ignorez un message d'avertissement indiquant qu'un Controller ou Cloud Connector ne peut pas être contacté (ou lorsque vous ne spécifiez pas d'adresses de Controller ou Cloud Connector au cours de l'installation de VDA), des messages de rappel sont envoyés.

Méthodes de configuration des adresses de Controller ou Cloud Connector

L'administrateur décide de la méthode de configuration à utiliser lorsque le VDA s'enregistre pour la première fois. (Il s'agit de l'enregistrement initial). Lors de l'enregistrement initial, un cache permanent est créé sur le VDA. Lors des enregistrements ultérieurs, le VDA récupère la liste de Controller ou Cloud Connector à partir de ce cache local, sauf si une modification de configuration est détectée.

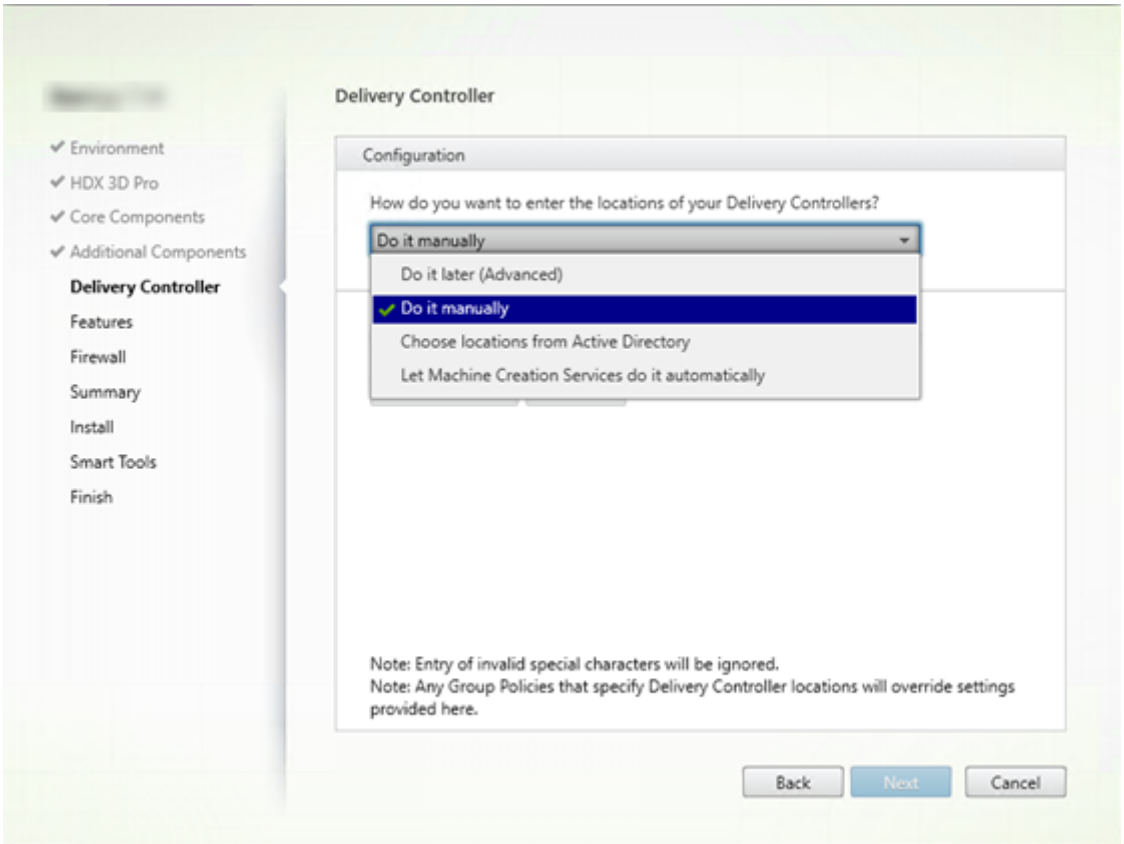
La meilleure façon de récupérer cette liste lors des enregistrements ultérieurs consiste à utiliser la fonction de mise à jour automatique. Par défaut, la mise à jour automatique est activée. Pour plus d'informations, consultez Mise à jour automatique.

Il existe plusieurs méthodes de configuration des adresses de Controller ou Cloud Connector sur un VDA.

- Basée une stratégie (LGPO ou GPO)
- Basée sur le Registre (manuelle, GPP, spécifiée lors de l'installation de VDA)
- Basée sur l'unité d'organisation Active Directory (découverte d'unité d'organisation ancienne génération)
- Basée sur MCS (personality.ini)

Vous spécifiez la méthode d'enregistrement initial lorsque vous installez un VDA. (Si vous désactivez la mise à jour automatique, la méthode que vous sélectionnez lors de l'installation d'un VDA sera également utilisée pour les enregistrements ultérieurs.)

Le graphique suivant montre la page **Delivery Controller** de l'Assistant d'installation de VDA.



Basée sur une stratégie (LGPO/GPO)

Citrix vous recommande d'utiliser un objet de stratégie de groupe (GPO) pour l'enregistrement initial de VDA. Cette méthode a la priorité la plus élevée. (La mise à jour automatique est répertoriée ci-dessus comme priorité la plus élevée, mais la mise à jour automatique est utilisée uniquement après l'enregistrement initial). L'enregistrement basé sur une stratégie offre les avantages que représente l'utilisation de la stratégie de groupe pour la configuration en terme de centralisation.

Pour spécifier cette méthode, effectuez les deux étapes suivantes :

- Sur la page **Delivery Controller** dans l'assistant d'installation VDA, sélectionnez **Le faire plus tard (avancé)**. L'assistant vous rappelle plusieurs fois de spécifier les adresses de Controller, même si vous ne les spécifiez pas lors de l'installation de VDA. (Car l'enregistrement de VDA est particulièrement important !)
- Activez ou désactivez l'enregistrement de VDA basé sur une stratégie par le biais de la stratégie

Citrix avec le paramètre Paramètres Virtual Delivery Agent > Controller. (Si la sécurité est votre priorité, utilisez Paramètres Virtual Delivery Agent >SID de Contrôleur.)

Ce paramètre est enregistré sous HKLM\Software\Policies\Citrix\VirtualDesktopAgent (ListOfDDCs).

Basée sur le Registre

Pour spécifier cette méthode, effectuez une des étapes suivantes :

- Sur la page **Delivery Controller** dans l'assistant d'installation VDA, sélectionnez **Effectuer manuellement**. Ensuite, entrez le nom de domaine complet d'un Controller installé, puis cliquez sur **Ajouter**. Si vous avez installé des Controller supplémentaires, ajoutez leurs adresses.
- Pour une installation de VDA par ligne de commande, utilisez l'option /controllers et spécifiez les noms de domaine complets des Controller ou Cloud Connector installés.

Ces informations sont généralement stockées dans la valeur de Registre ListOfDDCs sous la clé de Registre HKLM\Software\Citrix\VirtualDesktopAgent ou HKLM\Software\Wow6432Node\Citrix\VirtualDesktopAgent.

Vous pouvez également configurer cette clé de Registre manuellement ou utiliser les préférences de stratégie de groupe (GPP). Cette méthode peut être préférable à la méthode basée sur la stratégie (par exemple, si vous souhaitez un traitement conditionnel de différents Controller ou Cloud Connector, tel que : utiliser XDC-001 pour les noms d'ordinateur qui commencent par XDW-001-).

Mettez à jour la clé de registre ListOfDDCs, qui répertorie les noms de domaine complets de tous les Controller ou Cloud Connector du site. (Cette clé est l'équivalent de l'unité d'organisation du site Active Directory.)

HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfDDCs (REG_SZ)

Si l'emplacement de registre HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent contient les clés ListOfDDCs et FarmGUID, ListOfDDCs est utilisée pour la découverte de Controller ou Cloud Connector. La clé FarmGUID est présente si une unité d'organisation de site a été spécifiée lors de l'installation du VDA. (Elle peut être utilisée dans les déploiements d'ancienne génération).

Si vous le souhaitez, mettez à jour la clé de Registre ListOfSIDs (pour plus d'informations, consultez la section *ListOfSIDs* ci-dessous) :

HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs (REG_SZ)

> **Rappel :**
>
> Si vous activez également l'enregistrement de VDA via une stratégie Citrix, cette configuration remplace les paramètres que vous spécifiez lors de l'installation de VDA, car il s'agit d'une méthode à priorité plus élevée.

Basée sur l'unité d'organisation Active Directory (ancienne génération)

Cette méthode est prise en charge principalement pour la rétrocompatibilité et n'est pas recommandée. Si vous l'utilisez toujours, Citrix suggère de changer de méthode.

Pour spécifier cette méthode, effectuez les deux étapes suivantes :

- Sur la page **Delivery Controller** dans l'assistant d'installation VDA, sélectionnez **Choisir les emplacements d'Active Directory**.
- Utilisez le script Set-ADControllerDiscovery.ps1 (disponible sur chaque Controller). Configurez aussi l'entrée de Registre FarmGuid sur chaque VDA de manière à pointer vers l'unité d'organisation correcte. Ce paramètre peut être configuré à l'aide de la stratégie de groupe.

Pour plus amples informations, consultez la section Découverte basée sur unité d'organisation Active Directory.

Basée sur MCS

Si vous prévoyez d'utiliser uniquement MCS pour provisionner des VM, vous pouvez demander à MCS de configurer la liste des Delivery Controller ou Cloud Connector. Cette fonctionnalité fonctionne avec la mise à jour automatique : MCS injecte la liste des Controller ou Cloud Connector dans le fichier Personality.ini lors du provisioning initial (lorsque vous créez le catalogue de machines). La mise à jour automatique permet de conserver la liste à jour.

Cette méthode n'est pas recommandée pour les environnements de grande taille. Vous pouvez utiliser cette méthode si vous :

- disposez d'un environnement de petite taille ;
- ne déplacez pas les VDA entre sites ;
- utilisez uniquement MCS pour provisionner des VM ;
- ne souhaitez pas utiliser la stratégie de groupe.

Pour spécifier cette méthode :

- Sur la page **Delivery Controller** dans l'assistant d'installation VDA, sélectionnez **Laisser Machine Creation Services effectuer ceci automatiquement**.

Recommandations

Recommandations :

- Utilisez la méthode de stratégie de groupe pour l'enregistrement initial.
- Utilisez la mise à jour automatique (activée par défaut) pour garder votre liste de Controller à jour.

- Dans un déploiement multi-zone, utilisez la stratégie de groupe pour la configuration initiale (avec au moins deux Controller ou Cloud Connector). Pointez les VDA vers des Controller ou Cloud Connector locaux, dans leur zone. Utilisez la mise à jour automatique pour assurer leur mise à jour. La mise à jour automatique optimise automatiquement la liste ListOfDDCs pour les VDA dans des zones satellite.

Mise à jour automatique

La mise à jour automatique (introduite dans XenApp et XenDesktop 7.6) est activée par défaut. Il s'agit de la méthode la plus efficace pour assurer la mise à jour de vos enregistrements de VDA. Bien que la mise à jour automatique ne soit pas utilisée pour l'enregistrement initial, le logiciel de mise à jour automatique télécharge et stocke la liste ListOfDDCs dans un cache permanent sur le VDA lors de l'enregistrement initial. Ce processus se fait pour chaque VDA. (Le cache contient également des informations sur la stratégie de la machine, ce qui garantit que les paramètres de stratégie sont conservés après les redémarrages.)

La mise à jour automatique est prise en charge lors de l'utilisation de MCS ou PVS pour provisionner des machines, sauf pour le cache côté serveur PVS (qui n'est pas un scénario courant car il n'existe pas de stockage permanent pour le cache de mise à jour automatique).

Pour spécifier cette méthode :

- Activez ou désactivez la mise à jour automatique via une stratégie Citrix contenant le paramètre : Paramètres Virtual Delivery Agent > Activer la mise à jour automatique des Controller. Cette option est activée par défaut.

Fonctionnement

- Chaque fois qu'un VDA se réenregistre (par exemple, après un redémarrage de machine), le cache est mis à jour. Chaque Controller ou Cloud Connector vérifie également la base de données du site toutes les 90 minutes. Si un Controller ou Cloud Connector a été ajouté ou supprimé depuis la dernière vérification, ou si une modification de stratégie s'est produite qui affecte l'enregistrement du VDA, le Controller ou Cloud Connector envoie une liste actualisée vers les VDA enregistrés et le cache est mis à jour. Le VDA accepte les connexions provenant de tous les Controller ou Cloud Connector figurant dans la liste mise en cache le plus récemment.
- Si un VDA reçoit une liste qui ne comprend pas le Controller ou Cloud Connector auprès duquel il est enregistré (en d'autres termes, ce Controller ou Cloud Connector a été supprimé du site), le VDA s'enregistre de nouveau, en choisissant parmi les Controller ou Cloud Connector dans la liste ListOfDDCs.

Par exemple :

- Un déploiement dispose de trois Controller : A B et C. Un VDA s'enregistre auprès du Controller B (qui a été spécifié lors de l'installation du VDA).

- Deux Controller (D et E) sont ajoutés au site plus tard. Dans les 90 minutes qui suivent, le VDA reçoit les listes mises à jour et accepte les connexions provenant des Controller A, B, C, D et E. (La charge ne sera pas répartie de manière égale sur tous les Controller tant que les VDA ne sont pas redémarrés.)
- Plus tard, le Controller B est déplacé vers un autre site. Dans les 90 minutes qui suivent, le VDA sur le site d'origine reçoit les listes mises à jour car un Controller a été modifié depuis la dernière vérification. Le VDA qui s'est enregistré initialement auprès du Controller B (qui ne figure plus sur la liste) se réenregistre en choisissant parmi les Controller disponibles dans la liste actuelle (A, C, D et E).

Dans un déploiement multi-zone, la mise à jour automatique dans une zone satellite commence par mettre automatiquement en cache tous les Controller locaux. Tous les Controller de la zone principale sont mis en cache dans un groupe de secours. Si aucun Controller local de la zone satellite n'est disponible, une tentative d'enregistrement avec les Controller de la zone principale est effectuée.

Comme illustré dans l'exemple suivant, le fichier de cache contient des noms d'hôte et une liste d'ID de sécurité (ListOfSIDs). Le VDA n'interroge pas les SID, ce qui réduit la charge d'Active Directory.

```
<?xml version="1.0"?>
<ListOfDDcsListIfSids xmlns="http://schemas.datacontract.org/2004/07/Citrix.Cds.BrokerAgent" xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
  - <_x003C_GroupsOfDDCs_x003E_k__BackingField xmlns:d2p1="http://schemas.microsoft.com/2003/10/Serialization/Arrays">
      - <d2p1:ArrayOfstring>
          <d2p1:string>CTX-XDC-002.zugec.lan</d2p1:string>
          <d2p1:string>CTX-XDC-001.zugec.lan</d2p1:string>
        </d2p1:ArrayOfstring>
    </_x003C_GroupsOfDDCs_x003E_k__BackingField>
  - <_x003C_ListOfDDCs_x003E_k__BackingField xmlns:d2p1="http://schemas.microsoft.com/2003/10/Serialization/Arrays">
      <d2p1:string>CTX-XDC-002.zugec.lan</d2p1:string>
      <d2p1:string>CTX-XDC-001.zugec.lan</d2p1:string>
    </_x003C_ListOfDDCs_x003E_k__BackingField>
  - <_x003C_ListOfSids_x003E_k__BackingField xmlns:d2p1="http://schemas.microsoft.com/2003/10/Serialization/Arrays">
      <d2p1:string>S-1-5-21-726903571-3621260514-849154371-1119</d2p1:string>
      <d2p1:string>S-1-5-21-726903571-3621260514-849154371-1126</d2p1:string>
    </_x003C_ListOfSids_x003E_k__BackingField>
    <_x003C_NonAutoListOfDDCsMethod_x003E_k__BackingField>RegistryBasedFarm</_x003C_NonAutoListOfDDCsMethod_x003E_k__BackingField>
    <_x003C_NonAutoListOfDDCsOrOu_x003E_k__BackingField>CTX-XDC-002.zugec.lan</_x003C_NonAutoListOfDDCsOrOu_x003E_k__BackingField>
</ListOfDDcsListIfSids>
```

Vous pouvez récupérer le fichier de cache avec un appel WMI ; toutefois, il est stocké dans un emplacement lisible uniquement par le compte système. Important : cette information est fournie uniquement à titre indicatif. NE MODIFIEZ PAS CE FICHIER. Toute modification de ce fichier ou dossier entraîne une configuration non prise en charge.

Get-WmiObject -Namespace “Root\Citrix\DesktopInformation”
-Class “Citrix_VirtualDesktopInfo” -Property “PersistentDataLocation”

Si vous avez besoin de configurer manuellement la ListOfSIDs pour des raisons de sécurité (et non à des fins de réduction de la charge d'Active Directory), vous ne pouvez pas utiliser la fonctionnalité de mise à jour automatique. Pour plus amples informations, consultez la section *ListOfSIDs* ci-dessous.

Exception à la priorité de mise à jour automatique

Bien que la mise à jour automatique ait généralement la priorité la plus élevée de toutes les méthodes d'enregistrement de VDA et remplace les paramètres des autres méthodes, il existe une exception. Les

éléments NonAutoListOfDDCs dans le cache spécifient la méthode de configuration initiale de VDA. La mise à jour automatique contrôle ces informations. Si la méthode d'enregistrement initial est modifiée, le processus d'enregistrement ignore la mise à jour automatique et utilise parmi les méthodes configurées celle dont la priorité est la plus proche. Cela peut s'avérer utile lorsque vous déplacez un VDA vers un autre site (par exemple, lors d'une récupération d'urgence).

Considérations liées à la configuration

Adresses de Controller ou Cloud Connector

Quelle que soit la méthode que vous utilisez pour spécifier des Controller ou Cloud Connector, Citrix recommande d'utiliser une adresse de nom de domaine complet. Une adresse IP n'est pas considérée comme une configuration de confiance, car il est plus facile de compromettre une adresse IP qu'un enregistrement DNS. Si vous renseignez la liste ListOfSIDs manuellement, vous pouvez utiliser une adresse IP dans une liste ListOfDDCs. Cependant, un nom de domaine complet est toujours recommandé.

Équilibrage de charge

Comme indiqué précédemment, le VDA répartit automatiquement les connexions de manière équitable entre les Controller ou Cloud Connector dans la liste ListOfDDCs. La fonctionnalité d'équilibrage de charge et de basculement est intégrée au protocole CBP (Citrix Brokering Protocol). Si vous spécifiez plusieurs Controller ou Cloud Connector dans votre configuration, l'enregistrement bascule automatiquement de l'un à l'autre, si nécessaire. Avec la mise à jour automatique, le basculement automatique se produit automatiquement pour tous les VDA.

Pour des raisons de sécurité, vous ne pouvez pas utiliser un équilibreur de charge réseau, tel que Citrix ADC. L'enregistrement de VDA utilise l'authentification mutuelle Kerberos, où le client (VDA) doit prouver son identité au service (Controller). Toutefois, le Controller ou Cloud Connector doit prouver son identité au VDA. Cela signifie que le VDA et le Controller ou Cloud Connector agissent en tant que serveur et client en même temps. Comme indiqué au début de cet article, il existe deux canaux de communications : VDA -> Controller/Cloud Connector et Controller/Cloud Connector -> VDA.

Un composant de ce processus est appelé Nom de service principal (SPN) ; il est stocké en tant que propriété dans un objet ordinateur Active Directory. Lorsque votre VDA se connecte à un Controller ou Cloud Connector, il doit spécifier avec « qui » il souhaite communiquer ; cette adresse est un SPN. Si vous utilisez une adresse IP d'équilibrage de charge, l'authentification Kerberos mutuelle reconnaît correctement que l'adresse IP n'appartient pas au Controller ou Cloud Connector attendu.

Pour plus d'informations, consultez :

Introduction à Kerberos : https://blogs.technet.microsoft.com/askds/2008/03/06/kerberos-for-the-busy-admin/

Authentification mutuelle à l'aide de Kerberos : https://msdn.microsoft.com/en-us/library/ms677600

La mise à jour automatique remplace CNAME

La fonctionnalité de mise à jour automatique remplace la fonction CNAME (alias DNS) des versions XenApp et XenDesktop antérieures à 7.x. La fonctionnalité CNAME est désactivée, à compter de XenApp et XenDesktop 7. Utilisez la mise à jour automatique au lieu de CNAME. (Si vous devez utiliser CNAME, consultez la section CTX137960. Pour que l'alias DNS fonctionne de manière cohérente, n'utilisez pas la mise à jour automatique et CNAME en même temps.)

Groupes de Controller/Cloud Connector

Dans certains scénarios, vous pouvez gérer les Controller ou Cloud Connector sous forme de groupes, avec un groupe préféré et l'autre groupe utilisé pour le basculement si tous les Controller/Cloud Connector échouent. N'oubliez pas que les Controller ou Cloud Connector sont sélectionnés de manière aléatoire dans la liste, par conséquent le regroupement peut vous aider à imposer l'utilisation de certains Controller.

Pour spécifier des groupes de Controller/Cloud Connector, utilisez des parenthèses. Par exemple, avec quatre Controller (deux principaux et deux de sauvegarde), un regroupement peut être :

(XDC-001.cdz.lan XDC-002.cdz.lan) (XDC-003.cdz.lan XDC-004.cdz.lan).

Dans cet exemple, les Controller du premier groupe (001 et 002) sont traités en premier. Si deux échouent, les Controller du deuxième groupe (003 et 004) sont traités.

ListOfSIDs

La liste de Controller qu'un VDA peut contacter pour l'enregistrement est la liste ListOfDDCs. Un VDA doit également connaître les Controller à approuver ; les VDA ne font pas automatiquement confiance aux Controller de la liste ListOfDDCs. La liste ListOfSIDs (ID de sécurité) identifie les Controller de confiance. Les VDA tenteront de s'enregistrer uniquement avec les Controller de confiance.

Dans la plupart des environnements, la liste ListOfSIDs est générée automatiquement à partir de la liste ListOfDDCs. Vous pouvez utiliser une trace CDF pour lire la ListOfSIDs.

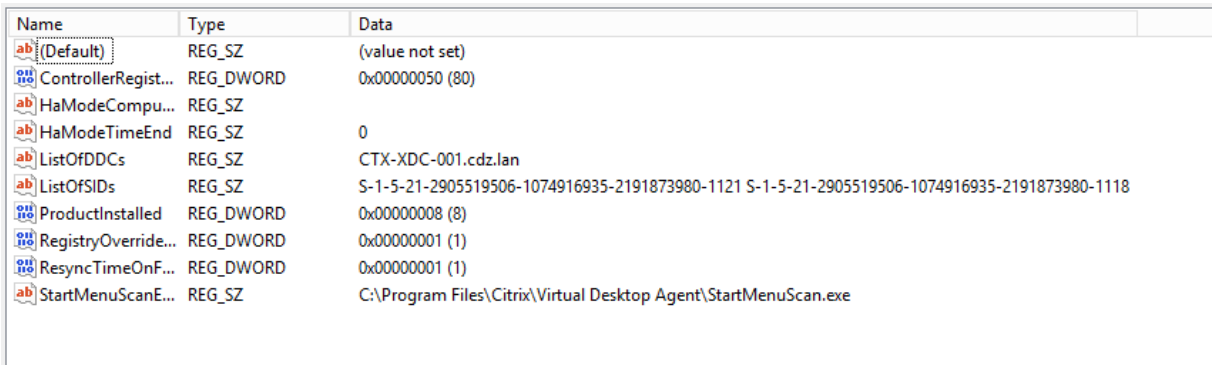
En général, il n'est pas nécessaire de modifier manuellement la ListOfSIDs. Il existe toutefois des exceptions. Les deux premières exceptions ne sont plus valides, car des technologies plus récentes sont disponibles.

- **Séparer les rôles pour les Controller :** avant que les zones soient introduites dans XenApp et XenDesktop 7.7, la ListOfSIDs était configurée manuellement lorsqu'un sous-ensemble de Controller était utilisé pour l'enregistrement. Par exemple, si vous utilisiez XDC-001 et XDC-002 en tant que brokers XML, et XDC-003 et XDC-004 pour l'enregistrement de VDA, vous deviez spécifier tous les Controller dans la ListOfSIDs et XDC-003 et XDC-004 dans la liste ListOfDDCs. Cela n'est pas une configuration type ou recommandée et ne doit pas être utilisée dans les environnements plus récents. Utilisez plutôt les zones.
- **Réduction de la charge d'Active Directory :** avant que la fonctionnalité de mise à jour automatique ait été introduite dans XenApp et XenDesktop 7.6, la ListOfSIDs était utilisée pour réduire la charge sur les contrôleurs de domaine. La résolution de noms DNS vers des SID pouvait être ignorée en prédéfinissant la liste ListOfSIDs. Toutefois, la fonctionnalité de mise à jour automatique supprime le besoin d'effectuer cette opération, car ce cache permanent contient les SID. Citrix recommande de toujours activer la fonctionnalité de mise à jour automatique.
- **Sécurité :** dans certains environnements hautement sécurisés, les SID de Controller de confiance étaient configurés manuellement pour éviter les menaces de sécurité depuis un serveur DNS non fiable. Toutefois, si vous utilisez ce processus, vous devez également désactiver la fonctionnalité de mise à jour automatique ; sinon, la configuration du cache permanent est utilisée.

Donc, à moins que vous ayez une bonne raison, ne modifiez pas la ListOfSIDs.

Si vous devez modifier la liste ListOfSIDs, créez une clé de Registre appelée ListOfSIDs (REG_SZ) sous HKLM\Software\Citrix\VirtualDesktopAgent. La valeur est une liste de SID de confiance, séparée par des espaces, s'il y en a plusieurs.

Dans l'exemple suivant, un Controller est utilisé pour l'enregistrement de VDA (ListOfDDCs), mais deux Controller sont utilisés pour la négociation des connexions (liste OfSIDs).



Name	Type	Data
(Default)	REG_SZ	(value not set)
ControllerRegist...	REG_DWORD	0x00000050 (80)
HaModeCompu...	REG_SZ	
HaModeTimeEnd	REG_SZ	0
ListOfDDCs	REG_SZ	CTX-XDC-001.cdz.lan
ListOfSIDs	REG_SZ	S-1-5-21-2905519506-1074916935-2191873980-1121 S-1-5-21-2905519506-1074916935-2191873980-1118
ProductInstalled	REG_DWORD	0x00000008 (8)
RegistryOverride...	REG_DWORD	0x00000001 (1)
ResyncTimeOnF...	REG_DWORD	0x00000001 (1)
StartMenuScanE...	REG_SZ	C:\Program Files\Citrix\Virtual Desktop Agent\StartMenuScan.exe

Résoudre les problèmes d'enregistrement de VDA

Comme indiqué précédemment, un VDA doit être enregistré auprès d'un Delivery Controller pour être pris en compte lors du lancement de sessions négociées. Des VDA non enregistrés peuvent entraîner une sous-utilisation des ressources disponibles. Il existe un certain nombre de raisons pour lesquelles

un VDA peut ne pas être enregistré, un grand nombre d'entre elles pouvant être résolues par un administrateur. Studio offre des informations de dépannage dans l'Assistant de création de catalogue de machines, et après la création d'un groupe de mise à disposition.

Identification de problèmes lors de la création de catalogue de machines :

Dans l'assistant Créer un catalogue de machines, lorsque vous ajoutez des machines existantes, la liste des noms de compte d'ordinateur indique si chaque machine peut être ajoutée au catalogue. Placez le pointeur de la souris sur l'icône située en regard de chaque machine pour afficher un message informatif sur cette machine.

Si le message identifie une machine problématique, vous pouvez supprimer cette machine (à l'aide du bouton **Supprimer**) ou ajouter la machine. Par exemple, si un message indique qu'il est impossible d'obtenir des informations sur une machine (peut-être parce qu'elle n'a jamais été enregistrée auprès d'un Delivery Controller), vous pouvez quand même choisir d'ajouter la machine.

Le niveau fonctionnel d'un catalogue détermine les fonctionnalités du produit qui sont disponibles pour les machines du catalogue. L'utilisation de fonctionnalités introduites dans les nouvelles versions de produit peut nécessiter un nouveau VDA. Définir un niveau fonctionnel met toutes les fonctionnalités introduites dans cette version (et les versions ultérieures, si le niveau fonctionnel ne change pas) à disposition des machines du catalogue. Toutefois, les machines de ce catalogue avec une version antérieure de VDA ne pourront pas s'enregistrer.

Identification de problèmes après la création de groupes de mise à disposition :

Une fois que vous avez créé un groupe de mise à disposition, Studio affiche davantage de détails sur les machines associées à ce groupe. Le panneau de détails pour un groupe de mise à disposition indique le nombre de machines qui devraient être enregistrées, mais ne le sont pas. En d'autres termes, une ou plusieurs machines peuvent être sous tension et pas en mode de maintenance, mais pas enregistrées auprès d'un Controller. Lors de l'affichage d'une machine « non enregistrée », mais qui devrait l'être, consultez l'onglet Dépannage dans le panneau Détails pour connaître les causes possibles et les actions correctives recommandées.

Pour de plus amples informations sur les niveaux fonctionnels, consultez la section *Versions VDA et niveaux fonctionnels* de la section Créer des catalogues de machines.

Pour plus d'informations sur le dépannage de l'enregistrement de VDA, voir l'article CTX136668.

Vous pouvez également utiliser l'Assistant d'intégrité Citrix pour résoudre les problèmes d'enregistrement de VDA et de lancement de session. Pour plus d'informations, veuillez consulter l'article CTX207624.

Sessions

February 28, 2019

La gestion de l'activité de session est critique pour offrir la meilleure expérience utilisateur possible. La perte de connectivité due à des réseaux non fiables, à des durées de latence réseau extrêmement variables ou à des limitations en termes de portée des appareils sans fil, peuvent faire naître une certaine frustration chez les utilisateurs. La possibilité de se déplacer entre plusieurs stations de travail rapidement, d'accéder aux mêmes applications chaque fois qu'ils ouvrent une session, est une priorité pour la plupart des travailleurs mobiles, tels que le personnel médical d'un hôpital.

Utilisez les fonctionnalités suivantes pour optimiser la fiabilité des sessions, réduire les désagréments, les temps d'arrêt et la perte de productivité ; à l'aide de ces fonctionnalités, les utilisateurs mobiles peuvent passer rapidement et facilement d'un périphérique à un autre.

La section Intervalle d'ouverture de session décrit comment modifier le paramètre par défaut.

Vous pouvez également fermer la session d'un utilisateur, déconnecter une session et configurer le pré-lancement et la persistance de session ; consultez l'article Gérer les groupes de mise à disposition.

Fiabilité de session

La fiabilité de session maintient les sessions actives et visibles sur l'écran de l'utilisateur lorsque la connexion au réseau est interrompue. L'utilisateur peut donc visualiser l'application jusqu'à ce que la connexion au réseau reprenne.

Cette fonction est particulièrement utile pour les utilisateurs mobiles utilisant des connexions sans fil. Par exemple, lorsqu'un utilisateur connecté via une connexion sans fil entre dans un tunnel ferroviaire, la connexion est momentanément interrompue. D'ordinaire, la session se déconnecte et disparaît de l'écran de l'utilisateur ; ce dernier est alors contraint de se reconnecter à la session déconnectée. Grâce à la fiabilité de session, la session reste active sur la machine. Pour indiquer que la connexion est interrompue, l'affichage fourni à l'utilisateur est figé et le curseur prend la forme d'un sablier jusqu'à ce que la connexion soit rétablie de l'autre côté du tunnel. L'utilisateur a toujours accès à l'affichage de l'application durant l'interruption et peut reprendre l'interaction avec l'application lorsque la connexion réseau est rétablie. La fonction de fiabilité de session permet aux utilisateurs de se reconnecter sans avoir à s'authentifier de nouveau.

Les utilisateurs de Citrix Receiver ne peuvent pas remplacer le paramètre du Controller.

Vous pouvez utiliser la fonction de fiabilité de session avec le protocole TLS (Transport Layer Security). TLS crypte uniquement les données envoyées entre la machine utilisateur et NetScaler Gateway.

Activez et configurez la fonction de fiabilité de session avec les paramètres de stratégie suivants :

- Le paramètre de stratégie Connexions de fiabilité de session autorise ou interdit la fiabilité de session.
- Le paramètre de stratégie Expiration de délai de la fiabilité de session est réglé par défaut sur 180 secondes, ou trois minutes. Même si vous pouvez étendre la durée pendant laquelle la fonction de fiabilité de session maintient une session ouverte, cette fonctionnalité est conçue pour

aider l'utilisateur et par conséquent ne pas demander à l'utilisateur de devoir s'authentifier à nouveau. Si vous augmentez la durée pour laquelle une session est gardée ouverte, les risques d'accès non autorisé sont accrus : un utilisateur distrait peut s'éloigner de sa machine cliente et il est alors possible que des utilisateurs non autorisés accèdent à sa session.

- Les connexions entrantes de fiabilité de session utilisent le port 2598, à moins que vous ne changiez le numéro de port défini dans le paramètre de stratégie Numéro de port de la fiabilité de session.
- Si vous ne souhaitez pas autoriser les utilisateurs à se reconnecter aux sessions interrompues sans authentification, utilisez la fonction de reconnexion automatique des clients. Vous pouvez configurer le paramètre de stratégie Authentification de la reconnexion automatique des clients pour inviter les utilisateurs à s'authentifier à nouveau lors de la reconnexion aux sessions interrompues.

Si vous utilisez la fonction de fiabilité de session et la fonction de reconnexion automatique des clients, ces fonctions agissent l'une après l'autre. La fonction de fiabilité de session ferme (ou déconnecte) la session utilisateur après la période spécifiée dans le paramètre de stratégie Expiration de délai de la fiabilité de session. Ensuite, les paramètres définis pour la fonction de reconnexion automatique des clients s'appliquent et la fonction tente d'opérer la reconnexion de l'utilisateur à la session déconnectée.

Reconnexion automatique des clients

Avec la fonction Reconnexion automatique des clients, Citrix Receiver peut détecter les déconnexions de session ICA involontaires et reconnecter automatiquement les utilisateurs à leurs sessions. Lorsque cette fonctionnalité est activée sur le serveur, les utilisateurs n'ont pas besoin de se reconnecter manuellement pour continuer à travailler.

Pour les sessions d'application, Citrix Receiver essaie de se reconnecter à la session jusqu'à ce que la reconnexion réussisse ou que l'utilisateur annule la tentative de reconnexion.

Pour les sessions de bureau, Citrix Receiver tente de se reconnecter à la session pendant une période de temps spécifiée, à moins que la reconnexion réussisse ou que l'utilisateur annule la tentative de reconnexion. Par défaut, cette durée est de cinq minutes. Pour modifier cette durée, modifiez le registre sur la machine utilisateur :

HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds; DWORD;<secondes>

où <*secondes*> est le nombre de secondes après lesquelles plus aucune tentative n'est faite pour reconnecter la session.

Activez et configurez la fonction de reconnexion automatique des clients avec les paramètres de stratégie suivants :

- **Reconnexion automatique des clients**. Active ou désactive la reconnexion automatique par Citrix Receiver après l'interruption d'une connexion.
- **Authentification de la reconnexion automatique des clients**. Active ou désactive l'authentification utilisateur après reconnexion automatique.
- **Journalisation de la reconnexion automatique des clients**. Active ou désactive la journalisation des événements de reconnexion dans le journal d'événements. Par défaut, la journalisation est désactivée. Lorsqu'il est activé, le Journal système du ou des serveurs reçoit les informations relatives aux échecs et aux succès des tentatives de reconnexion automatique. Chaque serveur stocke des informations sur les événements de reconnexion dans son propre Journal système ; le site ne fournit pas de journal combinant les événements de reconnexion de tous les serveurs.

La fonction de reconnexion automatique des clients intègre un mécanisme permettant une authentification basée sur les informations d'identification cryptées de l'utilisateur. Lorsqu'un utilisateur ouvre une session sur un site, le serveur crypte ses informations d'identification, les stocke en mémoire, puis envoie un cookie contenant la clé de cryptage à Citrix Receiver. Citrix Receiver transmet la clé au serveur pour reconnexion. Celui-ci décrypte les informations d'identification et les transmet au système d'ouverture de session Windows pour authentification. Lorsqu'un cookie expire, l'utilisateur doit à nouveau fournir ses informations d'identification pour se reconnecter à sa session.

Si le paramètre Authentification de la reconnexion automatique des clients est sélectionné, aucun cookie n'est utilisé. Au lieu de cela, les utilisateurs voient s'afficher une boîte de dialogue leur demandant de fournir leurs informations d'identification lorsque Citrix Receiver tente de se reconnecter automatiquement.

Pour une protection optimale des informations d'identification et des sessions des utilisateurs, utilisez le cryptage pour toutes les communications entre les clients et le site.

Désactivez la reconnexion automatique des clients sur Citrix Receiver pour Windows en utilisant le fichier icaclient.adm. Pour de plus amples informations, consultez la documentation relative à votre version de Citrix Receiver pour Windows.

Les paramètres des connexions affectent également la fonction de reconnexion automatique des clients.

- Par défaut, la fonction de reconnexion automatique des clients est activée via les paramètres de stratégie au niveau du site, comme décrit ci-dessus. Les utilisateurs n'ont pas besoin de se réauthentifier. Toutefois, si la connexion TCP ICA d'un serveur est configurée pour réinitialiser les sessions dont une liaison de communication a été interrompue, la reconnexion automatique n'a pas lieu. La fonction de reconnexion automatique des clients fonctionne uniquement si le serveur déconnecte les sessions en cas d'interruption ou d'expiration de délai d'une connexion. Dans ce contexte, la connexion TCP ICA fait référence au port virtuel d'un serveur (et non à une connexion réseau) utilisé pour les sessions sur les réseaux TCP/IP.

- Par défaut, la connexion TCP ICA d'un serveur est configurée pour déconnecter les sessions en cas d'interruption ou d'expiration de délai de leurs connexions. Les sessions déconnectées restent intactes dans la mémoire du système et sont disponibles pour la reconnexion par le Citrix Receiver
- La connexion peut être configurée pour réinitialiser ou fermer les sessions dont les connexions sont interrompues ou dont le délai a expiré. Lorsqu'une session est réinitialisée, une tentative de reconnexion lance une nouvelle session. L'utilisateur ne retrouve pas l'application dans l'état où elle était avant la reconnexion ; l'application est relancée.
- Si le serveur est configuré pour réinitialiser les sessions, la fonction de reconnexion automatique des clients crée une nouvelle session. Ce processus nécessite que les utilisateurs fournissent leurs informations d'identification pour ouvrir une session sur le serveur.
- La reconnexion automatique peut échouer si le Citrix Receiver ou le plug-in transmettent des informations d'identification incorrectes, ce qui peut se produire lors d'une attaque, ou si le serveur estime qu'une durée trop longue s'est écoulée depuis qu'il a détecté une connexion interrompue.

Persistance ICA

L'activation de la fonctionnalité de persistance ICA empêche la déconnexion des connexions rompues. Lorsqu'elle est activée, si le serveur ne détecte plus aucune activité (par exemple, aucun changement de l'horloge, aucun mouvement de la souris, aucune mise à jour de l'écran), cette fonctionnalité empêche les services Bureau à distance de se déconnecter de cette session. Le serveur envoie des paquets de persistance à quelques secondes d'intervalle pour détecter si la session est active. Si la session n'est plus active, le serveur marque la session en tant que déconnectée.

> **Remarque :**
>
> Cependant, la persistance ICA fonctionne uniquement si vous n'utilisez pas la fiabilité de session. La fiabilité de session dispose de ses propres mécanismes pour empêcher les connexions interrompues d'être déconnectées. Ne configurez la persistance ICA que pour les connexions qui n'utilisent pas la fiabilité de session.

Les réglages effectués dans la page Persistance ICA ont priorité sur les réglages correspondants configurés dans la Stratégie de groupe Microsoft Windows.

Activez et configurez les paramètres de persistance ICA avec les paramètres de stratégie suivants :

- **Délai d'expiration de persistance ICA**. Spécifie l'intervalle (1-3600 secondes) utilisé pour envoyer des messages de persistance ICA. Ne configurez pas cette option si vous voulez que votre logiciel de contrôle de réseau ferme les connexions inactives dans les environnements pour lesquels les interruptions de connexion sont si peu fréquentes que la reconnexion des utilisateurs aux sessions n'est pas un problème.

L'intervalle par défaut est de 60 secondes : les paquets de persistance ICA sont envoyés aux machines utilisateur toutes les 60 secondes. Si une machine utilisateur ne répond pas après 60 secondes, l'état des sessions ICA correspondantes passe à Déconnectée.

- **Persistances ICA**. Envoie ou empêche l'envoi de messages de persistance ICA.

Le contrôle de l'espace de travail

Le contrôle de l'espace de travail permet aux bureaux et aux applications de suivre un utilisateur d'un appareil à un autre. Cette itinérance permet à un utilisateur d'accéder à tous les bureaux ou d'ouvrir des applications à partir de n'importe quel emplacement simplement en ouvrant une session, sans avoir à redémarrer les bureaux ou applications sur chaque machine. Par exemple, le contrôle de l'espace de travail permet aux employés d'un centre hospitalier de se déconnecter rapidement d'une station de travail pour se reconnecter à une autre et d'accéder aux mêmes applications chaque fois qu'ils ouvrent une session. Si vous configurez le contrôle de l'espace de travail de la sorte, le personnel médical peut se déconnecter de plusieurs applications sur une machine cliente et s'y reconnecter sur une autre machine cliente.

Le contrôle de l'espace de travail affecte les activités suivantes :

- **Ouverture de session :** par défaut, le contrôle de l'espace de travail permet aux utilisateurs de se reconnecter automatiquement à tous les bureaux et applications en cours d'exécution lors de l'ouverture de session, sans avoir à les rouvrir manuellement. Via le contrôle de l'espace de travail, les utilisateurs peuvent ouvrir des bureaux ou applications déconnectés ainsi que des applications ou bureaux qui sont actifs sur une autre machine cliente. La déconnexion d'une application ou d'un bureau n'interrompt pas son exécution sur le serveur. Si des utilisateurs itinérants doivent maintenir la connexion avec certaines applications ou certains bureaux sur une machine cliente tandis qu'ils se reconnectent à d'autres applications ou bureaux sur une autre machine cliente, vous pouvez configurer le comportement de reconnexion de façon à n'ouvrir que les applications ou bureaux dont ils se sont déconnectés.
- **Reconnexion :** après avoir ouvert une session sur le serveur, les utilisateurs peuvent se reconnecter à tous leurs bureaux ou applications à tout moment en cliquant sur le bouton Se reconnecter. Par défaut, cette option ouvre les applications et bureaux qui sont déconnectés ainsi que ceux actuellement exécutés sur une autre machine cliente. Vous pouvez configurer cette option de façon à ce qu'elle n'ouvre que les applications ou bureaux précédemment déconnectés par l'utilisateur.
- **Fermeture de session :** pour les utilisateurs ouvrant des bureaux ou applications via StoreFront, vous pouvez configurer la commande Fermer la session afin de fermer la session utilisateur de StoreFront ainsi que toutes les sessions actives ou uniquement la session de StoreFront.
- **Déconnexion :** les utilisateurs peuvent se déconnecter simultanément de toutes les applications et tous les bureaux en cours d'exécution sans avoir à déconnecter chaque application ou

bureau individuellement.

Le contrôle de l'espace de travail est disponible uniquement pour les utilisateurs Citrix Receiver pour accéder aux bureaux et applications via une connexion Citrix StoreFront. Par défaut, le contrôle de l'espace de travail est désactivé pour les sessions de bureau virtuel, mais activé pour les applications hébergées. Le partage de session ne se produit pas par défaut entre les bureaux publiés et toute application publiée exécutée au sein de ces bureaux.

Lorsqu'un utilisateur passe à une nouvelle machine cliente, les stratégies utilisateur, les mappages des lecteurs clients et la configuration des imprimantes changent en conséquence. Les stratégies et les mappages sont appliqués en fonction de la machine cliente à partir de laquelle l'utilisateur a ouvert la session. Par exemple, si l'employé d'un centre hospitalier ferme la session qu'il a ouverte sur une machine cliente dans la salle des urgences et en ouvre une autre sur une machine dans le Service de radiologie, les stratégies, les mappages d'imprimante et de lecteur client correspondant à la machine cliente du Service de radiologie sont appliqués à l'ouverture de session sur cette machine.

Vous pouvez personnaliser les imprimantes qui s'affichent pour les utilisateurs lorsqu'ils changent d'emplacement. Vous pouvez également contrôler si les utilisateurs peuvent imprimer sur des imprimantes locales, la quantité de bande passante consommée lorsque les utilisateurs se connectent à distance, ainsi que d'autres aspects de leur expérience d'impression.

Pour plus d'informations sur l'activation et la configuration du contrôle de l'espace de travail pour les utilisateurs, consultez la documentation StoreFront.

Itinérance de session

Par défaut, les sessions sont partagées entre les machines clientes de l'utilisateur. Lorsque l'utilisateur ouvre une session et bascule sur une autre machine, la même session est utilisée et les applications sont disponibles sur les deux machines. Les applications suivent, quelle que soit la machine ou que les sessions en cours existent ou non. Dans la plupart des cas, les imprimantes et les autres ressources attribuées à l'application suivent également.

Bien que ce comportement par défaut offre de nombreux avantages, il n'est pas toujours idéal. Vous pouvez désactiver l'itinérance de session à l'aide du SDK du PowerShell.

Exemple 1 : un professionnel de la santé utilise deux machines ; il remplit un formulaire d'assurance sur un PC de bureau et recherche des informations sur le patient sur une tablette.

- Si l'itinérance de session est activée, les applications s'affichent toutes les deux sur les deux machines (une application lancée sur une machine est visible sur toutes les machines en cours d'utilisation). Ce comportement peut ne pas répondre aux exigences de sécurité.
- Si l'itinérance de session est désactivée, le dossier du patient ne s'affiche pas sur le PC de bureau et le formulaire d'assurance ne s'affiche pas sur la tablette.

Exemple 2 : un chef de production lance une application sur le PC de son bureau. Le nom et l'emplacement de la machine déterminent les imprimantes et autres ressources qui sont disponibles pour cette session. Plus tard dans la journée, il se rend dans un bureau situé dans un autre bâtiment pour une réunion pour laquelle il devra utiliser une imprimante.

- Si l'itinérance de session est activée, le chef de production ne peut probablement pas accéder aux imprimantes à proximité de la salle de réunion, car les applications qu'il a démarrées plus tôt dans son bureau ont entraîné l'attribution d'imprimantes et d'autres ressources situées près de cet emplacement.
- Si l'itinérance de session est désactivée, lorsqu'il ouvre une session sur une autre machine (en utilisant les mêmes informations d'identification), une nouvelle session est démarrée et les imprimantes et ressources à proximité sont disponibles.

Configurer l'itinérance de session

Pour configurer l'itinérance de session, utilisez les applets de commande de règle de stratégie d'admissibilité suivantes avec la propriété « SessionReconnection ». Si vous le souhaitez, vous pouvez également spécifier la propriété « LeasingBehavior » ; consultez la section Location de connexion et itinérance de session ci-dessous.

Pour les sessions de bureau :

Set-BrokerEntitlementPolicyRule <*nom_groupe_mise_à_disposition*> -SessionReconnection <*valeur*> -LeasingBehavior Allowed | Disallowed

Pour les sessions d'application :

Set-BrokerAppEntitlementPolicyRule <*nom_groupe_mise_à_disposition*> -SessionReconnection <*valeur*> -LeasingBehavior Allowed | Disallowed

Où <*valeur*> peut être l'un des paramètres suivants :

- **Always**. Les sessions sont toujours itinérantes, quelle que soit la machine cliente et que la session soit connectée ou déconnectée. Il s'agit de la valeur par défaut.
- **DisconnectedOnly**. Se reconnecte uniquement aux sessions déconnectées ; sinon, démarre une nouvelle session (vous pouvez activer l'itinérance de session entre les machines clientes en les déconnectant, ou en utilisant le contrôle de l'espace de travail pour activer explicitement l'itinérance). Une session connectée active sur une autre machine cliente n'est jamais utilisée ; une nouvelle session est lancée.
- **SameEndpointOnly**. Un utilisateur obtient une session unique pour chaque machine cliente qu'il utilise. L'itinérance est complètement désactivée. Les utilisateurs peuvent se reconnecter uniquement à la machine qui a été utilisée précédemment pour la session.

La propriété « LeasingBehavior » est décrite ci-dessous.

Effets d'autres paramètres

La désactivation de l'itinérance de session est affectée par la limite d'application « Autoriser une seule instance par utilisateur » définie dans les propriétés de l'application dans le groupe de mise à disposition.

- Si vous désactivez l'itinérance de session, désactivez la limite d'application « Autoriser une seule instance par utilisateur ».
- Si vous activez la limite d'application « Autoriser une seule instance par utilisateur », ne configurez pas les deux valeurs qui permettent de nouvelles sessions sur de nouvelles machines.

Location de connexion et itinérance de session

Si vous ne connaissez pas bien la location de connexion, consultez l'article Location de connexions.

Lorsqu'un Controller entre en mode de location de connexions, la reconnexion de session revient à sa valeur par défaut, reconnectant l'utilisateur à une seule des sessions actives ou déconnectées pour le bureau ou l'application.

Pour une sécurité accrue, si vous avez configuré une valeur autre que celle par défaut pour l'itinérance de session et que vous disposez de plusieurs utilisateurs partageant les mêmes informations d'identification d'ouverture de session sur plusieurs machines, il est recommandé de désactiver la fonctionnalité de location de connexion pour le groupe de mise à disposition qui comprend ce compte d'utilisateur.

Pourquoi ? Dans ce scénario, une session est partagée entre toutes les machines. Cette situation n'est pas idéale si, par exemple, une personne affiche des informations confidentielles qui ne sont pas destinées à être consultées par un autre utilisateur lorsque celui-ci se reconnecte avec les mêmes informations d'identification et que le Controller se trouve en mode de location de connexion.

La désactivation de la location de connexion dans la stratégie d'admissibilité élimine ce risque : un utilisateur ne sera pas en mesure de consulter la session d'un autre utilisateur avec les mêmes informations d'identification, même lorsque le Controller se trouve en mode de location de connexion. Les autres stratégies d'admissibilité peuvent rester inchangées ; les comptes utilisateur individuels peuvent utiliser la fonctionnalité de location de connexion via des droits distincts.

Pour désactiver la location de connexion dans une stratégie d'admissibilité, ajoutez la propriété « LeasingBehavior Disallowed » à l'applet de commande de la stratégie d'admissibilité. Si vous désactivez la location de connexion, vous devez supprimer manuellement toute location de lancement qui a déjà été créée et mise en cache pour cette stratégie d'admissibilité ; sinon, les utilisateurs seront toujours en mesure de se reconnecter au cours d'une panne de base de données.

Intervalle d'ouverture de session

Si une machine virtuelle contenant un VDA de bureau se ferme avant la fin du processus d'ouverture de session, vous pouvez attribuer plus de temps au processus. La valeur par défaut pour 7.6 et versions ultérieures est de 180 secondes (la valeur par défaut pour 7.0-7.5 est de 90 secondes).

Sur la machine (ou l'image principale utilisée dans un catalogue de machines), définissez la clé de registre suivante :

Clé : HKLM\SOFTWARE\Citrix\PortICA

Valeur : AutoLogonTimeout

Type : DWORD

Spécifiez une durée en secondes, au format décimal, dans la plage 0-3600.

Si vous modifiez une image principale, mettez à jour le catalogue.

> **Remarque :**
>
> Ce paramètre s'applique uniquement aux machines virtuelles avec VDA de bureau (station de travail) ; Microsoft contrôle le délai d'expiration de l'ouverture de session sur les machines avec VDA de serveur.

Utiliser la fonction de recherche dans Studio

February 28, 2019

Utilisez la fonction de recherche pour afficher des informations sur des machines spécifiques, des sessions, des catalogues de machines, des applications ou des groupes de mise à disposition.

1. Sélectionnez Rechercher dans le volet de navigation de Studio.

   Remarque : vous ne pouvez pas effectuer des recherches dans les catalogues de machines ou les onglets Groupes de mise à disposition à l'aide de la zone Rechercher. Utiliser le nœud Rechercher dans le volet de navigation.

   Pour afficher des critères de recherche supplémentaires, cliquez sur le signe plus en regard des champs déroulants de recherche. Supprimer des critères de recherche en cliquant sur le bouton moins.

2. Entrez le nom ou utilisez la liste déroulante pour sélectionner une autre option de recherche pour l'élément que vous souhaitez rechercher.

3. Si vous le souhaitez, vous pouvez enregistrer votre recherche en cliquant sur Enregistrer sous. La recherche s'affiche dans la liste des recherches enregistrées.

Vous pouvez également cliquer sur l'icône Développer la recherche (crochets pointus double) pour afficher une liste déroulante des propriétés de recherche ; vous pouvez effectuer une recherche avancée en créant une expression à partir des propriétés de la liste déroulante.

Conseils pour améliorer la recherche :

- Pour afficher des caractéristiques supplémentaires à inclure dans l'affichage sur lequel vous pouvez rechercher et trier, cliquez avec le bouton droit de la souris sur une colonne et cliquez sur Sélectionner les colonnes.
- Pour localiser une machine utilisateur connectée à une machine, utilisez le client (IP) et Est, puis entrez l'adresse IP de la machine.
- Pour localiser les sessions actives, utilisez État de session, Est et Connecté.
- Pour répertorier toutes les machines d'un groupe de mise à disposition, sélectionnez Groupes de mise à disposition dans le panneau de navigation, sélectionnez le groupe, puis sélectionnez Afficher les machines dans le volet Actions.

Balises

February 28, 2019

Introduction

Les balises sont des chaînes qui identifient les éléments tels que les machines, les applications, les bureaux, les groupes de mise à disposition, les groupes d'applications et les stratégies. Après la création d'une balise, puis son ajout à un élément, vous pouvez configurer certaines opérations pour qu'elles s'appliquent uniquement aux éléments avec une balise spécifique.

- La recherche personnalisée s'affiche dans Studio.

Par exemple, pour afficher uniquement les applications qui ont été optimisées pour les testeurs, créez une balise appelée « test », puis ajoutez (appliquez) cette balise à ces applications. Vous pouvez maintenant filtrer la recherche Studio avec la balise « test ».

- Publiez des applications à partir d'un groupe d'applications ou des bureaux spécifiques à partir d'un groupe de mise à disposition, prenant en compte un seul sous-ensemble de machines dans les groupes de mise à disposition sélectionnés. C'est ce qu'on appelle une *restriction de balise*.

Avec les restrictions de balise, vous pouvez utiliser des machines existantes pour plusieurs tâches de publication, éliminant ainsi les coûts associés avec le déploiement et la gestion de machines supplémentaires. L'utilisation d'une restriction de balise équivaut à diviser (ou partitionner) des machines dans un groupe de mise à disposition. Cette fonctionnalité est semblable, mais pas identique, aux groupes de travail dans les versions de XenApp antérieures à 7.x.

L'utilisation d'un groupe d'applications ou de bureaux avec une restriction de balise peut s'avérer utile pour isoler et dépanner un sous-ensemble de machines dans un groupe de mise à disposition.

Consultez la section ci-dessous pour plus de détails et des exemples sur l'utilisation d'une restriction de balise.

- Programmez des redémarrages périodiques pour un sous-ensemble de machines dans un groupe de mise à disposition.

L'utilisation d'une restriction de balise pour les machines vous permet d'utiliser de nouvelles applets de commande PowerShell pour configurer plusieurs programmes de redémarrage pour des sous-ensembles de machines dans un groupe de mise à disposition. Pour des exemples et des détails, voir la section « Créer plusieurs programmes de redémarrage pour les machines d'un groupe de mise à disposition » dans l'article Gérer les groupes de mise à disposition.

- Personnalisez l'application (affectation) de stratégies Citrix à un sous-ensemble de machines dans des groupes de mise à disposition, des types de groupe de mise à disposition ou des unités d'organisation qui ont (ou n'ont pas) une balise spécifique.

Par exemple, si vous souhaitez appliquer une stratégie Citrix uniquement aux stations de travail les plus puissantes, ajoutez une balise nommée « haute puissance » à ces machines. Ensuite, sur la page **Attribuer la stratégie** de l'assistant Créer une stratégie, sélectionnez cette balise ainsi que la case à cocher **Activer**. Vous pouvez également ajouter une balise à un groupe de mise à disposition, puis appliquer une stratégie Citrix à ce groupe. Pour de plus amples informations, consultez l'article Créer des stratégies et ce billet de blog. (Notez que l'interface de Studio pour ajouter une balise à une machine a été modifiée depuis que le billet de blog a été publié).

Vous pouvez appliquer des balises aux éléments suivants :

- Machines
- Applications
- Groupes de mise à disposition
- Groupes d'applications

Une restriction de balise peut être configurée lors de la création ou de la modification des éléments suivants dans Studio :

- Un bureau d'un groupe de mise à disposition partagé
- Un groupe d'applications

Restrictions de balise pour un bureau ou un groupe d'applications

Une restriction de balise implique plusieurs étapes :

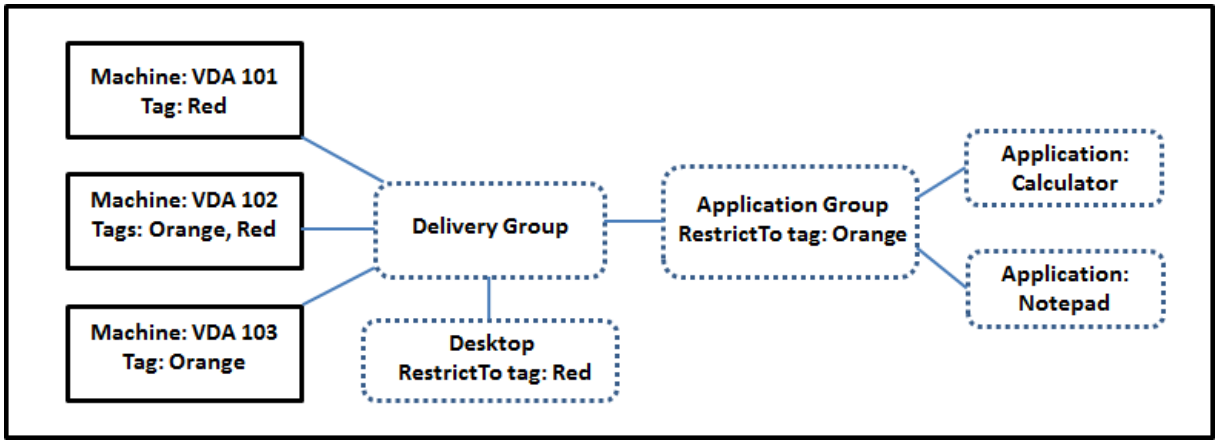
- Créer une balise, puis l'ajouter (appliquer) sur les machines.

- Créer ou modifier un groupe avec la restriction de balise (en d'autres termes, « restreindre les démarrages aux machines avec la balise x »).

Une restriction de balise étend le processus de sélection de machine du broker. Le broker sélectionne une machine dans un groupe de mise à disposition associé en fonction de la stratégie d'accès, des listes d'utilisateurs configurées, de la préférence de zone et de la disponibilité, ainsi que de la restriction de balise (le cas échéant). Pour les applications, le broker retourne sur d'autres groupes de mise à disposition dans l'ordre de priorité, appliquant les mêmes règles de sélection de machine pour chaque groupe de mise à disposition pris en compte.

Exemple 1

Cet exemple présente une configuration simple qui utilise des restrictions de balise pour limiter les machines qui seront prises en compte pour certains lancements de bureau et d'application. Le site dispose d'un groupe de mise à disposition partagé, d'un bureau publié et d'un groupe d'applications configuré avec deux applications.



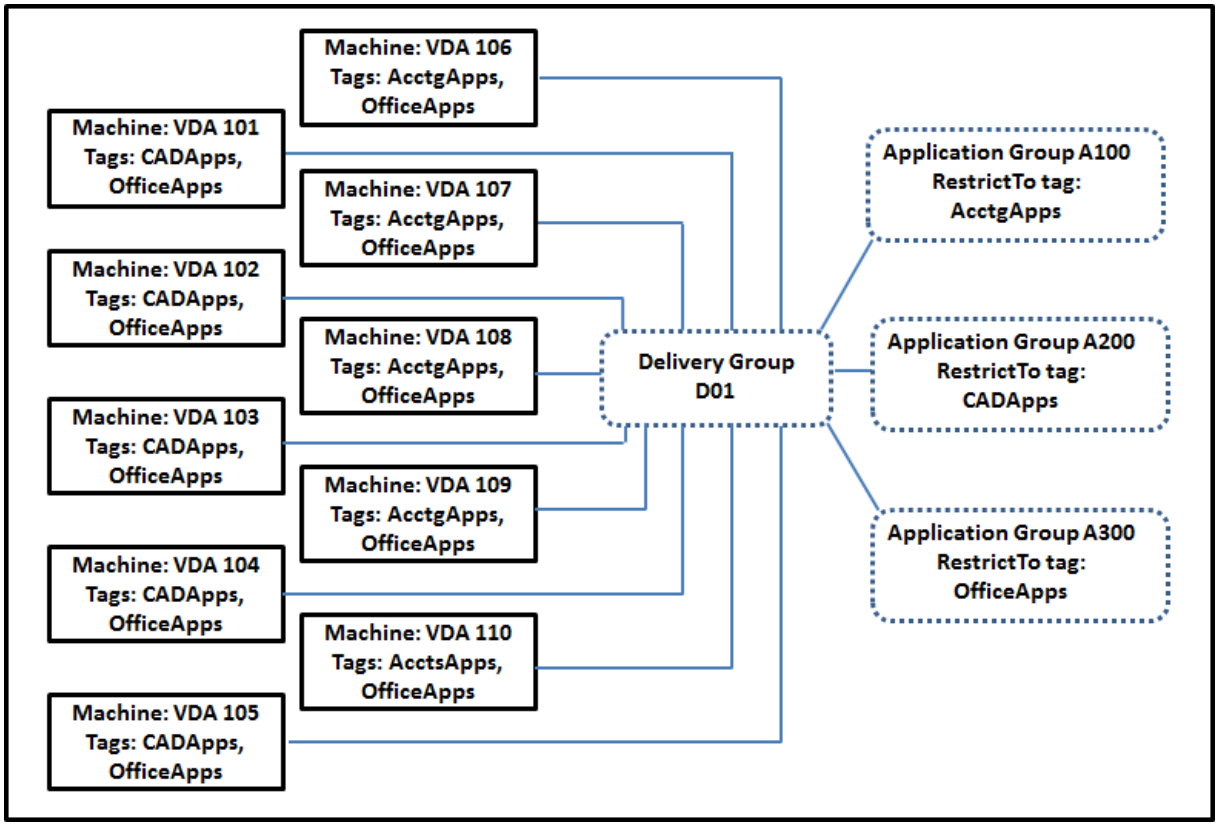
- Des balises ont été ajoutées à chacune des trois machines (VDA 101-103).
- Le bureau dans le groupe de mise à disposition partagé a été créé avec une restriction de balise appelée « Red », de façon à ce que le bureau puisse être démarré uniquement sur les machines de ce groupe de mise à disposition qui ont la balise « Red » : VDA 101 et 102.
- Le groupe d'applications a été créé avec la restriction de balise « Orange », de sorte que chacune de ses applications (calculatrice et Bloc-notes) puisse être lancée uniquement sur les machines de ce groupe de mise à disposition qui ont la balise « Orange » : VDA 102 et 103.

Veuillez noter que la machine VDA 102 a les deux balises (Rouge, Orange), elle sera donc prise en compte pour démarrer les applications et le bureau.

Exemple 2

Cet exemple contient plusieurs groupes d'applications qui ont été créés avec restrictions de balise. Cela permet de mettre à disposition un plus grand nombre d'applications avec moins de machines que nécessaire si uniquement des groupes de mise à disposition sont utilisés.

(La section « Comment configurer l'exemple 2 » présente les étapes utilisées pour créer et appliquer les balises, puis configurer les restrictions de balise dans cet exemple).



Cet exemple utilise dix machines (VDA 101 à 110), un groupe de mise à disposition (D01) et trois groupes d'applications (A100, A200, A300). Si vous appliquez des balises à chaque machine, puis spécifiez des restrictions de balise lors de la création de chaque groupe d'applications :

- Les utilisateurs du service Comptabilité (Acctg) du groupe peuvent accéder aux applications dont ils ont besoin sur cinq machines (VDA 101 à 105)
- Les concepteurs CAD du groupe peuvent accéder aux applications dont ils ont besoin sur cinq machines (VDA 106 à 110)
- Les utilisateurs du groupe qui ont besoin d'applications Office peuvent accéder aux applications Office sur dix machines (VDA 101 à 110)

Seules 10 machines sont utilisées, avec un seul groupe de mise à disposition. L'utilisation de groupes de mise à disposition uniquement (sans groupes d'applications) nécessiterait deux fois plus de machines, car une machine peut appartenir à un seul groupe de mise à disposition.

Gérer les balises et restrictions de balise

Les balises sont créées, ajoutées (appliquées), modifiées et supprimées des éléments sélectionnés via l'action **Gérer les balises** dans Studio.

Exception : les balises utilisées pour les attributions de stratégie sont créées, modifiées et supprimées via l'action **Gérer les balises** dans Studio ; toutefois, les balises sont appliquées (attribuées) lorsque vous créez la stratégie ; voir Créer des stratégies pour plus de détails.

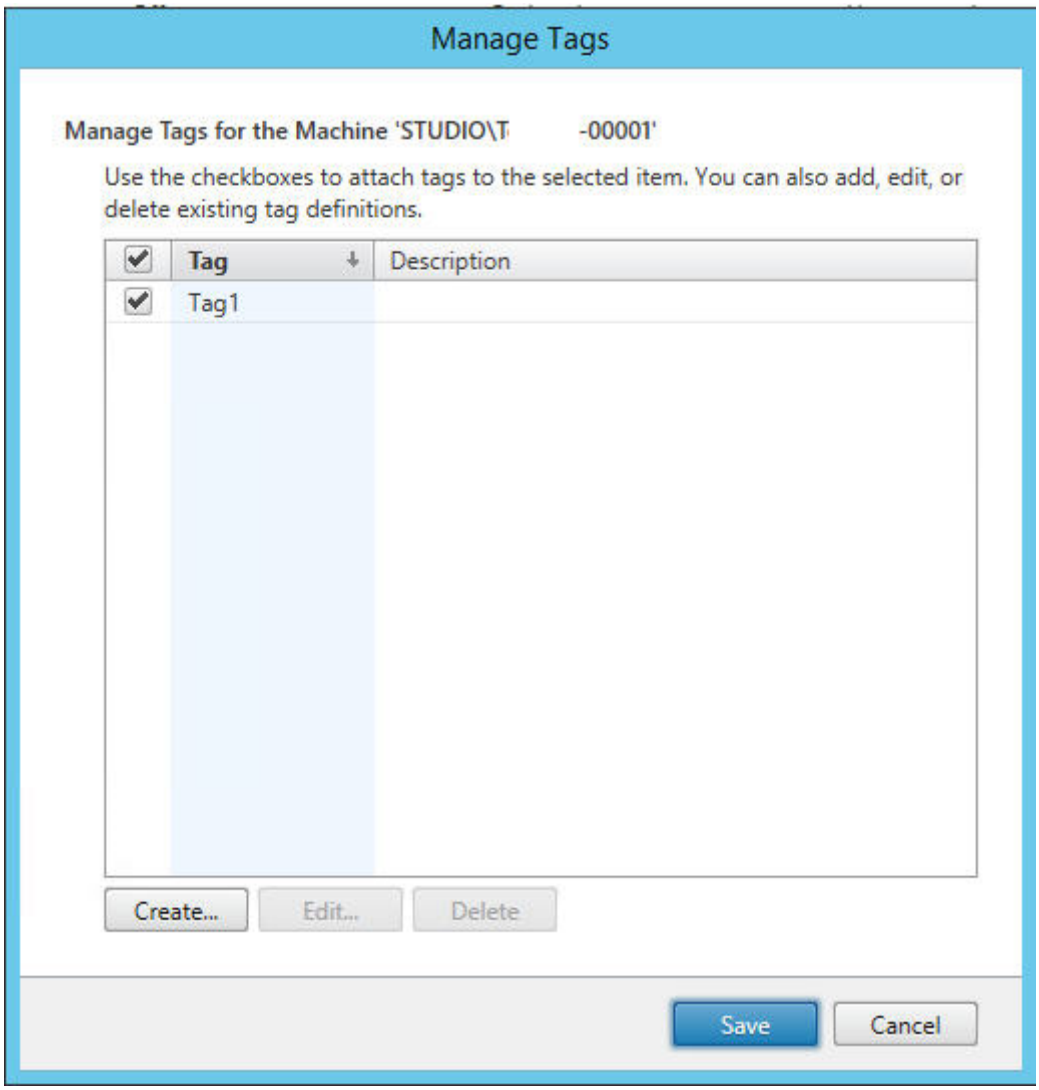
Les restrictions de balise sont configurées lorsque vous créez ou modifiez des bureaux dans des groupes de mise à disposition, et lorsque vous créez et modifiez des groupes d'applications. Pour de plus amples informations sur la création et la modification de groupes, consultez les articles suivants :

- Créer des groupes de mise à disposition
- Gérer les groupes de mise à disposition
- Créer des groupes d'applications
- Gérer des groupes d'applications

Utiliser la boîte de dialogue Gérer les balises dans Studio

Dans Studio, sélectionnez les éléments auxquels vous souhaitez appliquer une balise (une ou plusieurs machines, applications, un bureau, un groupe de mise à disposition ou un groupe d'applications), puis sélectionnez **Gérer les balises** dans le volet Actions. La boîte de dialogue Gérer les balises répertorie toutes les balises qui ont été créées dans le site, et pas seulement pour les éléments sélectionnés.

- Une case à cocher sélectionnée indique que la balise a déjà été ajoutée aux éléments sélectionnés. (Dans la capture d'écran ci-dessous, la balise appelée « Tag1 » est appliquée à la machine sélectionnée.)
- Si vous avez sélectionné plusieurs éléments, une case à cocher contenant un trait indique que certains, mais pas tous les éléments sélectionnés, ont une balise.



Les options suivantes sont disponibles dans la boîte de dialogue Gérer les balises : Veillez à consulter la section Précautions.

Pour créer une balise :

Cliquez sur **Créer**. Entrez un nom et une description. Les noms de balise doivent être uniques et ne sont pas sensibles à la casse. Cliquez ensuite sur **OK**. (La création d'une balise ne l'applique pas automatiquement à tous les éléments que vous avez sélectionnés. Utilisez les cases à cocher pour appliquer la balise).

Pour ajouter (appliquer) une ou plusieurs balises :

Activez la case à cocher en regard du nom de la balise. **Remarque :** si vous sélectionnez plusieurs éléments et que la case à cocher en regard d'une balise contient un trait (pour indiquer que la balise est déjà appliquée à certains, mais pas à tous les éléments sélectionnés), l'activation de la case affecte toutes les machines sélectionnées.

Si vous essayez d'ajouter une balise à une ou plusieurs machines, et que cette balise est actuellement utilisée comme restriction dans un groupe d'applications, vous êtes averti que cette action rendra ces machines disponibles pour le démarrage. Si c'est votre intention, continuez.

Pour retirer une ou plusieurs balises :

Désactivez la case à cocher en regard du nom de ma balise. **Remarque :** si vous sélectionnez plusieurs éléments et que la case à cocher en regard d'une balise contient un trait (pour indiquer que la balise est déjà appliquée à certains, mais pas à tous les éléments sélectionnés), la désactivation de la case retire la balise de toutes les machines sélectionnées.

Si vous tentez de retirer une balise d'une machine qui utilise cette balise comme restriction, un message d'avertissement s'affiche, indiquant que cela peut affecter les machines qui seront prises en compte pour le démarrage. Si c'est votre intention, continuez.

Pour modifier une balise :

Sélectionnez une balise, puis cliquez sur **Modifier**. Entrez un nouveau nom et/ou une description. Vous pouvez modifier une seule balise à la fois.

Pour supprimer une ou plusieurs balises :

Sélectionnez les balises, puis cliquez sur **Supprimer**. La boîte de dialogue Supprimer les balises indique le nombre d'éléments qui utilisent actuellement les balises sélectionnées (par exemple « 2 »). Cliquez sur un élément pour afficher des informations supplémentaires. Par exemple, le fait de cliquer sur un élément « 2 machines » affiche les noms des deux machines auxquelles cette balise est appliquée. Confirmez que vous souhaitez supprimer les balises.

Vous ne pouvez pas utiliser Studio pour supprimer une balise qui est utilisée comme restriction. Vous devez d'abord modifier le groupe d'applications et retirer la restriction de balise ou sélectionner une autre balise.

Cliquez sur **Enregistrer** lorsque vous avez terminé dans la boîte de dialogue Gérer les balises.

Conseil : pour vérifier si des balises ont été appliquées à une machine :

Sélectionnez **Groupes de mise à disposition** dans le volet de navigation. Sélectionnez un groupe de mise à disposition dans le volet central, puis sélectionnez **Afficher les machines** dans le volet Actions. Sélectionnez une machine dans le volet central, puis sélectionnez l'onglet Balises dans le panneau Détails.

Gérer les restrictions de balise

La configuration d'une restriction de balise est un processus à plusieurs étapes : vous devez d'abord créer la balise et l'ajouter (l'appliquer) aux machines. Ensuite, vous devez ajouter la restriction au groupe d'applications ou au bureau.

Créer et appliquer la balise :

Créez la balise, puis ajoutez-la (appliquez-la) aux machines qui seront affectées par la restriction de balise, à l'aide des actions **Gérer les balises** décrites ci-dessus.

Pour ajouter une restriction de balise à un groupe d'applications :

Créez ou modifiez le groupe d'applications. Sur la page Groupes de mise à disposition, sélectionnez **Restreindre les lancements aux machines dotées de balises** puis sélectionnez la balise dans la liste déroulante.

Pour modifier ou retirer la restriction de balise sur un groupe d'applications :

Modifiez le groupe. Sur la page Groupes de mise à disposition, sélectionnez une autre balise à partir de la liste déroulante ou supprimez la restriction de balise complètement en désactivant le paramètre **Restreindre les lancements aux machines dotées de balises**.

Pour ajouter une restriction de balise à un bureau :

Créez ou modifiez un groupe de mise à disposition. Cliquez sur **Ajouter** ou **Modifier** sur la page Bureaux. Dans la boîte de dialogue Ajouter un bureau, sélectionnez **Restreindre les lancements aux machines dotées de balises** puis sélectionnez la balise dans le menu déroulant.

Pour modifier ou retirer la restriction de balise sur un groupe de mise à disposition :

Modifiez le groupe. Sur la page Bureaux, cliquez sur **Modifier**. Dans la boîte de dialogue, sélectionnez une autre balise à partir de la liste déroulante ou supprimez la restriction de balise complètement en désactivant le paramètre **Restreindre les lancements aux machines dotées de balises**.

Précautions lors de l'ajout, du retrait ou de la suppression de balises

Une balise appliquée à un élément peut avoir plusieurs fonctions, donc n'oubliez pas que l'ajout, le retrait et la suppression d'une balise peut avoir des effets indésirables. Vous pouvez utiliser une balise pour trier l'affichage des machines dans le champ de recherche de Studio. Vous pouvez utiliser la même balise pour la restriction lors de la configuration d'un groupe d'applications ou d'un bureau, ce qui limite la prise en compte aux machines des groupes de mise à disposition spécifiés qui ont cette balise.

Si vous essayez d'ajouter une balise à une ou plusieurs machines après que cette balise a été configurée comme restriction de balise pour un bureau ou un groupe d'applications, Studio vous avertit que l'ajout de cette balise peut rendre les machines disponibles pour le démarrage d'applications ou de bureaux. Si c'est votre intention, continuez. Sinon, vous pouvez annuler l'opération.

Par exemple, supposons que vous créez un groupe d'applications avec la restriction de balise « Red ». Plus tard, vous ajoutez plusieurs autres machines au groupe de mise à disposition utilisé par ce groupe d'applications. Si vous essayez d'ajouter la balise « Red » à ces machines, Studio affiche un

message similaire au suivant : « La balise « Red » est utilisée en tant que restriction sur les groupes d'applications suivants. Si vous ajoutez cette balise, les machines sélectionnées pourront peut-être lancer des applications dans ces groupes d'applications. » Vous pouvez ensuite confirmer ou annuler l'ajout de cette balise à ces machines supplémentaires.

De même, si une balise est utilisée dans un groupe d'applications pour restreindre les démarrages, Studio vous avertit que vous ne pouvez pas supprimer la balise tant que vous ne l'avez pas retirée comme restriction en modifiant le groupe. (Si vous étiez autorisé à supprimer une balise qui est utilisée comme restriction dans un groupe d'applications, cela pourrait permettre le démarrage des applications sur toutes les machines des groupes de mise à disposition associés au groupe d'applications.) La même interdiction s'applique si la balise est actuellement utilisée comme restriction pour les démarrages de bureau. Après avoir modifié le groupe d'applications ou les bureaux du groupe de mise à disposition pour retirer cette restriction de balise, vous pouvez supprimer la balise.

Les machines peuvent ne pas toutes avoir le même ensemble d'applications. Un utilisateur peut appartenir à plusieurs groupes d'applications, chacun avec une restriction de balise différente et des ensembles de machines différents ou se chevauchant. Le tableau suivant explique comment la prise en compte des machines est décidée.

Lorsqu'une application a été ajoutée à	Ces machines dans les groupes de mise à disposition sélectionnés sont prises en compte pour le démarrage
Un groupe d'applications sans restriction de balise	Toutes les machines
Un groupe d'applications avec restriction de balise A	Les machines sur lesquelles est appliquée la balise A
Deux groupes d'applications, l'un avec la restriction de balise A et l'autre avec la restriction de balise B	Les machines qui ont une balise A et une balise B ; si aucune n'est disponible, les machines qui ont une balise A ou B
Deux groupes d'applications, l'un avec la restriction de balise A et l'autre sans restriction de balise	Les machines qui ont la balise A ; si aucune n'est disponible, toute machine

Si vous avez utilisé une restriction de balise dans un programme de redémarrage de machine, les modifications que vous apportez qui affectent les applications ou les restrictions de balise affecteront le prochain cycle de redémarrage de machine. Les cycles de redémarrage en cours d'exécution lorsque les modifications sont effectuées ne seront pas affectés. (Consultez l'article Gérer les groupes de mise à disposition).

Comment configurer - Exemple 2

La séquence suivante illustre les étapes permettant de créer et d'appliquer des balises, puis de configurer des restrictions de balise pour les groupes d'applications illustrés dans le deuxième exemple ci-dessus.

Les VDA et les applications ont déjà été installés sur les machines et le groupe de mise à disposition a été créé.

Créez et appliquez des balises aux machines :

1. Dans Studio, sélectionnez le groupe de mise à disposition D01, puis sélectionnez **Afficher les machines** dans le volet Action.
2. Sélectionnez les VDA de machine 101-105, puis sélectionnez **Gérer les machines** dans le volet Actions.
3. Dans la boîte de dialogue Gérer les balises, cliquez sur **Créer** puis créez une balise nommée CADApps. Cliquez sur **OK**.
4. Cliquez à nouveau sur **Créer** et créez une balise nommée OfficeApps. Cliquez sur **OK**.
5. Toujours dans la boîte de dialogue Gérer les balises, ajoutez (appliquez) les balises qui viennent d'être créées aux machines sélectionnées en activant les cases à cocher en regard de chaque nom de balise (CADApps et OfficeApps), puis fermez la boîte de dialogue.
6. Sélectionnez le groupe de mise à disposition D01, sélectionnez **Afficher les machines** dans le volet Actions.
7. Sélectionnez les VDA de machine 106-110, puis sélectionnez **Gérer les machines** dans le volet Actions.
8. Dans la boîte de dialogue Gérer les balises, cliquez sur **Créer** puis créez une balise nommée AcctgApps. Cliquez sur **OK**.
9. Appliquez la balise AcctgApps qui vient d'être créée et la balise OfficeApps aux machines sélectionnées en cliquant sur les cases à cocher en regard de chaque nom de balise, puis fermez la boîte de dialogue.

Créez les groupes d'applications avec des restrictions de balise.

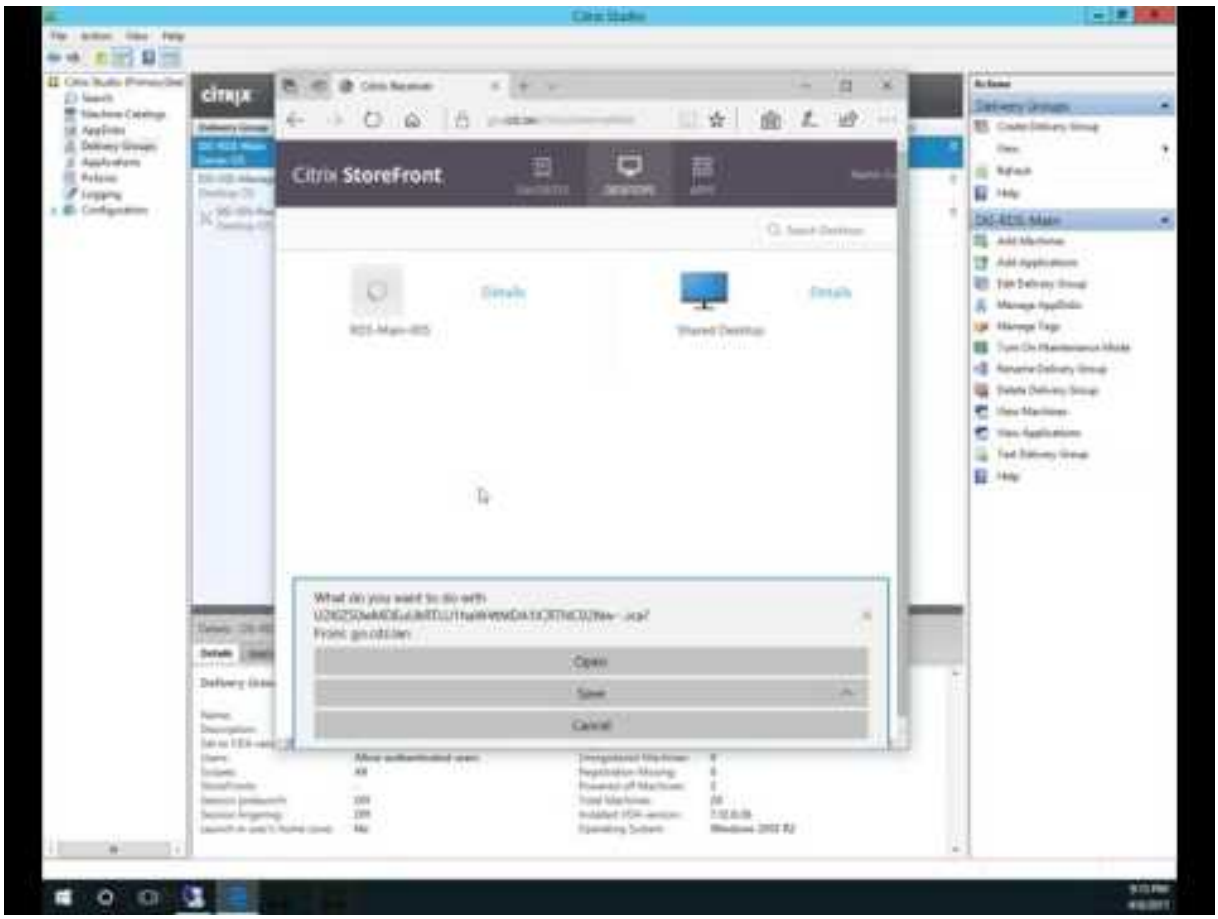
1. Dans Studio, sélectionnez **Applications** dans le panneau de navigation, puis sélectionnez **Créer groupe d'applications** dans le volet Actions. L'assistant Créer groupe d'applications démarre.
2. Sur la page **Groupes de mise à disposition** de l'assistant, sélectionnez Groupe de mise à disposition D01. Sélectionnez **Restreindre les lancements aux machines dotées de balises** puis sélectionnez la balise AcctgApps dans la liste déroulante.
3. Suivez les instructions de l'assistant, en spécifiant les utilisateurs de la comptabilité et les applications de comptabilité. (Lors de l'ajout de l'application, choisissez la source Depuis le menu Démarrer, qui recherchera l'application sur les machines dotées de la balise AcctgApps.) Sur la page **Résumé**, nommez le groupe A100.
4. Répétez ces étapes pour créer un groupe d'applications A200, en spécifiant les machines

auxquelles est appliquée la balise CADApps, ainsi que les utilisateurs et applications appropriés.

5. Répétez ces étapes pour créer un groupe d'applications A300, en spécifiant les machines auxquelles est appliquée la balise OfficeApps, ainsi que les utilisateurs et applications appropriés.

Plus d'informations

Post de blog : How to assign desktops to specific servers (Comment attribuer des postes de travail à des serveurs spécifiques). Ce post contient également la vidéo suivante.



Prise en charge de IPv4/IPv6

January 23, 2019

Cette version prend en charge les déploiements IPv4 purs, IPv6 purs et double pile qui utilisent des réseaux IPv4 et IPv6 qui se chevauchent.

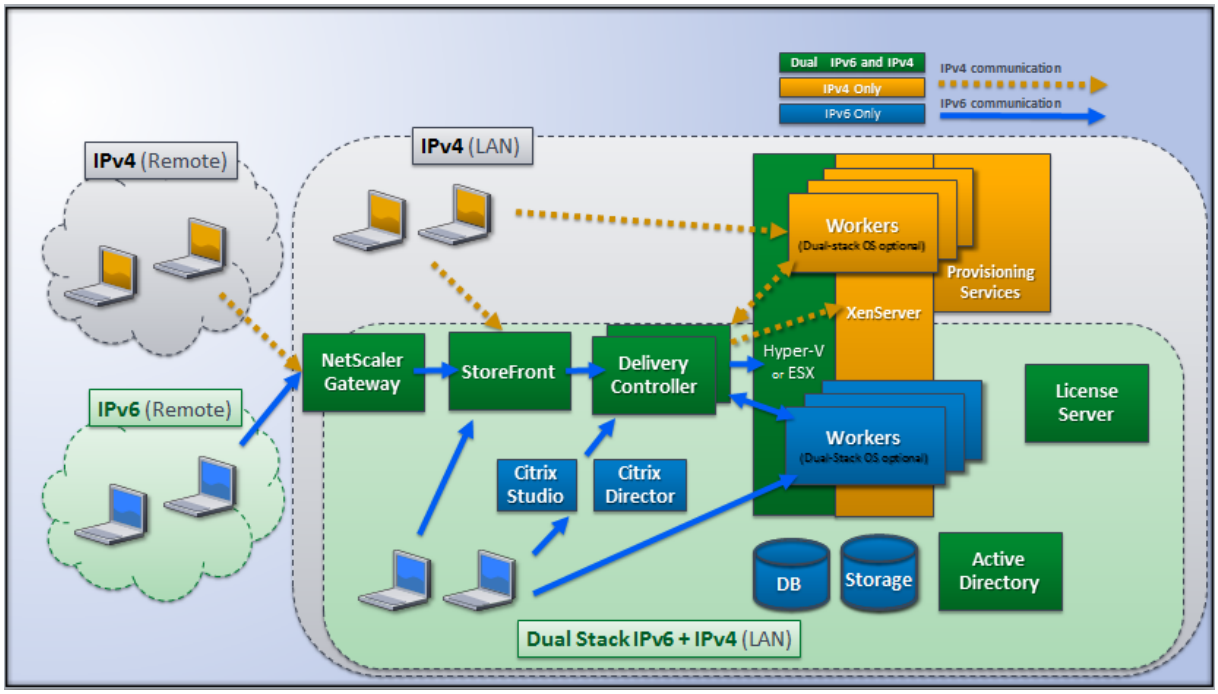
Les communications IPv6 sont contrôlées par deux paramètres de stratégie Citrix liés à la connexion au Virtual Delivery Agent (VDA) :

- Un paramètre principal qui applique l'utilisation de IPv6 : Uniquement utiliser l'enregistrement du contrôleur IPv6.
- Un paramètre dépendant qui définit un masque de réseau IPv6 : Masque réseau IPv6 d'enregistrement du contrôleur.

Lorsque le paramètre de stratégie Uniquement utiliser l'enregistrement du contrôleur IPv6 est activé, les VDA s'enregistrent auprès d'un Delivery Controller pour les connexions entrantes à l'aide d'une adresse IPv6.

Déploiement double pile IPv4/IPv6

La figure suivante illustre un déploiement double pile IPv4/IPv6. Dans ce scénario, un travailleur est un VDA installé sur un hyperviseur ou sur un système physique, qui est utilisé principalement pour autoriser les connexions aux applications et bureaux. Les composants qui prennent en charge IPv6 et IPv4 sont exécutés sur des systèmes d'exploitation qui utilisent le tunneling ou un logiciel à double protocole.



Ces produits, composants et fonctionnalités Citrix prennent uniquement en charge IPv4 :

- Provisioning Services
- XenServer version 6.x
- VDA non contrôlés par le paramètre de stratégie **Uniquement utiliser l'enregistrement du contrôleur IPv6**

- Les versions XenApp antérieures à la version 7.5, les versions XenDesktop antérieures à la version 7, et EdgeSight

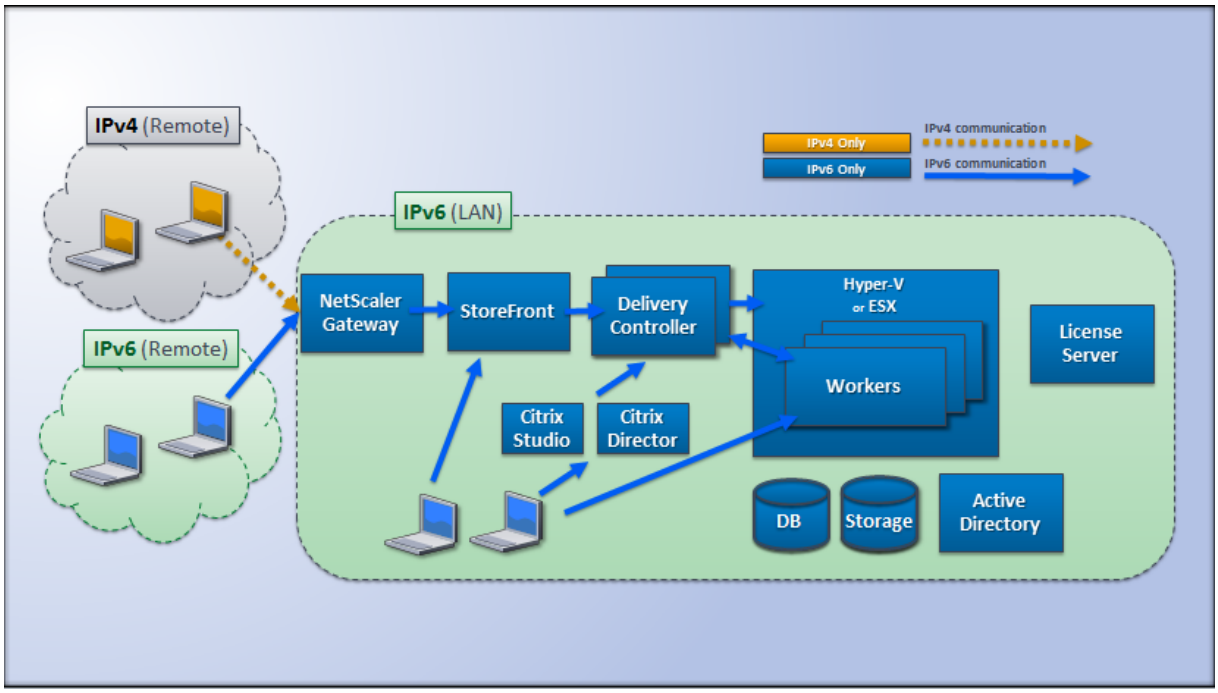
Dans ce déploiement :

- Si une équipe utilise fréquemment un réseau IPv6 et que l'administrateur souhaite qu'ils utilisent le trafic IPv6, l'administrateur publie des bureaux et applications IPv6 pour ces utilisateurs basés sur une image de travail ou une unité d'organisation (UO) sur laquelle le paramètre de stratégie est IPv6 activé (c'est-à-dire, Uniquement utiliser l'enregistrement du contrôleur IPv6 est activé).
- Si une équipe utilise fréquemment un réseau IPv4, l'administrateur publie des bureaux et applications IPv4 pour ces utilisateurs basés sur une image de travail ou une unité d'organisation sur laquelle le paramètre de stratégie IPv6 est désactivé (c'est-à-dire, Uniquement utiliser l'enregistrement du contrôleur IPv6 est désactivé).

Déploiement IPv6 pur

La figure suivante illustre un déploiement IPv6 pur. Dans ce scénario :

- Les composants sont exécutés sur des systèmes d'exploitation configurés pour prendre en charge un réseau IPv6.
- Le paramètre de stratégie Citrix principal (Uniquement utiliser l'enregistrement du contrôleur IPv6) est activé pour tous les VDA ; ils doivent s'enregistrer auprès du Controller à l'aide d'une adresse IPv6.



Paramètres de stratégie pour IPv6

Deux paramètres de stratégie Citrix affectent la prise en charge d'une implémentation IPv6 ou double pile IPv4/IPv6. Configurez les paramètres de stratégie suivants relatifs aux connexions :

- **Uniquement utiliser l'enregistrement du contrôleur IPv6 :** contrôle quelle forme d'adresse le Virtual Delivery Agent (VDA) utilise pour s'enregistrer auprès du Delivery Controller. Valeur par défaut = Désactivé
  - Lorsque le VDA communique avec le Controller, il utilise une seule adresse IPv6 choisie dans l'ordre suivant : adresse IP globale, adresse locale unique (ULA), adresse locale du lien (uniquement si aucune autre adresse IPv6 n'est disponible).
  - Lorsque cette stratégie est désactivée, le VDA s'enregistre et communique avec le Controller à l'aide de l'adresse IPv4 de la machine.
- **Masque réseau IPv6 d'enregistrement du contrôleur :** une machine peut disposer de plusieurs adresses IPv6 ; ce paramètre de stratégie permet aux administrateurs de restreindre le VDA à un sous-réseau préféré (plutôt qu'une adresse IP globale, si une telle adresse est enregistrée). Ce paramètre spécifie le réseau sur lequel le VDA va s'enregistrer : ce dernier s'enregistre uniquement sur la première adresse qui correspond au masque réseau spécifié. Ce paramètre est uniquement valide si le paramètre de stratégie Uniquement utiliser l'enregistrement du contrôleur IPv6 est activé. Valeur par défaut = chaîne vide

Important : l'utilisation de IPv4 ou IPv6 par un VDA est déterminée uniquement par ces paramètres de stratégie. En d'autres termes, pour utiliser l'adressage IPv6, le VDA doit être contrôlé par une stratégie Citrix avec le paramètre
Uniquement utiliser l'enregistrement du contrôleur IPv6 activé.

Considérations de déploiement

Si votre environnement contient à la fois les réseaux IPv4 et IPv6, vous aurez besoin de configurations de groupe de mise à disposition distinctes pour les clients IPv4 et pour les clients qui peuvent accéder au réseau IPv6. Pensez à différencier les utilisateurs à l'aide de noms différents, attributions manuelles de groupes Active Directory ou filtres Smart Access.

La reconnexion à une session peut échouer si la connexion est lancée sur un réseau IPv6, puis que des tentatives de reconnexion sont effectuées à partir d'un client interne ne disposant que d'un accès IPv4.

Profils utilisateur

February 28, 2019

Par défaut, Citrix Profile Management est installé de manière silencieuse sur les images principales lorsque vous installez Virtual Delivery Agent, mais vous n'avez pas à utiliser Profile Management en tant que solution de profils.

Afin de répondre aux besoins variés de vos utilisateurs, vous pouvez utiliser les stratégies XenApp et XenDesktop pour appliquer un comportement de profil différent aux machines dans chaque groupe de mise à disposition. Par exemple, un groupe de mise à disposition peut nécessiter des profils obligatoires Citrix, dont le modèle est stocké dans un emplacement réseau, mais un autre groupe de mise à disposition peut nécessiter des profils itinérants Citrix stockés dans un autre emplacement avec plusieurs dossiers redirigés.

- Si d'autres administrateurs de votre organisation sont responsables des stratégies XenApp et XenDesktop, travaillez avec eux pour vous assurer qu'ils définissent les stratégies liées aux profils sur vos groupes de mise à disposition.
- Les stratégies Profile Management peuvent également être définies dans la stratégie de groupe, dans le fichier .ini de Profile management et localement sur des machines virtuelles individuelles. Ces diverses méthodes permettant de définir le comportement de profil sont lues dans l'ordre suivant :

  1. Stratégie de groupe (fichiers .adm ou .admx)
  2. Les stratégies XenApp et XenDesktop dans le nœud Stratégie
  3. Stratégies locales sur la machine virtuelle à laquelle l'utilisateur se connecte
  4. Fichier .ini Profile Management

  Par exemple, si vous configurez la même stratégie dans le nœud Stratégie de groupe et le nœud Stratégie, le système lit le paramètre de stratégie dans la stratégie de groupe et ignore le paramètre de stratégie XenApp et XenDesktop.

Quelle que soit la solution de gestion des profils que vous choisissez, les administrateurs Director peuvent accéder à des informations de diagnostic afin de résoudre les problèmes liés aux profils utilisateur. Pour de plus amples informations, veuillez consulter la documentation de Director.

Si vous utilisez la fonctionnalité Personal vDisk, les profils utilisateur Citrix sont stockés sur les Personal vDisks des bureaux virtuels par défaut. Ne supprimez pas la copie d'un profil dans le magasin d'utilisateur alors qu'il reste une copie sur le Personal vDisk. Cela engendre une erreur Profile Management et entraîne l'utilisation d'un profil temporaire pour les ouvertures de session au bureau virtuel.

Configuration automatique

Le type de bureau est automatiquement détecté, basé sur l'installation de Virtual Delivery Agent et, en plus du choix de configuration que vous effectuez dans Studio, définit les valeurs par défaut de Profile Management en conséquence.

Les stratégies que Profile Management ajuste sont affichées dans le tableau ci-dessous. Les paramètres de stratégie autres que les paramètres par défaut sont préservés et ne sont pas écrasés par cette fonctionnalité. Consultez la documentation Profile Management pour de plus amples informations sur chaque stratégie. Les types de machines qui créent des profils affectent les stratégies qui sont modifiées. Votre choix doit se baser sur les facteurs principaux suivants : les machines sont-elles persistantes ou provisionnées, sont-elles partagées par de multiples utilisateurs ou dédiées à un seul utilisateur ?

Les systèmes persistants disposent d'un stockage local dont le contenu est conservé lorsque le système est éteint. Ils peuvent utiliser des technologies de stockage telles que les réseaux SAN pour mettre en miroir le disque local. En revanche, les systèmes provisionnés sont créés « à la volée » à partir d'un disque de base et d'un type de disque d'identité. Le stockage local est généralement imité par un disque RAM ou un disque réseau, ce dernier étant fourni la plupart du temps par un SAN doté d'un lien à haute vitesse. La technologie de provisioning utilisée est généralement Provisioning Services ou Machine Creation Services (ou une technologie tierce). Parfois, les systèmes provisionnés sont dotés d'un stockage local persistant sous la forme de Personal vDisks ; ces derniers sont classés comme persistants.

Ensemble, ces deux facteurs définissent les types de machines suivants :

- **Persistantes et dédiées :** machines dotées d'un système d'exploitation de bureau avec une attribution statique et un Personal vDisk créées avec Machine Creation Services, bureaux avec Personal vDisks créés avec VDI-in-a-Box, postes de travail physiques et ordinateurs portables.
- **Persistantes et partagées :** machines dotées d'un système d'exploitation de serveur créées avec Machine Creation Services.
- **Provisionnées et dédiées :** machines dotées d'un système d'exploitation de bureau avec une attribution statique mais sans Personal vDisk créées avec Provisioning Services.
- **Provisionnées et partagées :** machines dotées d'un système d'exploitation de bureau avec une attribution aléatoire créées avec Provisioning Services et bureaux sans Personal vDisks créés avec VDI-in-a-Box.

Les paramètres de stratégie Profile Management suivants sont suggérés pour les types de machines différents. Ils sont adaptés à la plupart des cas, mais vous pouvez en choisir d'autres plus adaptés à votre déploiement.

Important :
Supprimer les profils mis en cache localement à la fermeture de session,
Streaming des profils et
Toujours mettre en cache sont appliqués par la fonctionnalité de configuration automatique. Ajustez les autres stratégies manuellement.

Machines persistantes

Stratégie	Persistantes et dédiées	Persistantes et partagées
Supprimer les profils mis en cache localement à la fermeture de session	Désactivée	Activée
Streaming des profils	Désactivée	Activée
Toujours mettre en cache	Activée (remarque 1)	Désactivée (remarque 2)
Réécriture active	Désactivée	Désactivée (remarque 3)
Traiter les connexions des administrateurs locaux	Activée	Désactivée (remarque 4)

Machines provisionnées

Stratégie	Provisionnées et dédiées	Provisionnées et partagées
Supprimer les profils mis en cache localement à la fermeture de session	Désactivée (remarque 5)	Activée
Streaming des profils	Activée	Activée
Toujours mettre en cache	Désactivée (remarque 6)	Désactivée
Réécriture active	Activée	Activée
Traiter les connexions des administrateurs locaux	Activée	Activée (remarque 7)

1. Étant donné que la stratégie Streaming des profils est désactivée pour ce type de machine, le paramètre Toujours mettre en cache est toujours ignoré.
2. Désactivez Toujours mettre en cache. Toutefois, vous pouvez vous assurer que les fichiers volumineux sont chargés dans les profils dès que possible après l'ouverture de session en activant cette stratégie et en l'utilisant pour définir une limite de taille de fichier (en Mo). Tout fichier de taille égale ou supérieure est placé en cache dès que possible.
3. Désactivez Réécriture active sauf pour enregistrer des modifications dans les profils des utilisateurs qui passent d'un serveur XenApp à un autre. Dans ce cas, activez cette stratégie.
4. Désactivez Traiter les ouvertures de session des administrateurs locaux sauf pour les bureaux partagés hébergés. Dans ce cas, activez cette stratégie.
5. Désactivez Supprimer les profils mis en cache localement à la fermeture de session. Les profils mis en cache localement sont conservés. Étant donné que les machines sont réinitialisées à la

fermeture de session mais attribuées à des utilisateurs individuels, les ouvertures de session sont plus rapides si leurs profils sont mis en cache.

6. Désactivez Toujours mettre en cache. Toutefois, vous pouvez vous assurer que les fichiers volumineux sont chargés dans les profils dès que possible après l'ouverture de session en activant cette stratégie et en l'utilisant pour définir une limite de taille de fichier (en Mo). Tout fichier de taille égale ou supérieure est placé en cache dès que possible.
7. Activez Traiter les ouvertures de session des administrateurs locaux sauf pour les profils des utilisateurs qui itinèrent entre serveurs XenApp et XenDesktop. Dans ce cas, désactivez cette stratégie.

Redirection de dossiers

La redirection de dossiers vous permet de stocker les données utilisateur sur des partages réseau autres que l'emplacement dans lequel les profils sont stockés. Cela permet de réduire la taille du profil et de la durée de chargement, mais peut avoir un impact sur la bande passante réseau. La redirection de dossiers ne nécessite pas que les profils utilisateur Citrix soient utilisés. Vous pouvez gérer les profils utilisateur vous-mêmes, et toujours rediriger les dossiers.

Configurez la redirection de dossiers à l'aide de stratégies Citrix dans Studio.

- Assurez-vous que les emplacements réseau utilisés pour stocker le contenu de ces dossiers redirigés sont disponibles et que vous avez les permissions appropriées. Les propriétés d'emplacement sont validées.
- Les dossiers redirigés sont configurés sur le réseau et leur contenu rempli depuis les bureaux virtuels des utilisateurs à l'ouverture de session.

Remarque : configurez la redirection de dossiers à l'aide des stratégies Citrix ou des objets de stratégie de groupe Active Directory, mais pas les deux. La configuration de la redirection de dossiers à l'aide des deux moteurs de stratégie peut résulter en un comportement imprévisible.

Redirection vers les dossiers spéciaux avancée

Dans les déploiements comportant plusieurs systèmes d'exploitation (OS), il se peut que vous souhaitiez partager un profil utilisateur avec chaque système d'exploitation. Le reste du profil n'est pas partagé et est uniquement utilisé par un seul système d'exploitation. Pour assurer une expérience utilisateur cohérente sur les systèmes d'exploitation, vous devez disposer d'une autre configuration pour chaque système d'exploitation. Cette valeur est la redirection de dossiers avancée. Par exemple, les différentes versions d'une application s'exécutant sur deux systèmes d'exploitation peuvent être nécessaires pour lire ou modifier un fichier partagé, vous décidez ainsi de le rediriger vers un emplacement réseau sur lequel les deux versions peuvent y accéder. Éventuellement, car le contenu du dossier Menu Démarrer est conçu différemment dans les deux systèmes d'exploitation, si vous

décidez de rediriger uniquement un dossier, mais pas les deux. Ceci sépare le dossier Menu Démarrer et son contenu sur chaque système d'exploitation, en assurant aux utilisateurs une expérience cohérente.

Si votre déploiement requiert la redirection de dossiers avancée, vous devez comprendre la structure des données de profil de vos utilisateurs et déterminer quelles parties peuvent être partagées entre systèmes d'exploitation. Ceci est important, car un comportement imprévisible peut survenir si la redirection de dossiers est utilisée.

Pour rediriger les dossiers dans les déploiements avancés :

- Utilisez un groupe de mise à disposition distinct pour chaque système d'exploitation.
- Comprenez l'emplacement où vos applications virtuelles, y compris celles se trouvant sur des bureaux virtuels, stockent des données et des paramètres utilisateur, et la façon dont les données sont structurées.
- Pour partager les données de profil qui peuvent itinérer en toute sécurité (car elles sont conçues de manière identique dans chaque système d'exploitation), redirigez les dossiers contenant dans chaque groupe de mise à disposition.
- Pour les données de profil non partagées qui ne peuvent pas itinérer, redirigez le dossier contenant uniquement dans l'un des groupes de bureaux, généralement celui avec le système d'exploitation le plus utilisé ou celui dans lequel les données sont plus pertinentes. Éventuellement, pour les données non partagées qui ne peuvent pas itinérer entre systèmes d'exploitation, redirigez les dossiers contenant sur les deux systèmes pour séparer les emplacements réseau.

Exemple de déploiement avancé : le déploiement possède des applications, y compris des versions de Microsoft Outlook et Internet Explorer, en cours d'exécution sur des bureaux et des applications Windows 8, y compris d'autres versions d'Outlook et Internet Explorer, mises à disposition par Windows Server 2008. Pour ce faire, vous avez déjà configuré deux groupes de mise à disposition pour les deux systèmes d'exploitation. Les utilisateurs souhaitent accéder à la même série de contacts et de favoris dans les deux versions de ces deux applications.

Important : les décisions et les conseils suivants sont valides pour les systèmes d'exploitation et le déploiement décrits. Dans votre organisation, les dossiers que vous choisissez de rediriger et si vous décidez de les partager dépend d'un certain nombre de facteurs qui sont uniques à votre déploiement spécifique.

- À l'aide des stratégies appliquées aux groupes de mise à disposition, vous choisissez les dossiers suivants à rediriger.

Dossier	Redirigé dans Windows 8 ?	Redirigé dans Windows Server 2008 ?
Mes documents	Oui	Oui

Dossier	Redirigé dans Windows 8 ?	Redirigé dans Windows Server 2008 ?
Données d'application	Non	Non
Contacts	Oui	Oui
Bureau	Oui	Non
Téléchargements	Non	Non
Favoris	Oui	Oui
Liens	Oui	Non
Ma musique	Oui	Oui
Mes images	Oui	Oui
Mes vidéos	Oui	Oui
Recherches	Oui	Non
Parties enregistrées	Non	Non
Menu Démarrer	Oui	Non

- Pour les dossiers partagés et redirigés :
  - Une fois l'analyse de la structure des données enregistrées par les différentes versions d'Outlook et Internet Explorer, vous décidez qu'il est préférable de partager les dossiers Contacts et Favoris
  - Vous savez que la structure des dossiers Documents, Musique, Images et Vidéos est standard sur tous les systèmes d'exploitation, il est conseillé de les stocker au même emplacement réseau pour chaque groupe de mise à disposition
- Pour les dossiers non partagés et redirigés :
  - Vous ne redirigez pas les dossiers Bureau, Liens, Recherches ou Menu Démarrer dans le groupe de mise à disposition Windows Server, car les données de ces dossiers sont organisées différemment dans les deux systèmes d'exploitation. Il ne peut donc pas être partagé.
  - Pour vous assurer un comportement prévisible de ces données non partagées, vous redirigez uniquement vers le groupe de mise à disposition de Windows 8. Vous choisissez ceci, plutôt que le groupe de mise à disposition Windows Server, car Windows 8 sera utilisé plus souvent par les utilisateurs dans leur travail quotidien ; ils peuvent uniquement accéder occasionnellement aux applications mises à disposition par le serveur. Par ailleurs, dans ce cas, les données non partagées sont plus pertinentes dans un environnement de bureau plutôt qu'un environnement d'application. Par exemple, des raccourcis Bureau sont stockés dans le dossier Bureau et peuvent être utiles s'ils

proviennent d'une machine Windows 8, mais pas depuis une machine Windows Server.

- Pour les dossiers non redirigés :
  - Vous ne souhaitez pas embarrasser vos serveurs avec les fichiers téléchargés de l'utilisateur, de sorte que vous choisissez de ne pas rediriger le dossier Téléchargements.
  - Les données d'applications individuelles peuvent entraîner des problèmes de compatibilité et de performances, vous décidez ainsi de ne pas rediriger le dossier Données d'application.

Pour plus d'informations sur la redirection de dossiers, voir https://technet.microsoft.com/en-us/library/cc766489%28v=ws.10%29.aspx.

Redirection de dossiers et exclusions

Dans Citrix Profile Management (mais pas dans Studio), une amélioration des performances vous permet d'éviter que les dossiers soient traités à l'aide d'exclusions. Si vous utilisez cette fonctionnalité, n'excluez pas les dossiers redirigés. Les fonctionnalités de redirection et d'exclusion de dossiers fonctionnent ensemble, afin de garantir qu'aucun dossier redirigé n'est exclus et permet à Profile Management de les déplacer à nouveau dans la structure de dossiers du profil, tout en conservant l'intégrité des données, si vous décidez de ne pas de les rediriger ultérieurement. Pour plus d'informations sur les exclusions, veuillez consulter la section Inclure et exclure des éléments.

Accéder à Citrix Insight Services

February 28, 2019

Citrix Insight Services (CIS) est une plate-forme Citrix depuis laquelle vous pouvez générer des informations d'instrumentation, de télémétrie et autres données stratégiques. Ses fonctionnalités d'instrumentation et de télémétrie permettent aux utilisateurs techniques (clients, partenaires et techniciens) de diagnostiquer et de résoudre les problèmes ainsi que d'optimiser leurs environnements. Pour plus d'informations sur CIS et son fonctionnement, veuillez consulter le site https://cis.citrix.com(informations d'identification de compte Citrix requises).

Les fonctionnalités offertes par Citrix Insight Services continuent à se développer et à évoluer et font maintenant partie intégrante de Citrix Smart Tools. Citrix Smart Tools vous permet d'automatiser les tâches de déploiement, les vérifications d'intégrité et la gestion de l'alimentation. Pour plus d'informations sur les technologies, consultez la documentation de Citrix Smart Tools.

Toutes les informations chargées sur Citrix sont utilisées à des fins de dépannage et de diagnostic, ainsi que pour améliorer la qualité, la fiabilité et les performances des produits, sous réserve de ce qui suit :

- la politique Citrix Insight Services sur https://cis.citrix.com/legal

- la déclaration de confidentialité Citrix sur https://www.citrix.com/about/legal/privacy.html

Cette version de XenApp et XenDesktop prend en charge les technologies et outils suivants.

- Analyses d'installation et de mise à jour de XenApp et XenDesktop
- Programme d'amélioration de l'expérience cliente Citrix
- Citrix Smart Tools
- Citrix Call Home (composant de Citrix Smart Tools)
- Citrix Scout

Installer et mettre à niveau les outils d'analyse

Lorsque vous utilisez le programme d'installation du produit complet pour déployer et mettre à niveau les composants XenApp ou XenDesktop, des informations anonymes sur le processus d'installation sont collectées et stockées sur la machine sur laquelle vous installez/mettez à niveau le composant. Ces données sont utilisées pour aider Citrix à améliorer l'expérience de ses clients avec l'installation. Pour plus d'informations, voir https://more.citrix.com/XD-INSTALLER.

Les informations sont stockées localement sous %ProgramData%\Citrix\CTQs.

Le chargement automatique de ces données est activé par défaut dans les interfaces graphique et de ligne de commande du programme d'installation du produit entier.

- Vous pouvez changer la valeur par défaut dans un paramètre de registre. Si vous modifiez le paramètre de registre avant l'installation ou la mise à niveau, cette valeur est utilisée lorsque vous utilisez le programme d'installation du produit entier.
- Vous pouvez remplacer le paramètre par défaut si vous installez ou mettez à niveau à l'aide de l'interface de ligne de commande en spécifiant une option avec la commande.

Paramètre de registre qui contrôle le chargement automatique des outils d'analyse d'installation et de mise à niveau (valeur par défaut=1) :

Emplacement : HKLM:\Software\Citrix\MetaInstall
Nom : SendExperienceMetrics
Valeur : 0 = désactivé, 1 = activé

L'applet de commande PowerShell suivante désactive le chargement automatique des outils d'analyse d'installation et de mise à niveau :

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\MetaInstall -Name SendExperienceMetrics -PropertyType DWORD -Value 0
```

Pour désactiver les chargements automatiques à l'aide de la commande XenDesktopServerSetup.exe ou XenDesktopVDASetup.exe, spécifiez l'option /disableexperiencemetrics.

Pour activer les chargements automatiques à l'aide de la commande XenDesktopServerSetup.exe ou XenDesktopVDASetup.exe, spécifiez l'option /sendexperiencemetrics.

Programme d'amélioration de l'expérience du client Citrix (CEIP)

Lorsque vous choisissez de participer au Programme d'amélioration de l'expérience utilisateur (CEIP), des informations d'utilisation et des statistiques anonymes sont envoyées à Citrix pour nous aider à améliorer la qualité et les performances des produits Citrix. Pour plus d'informations, consultez https://more.citrix.com/XD-CEIP.

Inscription lors de la création ou de la mise à niveau du site

Vous êtes automatiquement inscrit au programme CEIP lorsque vous créez un site XenApp ou XenDesktop (lorsque vous installez le premier Delivery Controller). Le premier chargement de données se produit approximativement sept jours après la création du site. Vous pouvez mettre fin à votre participation à tout moment après la création du site ; sélectionnez **Configuration** dans le volet de navigation Studio (onglet Assistance produit) et suivez les instructions.

Lorsque vous mettez à niveau un déploiement de XenApp ou XenDesktop :

- Si vous mettez à niveau à partir d'une version qui ne prend pas en charge le programme CEIP, le système vous demandera si vous souhaitez y prendre part.
- Si vous mettez à niveau à partir d'une version qui prend en charge le programme CEIP et que la participation a été activée, CEIP sera activé dans le site mis à niveau.
- Si vous mettez à niveau à partir d'une version qui prend en charge le programme CEIP et que la participation a été désactivée, CEIP sera désactivé dans le site mis à niveau.
- Si vous mettez à niveau à partir d'une version qui prend en charge le programme CEIP et que la participation est inconnue, le système vous demandera si vous souhaitez y prendre part.

Les informations collectées sont anonymes, de façon à ce qu'elles ne puissent pas être consultées après leur chargement auprès de Citrix Insight Services.

Inscription lors de l'installation d'un VDA

Par défaut, vous êtes automatiquement inscrit au programme CEIP lorsque vous installez un VDA Windows. Vous pouvez modifier cette valeur par défaut dans un paramètre de registre. Si vous modifiez le paramètre de registre avant d'installer le VDA, cette valeur est utilisée.

Paramètre de registre qui contrôle l'inscription automatique dans CEIP (valeur par défaut=1) :

Emplacement : HKLM:\Software\Citrix\Telemetry\CEIP
Nom : Enabled
Valeur : 0 = désactivé, 1 = activé

Par défaut, la propriété « Enabled » est masquée dans le registre. Si elle n'est pas spécifiée, la fonctionnalité de chargement automatique est activée.

L'applet de commande PowerShell suivante désactive l'inscription au programme CEIP :

New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\Telemetry\CEIP -Name Enabled -PropertyType DWORD -Value 0

Les points de données d'exécution collectés sont périodiquement écrits sous forme de fichiers dans un dossier de sortie (par défaut %programdata%/Citrix/VdaCeip).

Le premier chargement de données se produit approximativement sept jours après l'installation du VDA.

Inscription lors de l'installation d'autres produits et composants

Vous pouvez également participer au programme CEIP lorsque vous installez des produits, composants et technologies Citrix, tels que Provisioning Services, AppDNA, le serveur de licences Citrix, Citrix Receiver pour Windows, le serveur d'impression universelle et l'enregistrement de session. Consultez la documentation respective de chaque composant pour de plus amples informations sur l'installation et les valeurs de participation par défaut.

Citrix Smart Tools

Vous pouvez activer l'accès à Smart Tools lorsque vous installez un Delivery Controller.

L'accès à Smart Tools est activé par défaut (et la participation à Call Home, si elle n'est pas déjà activée). Cliquez sur **Connect**. Une fenêtre de navigateur s'ouvre et ouvre automatiquement une page web Smart Services, où vous entrez les informations d'identification de votre compte Citrix Cloud. (Si vous ne disposez pas de compte Citrix Cloud, il suffit d'entrer vos informations d'identification de compte Citrix, et un nouveau compte Citrix Cloud est automatiquement créé pour vous.) Une fois que vous êtes authentifié, un certificat est installé en mode silencieux dans le répertoire Smart Tools Agent.

Pour utiliser les technologies Smart Tools, reportez-vous à la documentation de Smart Tools.

Citrix Call Home

Lors de l'installation de certains composants et fonctionnalités de XenApp ou XenDesktop, vous aurez la possibilité de participer à Citrix Call Home. Call Home collecte des données de diagnostic, puis charge périodiquement des paquets de télémétrie contenant ces données directement à Citrix Insight Services (via HTTPS sur le port 443 par défaut) à des fins d'analyse et de résolution des problèmes.

Dans XenApp et XenDesktop, Call Home s'exécute en tant que service d'arrière-plan sous le nom Service de télémétrie Citrix. Pour plus d'informations, voir https://more.citrix.com/XD-CALLHOME.

La fonction de planification de Call Home est également disponible dans Citrix Scout. Pour plus d'informations, consultez Citrix Scout.

Quelles informations sont collectées

Le traçage Citrix Diagnostic Facility (CDF) consigne les informations qui peuvent être utiles pour la résolution des problèmes. Call Home collecte un sous-ensemble des traces CDF qui peut être utile lors de la résolution des problèmes courants, par exemple, les enregistrements de VDA et le lancement d'application/bureau. Cette technologie est appelée traçage permanent (AOT). Call Home ne recueille pas d'autres informations de Suivi d'événements pour Windows (ETW), et ne peut pas être configuré pour le faire.

Call Home recueille également d'autres informations, telles que :

- Clés de registre créées par XenApp et XenDesktop sous HKEY_LOCAL_MACHINE\SOFTWARE\Citrix
- Informations Infrastructure de gestion Windows (WMI) sous l'espace de noms de Citrix
- Liste des processus en cours d'exécution
- Vidages sur incident des processus Citrix qui sont stockés dans %PROGRAM DATA%\Citrix\CDF

Les informations de trace sont compressées lorsqu'elles sont collectées. Le Citrix Telemetry Service conserve un maximum de 10 Mo d'informations de traçage récentes comprimées, pendant une période maximale de huit jours.

- La compression des données permet à Call Home de limiter l'encombrement sur le VDA.
- Les traces sont stockées dans la mémoire pour éviter des opérations d'entrées/sortie sur les machines provisionnées.
- Le tampon de suivi utilise un mécanisme circulaire pour conserver les traces en mémoire.

Call Home collecte ces points de données clés :Points de données clés Call Home

Configurer et gérer : résumé

Vous pouvez vous inscrire à Call Home lors de l'utilisation de l'assistant d'installation du produit complet ou plus tard, à l'aide d'applets de commande PowerShell. Si vous vous inscrivez, par défaut, des diagnostic sont collectés et chargés vers Citrix tous les dimanches à environ 3 h 00, heure locale. Le chargement est aléatoire avec un intervalle de deux heures depuis l'heure spécifiée. Cela signifie qu'un chargement avec la programmation par défaut se produit entre 3h00 et 5h00.

Si vous ne souhaitez pas charger d'informations de diagnostic à intervalles réguliers (ou si vous souhaitez changer une planification), vous pouvez toujours utiliser les applets de commande PowerShell pour collecter et charger manuellement les diagnostics ou les stocker localement.

Si vous avez opté pour le chargement de données Call Home à intervalles réguliers et que vous chargez manuellement des informations de diagnostic sur Citrix, vous devez fournir les informa-

tions d'identification d'accès au compte Citrix ou Citrix Cloud. Citrix échange les informations d'identification contre un jeton de chargement qui est utilisé pour identifier le client et charger les données. Les informations d'identification ne sont pas enregistrées.

Lorsqu'un chargement se produit, une notification est envoyée par e-mail à l'adresse associée au compte Citrix.

Conditions préalables

- La machine doit exécuter PowerShell 3.0 ou version ultérieure.
- Le Service de télémétrie Citrix doit être en cours d'exécution sur la machine.
- La variable système PSModulePath doit être définie sur le chemin d'installation de la télémétrie, par exemple, C:\Program Files\Citrix\Telemetry Service\.

Activer Call Home lors de l'installation de composants

Lors de l'installation ou la mise à niveau de VDA : lorsque vous installez ou mettez à niveau un VDA à l'aide de l'interface graphique du programme d'installation du produit entier, il vous est demandé si vous souhaitez participer à Call Home. Il existe deux options :

- Participer au programme Call Home
- Je ne veux pas participer au programme Call Home

Si vous mettez à niveau un VDA et êtes déjà inscrit à Call Home, cette page de l'assistant n'apparaît pas.

Lors de l'installation ou la mise à niveau de Controller : lorsque vous installez ou mettez à niveau un Controller à l'aide de l'interface graphique, il vous est demandé si vous souhaitez participer à Call Home et vous connecter à Citrix Smart Tools. Il existe trois options :

- Se connecter à Citrix Smart Tools, qui inclut la fonctionnalité Call Home via l'agent Smart Tools. Il s'agit de l'option par défaut et recommandée. Si vous choisissez cette option, l'agent Smart Tools est configuré. (L'agent Smart Tools est installé, que cette option soit sélectionnée ou non.)
- Participer uniquement à Call Home, mais ne pas se connecter à Smart Tools. Si vous choisissez cette option, l'agent Smart Tools est installé mais n'est pas configuré. La fonctionnalité Call Home est fournie par le Service de télémétrie Citrix et Citrix Insight Services.
- Ne pas se connecter à Smart Tools et ne pas participer à Call Home.

Lorsque vous installez un Controller, vous ne pouvez pas configurer d'informations sur la page Call Home de l'assistant d'installation si le serveur possède un objet de stratégie de groupe Active Directory dans lequel le paramètre de stratégie « Ouvrir une session en tant que service » est activé. Pour plus d'informations, veuillez consulter l'article CTX218094.

Si vous mettez un Controller à niveau et êtes déjà inscrit à Call Home, la page mentionne uniquement Smart Tools. Si vous êtes déjà inscrit à Call Home et que l'agent Smart est déjà installé, la page de l'assistant n'apparaît pas.

Pour plus d'informations sur Smart Tools, consultez la documentation de Smart Tools.

Applets de commande PowerShell

L'aide de PowerShell fournit une syntaxe complète, y compris des descriptions des applets de commande et des paramètres qui ne sont pas utilisés dans ces cas d'utilisation courants.

Pour utiliser un serveur proxy pour les chargements, reportez-vous à la section Configurer un serveur proxy.

Activer des chargements programmés

Les collectes de diagnostics sont automatiquement chargées vers Citrix. Si vous n'entrez pas d'applets de commande supplémentaires pour un programme personnalisé, le programme par défaut est utilisé.

```
$cred = Get-Credential
Enable-CitrixCallHome -Credential $cred
```

Pour confirmer que les chargements programmés sont activés, entrez Get-CitrixCallHome. Cette commande devrait renvoyer IsEnabled=True et IsMasterImage=False.

Activer les téléchargements planifiés pour les machines créées à partir d'une image principale

L'activation de chargements programmés dans une image principale vous évite d'avoir à configurer chaque machine qui est créée dans le catalogue de machines.

```
Enable-CitrixCallHome -Credential $cred -MasterImage
```

Pour confirmer que les chargements programmés sont activés, entrez Get-CitrixCallHome. Cette commande devrait renvoyer IsEnabled=True et IsMasterImage=True.

Créer un programme personnalisé

Créez une planification quotidienne ou hebdomadaire pour les collectes de diagnostics et les chargements.

```
$timespan = New-TimeSpan –Hours <heures> -Minutes <minutes>
Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek <jour> -UploadFrequency {Daily|Weekly}
```


Annuler les téléchargements planifiés

Après l'annulation des chargements programmés, vous pouvez continuer à charger des données de diagnostic à l'aide d'applets de commande PowerShell.

Disable-CitrixCallHome

Pour confirmer que les chargements programmés sont désactivés, entrez Get-CitrixCallHome. Cette commande devrait renvoyer IsEnabled=False et IsMasterImage=False.

Exemples

Les applets de commande suivantes créent un programme qui collecte et charge les données à 23:20 chaque soir. Notez que le paramètre Heures utilise une horloge de 24 heures. Lorsque la valeur du paramètre UploadFrequency est Daily, le paramètre DayOfWeek est ignoré, s'il est spécifié.

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20
Set-CitrixCallHomeSchedule –TimeOfDay $timespan -UploadFrequency Daily
```

Pour confirmer le programme, entrez Get-CitrixCallHomeSchedule. Dans l'exemple ci-dessus, cette commande devrait renvoyer StartTime=22:20:00, DayOfWeek=Sunday (ignored), Upload Frequency=Daily.

Les applets de commande suivantes créent un programme qui collecte et charge les données à 23:20 chaque mercredi soir.

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20
Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek Wed -UploadFrequency Weekly
```

Pour confirmer le programme, entrez Get-CitrixCallHomeSchedule. Dans l'exemple ci-dessus, cette commande devrait renvoyer StartTime=22:20:00, DayOfWeek=Wednesday, Upload Frequency=Weekly.

Configurer un serveur proxy pour les chargements effectués par Call Home

Effectuez les tâches suivantes sur la machine où Call Home est activé. Les diagrammes de la procédure suivante contiennent l'adresse et le port du serveur 10.158.139.37:3128. Vos informations seront différentes.

Étape 1 – Ajoutez les informations du serveur proxy dans votre navigateur. Dans Internet Explorer, sélectionnez **Options Internet > Connexions > Paramètres LAN**. Sélectionnez **Utiliser un serveur proxy pour le réseau local**, puis entrez le numéro d'adresse et le port du serveur proxy.

Étape 2 – Dans PowerShell, exécutez **netsh winhttp import proxy source=ie**.


```
PS C:\Users\administrator.JLGXH> netsh winhttp import proxy source=ie

Current WinHTTP proxy settings:

    Proxy Server(s) :  10.108.124.245:8080
    Bypass List     :  (none)
```

Étape 3 – À l'aide d'un éditeur de texte, modifiez le fichier de configuration TelemetryService.exe, qui se trouve dans C:\Program Files\Citrix\Telemetry Service. Ajoutez les informations affichées dans la zone rouge ci-dessous.

Étape 4 – Redémarrez le service de télémétrie.

Exécutez les applets de commande Call Home dans PowerShell.

Collecter et charger manuellement des informations de diagnostic

Vous pouvez utiliser le site Web CIS pour charger des packages d'informations de diagnostic sur CIS. Vous pouvez également utiliser les applets de commande PowerShell pour collecter et charger des informations de diagnostic sur CIS.

Pour charger un package à l'aide du site Web CIS :

1. Connectez-vous à Citrix Insight Services à l'aide des informations d'identification de votre compte Citrix.
2. Sélectionnez **My Workspace**.
3. Sélectionnez **Healthcheck**, puis accédez à l'emplacement de vos données.

CIS prend en charge plusieurs applets de commande PowerShell qui gèrent le chargement de données. Cette documentation couvre les applets de commande pour deux cas courants :

- Utilisez l'applet de commande Start-CitrixCallHomeUpload pour collecter et charger manuellement un package d'informations de diagnostic sur CIS. (Le package n'est pas enregistré localement).
- Utilisez l'applet de commande Start-CitrixCallHomeUpload pour collecter manuellement des données et stocker un package d'informations de diagnostic localement. Cela vous permet d'afficher un aperçu des données. Ensuite, à une date ultérieure, utilisez l'applet de commande Send-CitrixCallHomeBundle pour charger manuellement une copie de ce package sur CIS. (Les données que vous avez enregistrées à l'origine restent locales).

L'aide de PowerShell fournit une syntaxe complète, y compris des descriptions des applets de commande et des paramètres qui ne sont pas utilisés dans ces cas d'utilisation courants.

Lorsque vous entrez une applet de commande pour charger des données sur CIS, vous êtes invité à confirmer le chargement. Si l'applet de commande expire avant que le chargement ne soit terminé, vérifiez l'état du chargement dans le journal d'événements système. La demande de chargement peut être rejetée si le service est déjà en train d'effectuer un chargement.

Collecter des données et charger le package sur CIS

Start-CitrixCallHomeUpload [-Credential] <PSCredential> [-InputPath <Chaîne>] [-Description <Chaîne>] [-IncidentTime <Chaîne>] [-SRNumber <Chaîne>] [-Name <Chaîne>] [-UploadHeader <String>] [-AppendHeaders <Chaîne>] [-Collect <Chaîne>] [<CommonParameters>]

Collecter des données et les enregistrer localement

Start-CitrixCallHomeUpload -OutputPath <Chaîne> [-InputPath <Chaîne>] [-Description <Chaîne>] [-IncidentTime <Chaîne>] [-SRNumber <Chaîne>] [-Name <Chaîne>] [-UploaderHeader <Chaîne>] [-AppendHeaders <Chaîne>] [-Collect <Chaîne>] [<CommonParameters>]

Paramètre	Description
Certificats	Dirige le chargement sur CIS.
InputPath	Emplacement du fichier zip à inclure dans le package. Il peut s'agir d'un fichier supplémentaire qui vous a été demandé par l'assistance de Citrix. Veillez à inclure l'extension .zip.
OutputPath	Emplacement où les informations de diagnostic seront enregistrées. Ce paramètre est requis lors de l'enregistrement des données Call Home localement.

Paramètre	Description
Description et Incident Time	Informations sur le chargement en format libre.
SRNumber	Numéro d'incident de l'assistance technique de Citrix.
Name	Nom qui identifie le package.
UploadHeader	Chaîne au format JSON qui spécifie les en-têtes de chargement chargés sur CIS.
AppendHeaders	Chaîne au format JSON qui spécifie les en-têtes ajoutés chargés sur CIS.
Collect	Chaîne au format JSON qui spécifie les données à collecter ou ignorer, au format {'collector':{'enabled':Boolean}}", où Boolean est true ou false. Les valeurs valides du collecteur sont les suivantes : 'wmi'; 'process'; 'registry'; 'crashreport'; 'trace'; 'localdata'; 'sitedata'; 'sfb'. Par défaut, tous les collecteurs mis à part « sfb » sont activés. Le collecteur « sfb » est conçu pour être utilisé sur demande pour diagnostiquer les problèmes de Skype Entreprise. Outre le paramètre « enabled », le collecteur « sfb » prend en charge les paramètres « account » et « accounts » pour spécifier des utilisateurs cibles. Utilisez une des formes suivantes : "-Collect "{'sfb':{'account':'domain\user1'}}"; -Collect "{'sfb':{'accounts':['domain\user1', 'domain\user2']}}"
Paramètres courants	Consultez l'aide de PowerShell.

Charger des données qui étaient préalablement enregistrées localement

Send-CitrixCallHomeBundle -Credential <PSCredential> -Path <Chaîne> [<CommonParameters>]

Le paramètre Path spécifie l'emplacement dans lequel le package était préalablement enregistré.

Exemples

L'applet de commande suivante demande le chargement des données Call Home (à l'exception des données du collecteur WMI) sur CIS. Ces données sont liées aux échecs d'enregistrement des VDA PVS, ce qui est indiqué à 14:30 pour le ticket de support technique de Citrix 123456. En plus des données Call Home, le fichier « c:\Diagnostics\ExtraData.zip » sera incorporé au package chargé.

C:\PS>Start-CitrixCallHomeUpload -InputPath "c:\Diagnostics\ExtraData.zip" -Description "Registration failures with PVS VDAs" -IncidentTime "14:30" -SRNumber 123456 -Name "RegistrationFailure-021812016" -Collect "{'wmi':{'enabled':false}}" -UploadHeader "{'key1':'value1'}" -AppendHeaders "{'key2':'value2'}"

L'applet de commande suivante enregistre les données Call Home liées au ticket de support technique de Citrix 223344, ce qui est indiqué à 8:15. Les données seront enregistrées dans le fichier mydata.zip sur un partage réseau. En plus des données Call Home, le fichier« c:\Diagnostics\ExtraData.zip » sera incorporé au package enregistré.

C:\PS>Start-CitrixCallHomeUpload -OutputPath \\mynetwork\myshare\mydata.zip -InputPath "c:\Diagnostics\ExtraData.zip" -Description "Diagnostics for incident number 223344" -IncidentTime "8:15" -SRNumber 223344

L'applet de commande suivante charge le package de données que vous avez enregistré précédemment.

$cred=Get-Credential
C:\PS>Send-CitrixCallHomeBundle –Credential $cred -Path \\mynetwork\myshare\mydata.zip

Citrix Scout

Pour plus d'informations, consultez Citrix Scout.

Citrix Scout

February 28, 2019

Introduction

Citrix Scout collecte des diagnostics qui peuvent être utilisés à des fins de maintenance proactive dans votre déploiement XenApp et XenDesktop. Citrix offre une analyse complète et automatique via Citrix Insight Services. Vous pouvez également utiliser Scout pour résoudre les problèmes, vous-même ou avec des instructions de l'assistance Citrix. Vous pouvez charger des fichiers de collecte vers Citrix à

des fins d'analyse et pour obtenir des instructions de l'assistance Citrix. Ou, vous pouvez enregistrer une collecte localement pour votre propre vérification et plus tard charger le fichier de la collecte vers Citrix pour analyse.

Scout offre trois procédures principales :

- **Collecter :** exécute une collecte ponctuelle de diagnostics sur les machines que vous sélectionnez dans un site. Ensuite, chargez le fichier contenant la collecte vers Citrix ou enregistrez-le localement.
- **Tracer et reproduire :** démarre une trace manuelle sur les machines que vous sélectionnez. Vous recréez ensuite les problèmes sur ces machines. Après la reproduction du problème, la trace est arrêtée. Ensuite, Scout collecte d'autres diagnostics et charge le fichier contenant la trace et la collecte vers Citrix ou enregistre le fichier en local.
- **Planifier :** planifie des collectes de diagnostics quotidiennes ou hebdomadaires à une heure spécifique, sur les machines que vous sélectionnez. Le fichier contenant chaque collecte est automatiquement chargé vers Citrix.

L'interface graphique décrite dans cet article est le principal moyen d'utiliser Scout. Vous pouvez aussi utiliser l'interface PowerShell pour configurer des collectes de diagnostics ponctuelles ou planifiées et leurs chargements. Voir [Call Home].(/fr-fr/xenapp-and-xendesktop/7-15-ltsr/manage-deployment/cis.html)

Où exécuter Scout :

- Dans un déploiement de XenApp et XenDesktop sur site, exécutez Scout à partir d'un Delivery Controller pour capturer les diagnostics à partir d'un ou de plusieurs Virtual Delivery Agent (VDA) et Delivery Controller. Vous pouvez également exécuter Scout à partir d'un VDA pour collecter les diagnostics locaux.
- Dans un environnement Citrix Cloud qui utilise le service XenApp et XenDesktop, exécutez Scout à partir d'un VDA pour collecter les diagnostics locaux.

Quelles informations sont collectées

Les diagnostics collectés par Scout incluent des fichiers journaux de trace Citrix Diagnostic Facility (CDF). Un sous-ensemble des traces CDF appelé Suivi permanent (AOT, Always-On Tracing) est également inclus. Les informations AOT peuvent s'avérer utiles lors de la résolution de problèmes courants tels que des enregistrements de VDA et des lancements d'application ou de bureau. Aucune autre information de Suivi d'événements pour Windows (ETW) n'est collectée.

Les informations collectées incluent notamment :

- Clés de registre créées par XenApp et XenDesktop sous HKEY_LOCAL_MACHINE\SOFTWARE\CITRIX.
- Informations Infrastructure de gestion Windows (WMI) sous l'espace de noms de Citrix.
- Processus qui sont en cours d'exécution.

- Vidages sur incident des processus Citrix qui sont stockés dans %PROGRAM DATA%\Citrix\CDF.

À propos des informations de trace :

- Les informations de trace sont compressées lorsqu'elles sont collectées, ce qui permet d'éviter l'encombrement de la machine.
- Sur chaque machine, le Citrix Telemetry Service conserve un maximum de 10 Mo d'informations de traçage récentes comprimées, pendant une période maximale de huit jours.
- Les traces sont stockées dans la mémoire pour éviter des opérations d'entrées/sortie sur les machines provisionnées.
- Le tampon de suivi utilise un mécanisme circulaire pour conserver les traces en mémoire.

Pour obtenir une liste des points de données que Scout collecte, consultez la section Points de données clés Scout.

Composants requis et considérations

Autorisations

- Vous devez être un administrateur local et un utilisateur de domaine pour chaque machine depuis laquelle vous collectez des diagnostics.
- Vous devez disposer des permissions d'écriture dans le répertoire LocalAppData sur chaque machine.
- Utilisez **Exécuter en tant qu'administrateur** lors du lancement de Scout.

Pour chaque machine à partir de laquelle vous collectez des diagnostics :

- Scout doit être en mesure de communiquer avec la machine.
- Le partage de fichiers et d'imprimantes doit être activé.
- PSRemoting et WinRM doivent être activés. La machine doit également exécuter PowerShell 3.0 ou version ultérieure.
- Le Service de télémétrie Citrix doit être en cours d'exécution sur la machine.
- Pour planifier la collecte de diagnostics, la machine doit exécuter une version de Scout fournie avec XenApp et XenDesktop 7.14 ou une version ultérieure prise en charge.

Scout exécute des tests de vérification sur les machines que vous sélectionnez pour s'assurer que ces conditions sont remplies.

Tests de vérification

Avant le démarrage d'une collecte de diagnostics, des tests de vérification sont exécutés automatiquement pour chaque machine sélectionnée. Ces tests garantissent que les conditions requises décrites ci-dessus sont remplies. Si un test échoue pour une machine, Scout affiche un message avec actions correctives proposées.

Message d'erreur	Action corrective
Scout ne peut accéder à cette machine	Assurez-vous que la machine est démarrée. Assurez-vous que la connexion réseau fonctionne correctement. (il peut vérifier que votre pare-feu est correctement configuré.) Assurez-vous que le partage de fichiers et d'imprimantes est activé. Consultez la documentation Microsoft pour obtenir des instructions.
Activer PSRemoting et WinRM	Vous pouvez activer la communication à distance PowerShell et WinRM en même temps. À l'aide de l'option « Exécuter en tant qu'administrateur », exécutez l'applet de commande **Enable-PSRemoting**. Pour de plus amples informations, consultez l'aide de Microsoft pour l'applet de commande.
Scout requiert PowerShell 3.0 (minimum)	Installez PowerShell 3.0 (ou version ultérieure) sur la machine et activez la communication à distance PowerShell.
Impossible d'accéder au répertoire LocalAppData sur cette machine	Assurez-vous que votre compte est autorisé à écrire sur le répertoire LocalAppData de cette machine.
Impossible de trouver Citrix Telemetry Service	Assurez-vous que le service de télémétrie Citrix Telemetry Service est installé et démarré sur la machine.
Impossible d'obtenir la planification	Mettez la machine à niveau vers XenApp et XenDesktop 7.14 (minimum).

Compatibilité de version

Cette version de Scout (3.x) est conçue pour être exécutée sur des Controller et des VDA XenApp et XenDesktop 7.14 (au minimum).

Une version antérieure de Scout est fournie avec les déploiements XenApp et XenDesktop antérieurs. Pour de plus amples informations sur cette version antérieure, consultez l'article CTX130147.

Si vous mettez à niveau un Controller ou un VDA antérieur à 7.14 vers la version 7.14 (ou une version supérieure prise en charge), la version antérieure de Scout est remplacée par la version actuelle.

Fonctionnalité	Scout 2.23	Scout 3.0
Prise en charge de XenApp et XenDesktop 7.14 (minimum)	Oui	Oui
Prise en charge de XenDesktop 5.x, 7.1 à 7.13	Oui	Non
Prise en charge de XenApp 6.x, 7.5 à 7.13	Oui	Non
Mis à disposition avec le produit	7.1 à 7.13	À compter de 7.14
Peut être téléchargé à partir de l'article CTX	Oui	Non
Capturer des traces CDF	Oui	Oui
Capturer des traces de suivi permanent (AOT)	Non	Oui
Autoriser la collecte de données de diagnostics	Jusqu'à 10 machines en même temps (par défaut)	Un nombre illimité (sous réserve de disponibilité des ressources)
Autoriser l'envoi des données de diagnostics à Citrix	Oui	Oui
Autoriser l'enregistrement local des données de diagnostics	Oui	Oui
Prise en charge des informations d'identification Citrix Cloud	Non	Oui
Prise en charge des informations d'identification Citrix	Oui	Oui
Prise en charge du serveur proxy pour les chargements	Oui	Oui
Régler les planifications	S.O.	Oui
Prise en charge de script	Ligne de commande (Controller local uniquement)	PowerShell à l'aide des applets de commande Call Home (toute machine avec télémétrie installée)

Installation

Par défaut, Scout est installé automatiquement dans le cadre du Service de télémétrie Citrix lorsque vous installez un VDA ou un Controller.

Si vous omettez le Service de télémétrie Citrix lorsque vous installez un VDA, ou que vous supprimez le service ultérieurement, exécutez TelemetryServiceInstaller_xx.msi à partir du dossier x64\Virtual Desktop Components ou x86\Virtual Desktop Components sur l'ISO XenApp ou XenDesktop.

Autorisation de chargement

Si vous voulez charger les collectes de diagnostic vers Citrix, vous devez disposer d'un compte Citrix ou Citrix Cloud. (Il s'agit des informations d'identification que vous utilisez pour accéder aux téléchargements de Citrix ou pour accéder au Centre de contrôle Citrix Cloud.) Une fois vos informations d'identification de compte validées, un jeton est émis.

- Si vous vous authentifiez avec un compte Citrix, le processus d'émission de jeton n'est pas visible. Entrez les informations d'identification de votre compte. Une fois que Citrix a validé les informations d'identification, vous êtes autorisé à continuer avec l'Assistant de Scout.
- Si vous vous authentifiez avec un compte Citrix Cloud, vous cliquez sur un lien pour accéder à Citrix Cloud à l'aide de HTTPS avec votre navigateur par défaut. Une fois que vous avez entré vos informations d'identification Citrix Cloud, le jeton s'affiche. Copiez le jeton et collez-le dans Scout. Vous êtes alors autorisé à poursuivre dans l'Assistant de Scout.

Le jeton est stocké localement sur la machine sur laquelle vous exécutez Scout. Si vous souhaitez utiliser ce jeton la prochaine fois que vous sélectionnez **Collecter** ou **Tracer et reproduire**, sélectionnez la case **Stocker le jeton et ignorer cette étape dans le futur**.

Vous devez renouveler l'autorisation chaque fois que vous sélectionnez **Planifier** sur la page d'ouverture de Scout. Vous ne pouvez pas utiliser un jeton stocké lors de la création ou modification d'une planification.

Utiliser un proxy pour les chargements

Si vous souhaitez utiliser un serveur proxy pour le chargement des collectes vers Citrix, vous pouvez demander à Scout d'utiliser les paramètres de proxy configurés pour les propriétés d'Internet de votre navigateur, ou vous pouvez spécifier l'adresse IP du serveur proxy et son numéro de port.

Collecter informations de diagnostic

La procédure de collecte consiste à sélectionner des machines, à démarrer la collecte de diagnostics et à charger ensuite le fichier contenant la collecte vers Citrix ou à l'enregistrer localement.

Étape 1 – Lancer Scout.

Depuis le menu Démarrer de la machine : **Citrix > Citrix Scout**. Sur la page d'ouverture, cliquez sur **Collecter**.

Étape 2 – Sélectionner des machines.

La page Sélectionner des machines répertorie tous les VDA et Controller du site. Vous pouvez filtrer l'affichage par nom de machine. Sélectionnez la case à cocher en regard de chaque machine à partir de laquelle vous voulez collecter des diagnostics, puis cliquez sur **Continuer**.

Scout démarre automatiquement des tests de vérification sur chaque machine que vous avez sélectionnée, s'assurant ainsi que celle-ci remplit les critères répertoriés dans Tests de vérification. En cas d'échec de la vérification, un message est affiché dans la colonne État et la case à cocher de cette machine n'est plus sélectionnée. Vous pouvez :

- Corriger le problème, puis sélectionner de nouveau la case à cocher de la machine. Cela déclenche une nouvelle tentative de tests de vérification.
- Ignorer cette machine (laisser la case à cocher non sélectionnée). Les diagnostics ne seront pas collectés à partir de cette machine.

Lorsque les tests de vérification sont terminés, cliquez sur **Continuer**.

Étape 3 – Collecter des informations de diagnostics depuis les machines.

Le résumé répertorie toutes les machines à partir desquelles les diagnostics seront collectés (les machines que vous avez sélectionnées et qui ont réussi les tests de vérification). Cliquez sur **Collecte**.

Lors de la collecte :

- La colonne État indique l'état actuel de collecte pour une machine.
- Pour arrêter une collecte en cours sur une seule machine, cliquez sur **Annuler** dans la colonne Action pour cette machine.
- Pour arrêter toutes les collectes en cours, cliquez sur **Arrêter la collecte** dans le coin inférieur droit de la page. Les diagnostics à partir de machines qui ont terminé la collecte sont conservés. Pour reprendre la collecte, cliquez sur **Réessayer** dans la colonne Action pour chaque machine.
- Lorsque la collecte est terminée pour toutes les machines sélectionnées, le bouton **Arrêter la collecte** dans le coin inférieur droit devient **Continuer**.
- Si la collecte pour une machine réussit et que vous souhaitez de nouveau collecter des diagnostics à partir de cette machine, cliquez sur **Collecter de nouveau** dans la colonne Action de cette machine. La collecte plus récente remplace la version antérieure.
- Si une collecte échoue, vous pouvez cliquer sur **Réessayer** dans la colonne Action. Seules les collectes réussies sont chargées ou enregistrées.
- Une fois que la collecte est terminée pour toutes les machines sélectionnées, ne cliquez pas sur **Précédent**. Si vous cliquez sur ce bouton et confirmez l'invite, la collecte est perdue.

Lorsque la collecte est terminée, cliquez sur **Continuer**.

Étape 4 – Enregistrer ou charger la collecte.

Choisissez si vous souhaitez charger le fichier contenant les diagnostics collectés vers Citrix, ou les enregistrer sur la machine locale.

Si vous choisissez de charger le fichier maintenant, passez à l'étape 5.

Si vous choisissez d'enregistrer le fichier localement :

- La boîte de dialogue Enregistrer de Windows s'affiche. Naviguez jusqu'à l'emplacement souhaité.
- Lorsque l'enregistrement local est terminé, le nom de chemin du fichier est affiché et lié. Vous pouvez afficher le fichier. Vous pouvez charger le fichier plus tard à partir de Citrix ; consultez l'article CTX136396 pour Citrix Insight Services, ou l'assistance Smart Tools.

Cliquez sur **Terminé** pour revenir sur la page d'ouverture de Scout. Vous n'avez pas besoin de suivre les autres étapes de cette procédure.

Étape 5 – S'authentifier pour les chargements et spécifier le proxy (facultatif).

Consultez la section Autorisation de chargement pour plus de détails sur ce processus.

- Si vous ne vous êtes pas déjà authentifié via Scout, passez à cette étape.
- Si vous vous êtes précédemment authentifié via Scout, le jeton d'autorisation stocké est utilisé par défaut. Si cela vous convient, choisissez cette option et cliquez sur **Continuer**. Vous n'êtes pas invité à entrer d'informations d'identification pour cette collecte ; passez à l'étape 6.
- Si vous vous êtes précédemment authentifié, mais souhaitez renouveler l'autorisation avec émission d'un nouveau jeton, cliquez sur **Changer/réautoriser** et poursuivez avec cette étape.

Choisissez si vous souhaitez utiliser les informations d'identification Citrix ou les informations d'identification Citrix Cloud pour authentifier le chargement. Cliquez sur Continuer. La page d'informations d'identification s'affiche uniquement si vous n'utilisez pas de jeton stocké.

Sur la page d'informations d'identification :

- Si vous souhaitez utiliser un serveur proxy pour le chargement du fichier, cliquez sur **Configurer le proxy**. Vous pouvez demander à Scout d'utiliser les paramètres de proxy configurés pour les propriétés d'Internet de votre navigateur, ou vous pouvez spécifier l'adresse IP du serveur proxy et son numéro de port. Fermez la boîte de dialogue de proxy.
- Pour un compte Citrix Cloud, cliquez sur **Générer jeton**. Votre navigateur par défaut s'ouvre sur une page de Citrix Cloud où un jeton s'affiche. Copiez le jeton et collez-le sur la page Scout.
- Pour un compte Citrix, entrez vos informations d'identification.

Lorsque vous avez terminé, cliquez sur **Continuer**.

Étape 6 – Fournir des informations sur le chargement.

Entrez les détails de chargement :

- Le champ de nom contient le nom par défaut du fichier qui contiendra les diagnostics collectés. Il devrait convenir à la plupart des collectes, mais vous pouvez le modifier. (Si vous supprimez le nom par défaut et laissez le champ de nom vide, le nom par défaut sera utilisé.)
- Si vous le souhaitez, vous pouvez spécifier un numéro de ticket d'assistance Citrix à 8 chiffres.
- Dans le champ Description (facultatif), décrivez le problème et indiquez lorsque le problème s'est produit, le cas échéant.

Lorsque vous avez terminé, cliquez sur **Démarrer le chargement**.

Durant le chargement, la partie inférieure gauche de la page indique le pourcentage du chargement qui a été effectué. Pour annuler le chargement en cours, cliquez sur **Arrêter le chargement**.

Lorsque le chargement est terminé, l'adresse URL de son emplacement est affichée et liée. Vous pouvez suivre le lien vers l'emplacement Citrix pour afficher l'analyse du chargement, ou vous pouvez copier le lien.

Cliquez sur **Terminé** pour revenir sur la page d'ouverture de Scout.

Tracer et reproduire

La procédure Tracer et reproduire consiste à sélectionner des machines, à démarrer une trace sur ces machines, à reproduire les problèmes sur ces machines, à effectuer la collecte de diagnostics et à charger ensuite le fichier contenant les traces et la collecte vers Citrix ou à l'enregistrer localement.

Cette procédure est similaire à la procédure de collecte standard. Toutefois, elle vous permet de démarrer une trace sur les machines, puis de recréer les problèmes sur ces machines. Toutes les collectes de diagnostics incluent les informations de traçage AOT ; cette procédure ajoute des traces CDF pour faciliter la résolution des problèmes.

Étape 1 – Lancer Scout.

Depuis le menu Démarrer de la machine : **Citrix > Citrix Scout**. Sur la page d'ouverture, cliquez sur **Tracer et reproduire**.

Étape 2 – Sélectionner des machines.

La page Sélectionner des machines répertorie tous les VDA et Controller du site. Vous pouvez filtrer l'affichage par nom de machine. Sélectionnez la case à cocher en regard de chaque machine à partir de laquelle vous voulez collecter des diagnostics, puis cliquez sur **Continuer**.

Scout démarre des tests de vérification sur chaque machine que vous avez sélectionnée, s'assurant ainsi que celle-ci remplit les critères répertoriés dans Tests de vérification. En cas d'échec de la vérification pour une machine, un message est affiché dans la colonne État et la case à cocher de cette machine n'est plus sélectionnée. Vous pouvez :

- Corriger le problème, puis sélectionner de nouveau la case à cocher de la machine. Cela déclenche une nouvelle tentative de tests de vérification.

- Ignorer cette machine (laisser la case à cocher non sélectionnée). Les diagnostics et les traces ne seront pas collectés à partir de cette machine.

Lorsque les tests de vérification sont terminés, cliquez sur **Continuer**.

Étape 3 – Effectuer le traçage.

Le résumé répertorie toutes les machines à partir desquelles les traces seront collectées. Cliquez sur **Démarrer le traçage**.

Sur une ou plusieurs des machines sélectionnées, reproduisez les problèmes que vous avez rencontrés. La collecte de traces continue pendant que vous procédez. Lorsque vous avez terminé de reproduire le problème, cliquez sur **Continuer** dans Scout. Le traçage s'arrête.

Une fois que vous avez arrêté la trace, indiquez si vous avez reproduit le problème lors du traçage.

Étape 4 – Collecter des informations de diagnostics depuis les machines.

Cliquez sur **Collecte**.

Lors de la collecte :

- La colonne État indique l'état actuel de collecte pour une machine.
- Pour arrêter une collecte en cours sur une seule machine, cliquez sur **Annuler** dans la colonne Action pour cette machine.
- Pour arrêter toutes les collectes en cours, cliquez sur **Arrêter la collecte** dans le coin inférieur droit de la page. Les diagnostics à partir de machines qui ont terminé la collecte sont conservés. Pour reprendre la collecte, cliquez sur **Réessayer** dans la colonne Action pour chaque machine.
- Lorsque la collecte est terminée pour toutes les machines sélectionnées, le bouton **Arrêter la collecte** dans le coin inférieur droit devient **Continuer**.
- Si la collecte pour une machine réussit et que vous souhaitez de nouveau collecter des diagnostics à partir de cette machine, cliquez sur **Collecter de nouveau** dans la colonne Action de cette machine. La collecte plus récente remplace la version antérieure.
- Si une collecte échoue, vous pouvez cliquer sur **Réessayer** dans la colonne Action. Seules les collectes réussies sont chargées ou enregistrées.
- Une fois que la collecte est terminée pour toutes les machines sélectionnées, ne cliquez pas sur **Précédent**. Si vous cliquez sur ce bouton et confirmez l'invite, la collecte est perdue.

Lorsque la collecte est terminée, cliquez sur **Continuer**.

Étape 5 – Enregistrer ou charger la collecte.

Choisissez si vous souhaitez charger le fichier contenant les diagnostics collectés vers Citrix, ou les enregistrer sur la machine locale.

Si vous choisissez de charger le fichier maintenant, passez à l'étape 6.

Si vous choisissez d'enregistrer le fichier localement :

- La boîte de dialogue Enregistrer de Windows s'affiche. Sélectionnez l'emplacement souhaité.
- Lorsque l'enregistrement local est terminé, le nom de chemin du fichier est affiché et lié. Vous pouvez afficher le fichier. Rappel : vous pouvez charger le fichier plus tard à partir de Citrix ; consultez l'article CTX136396 pour Citrix Insight Services, ou Citrix Smart Tools.

Cliquez sur **Terminé** pour revenir sur la page d'ouverture de Scout. Vous n'avez pas besoin de suivre les autres étapes de cette procédure.

Étape 6 – Authentifiez-vous pour les chargements et spécifiez le proxy (facultatif).

Consultez la section Autorisation de chargement pour plus de détails sur ce processus.

- Si vous ne vous êtes pas déjà authentifié via Scout, passez à cette étape.
- Si vous vous êtes précédemment authentifié via Scout, le jeton d'autorisation stocké est utilisé par défaut. Si cela vous convient, choisissez cette option et cliquez sur **Continuer**. Vous n'êtes pas invité à entrer d'informations d'identification pour cette collecte ; passez à l'étape 7.
- Si vous vous êtes précédemment authentifié, mais souhaitez renouveler l'autorisation avec émission d'un nouveau jeton, cliquez sur **Changer/réautoriser** et poursuivez avec cette étape.

Choisissez si vous souhaitez utiliser les informations d'identification Citrix ou les informations d'identification Citrix Cloud pour authentifier le chargement. Cliquez sur **Continuer**. La page d'informations d'identification s'affiche uniquement si vous n'utilisez pas de jeton stocké.

Sur la page d'informations d'identification :

- Si vous souhaitez utiliser un serveur proxy pour le chargement du fichier, cliquez sur **Configurer le proxy**. Vous pouvez demander à Scout d'utiliser les paramètres de proxy configurés pour les propriétés d'Internet de votre navigateur, ou vous pouvez spécifier l'adresse IP du serveur proxy et son numéro de port. Fermez la boîte de dialogue de proxy.
- Pour un compte Citrix Cloud, cliquez sur **Générer jeton**. Votre navigateur par défaut s'ouvre sur une page de Citrix Cloud où un jeton s'affiche. Copiez le jeton et collez-le sur la page Scout.
- Pour un compte Citrix, entrez vos informations d'identification.

Lorsque vous avez terminé, cliquez sur **Continuer**.

Étape 7 – Fournir des informations sur le chargement.

Entrez les détails de chargement :

- Le champ de nom contient le nom par défaut du fichier qui contiendra les diagnostics collectés. Il devrait convenir à la plupart des collectes, mais vous pouvez le modifier. (Si vous supprimez le nom par défaut et laissez le champ de nom vide, le nom par défaut sera utilisé.)
- Si vous le souhaitez, vous pouvez spécifier un numéro de ticket d'assistance Citrix à 8 chiffres.
- Dans le champ Description (facultatif), décrivez le problème et indiquez lorsque le problème s'est produit, le cas échéant.

Lorsque vous avez terminé, cliquez sur **Démarrer le chargement**.

Durant le chargement, la partie inférieure gauche de la page indique le pourcentage du chargement qui a été effectué. Pour annuler le chargement en cours, cliquez sur **Arrêter le chargement**.

Lorsque le chargement est terminé, l'adresse URL de son emplacement est affichée et liée. Vous pouvez suivre le lien vers l'emplacement Citrix pour afficher l'analyse du chargement, ou vous pouvez copier le lien.

Cliquez sur **Terminé** pour revenir sur la page d'ouverture de Scout.

Planifier des collectes

La procédure de planification consiste à sélectionner des machines et à définir ou à annuler la planification. Les collectes planifiées sont automatiquement chargées vers Citrix. (Vous pouvez enregistrer les collectes planifiées localement à l'aide de l'interface PowerShell. Voir Citrix Call Home.)

Étape 1 – Lancer Scout.

Depuis le menu Démarrer de la machine : **Citrix > Citrix Scout**. Sur la page d'ouverture, cliquez sur **Planifier**.

Étape 2 – Sélectionner des machines.

La page Sélectionner des machines répertorie tous les VDA et Controller du site. Vous pouvez filtrer l'affichage par nom de machine.

Lorsque vous avez installé les VDA et les Controller à l'aide de l'interface graphique, vous avez eu l'option de participer au programme Call Home. Pour de plus amples informations, consultez la section Citrix Call Home. (Call Home comprend une fonctionnalité de planification équivalente à Scout.) Scout affiche ces paramètres, par défaut. Vous pouvez utiliser cette version de Scout pour démarrer les collectes planifiées pour la première fois, ou modifier une planification configurée précédemment.

N'oubliez pas que, si vous activiez/désactiviez Call Home machine par machine, la définition d'une planification dans Scout utilise les mêmes commandes, mais affecte toutes les machines que vous sélectionnez.

Sélectionnez la case à cocher en regard de chaque machine à partir de laquelle vous voulez collecter des diagnostics, puis cliquez sur **Continuer**.

Scout démarre des tests de vérification sur chaque machine que vous avez sélectionnée, s'assurant ainsi que celle-ci remplit les critères répertoriés dans Tests de vérification. En cas d'échec de la vérification pour une machine, un message est affiché dans la colonne État et la case à cocher de cette machine n'est plus sélectionnée. Vous pouvez :

- Corriger le problème, puis sélectionner de nouveau la case à cocher de la machine. Cela déclenche une nouvelle tentative de tests de vérification.
- Ignorer cette machine (laisser la case à cocher non sélectionnée). Les diagnostics (ou traces) ne seront pas collectés à partir de cette machine.

Lorsque les tests de vérification sont terminés, cliquez sur **Continuer**.

La page Résumé répertorie les machines auxquelles seront appliquées les planifications. Cliquez sur **Continuer**.

Étape 3 – Définir la planification.

Indiquez quand vous souhaitez que les diagnostics soient collectés. Rappel : la planification affecte toutes les machines sélectionnées.

- Pour configurer une planification hebdomadaire pour les machines sélectionnées, cliquez sur **Hebdomadaire**. Choisissez le jour de la semaine et entrez l'heure de la journée (horloge 24 heures) à laquelle commencera la collecte de diagnostics.
- Pour configurer une planification quotidienne pour les machines sélectionnées, cliquez sur **Quotidien**. Entrez l'heure de la journée (horloge 24 heures) à laquelle commencera la collecte de diagnostics.
- Pour annuler une planification existante pour les machines sélectionnées (et ne pas la remplacer par une autre), cliquez sur **Désactiver**. Cela annule toute planification qui a été configurée précédemment pour ces machines.

Cliquez sur **Continuer**.

Étape 4 – S'authentifier pour les chargements et spécifier le proxy (facultatif).

Consultez la section Autorisation de chargement pour plus de détails sur ce processus. Rappel : vous ne pouvez pas utiliser de jeton stocké pour vous authentifier lorsque vous travaillez avec une planification Scout.

Choisissez si vous souhaitez utiliser les informations d'identification Citrix ou les informations d'identification Citrix Cloud pour authentifier le chargement. Cliquez sur **Continuer**.

Sur la page d'informations d'identification :

- Si vous souhaitez utiliser un serveur proxy pour le chargement du fichier, cliquez sur Configurer le proxy. Vous pouvez demander à Scout d'utiliser les paramètres de proxy configurés pour les propriétés d'Internet de votre navigateur, ou vous pouvez spécifier l'adresse IP du serveur proxy et son numéro de port. Fermez la boîte de dialogue de proxy.
- Pour un compte Citrix Cloud, cliquez sur **Générer jeton**. Votre navigateur par défaut s'ouvre sur une page de Citrix Cloud où un jeton s'affiche. Copiez le jeton et collez-le sur la page Scout.
- Pour un compte Citrix, entrez vos informations d'identification.

Lorsque vous avez terminé, cliquez sur **Continuer**.

Passez en revue la planification configurée. Cliquez sur **Terminé** pour revenir sur la page d'ouverture de Scout.

Chaque collecte planifiée se produit, le journal des applications Windows de chaque machine sélectionnée contient des entrées sur la collecte et le chargement.

Analyse

February 28, 2019

Les administrateurs et le personnel d'assistance technique peuvent surveiller les sites XenApp et XenDesktop à l'aide d'un grand nombre de fonctionnalités et d'outils. À l'aide de ces outils, vous pouvez surveiller :

- les sessions utilisateur et l'utilisation des sessions ;
- les performances d'ouverture de session ;
- les connexions et les machines, y compris les échecs ;
- le calcul de charge ;
- Tendances historiques
- l'infrastructure.

Citrix Director

Director est un outil Web en temps réel que vous pouvez utiliser pour effectuer la surveillance et la résolution des problèmes, et réaliser des tâches d'assistance pour les utilisateurs finaux.

Pour de plus amples informations, veuillez consulter les articles Director.

Enregistrement de session

L'enregistrement de session vous permet d'enregistrer les activités à l'écran de toute session utilisateur, sur tout type de connexion, depuis n'importe quel serveur exécutant XenApp sous réserve du respect des stratégies d'entreprise et des exigences réglementaires. L'enregistrement de session enregistre, catalogue et archive les sessions pour en permettre la récupération et la lecture.

L'enregistrement de session utilise des stratégies flexibles pour déclencher l'enregistrement automatique des sessions d'application. Cela permet aux services informatiques de vérifier et d'examiner l'activité des utilisateurs sur les applications - par exemple pour des opérations financières ou des systèmes de gestion d'informations des patients dans un contexte médical - tout en assurant un contrôle interne dans un souci de conformité à la règlementation et de surveillance de la sécurité. De même, l'enregistrement de session facilite également le travail du support technique en accélérant l'identification et la résolution des problèmes.

Pour plus d'informations, veuillez consulter les articles Enregistrement de session.

Journalisation de la configuration

La journalisation de la configuration est une fonctionnalité qui permet aux administrateurs de garder un suivi des modifications administratives apportées à un site. La journalisation de la configuration peut aider les administrateurs à identifier et résoudre les problèmes lorsque des modifications sont apportées à la configuration, à la gestion des modifications et au suivi des modifications, et à la création d'un rapport d'activité d'administration.

Vous pouvez afficher et générer des rapports sur les informations de journalisation à partir de Studio. Vous pouvez également afficher les éléments journalisés dans Director avec l'interface Trend View pour fournir des notifications des modifications apportées à la configuration. Cette fonctionnalité est utile pour les administrateurs qui n'ont pas accès à Studio.

La vue Trend View fournit des données d'historique des modifications apportées à la configuration sur une période de temps afin que les administrateurs puissent évaluer les modifications qui ont été apportées au site, lorsqu'ils ont été générés et qui les a effectuées pour trouver la cause d'un problème. Cette vue trie les informations de configuration en trois catégories.

- Échecs de connexion
- Machines de bureau en échec
- Machines de serveur en échec

Pour de plus amples informations sur la marche à suivre pour activer et configurer la journalisation de la configuration, consultez l'article Journalisation de la configuration. Les articles Director décrivent comment afficher les informations de session à partir de cet outil.

Journaux d'événements

Les services XenApp et XenDesktop consignent les événements qui se produisent. Les journaux d'événements peuvent être utilisés pour les opérations de surveillance et de dépannage.

Pour de plus amples informations, consultez l'article Journaux d'événements. Les articles sur chaque fonctionnalité peuvent également contenir des informations sur les événements.

Enregistrement de session 7.15

February 28, 2019

L'enregistrement de session vous permet d'enregistrer les activités à l'écran de toute session utilisateur hébergée sur un VDA pour OS de serveur ou bureau, avec tout type de connexion, sous réserve du respect des stratégies d'entreprise et des exigences réglementaires. L'enregistrement de session enregistre, catalogue et archive les sessions pour en permettre la récupération et la lecture.

L'enregistrement de session utilise des stratégies flexibles pour déclencher l'enregistrement automatique des sessions d'application. Cela permet aux services informatiques de vérifier et d'examiner l'activité des utilisateurs sur les applications - par exemple pour des opérations financières ou des systèmes de gestion d'informations des patients dans un contexte médical - tout en assurant un contrôle interne dans un souci de conformité à la règlementation et de surveillance de la sécurité. De même, l'enregistrement de session facilite également le travail du support technique en accélérant l'identification et la résolution des problèmes.

Avantages

Sécurité renforcée grâce à la journalisation et à la surveillance. L'enregistrement de session permet aux organisations d'enregistrer l'activité des utilisateurs à l'écran pour les applications traitant des informations sensibles. Ceci est particulièrement important dans les secteurs réglementés tels que la santé et les finances. Dans les situations dans lesquelles les informations personnelles ne doivent pas être enregistrées, un enregistrement sélectif peut être défini à l'aide de stratégies.

Puissante surveillance des activités. L'enregistrement de session capture et met en archive les mises à jour d'écran, notamment les activités de la souris et le résultat visible de frappes clavier sur des fichiers vidéo sécurisés afin de fournir un enregistrement des activités d'utilisateurs, d'applications et de serveurs spécifiques.

L'enregistrement de session n'est pas conçu pour contribuer à la collecte de preuves en vue de poursuites judiciaires. Citrix recommande que les organisations utilisant l'enregistrement de session utilisent d'autres techniques pour la collecte de preuves, telles que des enregistrements vidéo conventionnels combinés avec des outils d'eDiscovery traditionnels.

Réduction de la durée de résolution de problèmes. Lorsque les utilisateurs appellent pour exposer un problème difficile à reproduire, le personnel de support technique peut activer les enregistrements des sessions utilisateur. Lorsque le problème se reproduit, l'enregistrement de session fournit un enregistrement visuel horodaté de l'erreur, qui peut être utilisé ensuite pour une résolution plus rapide des problèmes.

Prise en main de l'enregistrement de session

January 23, 2019

Après avoir effectué les étapes suivantes, vous pouvez commencer l'enregistrement et la vérification des sessions XenApp et XenDesktop.

1. Familiarisation avec les composants d'enregistrement de session.
2. Sélection du scénario de déploiement pour votre environnement.
3. Vérification des conditions requises pour l'installation.

4. Installation des fonctionnalités et des rôles Windows requis.
5. Installation de l'enregistrement de session.
6. Configuration des composants d'enregistrement de session pour permettre l'enregistrement et l'affichage de sessions.

L'enregistrement de session se compose de cinq composants :

- **Agent d'enregistrement de session.** Composant installé sur chaque VDA pour OS de serveur ou de bureau pour activer l'enregistrement. Il est responsable de l'enregistrement des données de session.
- **Serveur d'enregistrement de session.** Il s'agit d'un serveur hébergeant ce composant :
  - Le broker. Une application Web IIS 6.0+ hébergée qui traite les requêtes de recherche et les demandes de fichier du lecteur d'enregistrement de session, qui gère les demandes d'administration de stratégies de la console de stratégie d'enregistrement de session et qui évalue les stratégies d'enregistrement pour chaque session XenApp et XenDesktop.
  - Le gestionnaire de stockage. Service Windows qui gère les fichiers de sessions enregistrées reçues de chaque ordinateur d'enregistrement de session exécutant XenApp et XenDesktop.
  - Journalisation de l'administrateur. Sous-composant facultatif installé avec le serveur d'enregistrement de session pour consigner les activités d'administration. Toutes les données de journalisation sont stockées dans une base de données SQL Server nommée **CitrixSessionRecordingLogging**.
- **Lecteur d'enregistrement de session.** Il s'agit d'une interface utilisateur à laquelle les utilisateurs accèdent depuis une station de travail pour lire des fichiers de sessions XenApp et XenDesktop enregistrées.
- **Base de données d'enregistrement de session.** Composant qui gère la base de données SQL Server pour stocker les données de sessions enregistrées. Lorsque ce composant est installé, il crée une base de données appelée **CitrixSessionRecording**. Vous ne pouvez pas modifier le nom.
- **Console de stratégie d'enregistrement de session.** Console utilisée pour créer des stratégies afin de spécifier les sessions à enregistrer.

Illustration des composants d'enregistrement de session et des relations qu'ils ont entre eux.

Dans l'exemple de déploiement représenté par cette illustration, l'agent d'enregistrement de session, le serveur d'enregistrement de session, la base de données d'enregistrement de session, la console de stratégie d'enregistrement de session et le lecteur d'enregistrement de session résident sous la protection d'un pare-feu de sécurité. L'agent d'enregistrement de session est installé sur un VDA pour OS de serveur ou de bureau. Un second serveur héberge la console de stratégie d'enregistrement de session, un troisième remplit les fonctions de serveur d'enregistrement de session, tandis qu'un quatrième serveur héberge la base de données d'enregistrement de session. Le lecteur d'enregistrement de session est installé sur une station de travail séparée. Une machine cliente, située en-dehors

du pare-feu, communique avec le VDA pour OS de serveur sur lequel l'agent d'enregistrement de session est installé. À l'intérieur du pare-feu, l'agent d'enregistrement de session, la console de stratégie d'enregistrement de session, le lecteur d'enregistrement de session et la base de données d'enregistrement de session communiquent tous avec le serveur d'enregistrement de session.

Planifier votre déploiement

November 13, 2018

Limitations et restrictions

L'enregistrement de session ne prend pas en charge le mode d'affichage de redirection Desktop Composition (DCR). Par défaut, l'enregistrement de session désactive DCR dans une session si la session doit être enregistrée par stratégie d'enregistrement. Vous pouvez configurer ce comportement dans les propriétés de l'agent d'enregistrement de session.

En fonction de votre environnement, vous pouvez déployer les composants d'enregistrement de session selon des scénarios différents.

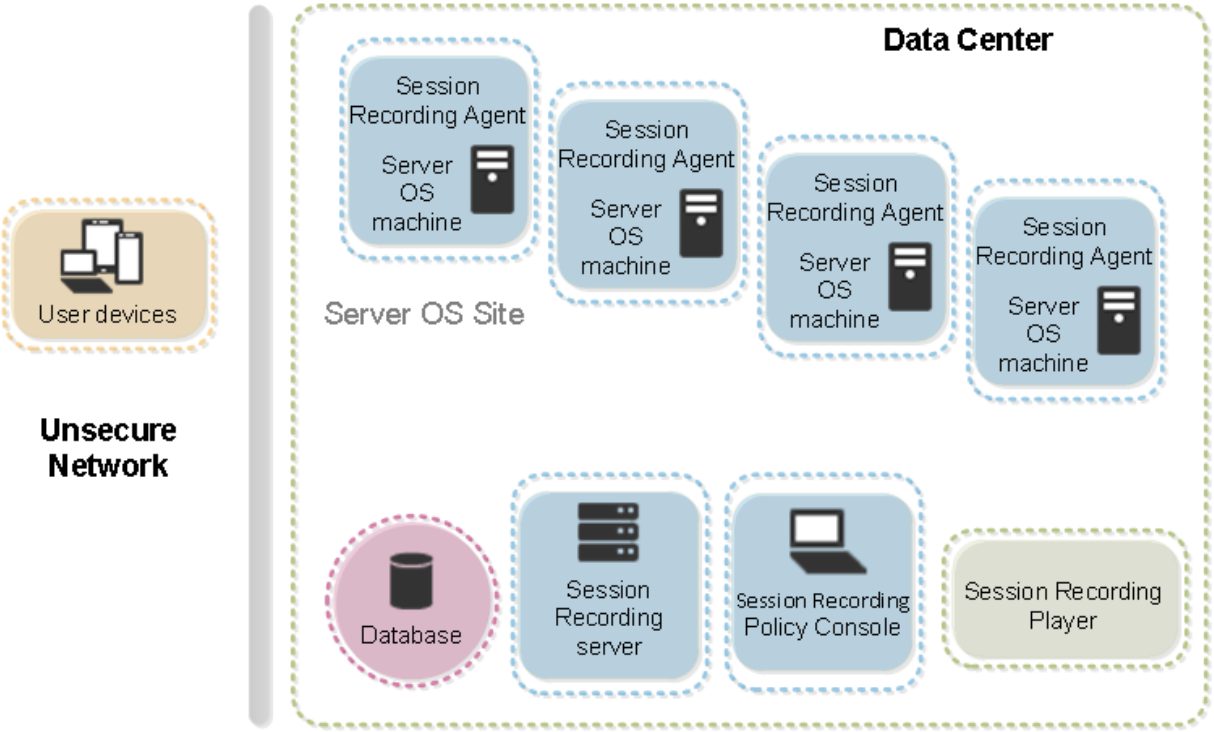
Un déploiement d'enregistrement de session ne se limite pas nécessairement à un seul site. À l'exception de l'agent d'enregistrement de session, tous les composants sont indépendants du site de serveur. Vous pouvez par exemple configurer plusieurs sites pour utiliser un serveur d'enregistrement de session unique.

De même, si vous avez un site de grande taille comptant de nombreux agents et que vous prévoyez d'enregistrer un grand nombre d'applications au graphisme intensif (applications AutoCAD par exemple), ou si vous avez un nombre élevé de sessions à enregistrer, il est possible qu'un serveur d'enregistrement de session doive répondre à des demandes de performances élevées. Pour remédier à tout problème de performance, vous pouvez installer plusieurs serveurs d'enregistrement de session sur des ordinateurs différents et orienter les agents d'enregistrement de session vers ces différents ordinateurs. Souvenez-vous qu'un Agent ne peut pointer que vers un seul serveur à la fois.

Suggestion de déploiement d'un site de serveurs

Utilisez ce type de déploiement pour l'enregistrement de sessions pour un ou plusieurs sites. L'agent d'enregistrement de session est installé sur chaque VDA pour OS de serveur dans un site. Le site réside dans un centre de données protégé par un pare-feu de sécurité. Les composants d'administration d'enregistrement de session (base de données d'enregistrement de session, serveur d'enregistrement de session et console de stratégie d'enregistrement de session) sont installés sur d'autres serveurs et le lecteur d'enregistrement de session est installé sur une station de travail, l'ensemble est protégé

par le pare-feu, mais ne se trouve pas dans le centre de données. À l'extérieur du pare-feu, dans un environnement de réseau non sécurisé, se trouvent les clients XenApp, par exemple une station de travail, un PDA et un ordinateur portable.



Remarques importantes sur le déploiement

- Pour activer les composants d'enregistrement de session de manière à ce qu'ils communiquent entre eux, veillez à les installer dans le même domaine ou sur des domaines de confiance. Le système ne peut pas être installé dans un groupe de travail ou à travers des domaines ayant une relation de confiance externe.
- En raison de sa nature graphique intensive et de l'utilisation faite de mémoire lors de la lecture des enregistrements de grande taille, Citrix déconseille d'installer le lecteur d'enregistrement de session en tant qu'application publiée.
- L'installation de l'enregistrement de session est configurée pour la communication TLS/HTTPS. Veillez à installer un certificat sur le serveur d'enregistrement de session et à ce que les composants d'enregistrement de session fassent confiance à la racine CA.
- Si vous installez la base de données d'enregistrement de session sur un serveur autonome exécutant SQL Server 2016 édition Express, SQL Server 2014 édition Express, SQL Server 2012 édition Express ou SQL Server 2008 R2 édition Express, veillez à activer le protocole TCP/IP sur le serveur et exécuter le service de navigateur SQL Server. Ces paramètres sont désactivés par défaut, mais vous devez les activer pour que le serveur d'enregistrement de session puisse communiquer avec la base de données. Pour plus d'informations sur l'activation de ces paramètres,

consultez les articles Microsoft Activer le protocole réseau TCP/IP pour SQL Server et Service de navigateur SQL Server.

- Considérez les effets du partage de session lors de la planification de votre déploiement d'enregistrement de session. Le partage de session pour les applications publiées peut entrer en conflit avec les règles de stratégie d'enregistrement de session pour les applications publiées. L'enregistrement de session fait correspondre la stratégie active à la première application publiée qu'un utilisateur ouvre. Après que l'utilisateur ouvre la première application, toute application suivante ouverte au cours de la même session continue d'observer la stratégie en vigueur pour la première application. Par exemple, si une stratégie indique que seul Outlook doit être enregistré, l'enregistrement commence lorsque l'utilisateur ouvre Outlook. Cependant, si l'utilisateur ouvre ensuite une application Microsoft Word publiée (pendant qu'Outlook est ouvert), Word est également enregistré. De la même manière, si la stratégie active n'indique pas que Word doit être enregistré, et que l'utilisateur démarre Word avant Outlook (qui devrait être enregistré, selon la stratégie), Outlook n'est pas enregistré.
- Bien que vous puissiez installer le serveur d'enregistrement de session sur un Delivery Controller, Citrix ne recommande pas de le faire en raison de problèmes de performances.
- Vous pouvez installer la console de stratégie d'enregistrement de session sur un Delivery Controller.
- Vous pouvez installer le serveur d'enregistrement de session et la console de stratégie d'enregistrement de session sur le même système.
- Assurez-vous que le nom NetBIOS du serveur d'enregistrement de session ne dépasse pas la limite de 15 caractères (Microsoft limite la longueur du nom d'hôte à 15 caractères).

Recommandations de sécurité

January 23, 2019

L'enregistrement de session est conçu pour un déploiement au sein d'un réseau sécurisé, son accès est réservé aux administrateurs et par conséquent il est lui-même sécurisé. Le déploiement prêt à l'emploi est conçu dans un souci de simplicité et les fonctionnalités de sécurité, telles que la signature et le cryptage numériques peuvent être configurés en option.

La communication entre les composants d'enregistrement de session est assurée par les Services Internet (IIS) et Microsoft Message Queuing (MSMQ). IIS fournit la liaison de communication des services Web entre chaque composant d'enregistrement de session. MSMQ fournit un mécanisme fiable de transport des données pour l'envoi des données de session de l'agent d'enregistrement de session vers le serveur d'enregistrement de session.

> **Avertissement :**
>
> Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pou-

> vant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Tenez compte des recommandations de sécurité suivantes lors de la planification de votre déploiement :

- Assurez-vous que vous isolez correctement les différents rôles administrateur dans le réseau de l'entreprise, dans le système d'enregistrement de session ou sur des machines individuelles. Sinon, vous vous exposez à des risques de sécurité qui peuvent avoir un impact sur la fonctionnalité du système ou entraîner une utilisation abusive du système. Citrix vous recommande d'attribuer des rôles d'administrateur différents à des personnes ou des comptes différents et de ne pas autoriser les utilisateurs de session à disposer de privilèges d'administrateur sur le système VDA.
  - Les administrateurs de XenApp et XenDesktop ne doivent pas accorder de rôle d'administrateur local VDA à des utilisateurs d'applications ou de bureaux publiés. Si le rôle d'administrateur local est requis, protégez les composants de l'agent d'enregistrement de session avec des mécanismes Windows ou des solutions tierces.
  - Attribuez séparément l'administrateur de base de données d'enregistrement de session et l'administrateur de stratégie d'enregistrement de session.
  - Citrix recommande de ne pas attribuer de privilèges d'administrateur VDA aux utilisateurs de sessions, particulièrement lors de l'utilisation de Remote PC Access.
  - Le compte d'administrateur local de serveur d'enregistrement de session doit être un compte à protection élevée.
  - Contrôlez l'accès aux machines installées avec le lecteur d'enregistrement de session. Si un utilisateur ne dispose pas du rôle Lecteur, n'accordez pas à cet utilisateur le rôle d'administrateur local pour une machine lecteur. Désactivez l'accès anonyme.
  - Citrix recommande d'utiliser une machine physique en tant que serveur de stockage pour l'enregistrement de session.
- L'enregistrement de session enregistre les activités graphiques des sessions sans tenir compte de la confidentialité des données. Dans certaines circonstances, des données sensibles (notamment, mais pas exclusivement, des informations d'identification d'utilisateur, des informations personnelles et des écrans de tierce partie) peuvent être enregistrées involontairement. Prenez les mesures suivantes pour éviter tout risque :
  - Désactivez l'image mémoire principale pour les VDA sauf pour un dépannage spécifique.

    Pour désactiver l'image mémoire principale :

    1. Cliquez avec le bouton droit sur **Poste de travail**, puis cliquez sur **Propriétés**.
    2. Cliquez sur l'onglet **Avancé**, puis dans la section **Démarrage et récupération**, cliquez sur **Paramètres**.

3. Sous **Écriture des informations de débogage**, sélectionnez **(aucune)**.

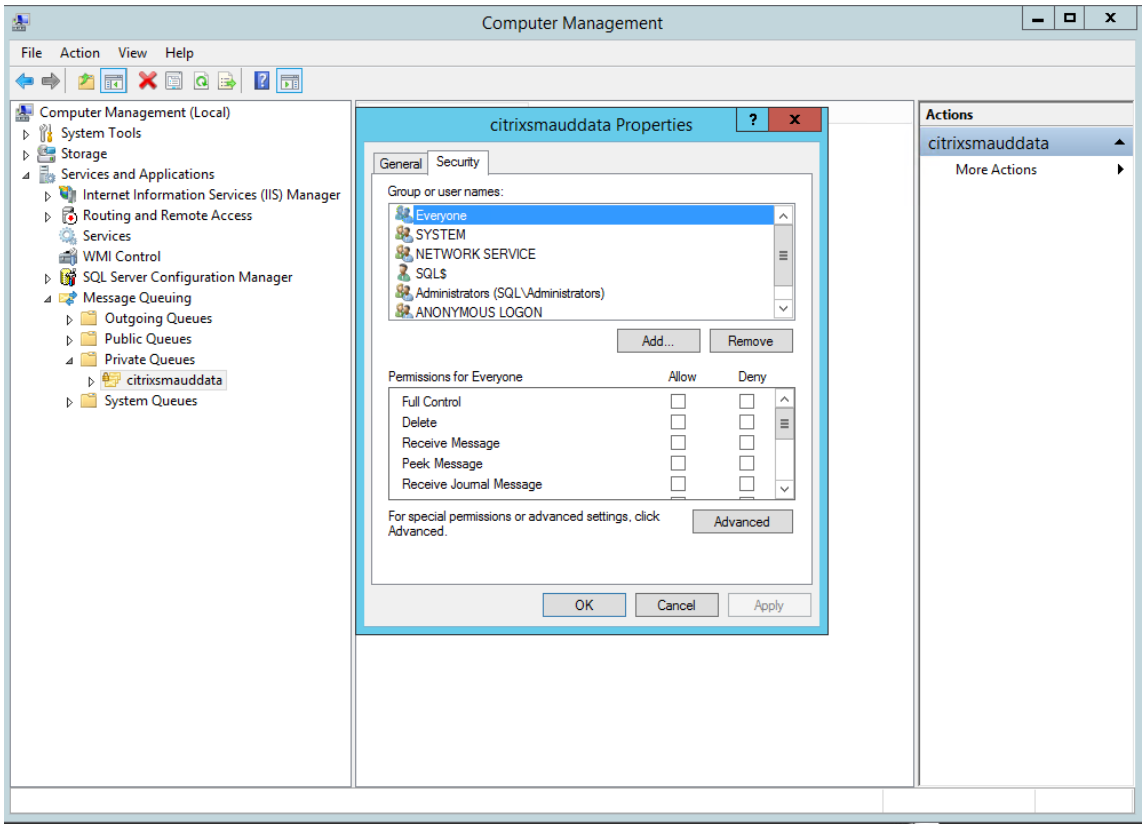
Voir l'article de Microsoft sur https://support.microsoft.com/en-us/kb/307973.

- Les propriétaires de session doivent avertir les participants que les logiciels de réunion en ligne et d'assistance à distance peuvent être enregistrés si une session de bureau est enregistrée.
- Assurez-vous que les informations d'identification d'ouverture de session ou les informations personnelles ne s'affichent pas dans les applications locales et Web publiées ou utilisées à l'intérieur de l'entreprise, sinon elles sont enregistrées par l'enregistrement de session.
- Les utilisateurs doivent fermer toutes les applications qui pourraient exposer des informations confidentielles avant de basculer vers une session ICA distante.
- Nous vous recommandons d'autoriser uniquement les méthodes d'authentification automatiques (par exemple, l'authentification unique, la carte à puce) pour accéder à des bureaux ou à des applications SaaS publiés.

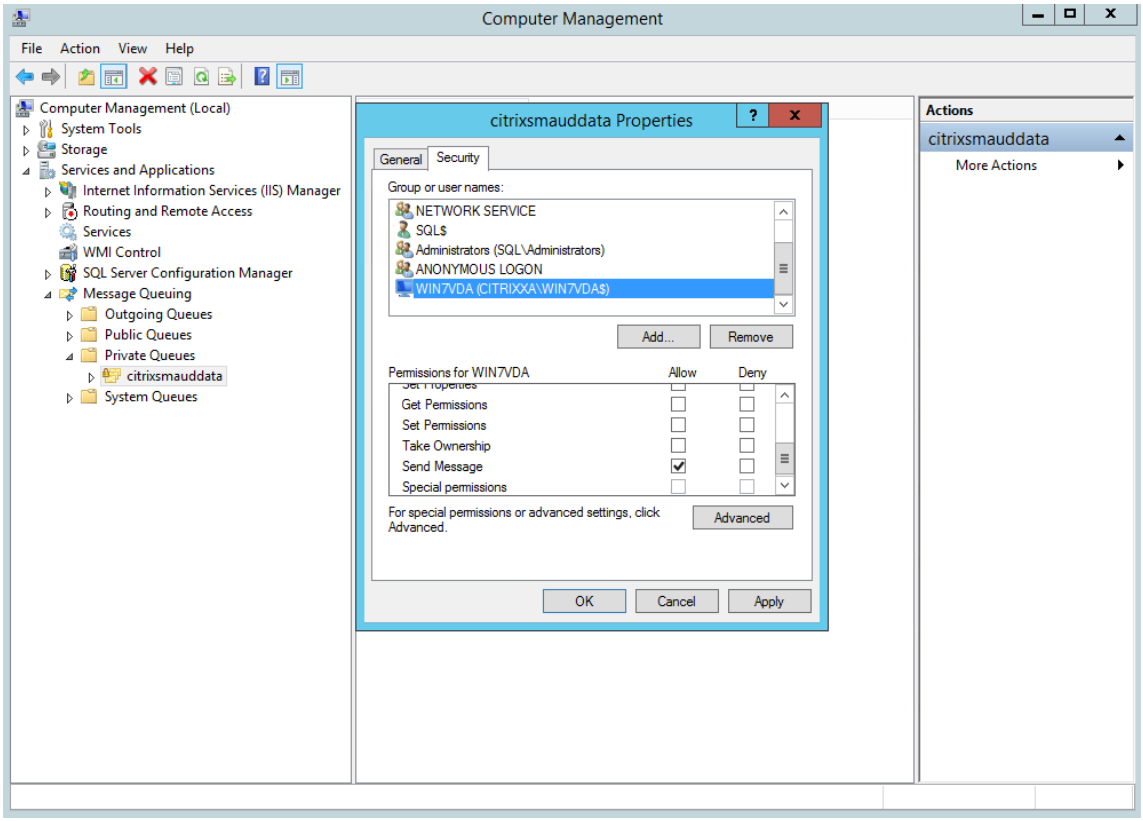
- L'enregistrement de session s'appuie sur des matériels et une infrastructure matérielle spécifiques (par exemple, des périphériques de réseau d'entreprise, un système d'exploitation) pour fonctionner correctement et pour satisfaire aux exigences en termes de sécurité. Prenez des mesures aux différents niveaux des infrastructures pour empêcher l'endommagement ou l'abus de ces infrastructures et sécuriser la fonction d'enregistrement de session.
  - Protégez correctement l'infrastructure réseau sur laquelle repose l'enregistrement de session et assurez sa disponibilité.
  - Citrix recommande d'utiliser une solution de sécurité tierce ou un mécanisme Windows pour protéger les composants d'enregistrement de session. Les composants d'enregistrement de session sont les suivants :
    * Sur le serveur d'enregistrement de session
      · Processus : SsRecStoragemanager.exe et SsRecAnalyticsService.exe
      · Services : CitrixSsRecStorageManager et CitrixSsRecAnalyticsService
      · Tous les fichiers du dossier d'installation du serveur d'enregistrement de session
      · Clés de registre dans HOTKEY_LOCAL_MACHINE\Software\Citrix\SmartAuditor\Server
    * Sur l'agent d'enregistrement de session
      · Processus : SsRecAgent.exe
      · Service : CitrixSmAudAgent
      · Tous les fichiers du dossier d'installation de l'agent d'enregistrement de session
      · Clés de registre dans HOTKEY_LOCAL_MACHINE\Software\Citrix\SmartAuditor\Agent
- Définissez la liste de contrôle d'accès (ACL) pour Message Queuing (MSMQ) sur le serveur d'enregistrement de session afin de restreindre les machines VDA ou VDI qui peuvent envoyer

des données MSMQ au serveur d'enregistrement de session et empêcher les machines non autorisées d'envoyer des données au serveur d'enregistrement de session.

1. Installez la fonctionnalité serveur Intégration du service d'annuaire sur chaque serveur d'enregistrement de session et la machine VDA ou VDI sur laquelle l'enregistrement de session est activé, puis redémarrez le service Message Queuing.
2. Dans le menu **Démarrer** de Windows sur chaque serveur d'enregistrement de session, ouvrez la fenêtre **Outils d'administration** > **Gestion de l'ordinateur**.
3. Ouvrez **Services et applications** > **Message Queuing** > **Files d'attente privées**.
4. Cliquez sur la file d'attente privée **citrixsmauddata** pour ouvrir la page **Propriétés** et sélectionnez l'onglet **Sécurité**.



5. Ajoutez les groupes d'ordinateurs ou les groupes de sécurité des VDA qui enverront des données MSMQ à ce serveur et accordez-leur l'autorisation **Envoyer un message**.



- Protégez correctement le journal d'événements du serveur d'enregistrement de session et des agents d'enregistrement de session. Nous recommandons l'utilisation d'une solution de journalisation à distance Windows ou tierce pour protéger le journal d'événements ou rediriger le journal d'événements vers le serveur distant.
- Veillez à ce que les serveurs exécutant les composants d'enregistrement de session sont physiquement sécurisés. Si possible, verrouillez ces ordinateurs dans une pièce sécurisée dont l'accès direct ne peut être accordé qu'au personnel autorisé.
- Isolez les serveurs exécutant les composants d'enregistrement de session sur un sous-réseau ou domaine séparé.
- Protégez les données de sessions enregistrées des utilisateurs accédant à d'autres serveurs en installant un pare-feu entre le serveur d'enregistrement de session et les autres serveurs.
- Actualisez fréquemment le serveur d'administration de l'enregistrement de sessions et la base de données SQL avec les dernières mises à jour de sécurité de Microsoft.
- Interdisez les non-administrateurs de se connecter à la machine d'administration.
- Limitez strictement les personnels autorisés à modifier les stratégies d'enregistrement et à afficher les sessions enregistrées.
- Installez des certificats numériques, utilisez la fonctionnalité de signature de fichiers d'enregistrement de session et paramétrez les communications TLS dans IIS.

- Configurez MSMQ pour utiliser HTTPS en tant que transport en définissant le protocole MSMQ figurant dans **Propriétés de l'agent d'enregistrement de session sur HTTPS**. Pour obtenir davantage d'informations, veuillez consulter la section Résolution des problèmes de MSMQ.
- Utilisez TLS 1.1 ou TLS 1.2 (recommandé) et désactivez SSLv2, SSLv3, TLS 1.0 sur le serveur d'enregistrement de session et la base de données d'enregistrement de session. Pour plus d'informations, veuillez consulter l'article Microsoft sur https://support.microsoft.com/default.aspx?scid=kb;en-us;187498.

  Désactivez les suites de chiffrement RC4 pour TLS sur le serveur d'enregistrement de session et la base de données d'enregistrement de session.

1. Dans l'éditeur de stratégie de groupe Microsoft, accédez à **Configuration ordinateur** > **Modèles d'administration** > **Réseau** > **Paramètres de configuration SSL**.
2. Définissez la stratégie **Ordre des suites de chiffrement SSL politique** sur **Activé**. Par défaut, cette stratégie est définie sur **Non configuré**.
3. Supprimez toutes les suites de chiffrement RC4.

- Utilisez la fonction Protection de lecture. La fonction Protection de lecture est une fonction de l'enregistrement de session qui crypte des fichiers enregistrés avant de les télécharger sur le lecteur d'enregistrement de session. Par défaut, cette option est activée et se trouve dans les **propriétés du serveur d'enregistrement de session**.
- Suivez les recommandations du NSIT pour la longueur des clés cryptographiques et les algorithmes cryptographiques.
- Configurez la prise en charge de TLS 1.2 pour l'enregistrement de session.
  - Citrix recommande TLS 1.2 comme protocole de communication pour assurer la sécurité de bout en bout des composants d'enregistrement de session.

    Pour configurer la prise en charge TLS 1.2 de l'enregistrement de session :

    1. Ouvrez une session sur l'ordinateur hébergeant le serveur d'enregistrement de session et installez le composant client et le pilote SQL Server appropriés et définissez une cryptographie forte pour .NET Framework (version 4 et ultérieure) a.
    1. Installez le pilote Microsoft ODBC 11 (ou une version ultérieure) pour SQL Server.
    2. Appliquez le dernier correctif Hotfix Rollup de .NET Framework.
    3. Installez `ADO.NET - SqlClient` en fonction de votre version de .NET Framework. Pour plus d'informations, veuillez consulter l'article https://support.microsoft.com/en-us/kb/3135244.
    4. Ajoutez une valeur DWORD SchUseStrongCrypto = 1 sous HKEY_LOCAL_MACHINE\SOFTWARE\Micr et HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NetFramework\v4.0.30319.
    5. Redémarrez l'ordinateur.

    2. Ouvrez une session sur l'ordinateur hébergeant la console de stratégie d'enregistrement de session pour appliquer le dernier Hotfix Rollup de .NET Framework et définir une cryptographie forte pour .NET Framework (version 4 et

versions ultérieures). La méthode permettant de définir une cryptographie forte est celle décrite dans les sous-étapes 1-d et 1-e. Il n'est pas nécessaire d'effectuer ces étapes si vous choisissez d'installer la console de stratégie d'enregistrement de session sur le même ordinateur que le serveur d'enregistrement de session.

Pour configurer la prise en charge TLS 1.2 de SQL Server avec les versions antérieures à 2016, consultez https://support.microsoft.com/en-us/kb/3135244. Pour utiliser TLS 1.2, configurez HTTPS comme protocole de communication pour les composants d'enregistrement de session.

Pour de plus amples informations sur la configuration des fonctionnalités de sécurité d'enregistrement de session, consultez l'article du Centre de connaissances CTX200868.

Considérations sur la capacité à monter en charge

November 13, 2018

L'installation et l'exécution de l'enregistrement de session nécessitent quelques ressources supplémentaires au-delà des éléments de base nécessaires à l'exécution de XenApp. Toutefois, si vous prévoyez d'utiliser l'enregistrement de session pour enregistrer un grand nombre de sessions ou si les sessions que vous prévoyez d'enregistrer produiront des fichiers volumineux (par exemple, des applications au graphisme intensif), tenez compte des performances de votre système dans la planification de votre déploiement d'enregistrement de session.

Pour de plus amples informations sur la création d'un système d'enregistrement de session hautement évolutif, consultez l'article CTX200869.

Recommandations matérielles

Considérez le volume de données que vous enverrez à chaque serveur d'enregistrement de session et la rapidité des délais de traitement et de stockage de ces données par les serveurs. Le taux auquel votre système peut stocker les données entrantes doit être supérieur au taux d'entrée des données.

Pour estimer votre taux d'entrée des données, multipliez le nombre de sessions enregistrées par la taille moyenne de chaque session enregistrée, puis divisez par la durée d'enregistrement des sessions. Par exemple, vous pouvez enregistrer 5 000 sessions Microsoft Outlook de 20 Mo chacune sur une durée de 8 heures par jour ouvrable. Dans ce cas, le taux d'entrée des données sera d'environ 3,5 Mo/s. (soit 5 000 sessions X 20 Mo divisés par 8 heures, divisés par 3 600 secondes/heure.).

Vous pouvez améliorer les performances globales en optimisant celles d'un seul serveur d'enregistrement de session ou en installant plusieurs serveurs d'enregistrement de session sur des machines différentes.

Disque et matériel de stockage

Le disque et le matériel de stockage sont les facteurs les plus importants à considérer dans la planification d'un déploiement d'enregistrement de session. Les performances d'écriture de votre solution de stockage est d'une importance particulière. Plus vite les données peuvent être écrites sur disques, plus élevées sont les performances du système dans son ensemble.

Les solutions de stockage convenant à une utilisation avec l'enregistrement de session comprennent une série de disques locaux contrôlés en tant que contrôleurs RAID par un contrôleur de disque local ou par un réseau dédié au stockage (SAN) connecté.

Remarque : l'enregistrement de session avec un serveur NAS (Network-Attached Storage) ne devrait pas être utilisé en raison des problèmes de performances et de sécurité liés à l'écriture des données d'enregistrement sur un lecteur réseau.

Pour une configuration de lecteur local, un contrôleur de disque avec mémoire cache intégré améliore les performances. Un contrôleur de disque de mise en cache doit posséder un dispositif de batterie de secours afin d'assurer le maintien de l'intégrité des données en cas de coupure de courant.

Capacité du réseau

Une liaison réseau de 100 Mbps convient aux connexions à un serveur d'enregistrement de session. Une connexion Ethernet en giga-octets peut améliorer les performances, mais ne se traduira pas par des performances de dix fois supérieures à une liaison 100 Mbps.

Veillez à ce que les commutateurs réseau utilisés par l'enregistrement de session ne soient pas partagés avec des applications tierces qui pourraient lui disputer la bande passante réseau disponible. Dans le meilleur des cas, les commutateurs réseau sont dédiés au serveur d'enregistrement de session.

Capacité de traitement de l'ordinateur

Tenez compte des spécifications suivantes pour l'ordinateur sur lequel un serveur d'enregistrement de session est installé :

- UC double ou UC dual-core recommandée.
- 4 Go de RAM recommandés

Le dépassement de ces spécifications ne produit pas de gains significatifs en performance.

Déployer plusieurs serveurs d'enregistrement de session

Si un seul serveur d'enregistrement de session ne correspond pas à vos besoins en matière de performances, vous pouvez en installer plusieurs, sur des ordinateurs différents. Pour ce type de déploiement, chaque serveur d'enregistrement de session dispose de son propre stockage, de ses propres commutateurs réseau et de sa propre base de données. Pour répartir la charge, pointez les agents d'enregistrement de session de votre déploiement vers différents serveurs d'enregistrement de session.

Capacité à monter en charge de la base de données

La base de données d'enregistrement de session nécessite Microsoft SQL Server 2016, Microsoft SQL Server 2014, Microsoft SQL Server 2012, ou Microsoft SQL Server 2008 R2. Le volume de données envoyées à la base de données est minime car celle-ci ne stocke que les métadonnées sur les sessions enregistrées. Pour leur part, les fichiers des sessions enregistrées sont inscrits sur un autre disque. Généralement, chaque session enregistrée ne nécessite qu'environ 1 Ko d'espace dans la base de données, à moins que l'API d'événements de l'enregistrement de session soit utilisé pour insérer des événements avec possibilité de recherche dans la session.

Les éditions Express de Microsoft SQL Server 2016, Microsoft SQL Server 2014, Microsoft SQL Server 2012 et Microsoft SQL Server 2008 R2 imposent une limite de taille de base de données de 10 Go. À 1 Ko par session d'enregistrement, la base de données peut cataloguer environ quatre millions de sessions. D'autres éditions de Microsoft SQL Server n'ont pas de restrictions de taille de base de données et ne sont limitées que par la quantité d'espace disque disponible. À mesure que le nombre de sessions augmente dans la base de données, les performances de la base de données et la vitesse des recherches ne diminuent que faiblement.

Si vous ne faites pas de personnalisations par le biais de l'API d'événements de l'enregistrement de session, chaque session enregistrée génère quatre transactions sur la base de données : deux au démarrage de l'enregistrement, une lorsque l'utilisateur se connecte aux sessions actuellement enregistrées et une à l'arrêt de l'enregistrement. Si vous utilisez l'API d'événements de l'enregistrement de session pour personnaliser des sessions, chaque événement avec possibilité de recherche enregistré génère une transaction. Puisque même le déploiement de base de données le plus élémentaire est en mesure de traiter des centaines de transactions par seconde, la charge de traitement sur la base de données n'est pas considérée comme étant excessivement sollicitée. L'impact est assez minime pour que la base de données d'enregistrement de session puisse s'exécuter sur le même serveur SQL que d'autres bases de données, notamment la base de données du magasin central de XenApp ou XenDesktop.

Si votre déploiement d'enregistrement de session nécessite de cataloguer plusieurs millions de sessions enregistrées dans la base de données, suivez les consignes de Microsoft pour la montée en charge de SQL Server.

Installer, mettre à niveau et désinstaller un enregistrement de session

February 28, 2019

Ce chapitre décrit en détail comment installer Enregistrement de session en utilisant le programme d'installation de XenApp/XenDesktop. Il contient les sections suivantes :

Check-list d'installation

À compter de la version 7.14, vous pouvez installer les composants d'enregistrement de session en utilisant le programme d'installation de XenApp/XenDesktop.

Avant de commencer l'installation, effectuez les tâches de cette liste :

☒	Étape
	Sélectionnez les ordinateurs sur lesquels vous souhaitez installer chaque composant d'enregistrement de session et veillez à ce que chaque ordinateur soit conforme aux configurations matérielles et logicielles requises correspondant au(x) composant(s) à y installer.
	Utilisez vos informations d'identification de compte Citrix pour accéder à la page de téléchargement de XenApp et XenDesktop et télécharger le fichier ISO du produit. Décompressez le fichier ISO ou gravez un DVD de ce dernier.

☒	Étape
	Pour utiliser le protocole TLS pour les communications entre les composants de l'enregistrement de session, installez les certificats corrects dans votre environnement.
	Installez toute correction requise pour les composants de l'enregistrement de session. Les corrections sont disponibles auprès du support de Citrix.
	Configurez Director pour créer et activer des stratégies d'enregistrement de session. Pour de plus amples informations, consultez Configurer Director pour utiliser le serveur d'enregistrement de session.

Remarque :

- Citrix recommande de séparer les applications publiées dans des groupes de mise à disposition distincts en fonction de vos stratégies d'enregistrement car le partage de session pour les applications publiées peut entrer en conflit avec des stratégies actives si elles se trouvent dans le même groupe de mise à disposition. L'enregistrement de session fait correspondre la stratégie active à la première application publiée qu'un utilisateur ouvre.
- Si vous prévoyez d'utiliser Machine Creation Services (MCS) ou Provisioning Services, préparez une QMId unique. Si vous ne respectez pas cette consigne, des données d'enregistrement peuvent être perdues.
- SQL Server requiert que TCP/IP soit activé, que le service SQL Server Browser soit exécuté et que l'authentification Windows soit utilisée.
- Pour utiliser HTTPS, configurez des certificats de serveur pour TLS/HTTPS.
- Assurez-vous que les utilisateurs sous **Utilisateurs et groupes locaux** > **Groupes** > **Utilisateurs** ont un accès en écriture au dossier C:\windows\Temp.

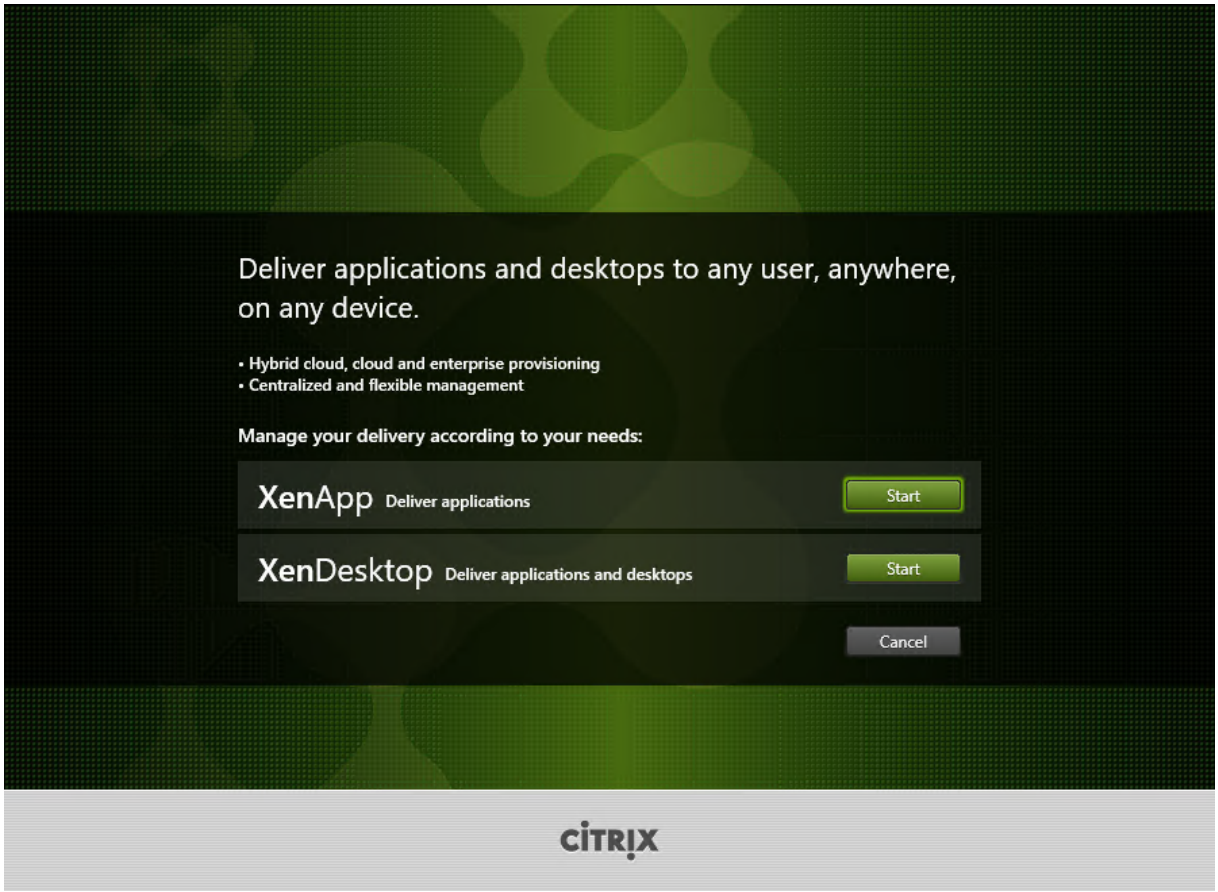
Installer les composants de l'administration de l'enregistrement de session

Citrix vous recommande d'installer les composants Administration de l'enregistrement de session, Agent d'enregistrement de session et Lecteur d'enregistrement de session sur des serveurs distincts. Les composants de l'administration de l'enregistrement de session sont les suivants : base de données d'enregistrement de session, serveur d'enregistrement de session et console de stratégie d'enregistrement de session. Vous pouvez choisir lequel de ces composants installer sur un serveur.

Étape 1 : Télécharger le logiciel du produit et démarrer l'assistant

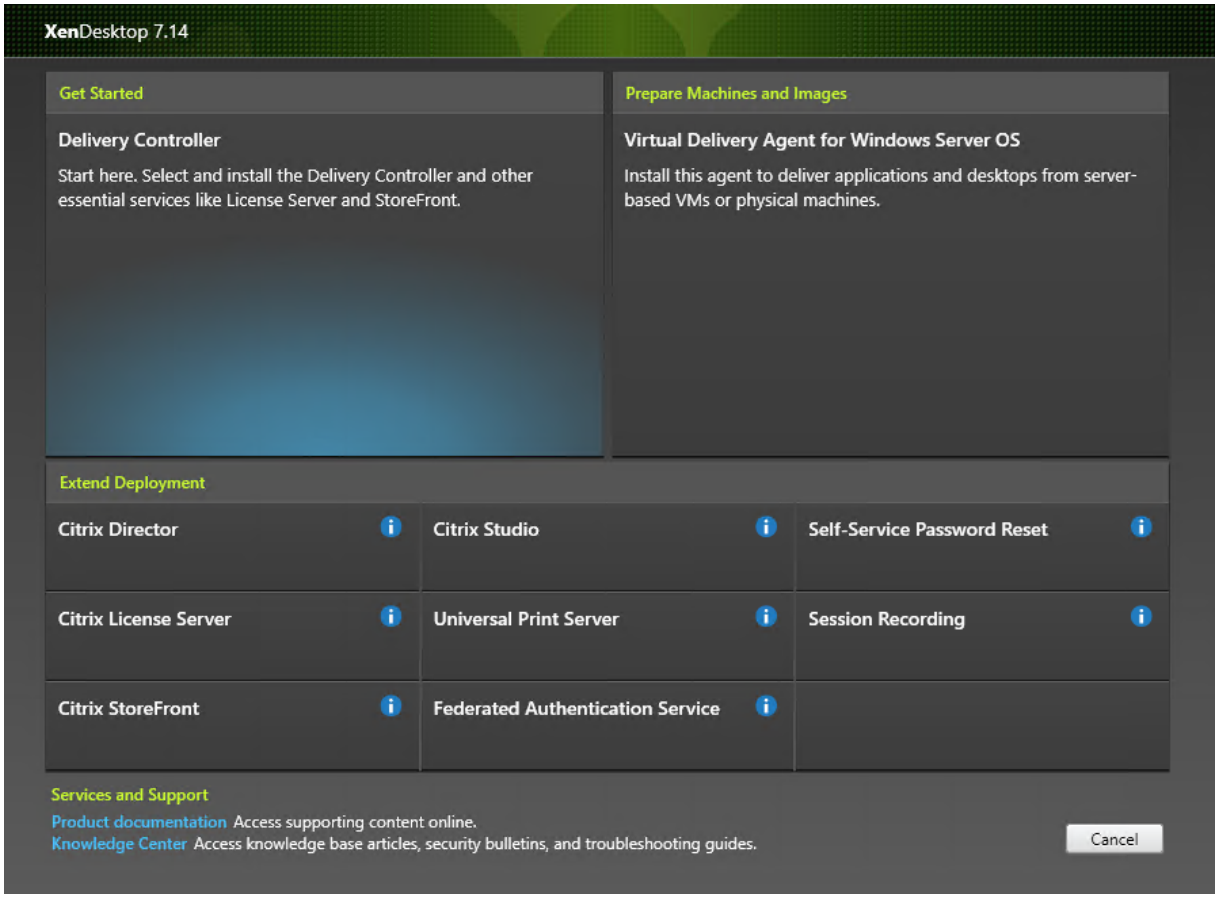
1. Si vous n'avez pas encore téléchargé le fichier ISO de XenApp et XenDesktop, utilisez vos informations d'identification de compte Citrix pour accéder à la page de téléchargement de XenApp et XenDesktop et télécharger le fichier ISO du produit. Décompressez le fichier ISO ou gravez un DVD de ce dernier.
2. Utilisez un compte d'administrateur local pour ouvrir une session sur la machine sur laquelle vous installez Administration de l'enregistrement de session. Insérez le DVD dans le lecteur ou montez le fichier ISO. Si le programme d'installation ne se lance pas automatiquement, double-cliquez sur l'application **AutoSelect** ou sur le lecteur monté.
   L'assistant d'installation démarre.

Étape 2 : Choisir le produit à installer



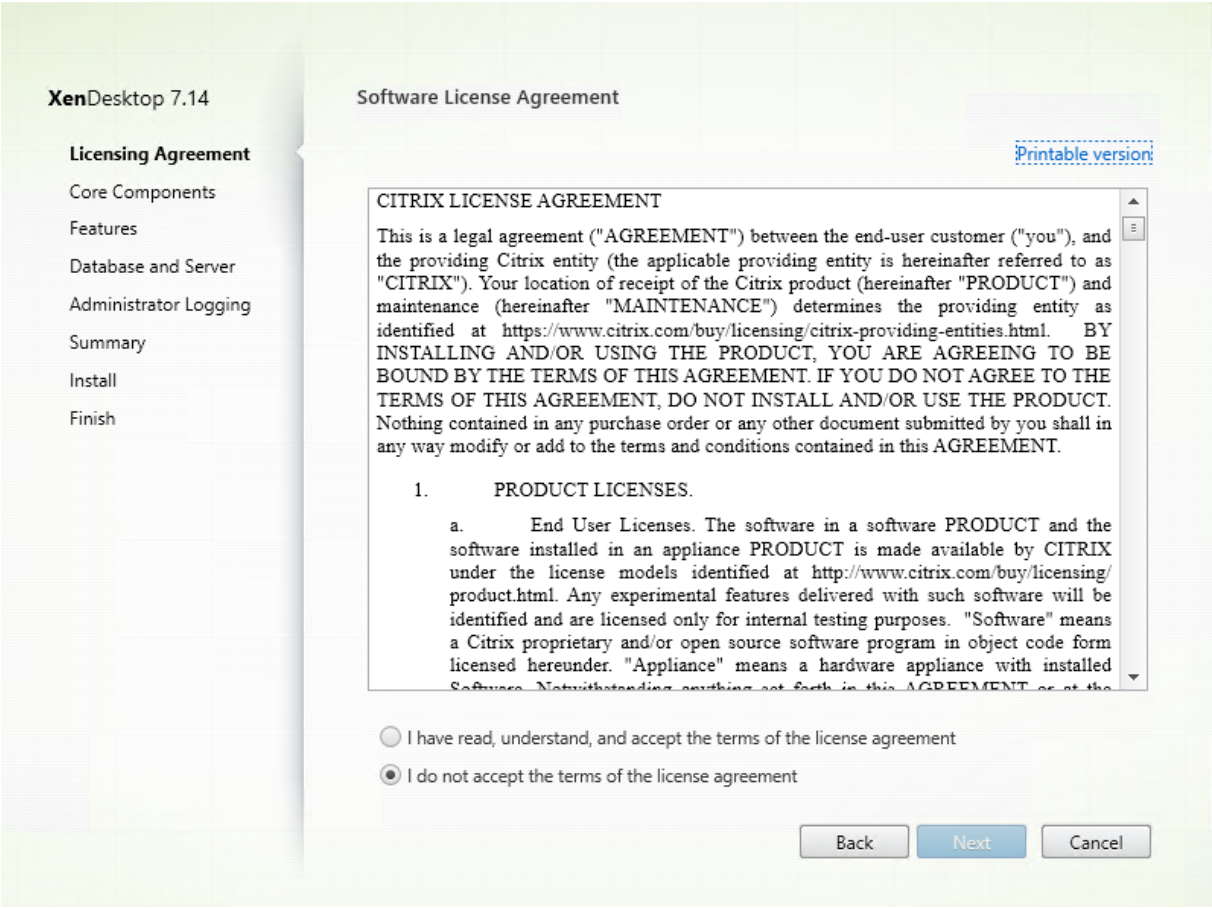
Cliquez sur **Démarrer** en regard du produit à installer : **XenApp** ou **XenDesktop**.

Étape 3 : Sélectionner Enregistrement de session



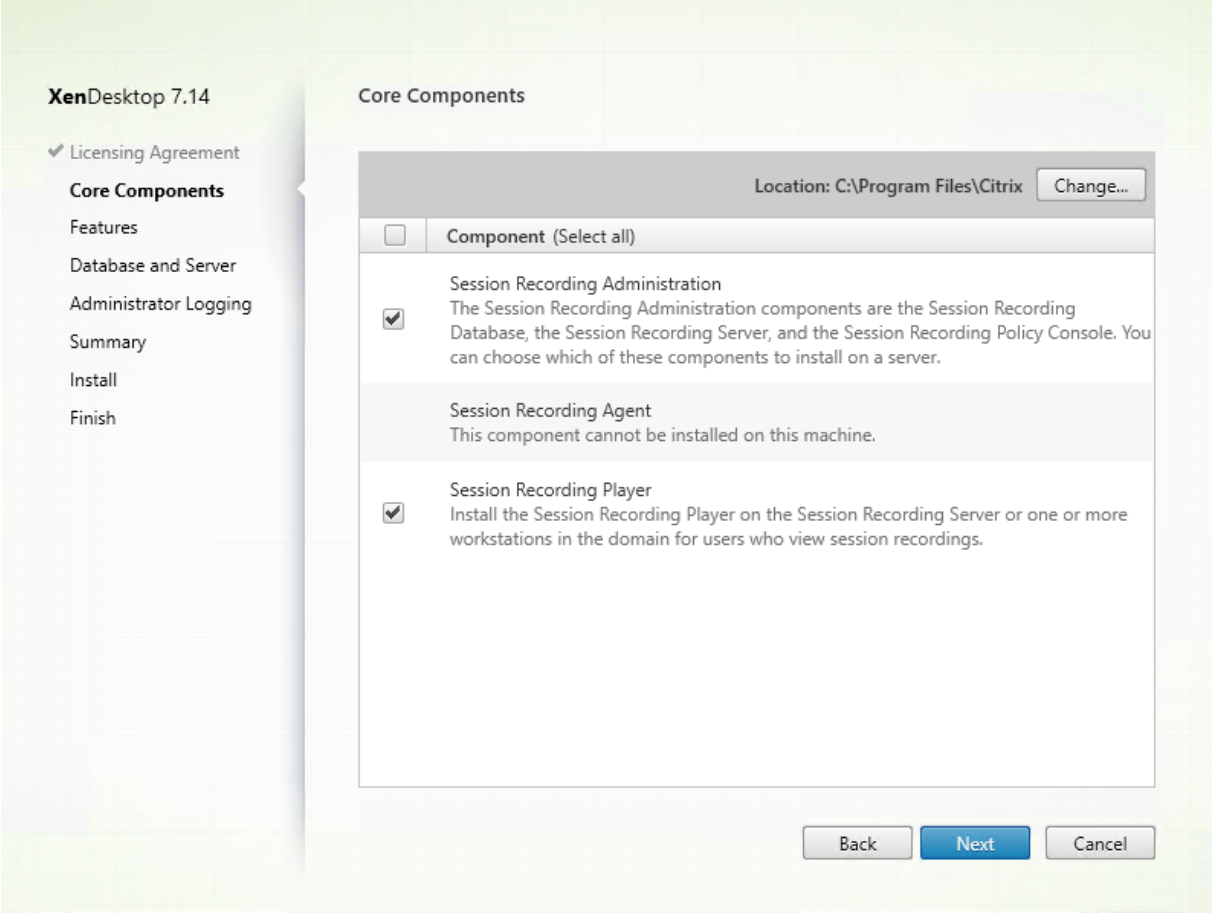
Sélectionnez l'entrée **Enregistrement de session**.

Étape 4 : Lire puis accepter le contrat de licence



Sur la page **Contrat de licence du logiciel**, lisez le contrat, acceptez-le, puis cliquez sur **Suivant**.

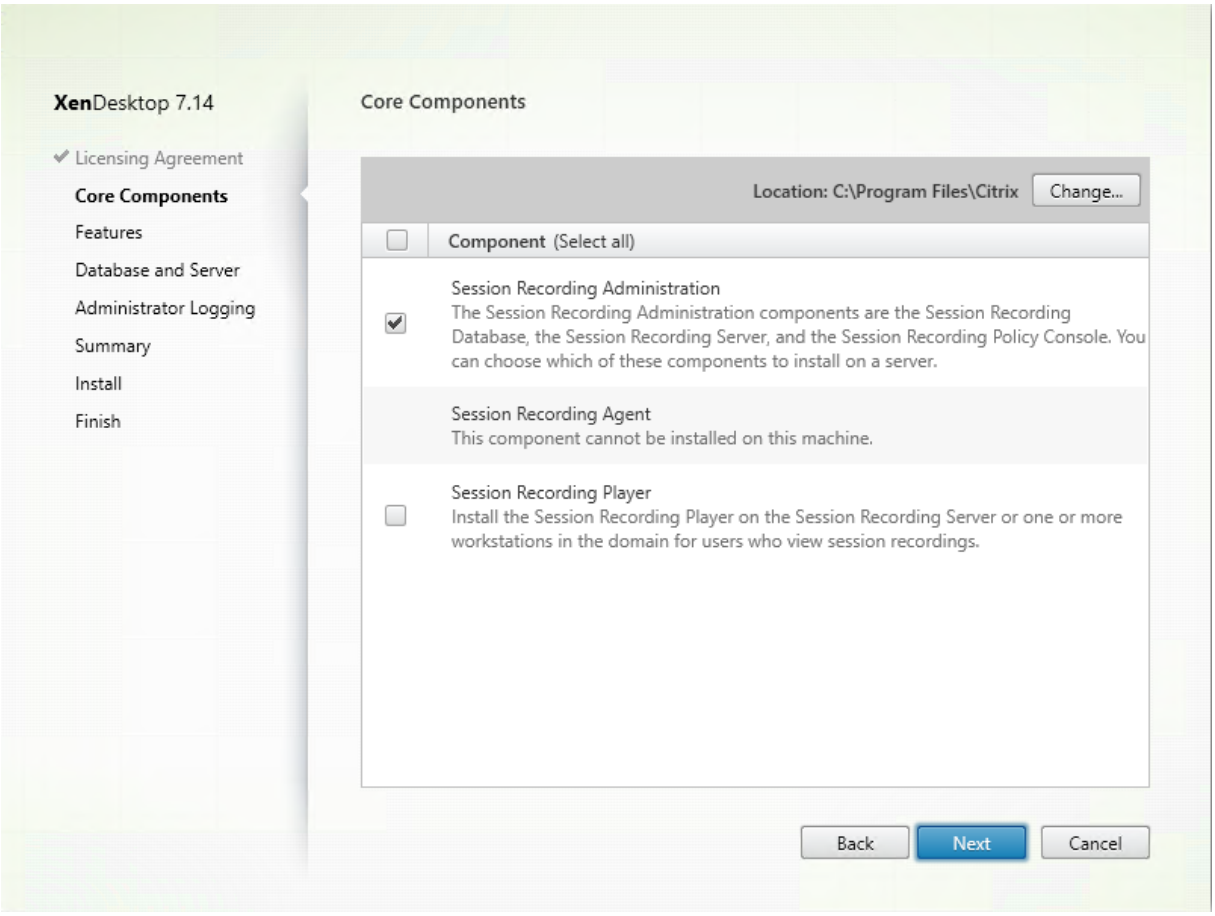
Étape 5 : Sélectionner les composants à installer et l'emplacement d'installation



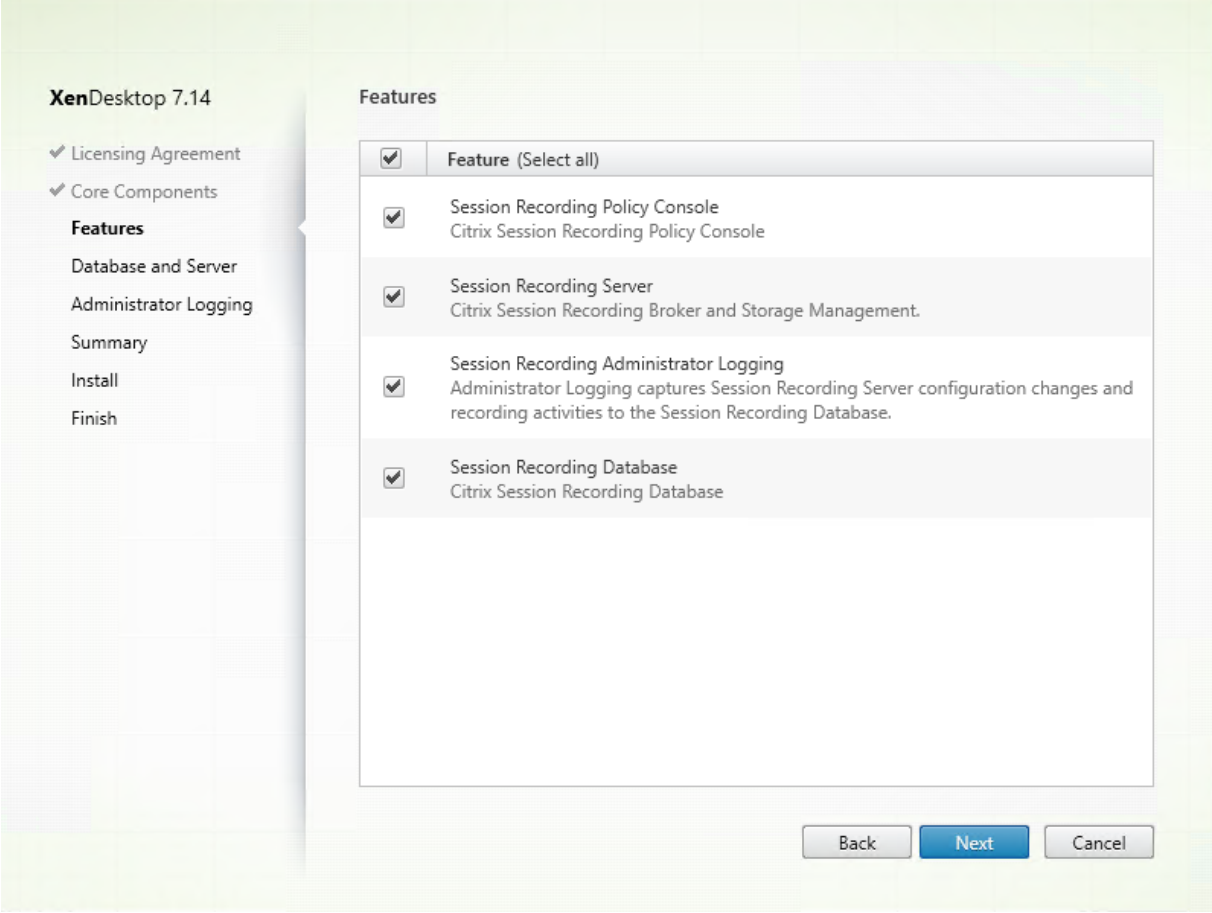
Sur la page **Composants principaux** :

- **Emplacement :** par défaut, les composants sont installés dans C:\Program Files\Citrix. L'emplacement par défaut fonctionne pour la plupart des déploiements. Vous pouvez spécifier un emplacement d'installation personnalisé.
- **Composant :** par défaut, toutes les cases à cocher en regard des composants qui peuvent être installés sont sélectionnées. Le programme d'installation sait s'il s'exécute sur un OS de bureau ou un OS de serveur. Il permet aux composants d'Administration de l'enregistrement de session d'être installés sur un OS de serveur uniquement, et n'autorise pas l'Agent d'enregistrement de session à être installé sur une machine sur laquelle aucun VDA n'est déjà installé. Si vous installez l'Agent d'enregistrement de session sur une machine qui ne dispose d'aucun VDA, l'option **Agent d'enregistrement de session** n'est pas disponible.

Sélectionnez **Administration de l'enregistrement de session** et cliquez sur **Suivant**.



Étape 6 : Sélectionner les fonctionnalités à installer



Sur la page **Fonctionnalités** :

- Par défaut, toutes les cases à cocher en regard des fonctionnalités qui peuvent être installées sont sélectionnées. L'installation de toutes ces fonctionnalités sur un seul serveur convient pour une preuve de concept. Toutefois, pour un environnement de production de grande taille, Citrix vous recommande d'installer la Console de stratégie d'enregistrement de session sur un serveur distinct et les composants Serveur d'enregistrement de session, Journalisation de l'Administrateur d'enregistrement de session et Base de données d'enregistrement de session sur un autre serveur. Veuillez noter que la journalisation de l'administrateur d'enregistrement de session est un sous-composant facultatif du serveur d'enregistrement de session. Vous devez sélectionner le serveur d'enregistrement de session avant de pouvoir sélectionner la journalisation de l'administrateur d'enregistrement de session.
- Pour ajouter une autre fonctionnalité sur le même serveur une fois que vous y avez sélectionné et installé une ou plusieurs fonctionnalités, vous pouvez uniquement exécuter le package msi mais vous ne pouvez pas à nouveau exécuter le programme d'installation.

Sélectionnez la ou les fonctionnalités que vous souhaitez installer et cliquez sur **Suivant**.

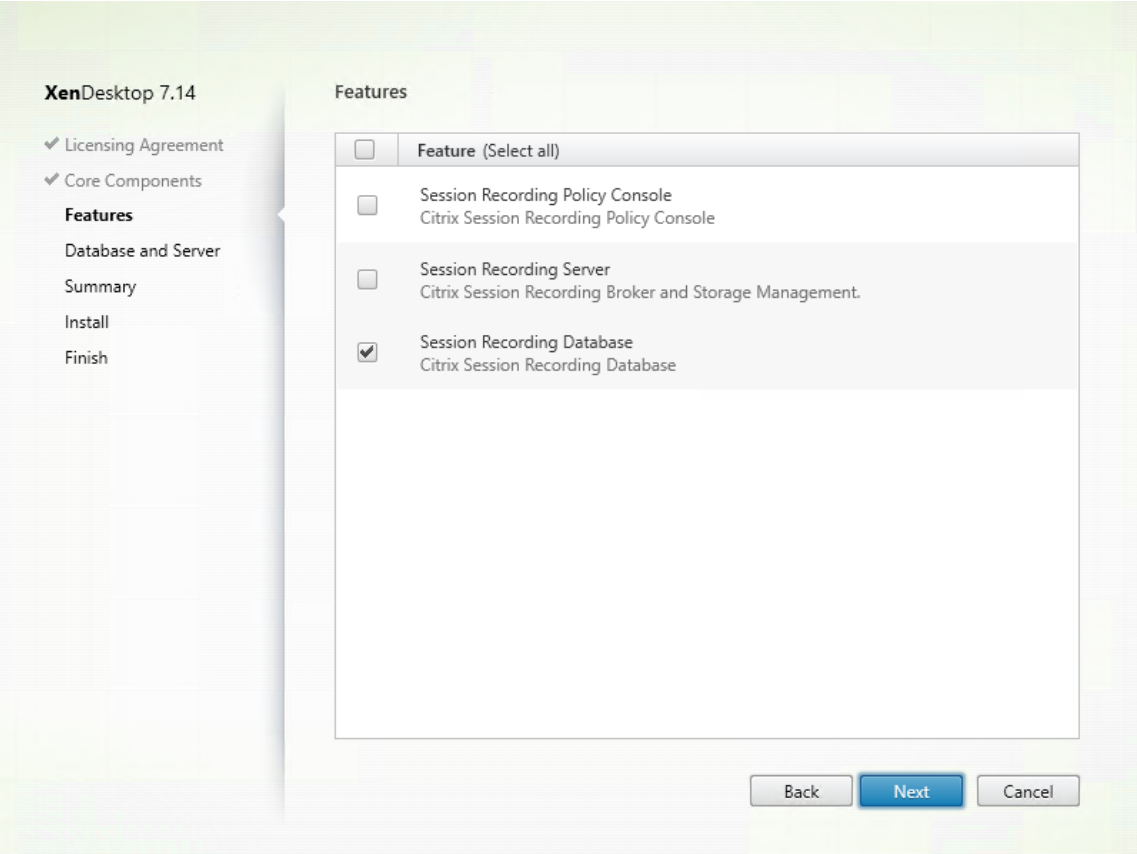
Étape 6.1 : Installer la base de données d'enregistrement de session

Remarque : la base de données d'enregistrement de session n'est pas une véritable base de données. Elle est le composant responsable de la création et de la configuration des bases de données requises dans l'instance Microsoft SQL Server au cours de l'installation. L'enregistrement de session prend en charge trois solutions pour la haute disponibilité de base de données basée sur Microsoft SQL Server. Pour plus d'informations, consultez la section Installer l'enregistrement de session avec une haute disponibilité de base de données.

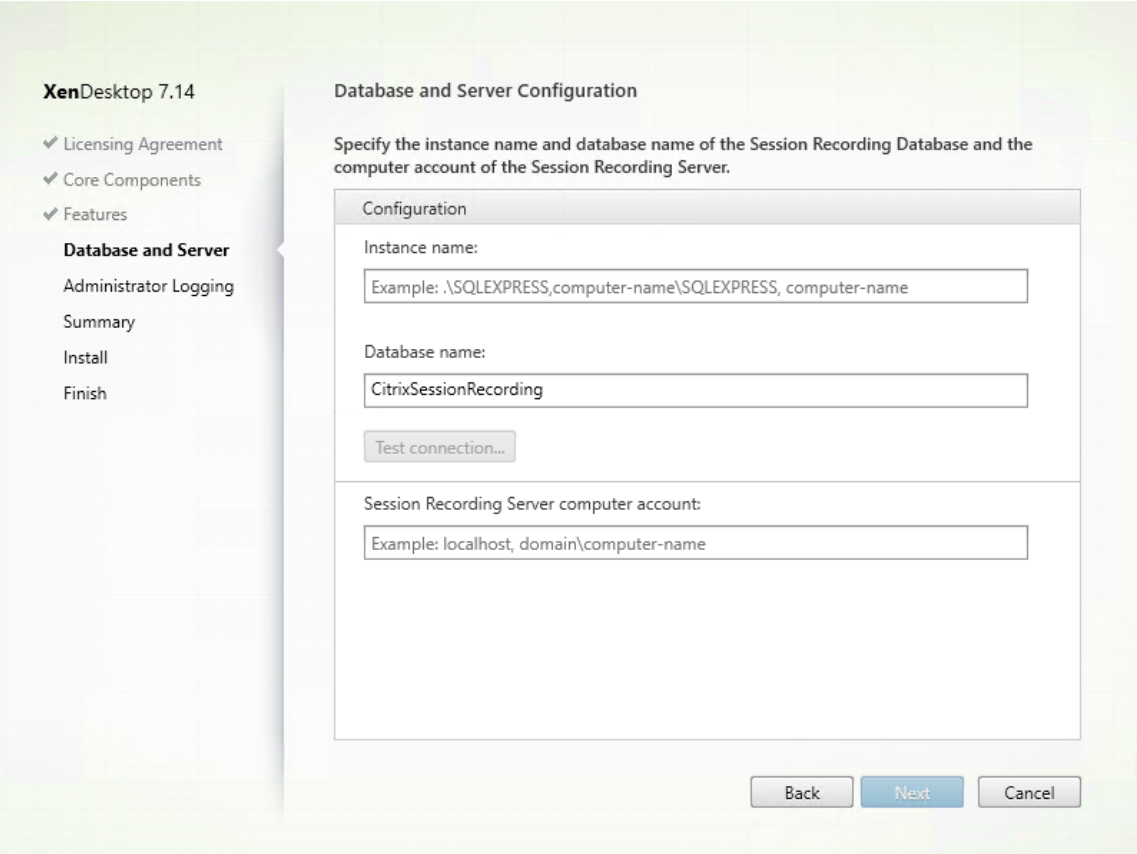
Il existe généralement trois types de déploiement pour Base de données d'enregistrement de session et Microsoft SQL Server :

- Déploiement 1 : Installer le serveur d'enregistrement de session et la base de données d'enregistrement de session sur la même machine et la base de données Microsoft SQL Server sur une machine distante. (**Recommandé**)
- Déploiement 2 : Installer le serveur d'enregistrement de session, la base de données d'enregistrement de session et la base de données Microsoft SQL Server sur la même machine.
- Déploiement 3 : Installer le serveur d'enregistrement de session sur une machine et installer la base de données d'enregistrement de session et Microsoft SQL Server sur une autre machine. (**Non recommandé**).

1. Sur la page **Fonctionnalités**, sélectionnez **Base de données d'enregistrement de session** et cliquez sur **Suivant**.



2. Sur la page **Configuration de la base de données et du serveur**, spécifiez le nom de l'instance et le nom de la base de données de la base de données d'enregistrement de session et le compte d'ordinateur du serveur d'enregistrement de session. Cliquez sur **Next**.



Sur la page **Configuration de la base de données et du serveur** :

- **Nom de l'instance :** si l'instance de base de données n'est pas une instance nommée comme configuré lors de la configuration de l'instance, vous pouvez uniquement utiliser le nom de l'ordinateur du serveur SQL Server. Si vous avez nommé l'instance, utilisez nom-ordinateur\nom-instance comme nom d'instance de la base de données. Pour déterminer le nom de l'instance du serveur que vous utilisez, exécutez **select @@servername** sur SQL Server. La valeur renvoyée est le nom exact de l'instance de base de données. Si votre serveur SQL est configuré pour écouter un port personnalisé (autre que le port par défaut 1433), définissez le port d'écoute personnalisé en ajoutant une virgule au nom de l'instance. Par exemple, tapez **DXSBC-SRD-1,2433** dans la zone de texte **Nom de l'instance**, où 2433, après la virgule, indique le port d'écoute personnalisé.
- **Nom de la base de données :** entrez un nom de base de données personnalisé dans la zone de texte **Nom de la base de données** ou utilisez le nom de base de données par défaut en sélectionnant Utiliser le nom par défaut de la base de données. Cliquez sur **Tester la connexion** pour tester la connectivité avec l'instance de SQL Server et la validité du nom de base de données.

> **Important :**
>
> Un nom de base de données personnalisé doit contenir uniquement les caractères A-Z, a-z

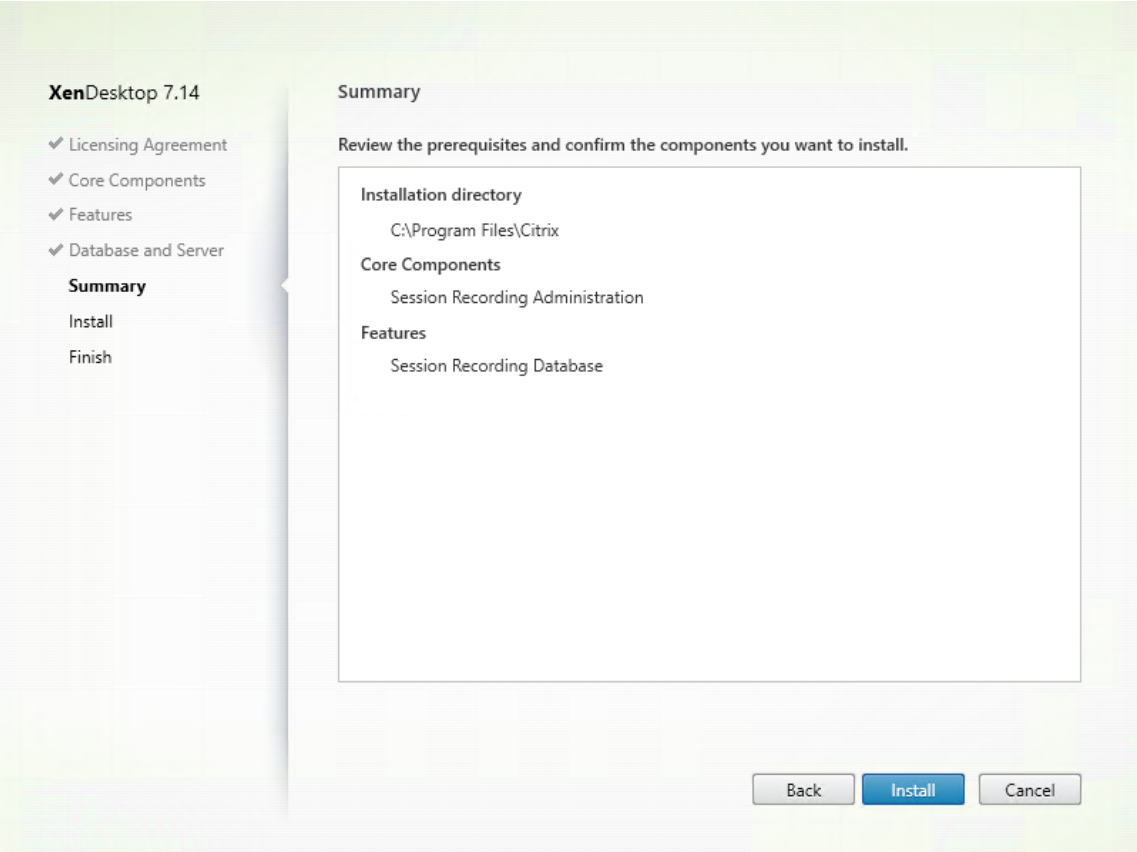
> et les chiffres 0-9 et ne doit pas dépasser 123 caractères.

- Vous devez disposer des autorisations de rôle de serveur **securityadmin** et **dbcreator** sur la base de données. Si vous ne disposez pas des autorisations, vous pouvez :
  - Demander à l'administrateur de base de données d'attribuer les permissions pour l'installation. Une fois l'installation terminée, les autorisations de rôle de serveur **securityadmin** et **dbcreator** ne sont plus nécessaires et peuvent être supprimées.
  - Ou, utiliser le pack SessionRecordingAdministrationx64.msi (décompressez le fichier ISO, et vous trouverez ce pack msi sous …\x64\Session Recording). Durant l'installation msi, une boîte de dialogue s'affiche, demandant les informations d'identification d'un administrateur de base de données avec les autorisations de rôle de serveur **securityadmin** et **dbcreator**. Entrez les informations d'identification correctes et cliquez sur **OK** pour continuer l'installation.

    L'installation crée la nouvelle base de données d'enregistrement de session et ajoute le compte de machine du serveur d'enregistrement de session en tant que **db_owner**.
- **Compte d'ordinateur du serveur d'enregistrement de session :**
  - **Déploiements 1 et 2 :** entrez la valeur **localhost** dans le champ **Compte d'ordinateur du serveur d'enregistrement de session**.
  - **Déploiement 3 :** entrez le nom de l'ordinateur hébergeant le serveur d'enregistrement de session dans le format domaine\nom-ordinateur. Le compte d'ordinateur du serveur d'enregistrement de session est le compte utilisateur utilisé pour accéder à la base de données d'enregistrement de session.

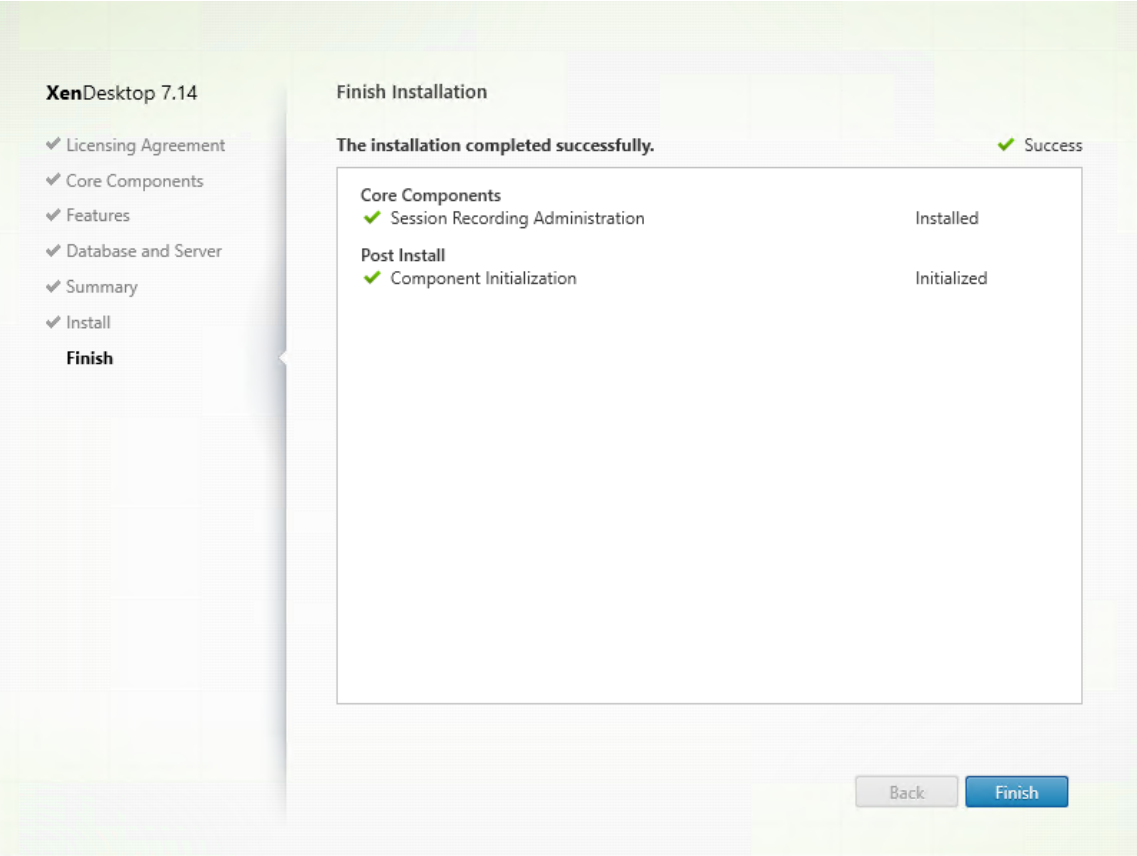
  Remarque : les tentatives d'installation des composants d'Administration de l'enregistrement de session peuvent échouer avec le code d'erreur 1603 lorsqu'un nom de domaine est défini dans le champ **Compte d'ordinateur du Serveur d'enregistrement de session**. Pour contourner le problème, tapez **localhost** ou le nom de domaine NetBIOS\nom de machine dans le champ **Compte d'ordinateur du Serveur d'enregistrement de session**.

3. Vérifiez les composants requis et confirmez l'installation.



La page **Résumé** affiche vos choix d'installation. Vous pouvez cliquer sur le bouton **Précédent** pour revenir sur les pages précédentes de l'assistant et apporter des modifications. Ou, cliquez sur **Installer** pour démarrer l'installation.

4. Terminez l'installation.

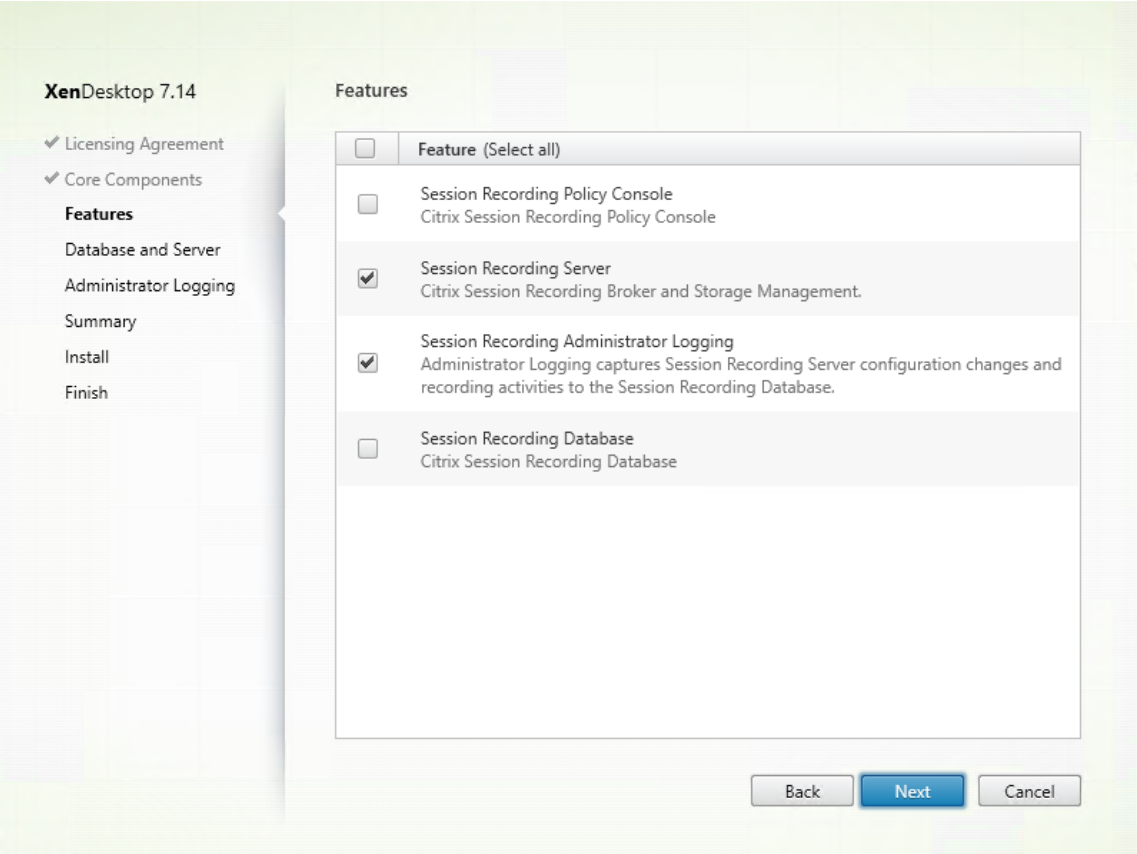


La page **Fin de l'installation** affiche des coches vertes pour tous les éléments pré-requis et composants installés et initialisés avec succès.

Cliquez sur **Terminer** pour terminer l'installation de la base de données d'enregistrement de session.

Étape 6.2 : Installer le serveur d'enregistrement de session

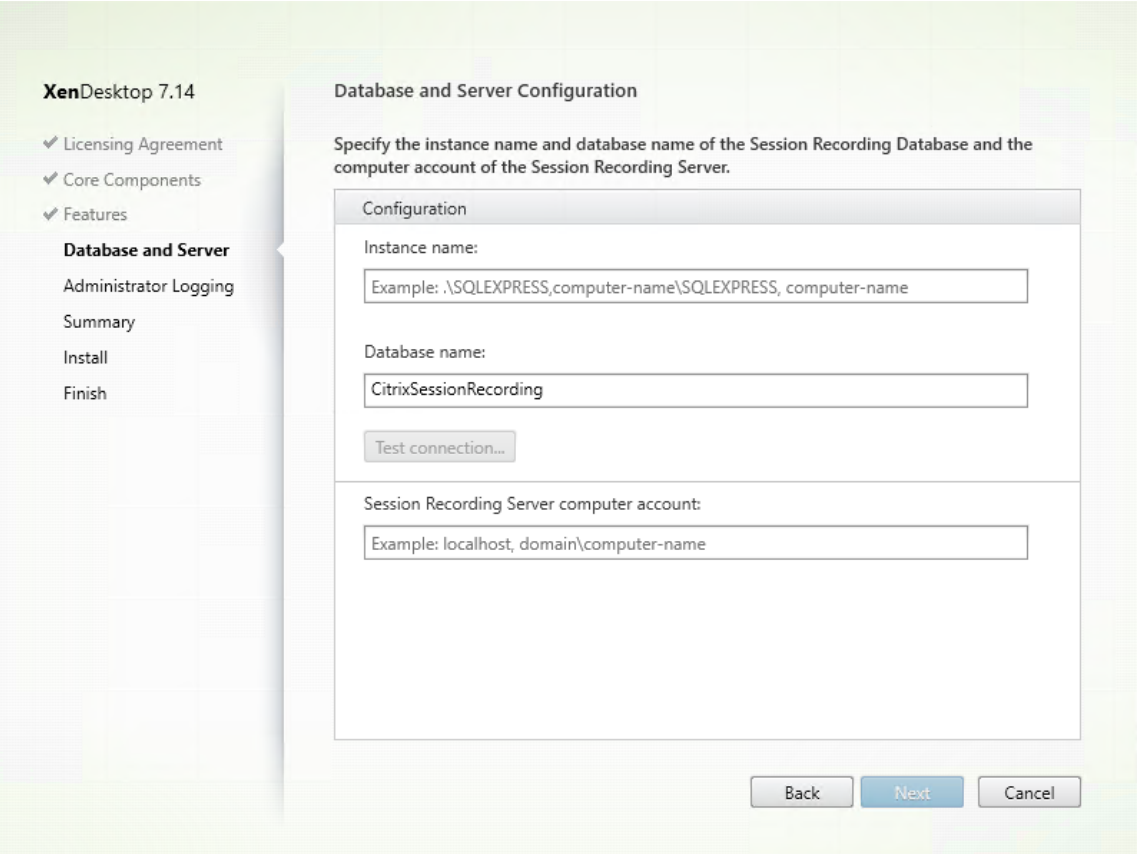
1. Sur la page **Fonctionnalités**, sélectionnez **Serveur d'enregistrement de session** et **Journalisation de l'administrateur d'enregistrement de session**. Cliquez sur **Next**.



Remarque :

- La journalisation de l'administrateur d'enregistrement de session est un sous-composant facultatif du serveur d'enregistrement de session. Vous devez sélectionner le serveur d'enregistrement de session avant de pouvoir sélectionner la journalisation de l'administrateur d'enregistrement de session.
- Citrix vous recommande d'installer la journalisation de l'administrateur d'enregistrement de session ainsi que le serveur d'enregistrement de session en même temps. Si vous ne souhaitez pas que la fonctionnalité de journalisation de l'administrateur soit activée, vous pouvez la désactiver sur une page ultérieure. Toutefois, si vous choisissez de ne pas installer cette fonctionnalité au début mais que vous souhaitez l'ajouter plus tard, vous pouvez uniquement l'ajouter manuellement à l'aide du pack SessionRecordingAdministrationx64.msi.

2. Sur la page **Configuration de la base de données et du serveur**, spécifiez les configurations.



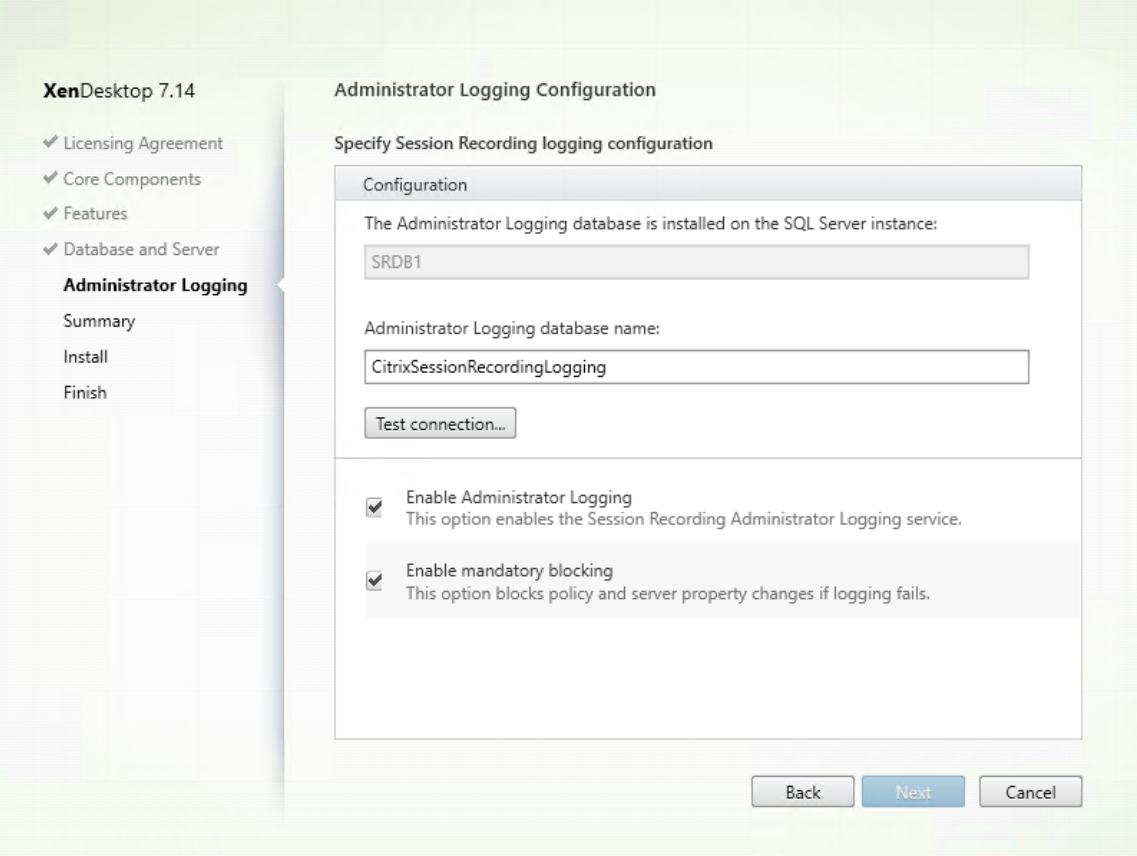
Sur la page **Configuration de la base de données et du serveur** :

- **Nom de l'instance :** entrez le nom de votre serveur SQL Server dans la case **Nom de l'instance**. Si vous utilisez une instance nommée, entrez nom-ordinateur\nom-instance ; sinon, entrez un nom-ordinateur uniquement. Si votre serveur SQL est configuré pour écouter un port personnalisé (autre que le port par défaut 1433), définissez le port d'écoute personnalisé en ajoutant une virgule au nom de l'instance. Par exemple, tapez **DXSBC-SRD-1,2433** dans la zone de texte **Nom de l'instance**, où 2433, après la virgule, indique le port d'écoute personnalisé.
- **Nom de la base de données :** entrez un nom de base de données personnalisé dans la zone de texte **Nom de la base de données** ou utilisez le nom de base de données par défaut **CitrixSessionRecording** qui est prédéfini dans la zone de texte.
- Vous devez disposer des autorisations de rôle de serveur **securityadmin** et **dbcreator** sur la base de données. Si vous ne disposez pas des autorisations, vous pouvez :
  - Demander à l'administrateur de base de données d'attribuer les permissions pour l'installation. Une fois l'installation terminée, les autorisations de rôle de serveur **securityadmin** et **dbcreator** ne sont plus nécessaires et peuvent être supprimées.
  - Ou, utilisez le pack SessionRecordingAdministrationx64.msi pour installer le serveur d'enregistrement de session. Durant l'installation msi, une boîte de dialogue s'affiche, demandant les informations d'identification d'un administrateur de base de données

avec les autorisations de rôle de serveur **securityadmin** et **dbcreator**. Entrez les informations d'identification correctes et cliquez sur **OK** pour continuer l'installation.

- Après avoir entré le nom d'instance et le nom de base de données corrects, cliquez sur **Tester la connexion** pour tester la connectivité à la base de données d'enregistrement de session.
- Entrez le compte d'ordinateur du serveur d'enregistrement de session, puis cliquez sur **Suivant**.

3. Sur la page **Configuration de la journalisation d'administration**, spécifiez les configurations pour la fonctionnalité de journalisation de l'administration.



Sur la page **Configuration de la journalisation d'administration** :

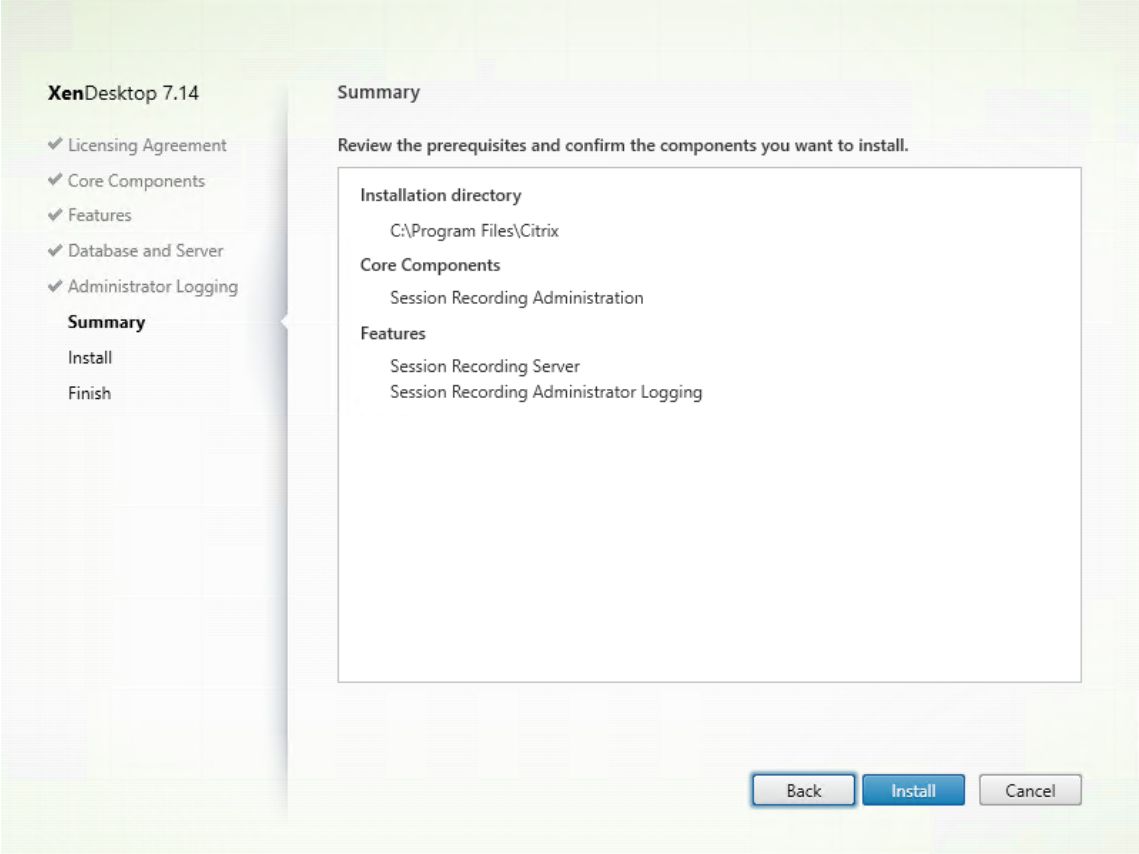
- **La base de données de journalisation de l'administration est installée sur l'instance SQL Server :** cette zone de texte n'est pas modifiable. Le nom d'instance SQL Server de la base de données de journalisation d'administration est récupéré automatiquement à partir du nom d'instance que vous avez tapé sur la page **Configuration de base de données et de serveur**.
- **Nom de la base de données de journalisation de l'administrateur :** si vous choisissez d'installer la fonctionnalité de journalisation de l'administrateur d'enregistrement de session, entrez un nom de base de données personnalisé pour la base de données de journal-

isation de l'administrateur dans la zone de texte ou utilisez le nom de la base de données par défaut **CitrixSessionRecordingLogging** prédéfini dans la zone de texte.
Remarque : le nom de la base de données de journalisation de l'administrateur doit être différent du nom de la base de données d'enregistrement de session défini dans la zone de texte **Nom de la base de données** sur la page **Configuration de la base de données et du serveur** précédente.

- Après avoir entré le nom de base de données de journalisation de l'administrateur, cliquez sur **Tester la connexion** pour tester la connectivité à la base de données de journalisation de l'administrateur.
- **Activer journalisation de l'administrateur :** par défaut, la fonctionnalité de journalisation de l'administrateur est activée. Vous pouvez la désactiver en désélectionnant la case à cocher.
- **Activer blocage obligatoire :** par défaut, le blocage obligatoire est activé. Les fonctionnalités normales peuvent être bloquées si la journalisation échoue. Vous pouvez désactiver le blocage obligatoire en désélectionnant la case à cocher.

Cliquez sur **Suivant** pour continuer l'installation.

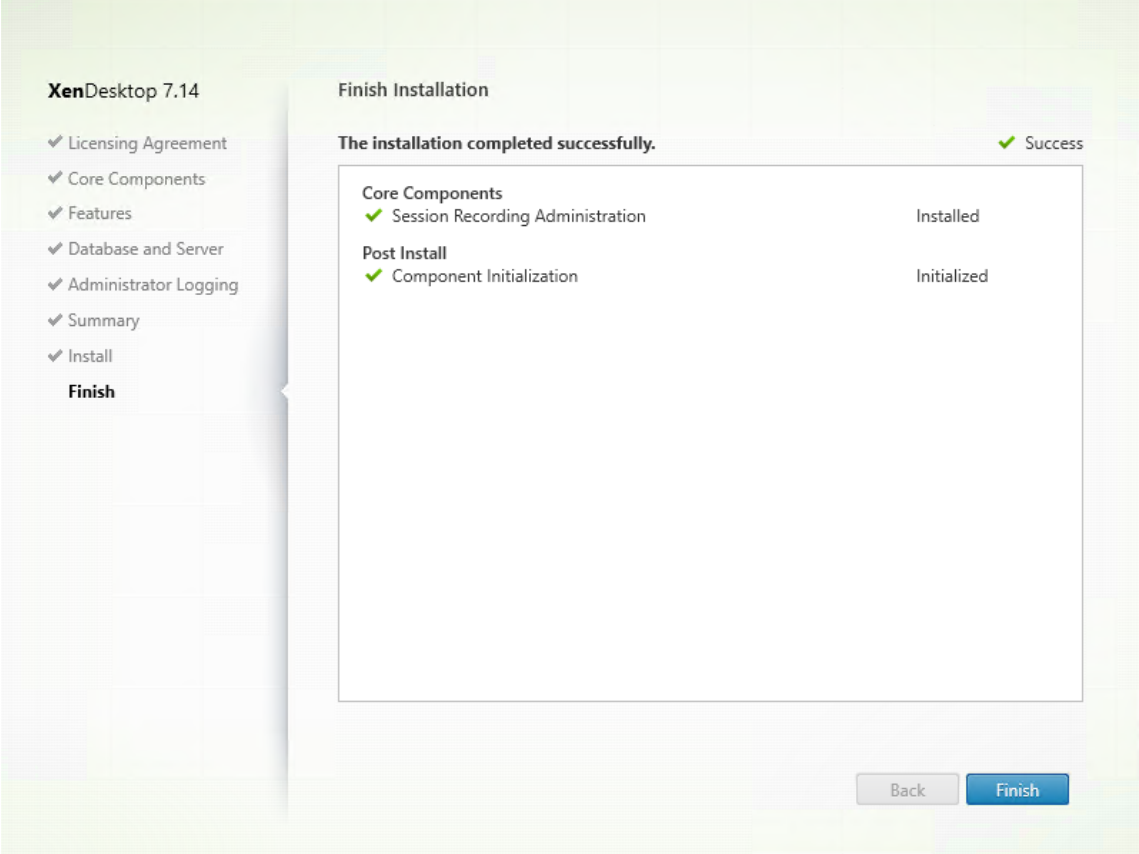
4. Vérifiez les composants requis et confirmez l'installation.



La page **Résumé** affiche vos choix d'installation. Vous pouvez cliquer sur le bouton **Précédent**

pour revenir sur les pages précédentes de l'assistant et apporter des modifications. Ou, cliquez sur **Installer** pour démarrer l'installation.

5. Terminez l'installation.



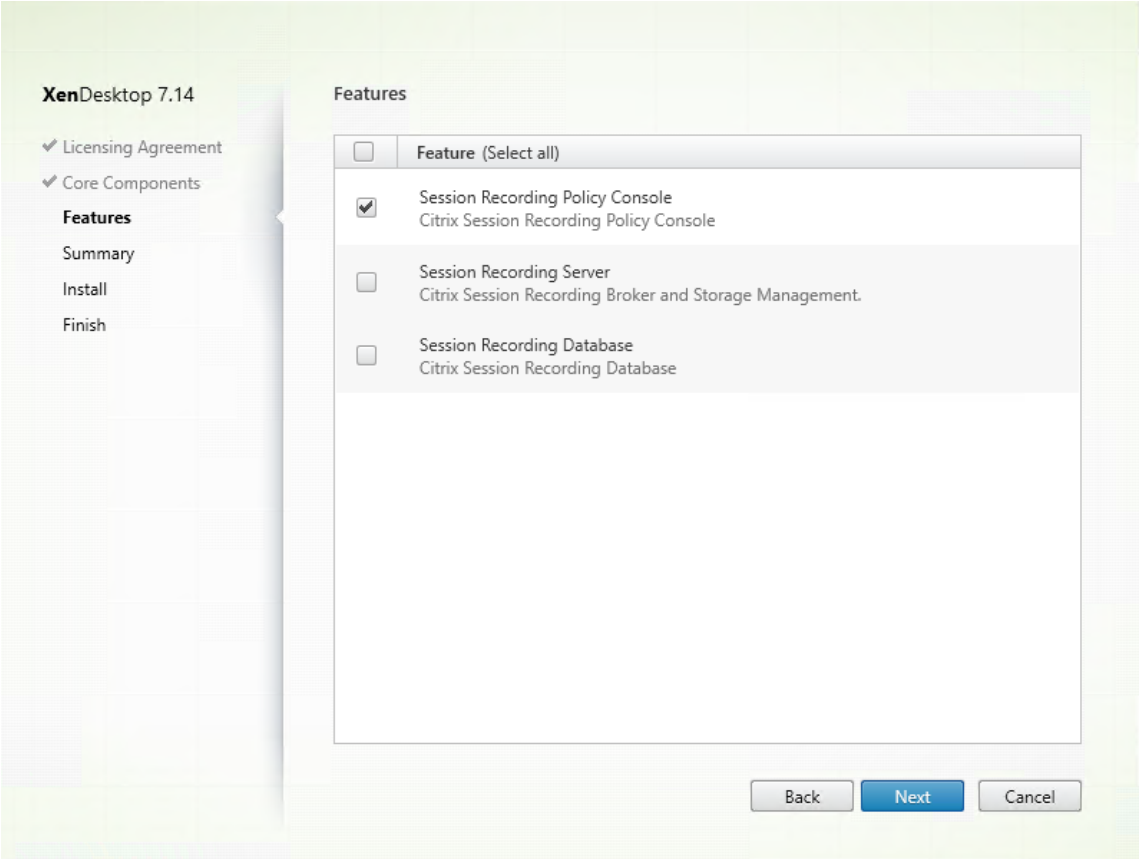
La page **Fin de l'installation** affiche des coches vertes pour tous les éléments pré-requis et composants installés et initialisés avec succès.

Cliquez sur **Terminer** pour terminer l'installation du serveur d'enregistrement de session.

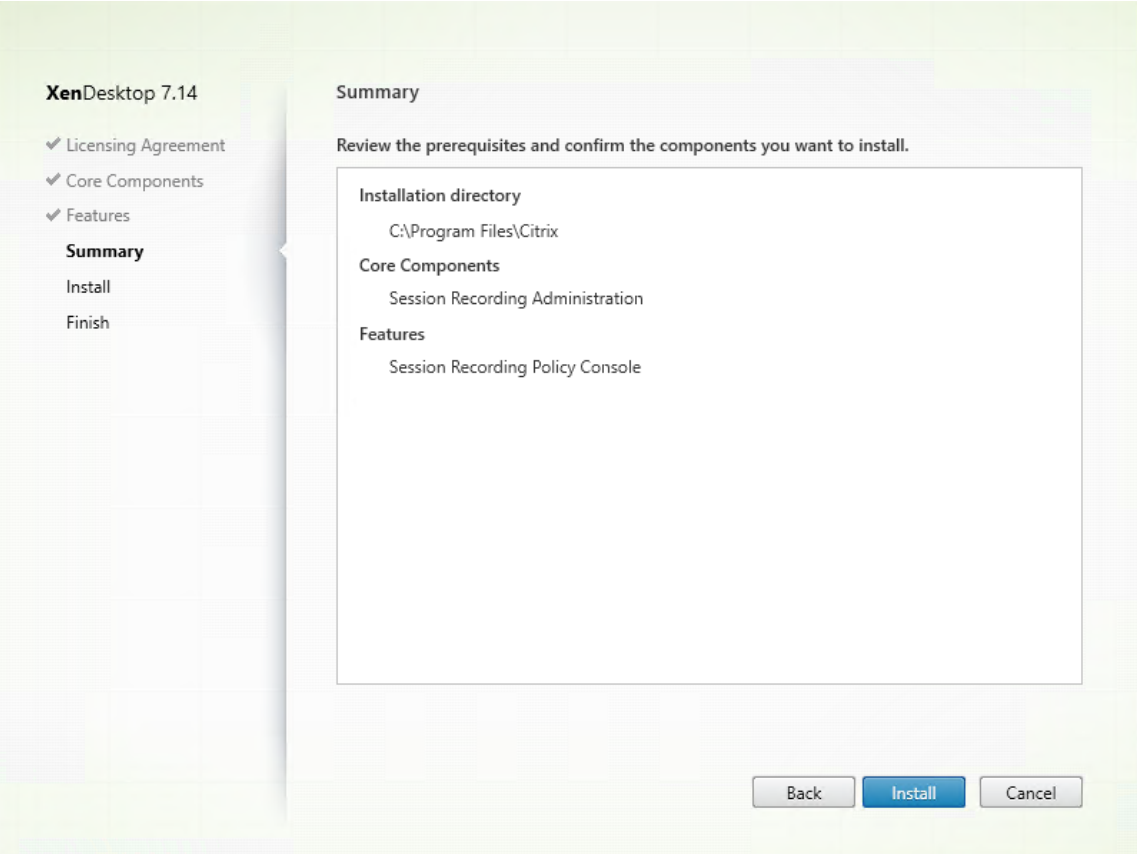
Remarque : l'installation du serveur d'enregistrement de session utilise par défaut HTTPS/TLS pour sécuriser les communications. Si TLS n'est pas configuré sur le site IIS par défaut du serveur d'enregistrement de session, utilisez HTTP. Pour ce faire, annulez la sélection de SSL dans la console de gestion IIS : accédez au site du broker d'enregistrement de session, ouvrez les paramètres SSL et désélectionnez la case **Exiger SSL**.

Étape 6.3 : Installer la console de stratégie d'enregistrement de session

1. Sur la page **Fonctionnalités**, sélectionnez **Console de stratégie d'enregistrement de session** et cliquez sur **Suivant**.

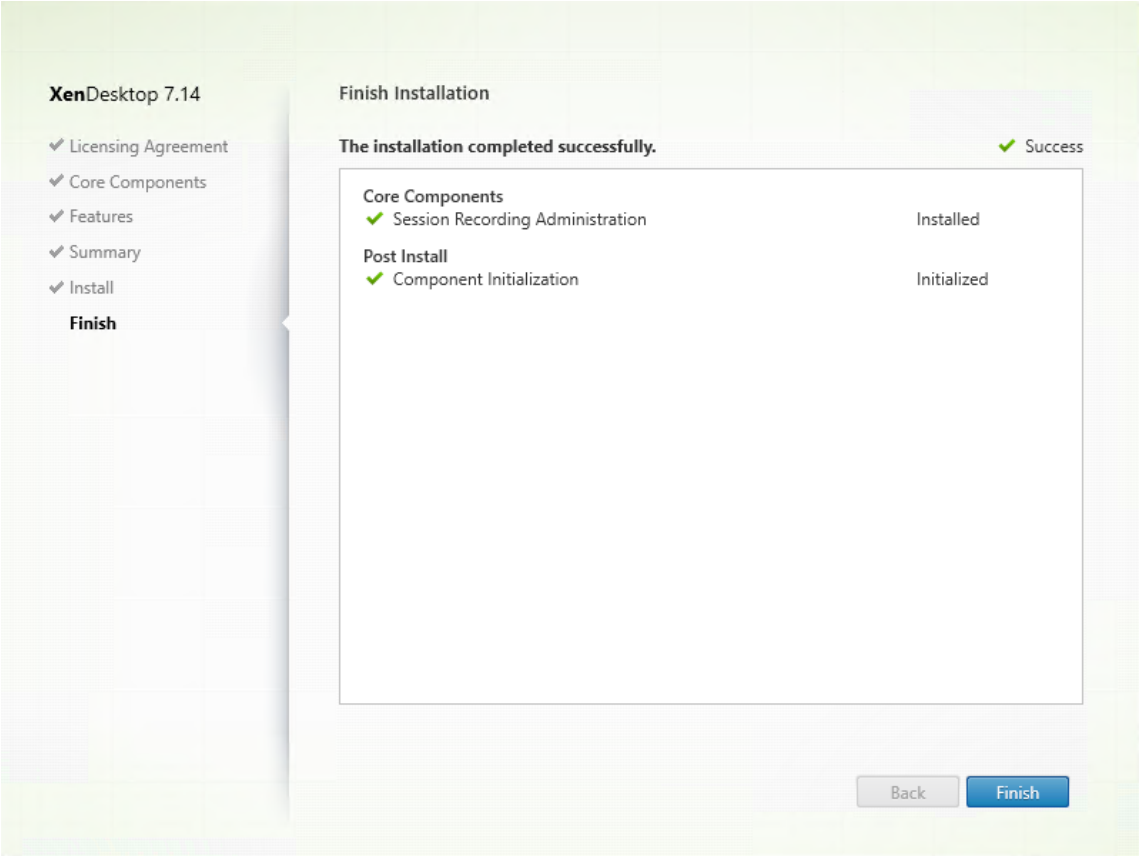


2. Vérifiez les composants requis et confirmez l'installation.



La page **Résumé** affiche vos choix d'installation. Vous pouvez cliquer sur le bouton **Précédent** pour revenir sur les pages précédentes de l'assistant et apporter des modifications. Ou, cliquez sur **Installer** pour démarrer l'installation.

3. Terminez l'installation.



La page **Terminer** contient des coches vertes pour tous les éléments pré-requis et composants installés et initialisés avec succès.

Cliquez sur **Terminer** pour terminer l'installation de la console de stratégie d'enregistrement de session.

Étape 7 : Installer Broker_PowerShellSnapIn_x64.msi

Important : pour utiliser la Console de stratégie d'enregistrement de session, le Broker PowerShell Snap-in (Broker_PowerShellSnapIn_x64.msi) doit être installé. Ce composant logiciel enfichable ne peut pas être installé automatiquement par le programme d'installation. Accédez au composant logiciel enfichable dans le fichier ISO de XenApp/XenDesktop (sous \layout\image-full\x64\Citrix Desktop Delivery Controller) et suivez les instructions pour l'installer manuellement. Si vous ne respectez pas cette consigne, cela peut entraîner une erreur.

Configurer Citrix Director pour utiliser le serveur d'enregistrement de session

Vous pouvez utiliser la console Director pour créer et activer des stratégies d'enregistrement de session.

1. Dans le cas d'une connexion HTTPS, installez le certificat destiné à approuver le serveur d'enregistrement de session dans les certificats racines de confiance du serveur Director.
2. Pour configurer le serveur Director pour utiliser le serveur d'enregistrement de session, exécutez la commande : **C:\inetpub\wwwroot\Director\tools\DirectorConfig.exe /configsessionrecording**
3. Entrez l'adresse IP ou le nom de domaine complet du serveur d'enregistrement de session, le numéro de port et le type de connexion (HTTP/HTTPS) que l'agent d'enregistrement de session utilise pour se connecter au broker d'enregistrement de session sur le serveur Director.

Installer l'agent d'enregistrement de session

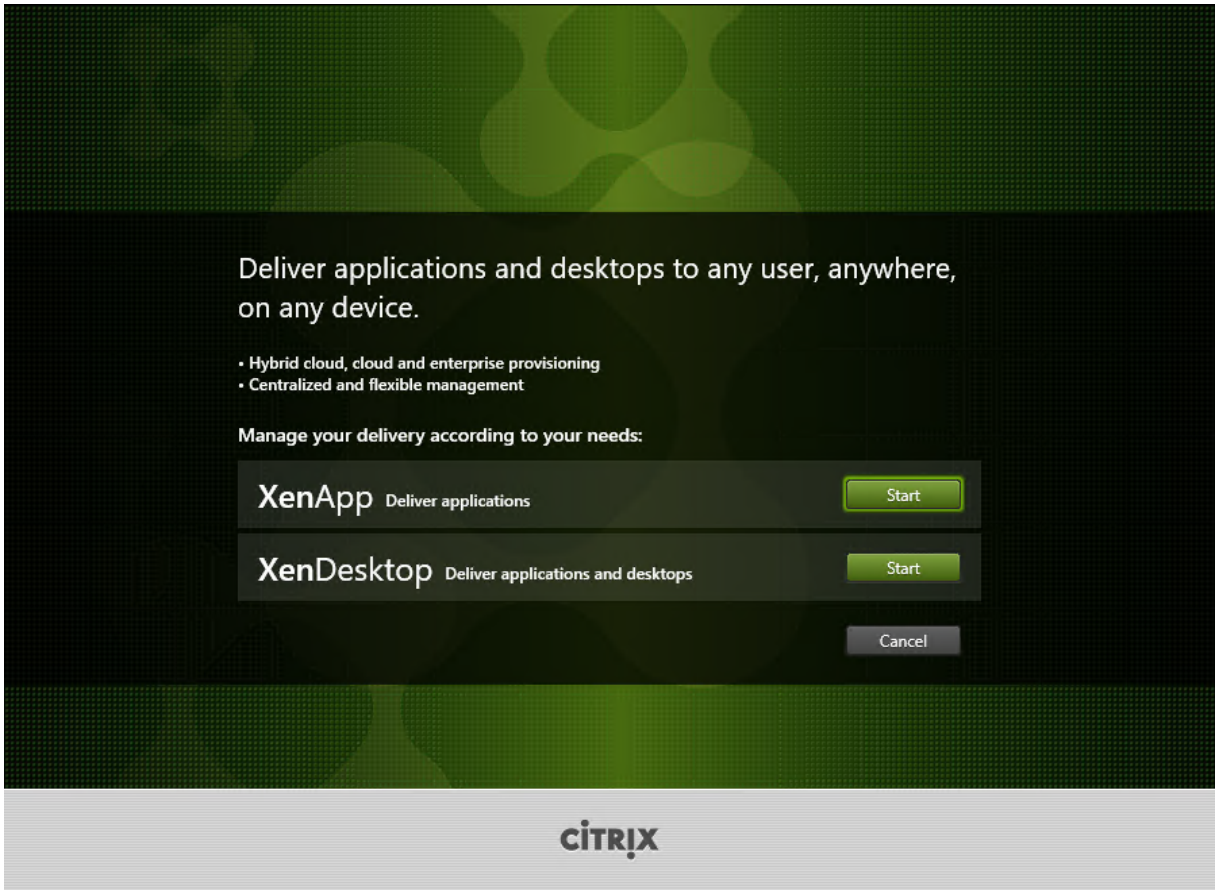
Vous devez installer l'agent d'enregistrement de session sur la machine VDA ou VDI sur laquelle vous voulez enregistrer les sessions.

Étape 1 : Télécharger le logiciel du produit et démarrer l'assistant

Utilisez un compte d'administrateur local pour ouvrir une session sur la machine sur laquelle vous installez le composant Agent d'enregistrement de session. Insérez le DVD dans le lecteur ou montez le fichier ISO. Si le programme d'installation ne se lance pas automatiquement, double-cliquez sur l'application **AutoSelect** ou sur le lecteur monté.

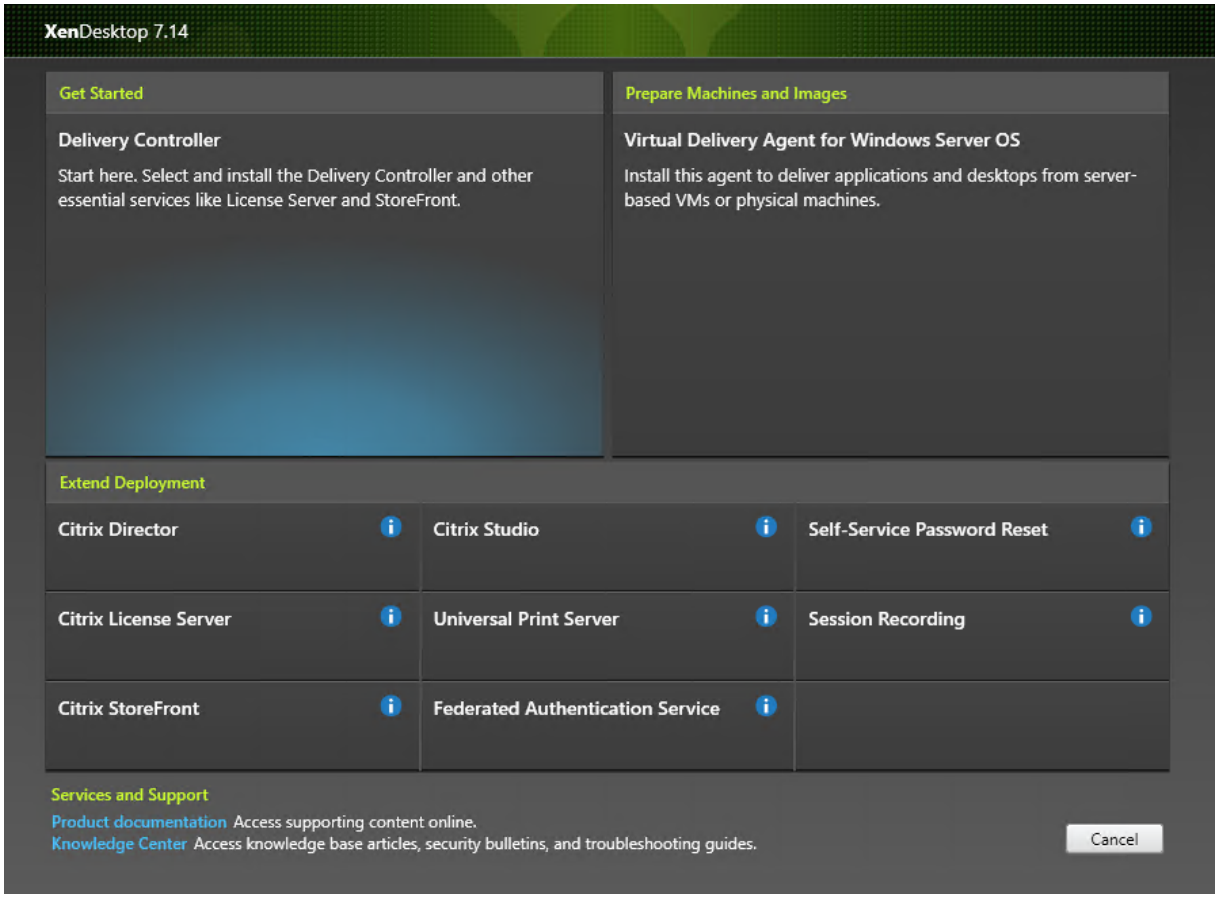
L'assistant d'installation démarre.

Étape 2 : Choisir le produit à installer



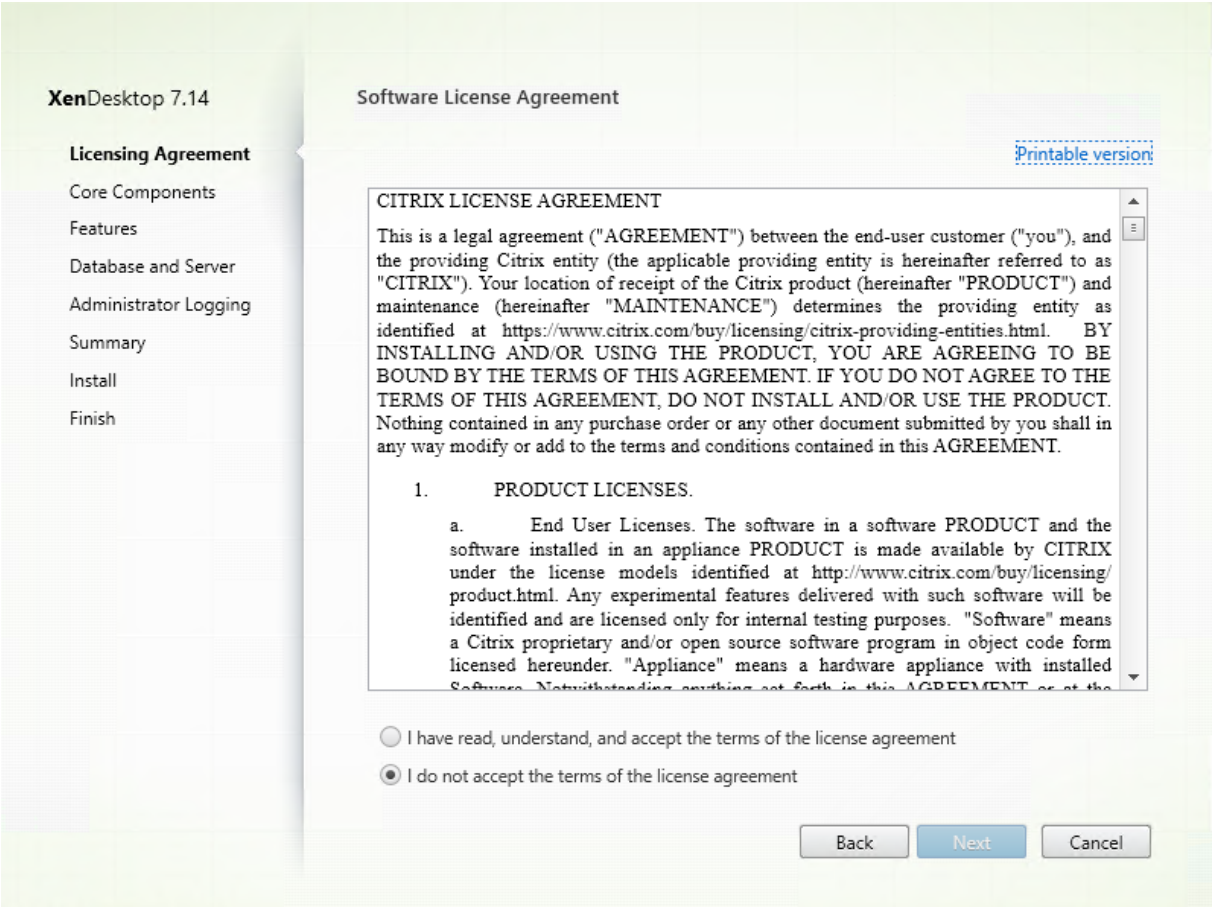
Cliquez sur **Démarrer** en regard du produit à installer : **XenApp** ou **XenDesktop**.

Étape 3 : Sélectionner Enregistrement de session



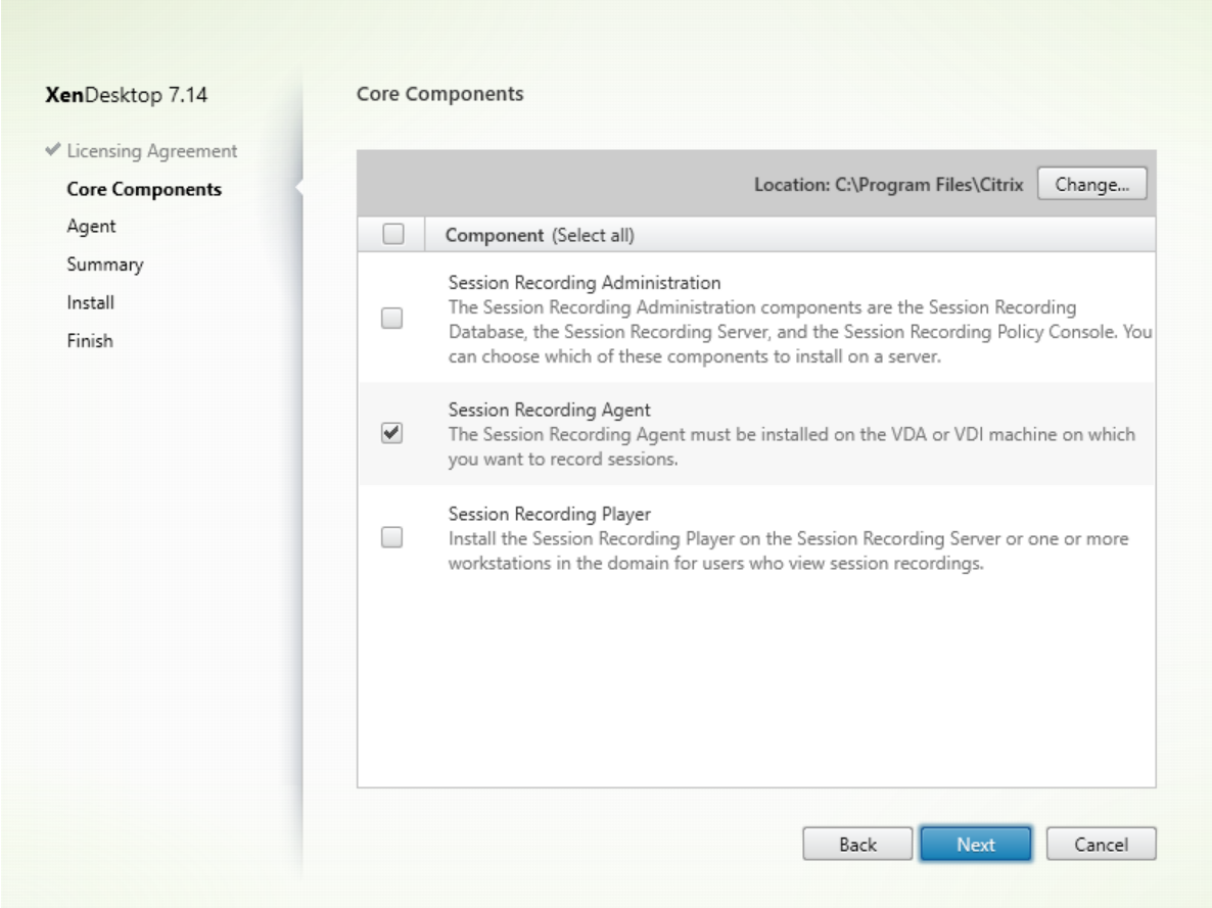
Sélectionnez l'entrée **Enregistrement de session**.

Étape 4 : Lire puis accepter le contrat de licence



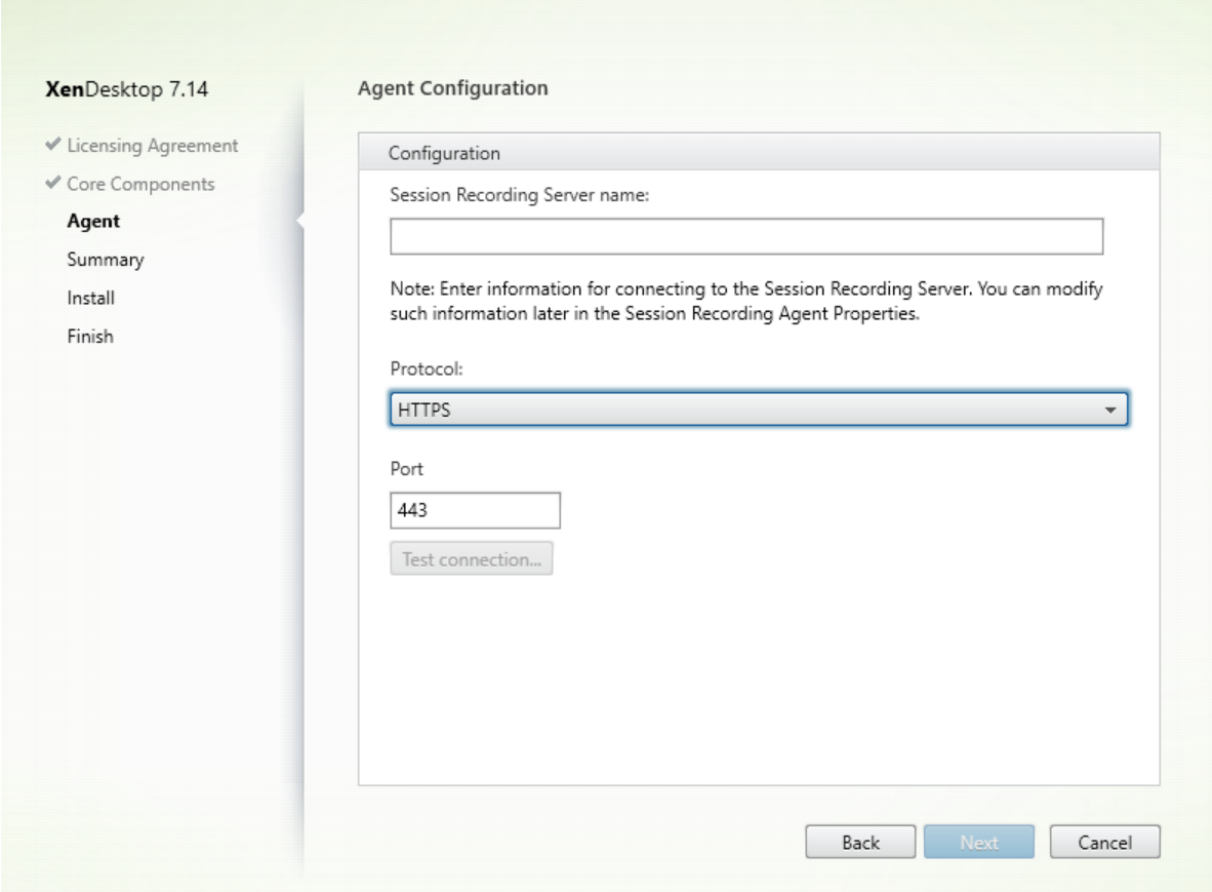
Sur la page **Contrat de licence du logiciel**, lisez le contrat, acceptez-le, puis cliquez sur **Suivant**.

Étape 5 : Sélectionner le composant à installer et l'emplacement d'installation



Sélectionnez **Agent d'enregistrement de session** et cliquez sur **Suivant**.

Étape 6 : Spécifier la configuration de l'agent

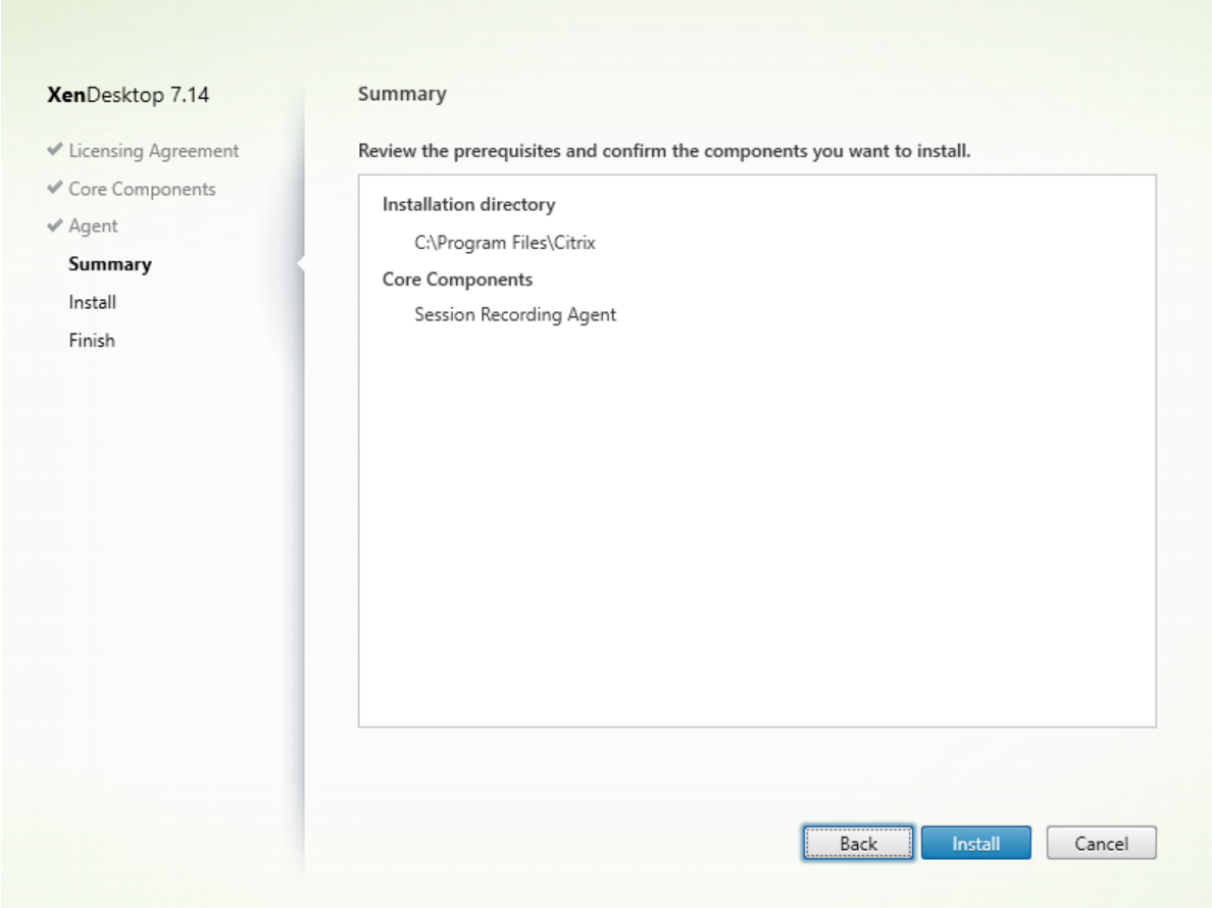


Sur la page **Configuration de l'agent** :

- Si vous avez déjà installé le serveur d'enregistrement de session, entrez le nom de l'ordinateur sur lequel vous avez installé le serveur d'enregistrement de session ainsi que les informations de protocole et de port requises pour la connexion au serveur d'enregistrement de session. Si vous n'avez pas encore installé Enregistrement de session, vous pouvez modifier ces informations ultérieurement dans **Propriétés de l'Agent d'enregistrement de session**.

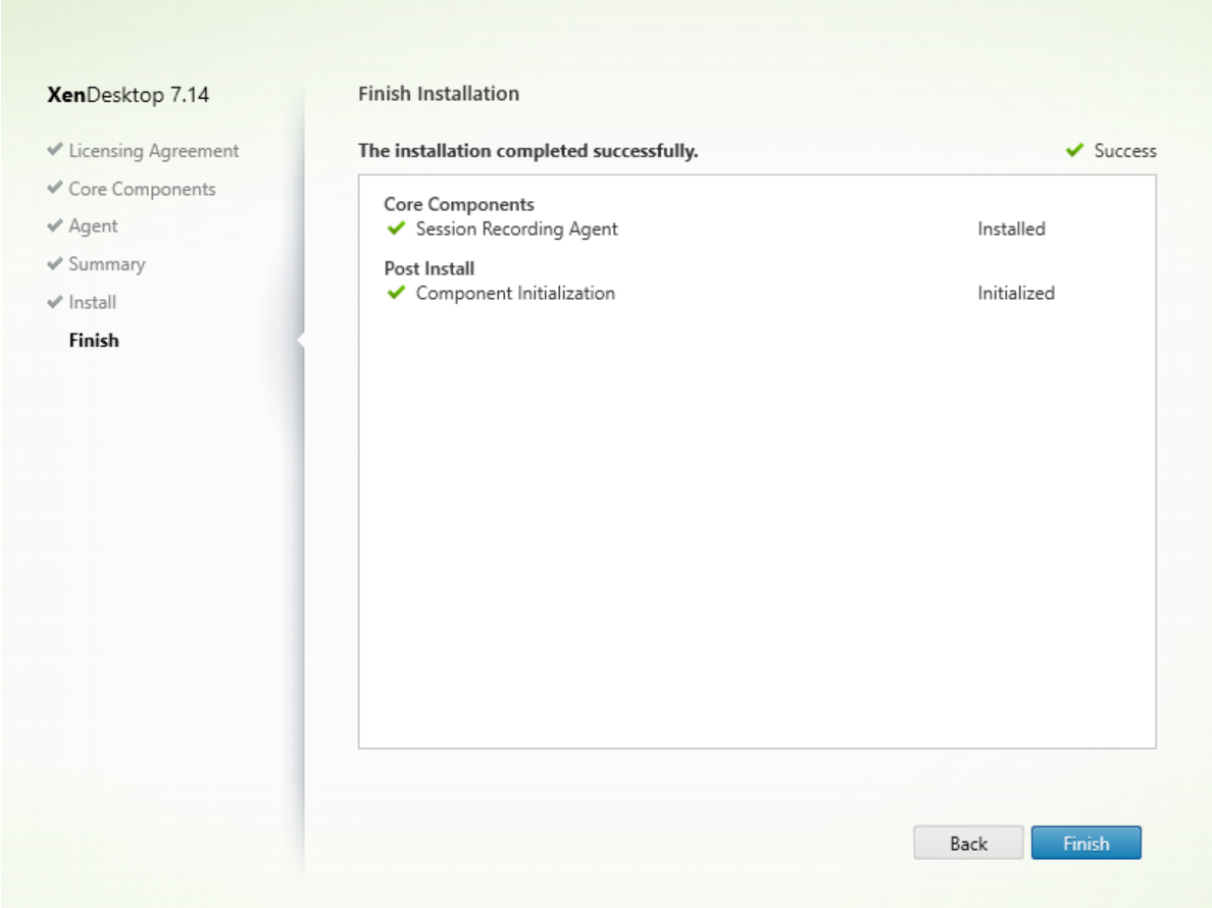
Remarque : il existe une limite de la fonction de test de connexion du programme d'installation. Elle ne prend pas en charge le scénario « HTTPS requiert TLS 1.2 ». Si vous utilisez le programme d'installation dans ce scénario, le test de la connexion échoue, mais vous pouvez ignorer l'échec et cliquer sur **Suivant** pour continuer l'installation. Cela n'affecte pas le fonctionnement normal.

Étape 7 : Vérifier les composants requis et confirmer l'installation



La page **Résumé** affiche vos choix d'installation. Vous pouvez cliquer sur le bouton **Précédent** pour revenir sur les pages précédentes de l'assistant et apporter des modifications. Ou, cliquez sur **Installer** pour démarrer l'installation.

Étape 8 : Terminer l'installation



La page **Fin de l'installation** affiche des coches vertes pour tous les éléments pré-requis et composants installés et initialisés avec succès.

Cliquez sur **Terminer** pour terminer l'installation de l'agent d'enregistrement de session.

Remarque : lorsque Machine Creation Services (MCS) ou Provisioning Services (PVS) crée plusieurs VDA avec une image principale configurée et Microsoft Message Queuing (MSMQ) installé, ces VDA peuvent disposer de la même QMId dans certaines conditions. Cela peut entraîner différents problèmes, tels que :

- Les sessions peuvent ne pas être enregistrées, même si l'accord d'enregistrement est accepté.
- Le serveur d'enregistrement de session peut ne pas pouvoir recevoir les signaux de fermeture de session, par conséquent l'état des sessions peut être toujours Actif.

La solution consiste à créer une QMId unique pour chaque VDA et elle varie selon les méthodes de déploiement.

Aucune action supplémentaire n'est requise si des VDA avec OS de bureau sur lesquels un agent d'enregistrement de session est installé seront créés avec PVS 7.7 ou version ultérieure et MCS ou

version ultérieure en mode de bureau statique ; par exemple, configurés pour rendre toutes les modifications persistantes avec un Personal vDisk ou disque local distinct du VDA.

Pour les VDA avec OS de serveur créés avec MCS ou PVS et les VDA avec OS de bureau qui sont configurés pour supprimer toutes les modifications lorsque l'utilisateur ferme sa session, utilisez le script GenRandomQMID.ps1 pour modifier la QMId au démarrage du système. Modifiez la stratégie de gestion de l'alimentation pour vous assurer qu'un nombre suffisant de VDA sont en cours d'exécution avant les tentatives de connexion des utilisateurs.

Pour utiliser le script GenRandomQMID.ps1, procédez comme suit :

1. Vérifiez que la stratégie d'exécution est définie sur **RemoteSigned** ou **Unrestricted** dans PowerShell.

   ```
   Set-ExecutionPolicy RemoteSigned
   ```

2. Créez une tâche planifiée, définissez le déclencheur sur Au démarrage du système et exécutez le compte SYSTEM sur la machine avec l'image principale PVS ou MCS.

3. Ajoutez la commande en tant que tâche de démarrage.

   ```
   powershell .exe -file C:\\GenRandomQMID.ps1
   ```

Résumé du script GenRandomQMID.ps1 :

1. Supprimez la QMId actuelle du registre.
2. Ajoutez SysPrep = 1 à HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSMQ\Parameters.
3. Arrêtez les services associés, notamment CitrixSmAudAgent et MSMQ.
4. Pour générer une QMId aléatoire, démarrez les services arrêtés précédemment.

```
# Supprimer l'ancien QMId du registre et définir l'indicateur SysPrep pour MSMQ
Remove-Itemproperty -Path HKLM:Software\Microsoft\MSMQ\Parameters\MachineCache -Name QMId -Force
Set-ItemProperty -Path HKLM:Software\Microsoft\MSMQ\Parameters -Name "SysPrep" -Type DWord -Value 1
# Obtenir les services dépendants
$depServices = Get-Service -name MSMQ -dependentservices | Select -Property Name
# Redémarrer MSMQ pour obtenir un nouveau QMId
Restart-Service -force MSMQ
# Démarrer les services dépendants
if ($depServices -ne $null) {

    foreach ($depService in $depServices) {

        $startMode = Get-WmiObject win32_service -filter "NAME = '$($depService.Name)'" | Select -Property StartMode
```



```
14          if ($startMode.StartMode -eq "Auto") {
15
16              Start-Service $depService.Name
17           }
18
19
20  }
21
22  }
```

Installer le lecteur d'enregistrement de session

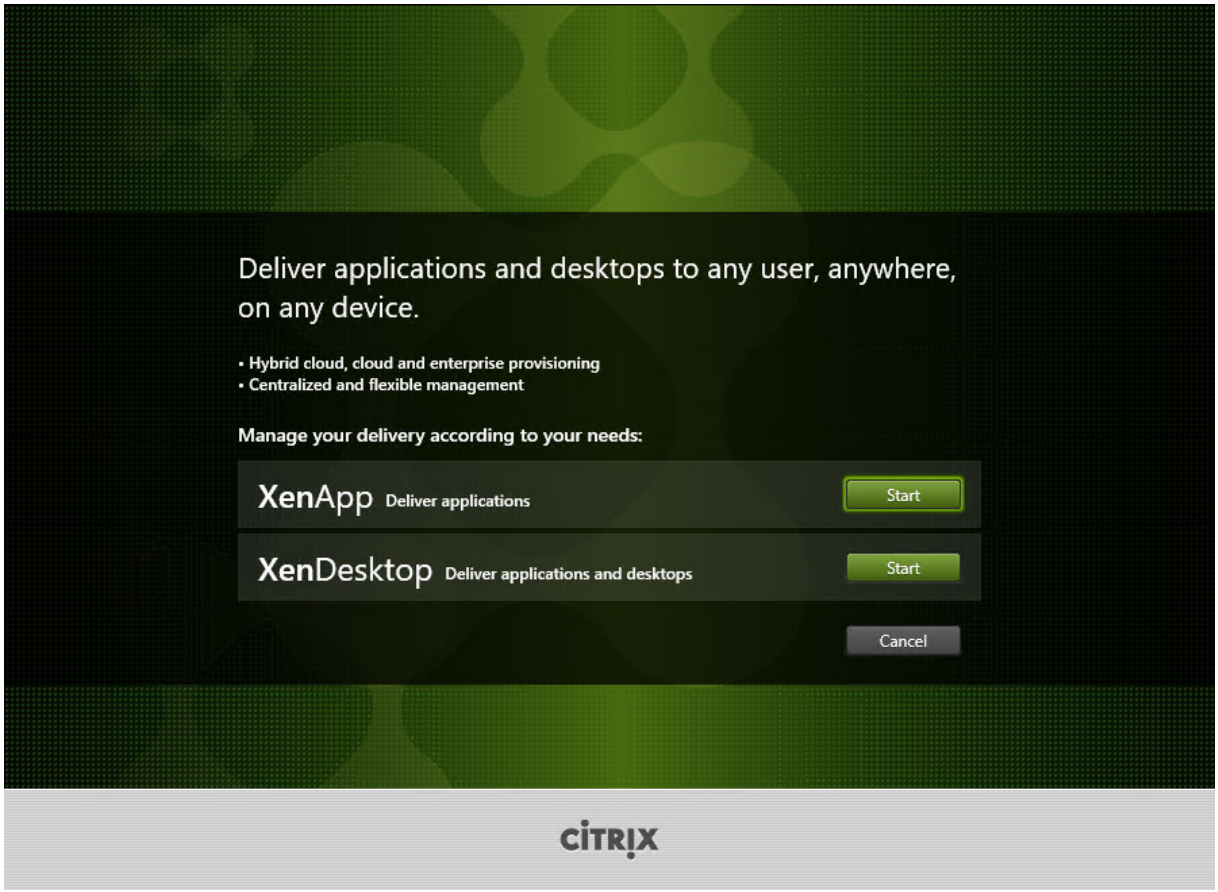
Installez le lecteur d'enregistrement de session sur le serveur d'enregistrement de session ou sur l'un ou plusieurs des postes de travail du domaine pour les utilisateurs qui visionnent les enregistrements de session.

Étape 1 : Télécharger le logiciel du produit et démarrer l'assistant

Utilisez un compte d'administrateur local pour ouvrir une session sur la machine sur laquelle vous installez le composant Lecteur d'enregistrement de session. Insérez le DVD dans le lecteur ou montez le fichier ISO. Si le programme d'installation ne se lance pas automatiquement, double-cliquez sur l'application **AutoSelect** ou sur le lecteur monté.

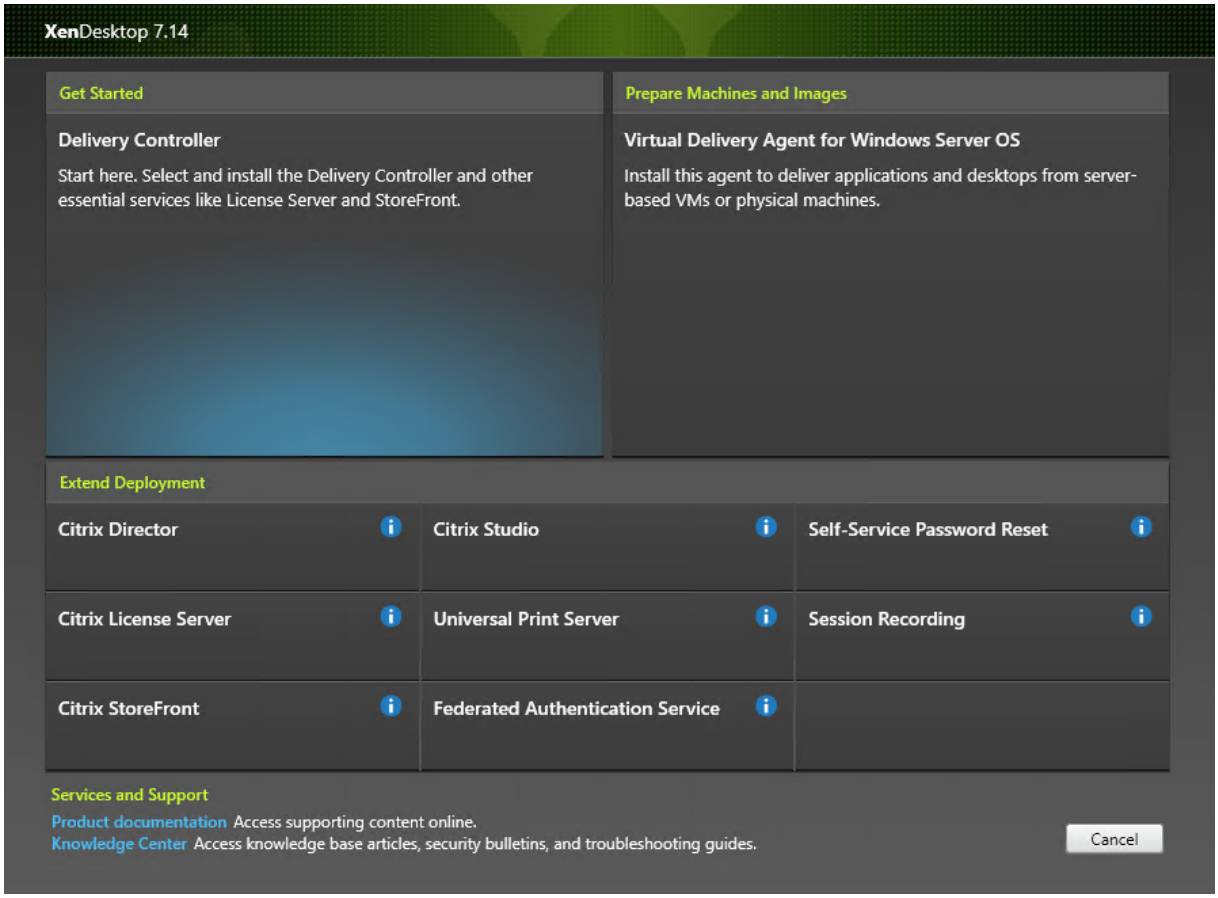
L'assistant d'installation démarre.

Étape 2 : Choisir le produit à installer



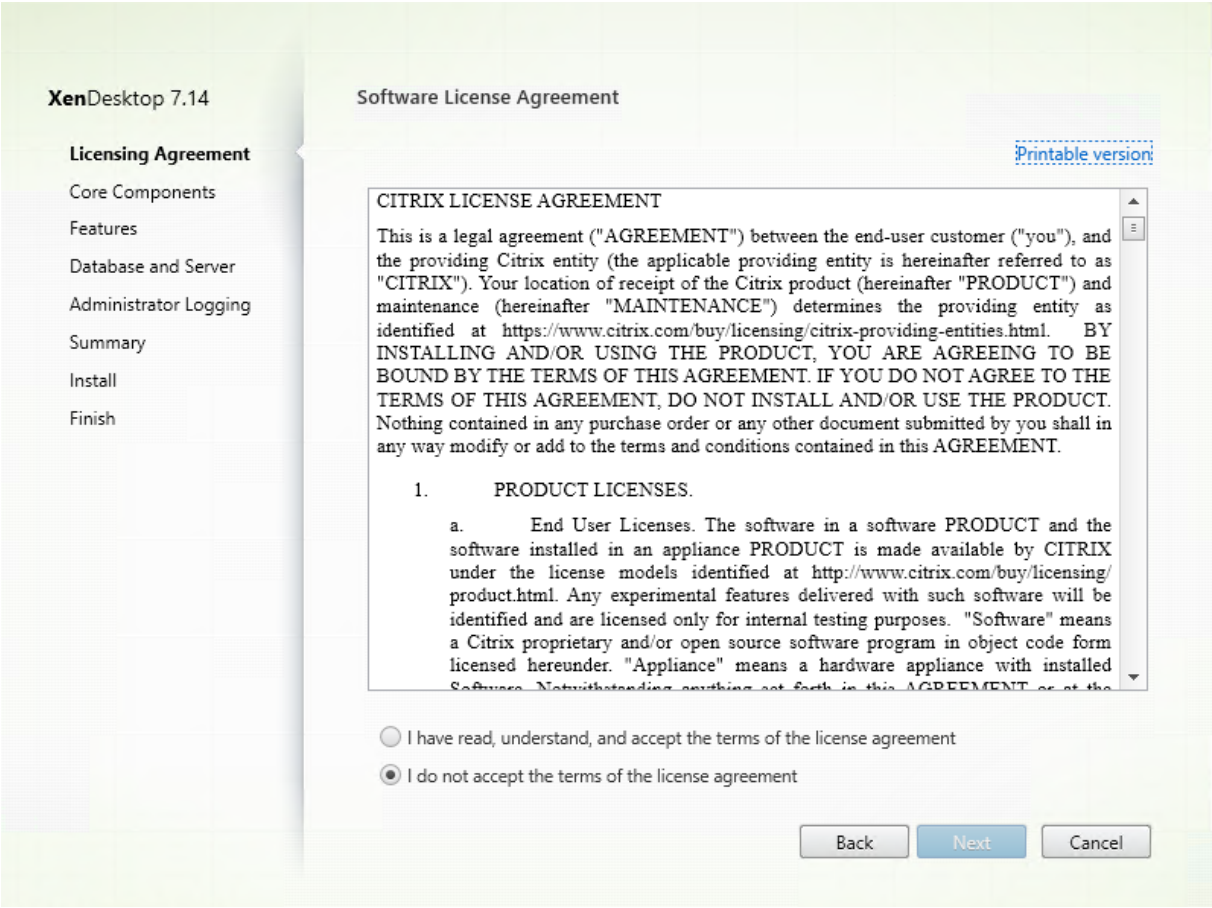
Cliquez sur **Démarrer** en regard du produit à installer : **XenApp** ou **XenDesktop**.

Étape 3 : Sélectionner Enregistrement de session



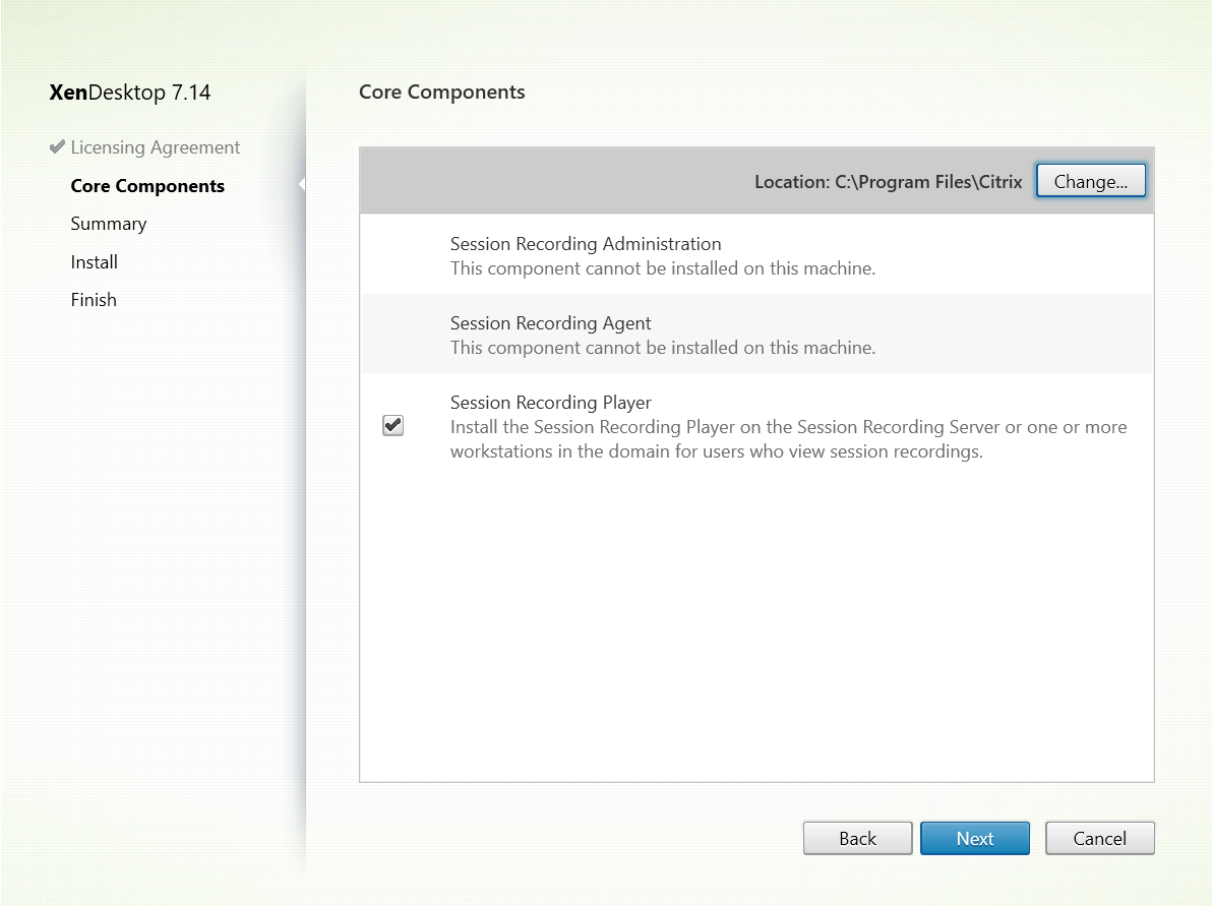
Sélectionnez l'entrée **Enregistrement de session**.

Étape 4 : Lire puis accepter le contrat de licence



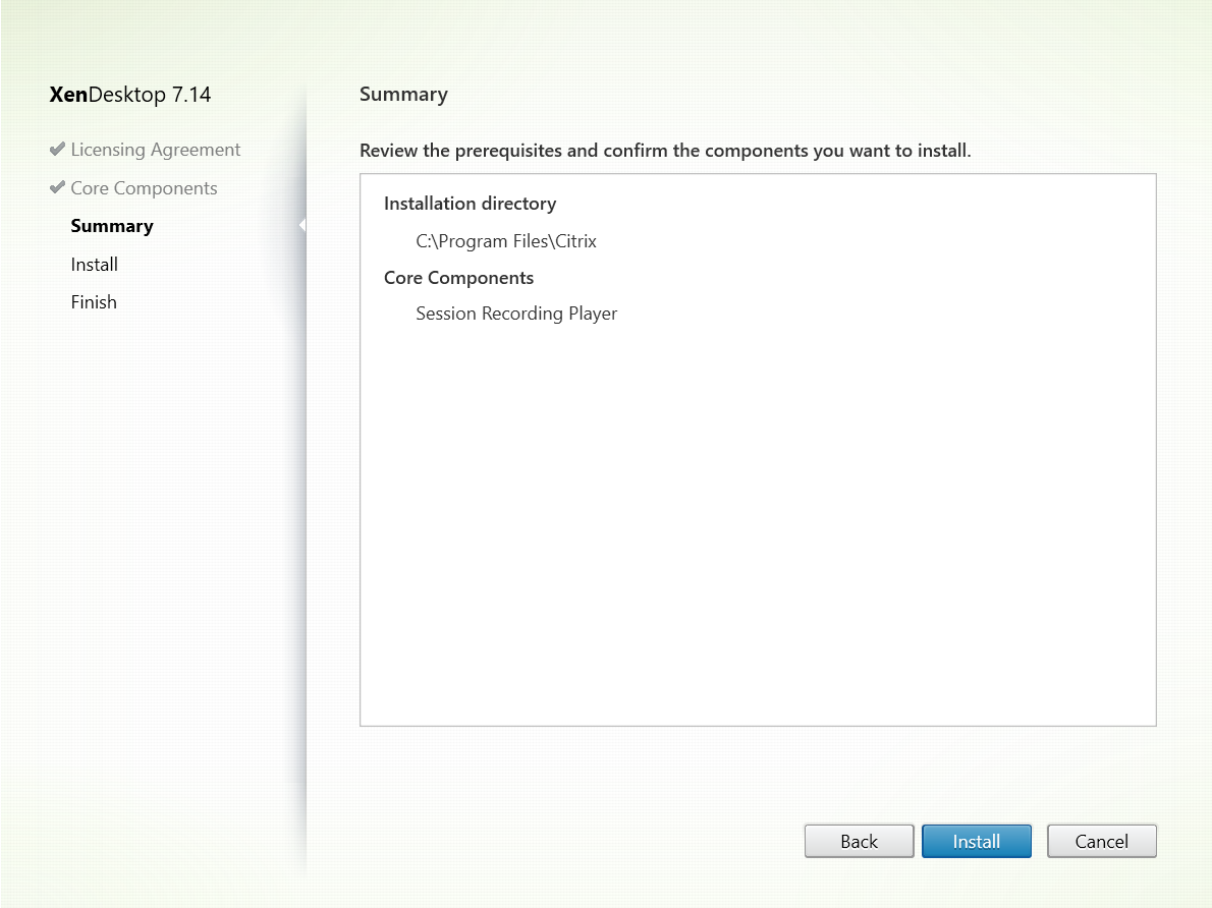
Sur la page **Contrat de licence du logiciel**, lisez le contrat, acceptez-le, puis cliquez sur **Suivant**.

Étape 5 : Sélectionner le composant à installer et l'emplacement d'installation



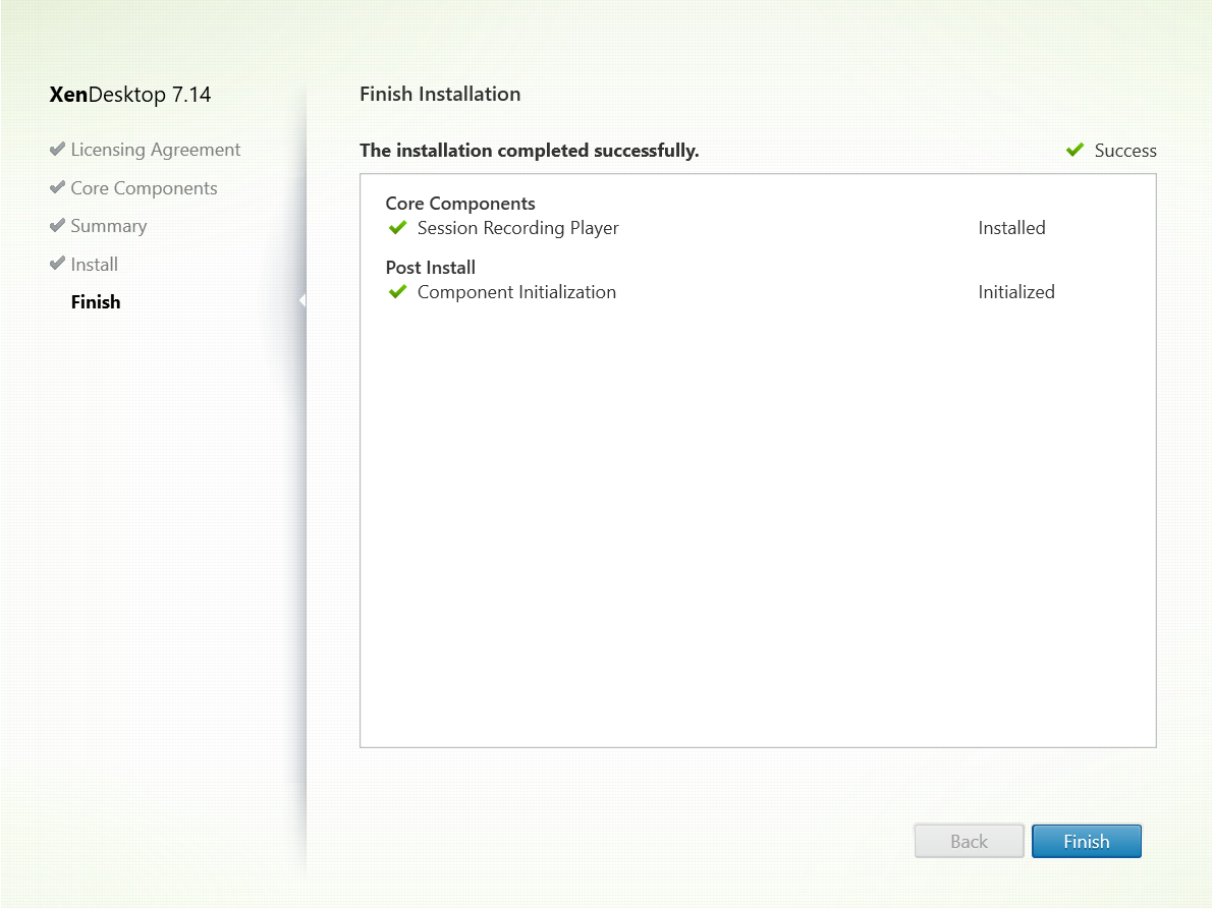
Sélectionnez **Lecteur d'enregistrement de session** et cliquez sur **Suivant**.

Étape 6 : Vérifier les composants requis et confirmer l'installation



La page **Résumé** affiche vos choix d'installation. Vous pouvez cliquer sur le bouton **Précédent** pour revenir sur les pages précédentes de l'assistant et apporter des modifications. Ou, cliquez sur **Installer** pour démarrer l'installation.

Étape 7 : Terminer l'installation



La page **Fin de l'installation** affiche des coches vertes pour tous les éléments pré-requis et composants installés et initialisés avec succès.

Cliquez sur **Terminer** pour terminer l'installation du lecteur d'enregistrement de session.

Automatiser les installations

Pour installer l'agent d'enregistrement de session sur plusieurs serveurs, créez un script utilisant l'installation silencieuse.

La ligne de commande suivante installe l'agent d'enregistrement de session et crée un fichier journal pour capturer les informations d'installation.

Pour les systèmes 64 bits :

msiexec /i SessionRecordingAgentx64.msi /q /l*vx *votre_journal_installation*SESSIONRECORDINGSERVERNAME=nc
SESSIONRECORDINGBROKERPROTOCOL=protocole_de_votre_broker SESSIONRECORDINGBROKER-
PORT=port_de_votre_broker

Remarque : le fichier SessionRecordingAgentx64.msi dans l'image ISO de XenApp/XenDesktop est sous \layout\image-full\x64\Session Recording.

Pour les systèmes 32 bits :

msiexec /i SessionRecordingAgent.msi /q /l*vx *votre_journal_installation*SESSIONRECORDINGSERVERNAME=nom_
SESSIONRECORDINGBROKERPROTOCOL=protocole_de_votre_broker SESSIONRECORDINGBROKER-
PORT=port_de_votre_broker

Remarque : le fichier SessionRecordingAgent.msi dans l'image ISO de XenApp/XenDesktop est sous \layout\image-full\x86\Session Recording.

où :

nom_de_votre_serveur correspond au nom NetBIOS ou au nom de domaine complet de l'ordinateur hébergeant le serveur d'enregistrement de session. Si elle n'est pas précisée, cette valeur prend par défaut la valeur **localhost**.

protocole_de_votre_broker est le protocole, HTTP ou HTTPS, que l'agent d'enregistrement de session utilise pour communiquer avec le broker d'enregistrement de session. Si elle n'est pas précisée, cette valeur prend par défaut la valeur HTTPS.

port_de_votre_broker est le numéro de port que l'agent d'enregistrement de session utilise pour communiquer avec le broker d'enregistrement de session. Si elle n'est pas précisée, la valeur par défaut de cette valeur est zéro, qui amène l'agent d'enregistrement de session à utiliser le numéro de port par défaut pour le protocole sélectionné : 80 pour HTTP ou 443 pour HTTPS.

/l*v spécifie l'enregistrement détaillé.

votre_journal_installation est l'emplacement de votre fichier journal d'installation.

/q spécifie le mode silencieux.

Mettre à niveau l'enregistrement de session

Vous pouvez mettre à niveau certains déploiements vers des versions ultérieures sans devoir d'abord configurer les nouvelles machines ou sites. Vous pouvez mettre à niveau à partir de l'enregistrement de session 7.6 (ou version ultérieure) vers la dernière version de l'enregistrement de session.

Remarques :

- Lorsque vous mettez à niveau Administration de l'enregistrement de session depuis la version 7.6 vers 7.13 ou version ultérieure et choisissez **Modifier** dans Administration de l'enregistrement de session pour ajouter le service de journalisation de l'administrateur, le nom de l'instance SQL Server ne s'affiche pas sur la page de **configuration de la journalisation d'administrateur**. Le message suivant s'affiche lorsque vous cliquez

sur **Suivant** : `Database connection test failed. Please enter correct Database instance name`. Pour contourner le problème, ajoutez le droit en lecture pour les utilisateurs localhost dans le dossier de registre de serveur SmartAuditor suivant : HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server.

- Les tentatives de mise à niveau de la base de données d'enregistrement de session peuvent échouer lorsque ce composant est le seul à être installé sur une machine. Dans ce cas, vérifiez si les entrées de Registre suivantes existent sous HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Sr
  Si ce n'est pas le cas, ajoutez manuellement les entrées avant la mise à niveau.

Nom de la clé	Type de clé	Valeur de clé
SmAudDatabaseInstance	Chaîne	Nom d'instance de votre base de données d'enregistrement de session
DatabaseName	Chaîne	Nom de votre base de données d'enregistrement de session

Configuration requise, préparation et limites

Remarque : vous ne pouvez pas mettre à niveau à partir d'une version Technology Preview.

- Vous devez utiliser l'interface graphique ou l'interface de ligne de commande du programme d'installation de l'enregistrement de session pour mettre à niveau les composants d'enregistrement de session sur la machine sur laquelle vous avez installé les composants.
- Avant de procéder à toute activité de mise à niveau, sauvegardez la base de données nommée CitrixSessionRecording dans l'instance de SQL Server, afin de pouvoir la restaurer en cas de problème après la mise à niveau de la base de données.
- En plus d'être un utilisateur du domaine, vous devez être un administrateur local sur les machines sur lesquelles vous mettez à niveau les composants d'enregistrement de session.
- Si le serveur d'enregistrement de session et la base de données d'enregistrement de session ne sont pas installés sur le même serveur, vous devez disposer de l'autorisation de rôle de base de données pour mettre à niveau la base de données d'enregistrement de session ; sinon, vous pouvez
  - Demander à l'administrateur de base de données d'attribuer les autorisations de rôle de serveur **securityadmin** et **dbcreator** pour la mise à niveau. Une fois la mise à niveau terminée, les autorisations de rôle de serveur **securityadmin** et **dbcreator** ne sont plus nécessaires et peuvent être supprimées pour l'utilisateur actuel.
  - Ou, utilisez le pack SessionRecordingAdministrationx64.msi pour effectuer la mise à niveau. Durant la mise à niveau msi, une boîte de dialogue s'affiche, demandant les infor-

mations d'identification d'un administrateur de base de données avec les autorisations de rôle de serveur **securityadmin** et **dbcreator**. Entrez les informations d'identification correctes et cliquez sur **OK** pour continuer la mise à niveau.

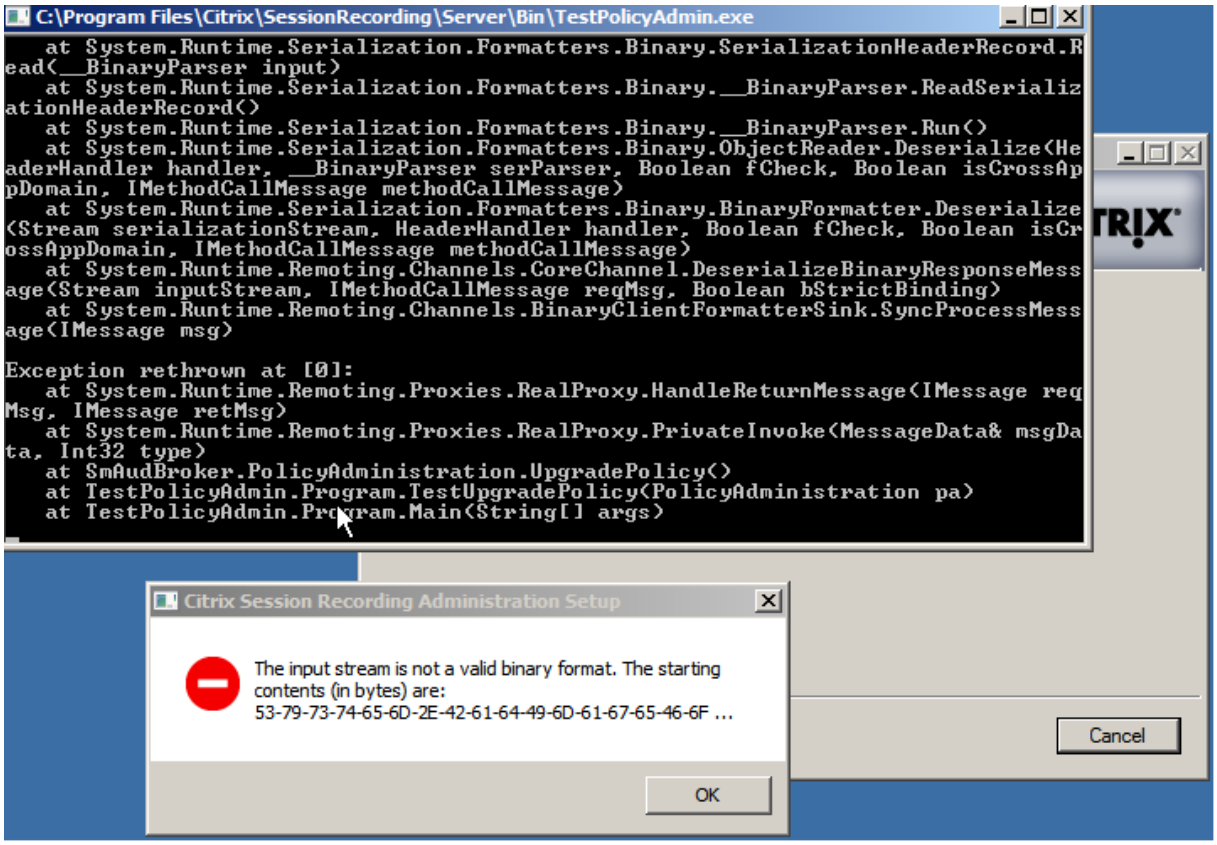
- Si vous n'envisagez pas de mettre à niveau tous les agents d'enregistrement de session en même temps, l'agent d'enregistrement de session 7.6.0 (ou une version ultérieure) peut fonctionner avec la dernière version (courante) du serveur d'enregistrement de session. Cependant, certaines nouvelles fonctionnalités et des corrections de bogues risquent de ne pas être appliquées.
- Les sessions lancées durant la mise à niveau du serveur d'enregistrement de session ne sont pas enregistrées.
- L'option **Réglage graphique** dans Propriétés de l'agent d'enregistrement de session est activée par défaut après une nouvelle installation ou mise à niveau pour maintenir la compatibilité avec le mode Redirection Desktop Composition. Vous pouvez désactiver cette option manuellement après une nouvelle installation ou mise à niveau.
- La fonctionnalité Journalisation de l'administrateur n'est pas installée après la mise à niveau de l'enregistrement de session à partir d'une version précédente qui ne contient pas cette fonctionnalité. Pour ajouter la nouvelle fonctionnalité, modifiez l'installation après la mise à niveau.
- S'il existe des sessions d'enregistrement actives lorsque le processus de mise à niveau démarre, l'enregistrement ne pourra probablement pas se terminer.
- Vérifiez la séquence de mise à niveau ci-dessous afin de pouvoir planifier et réduire tout problème potentiel.

Séquence de mise à niveau

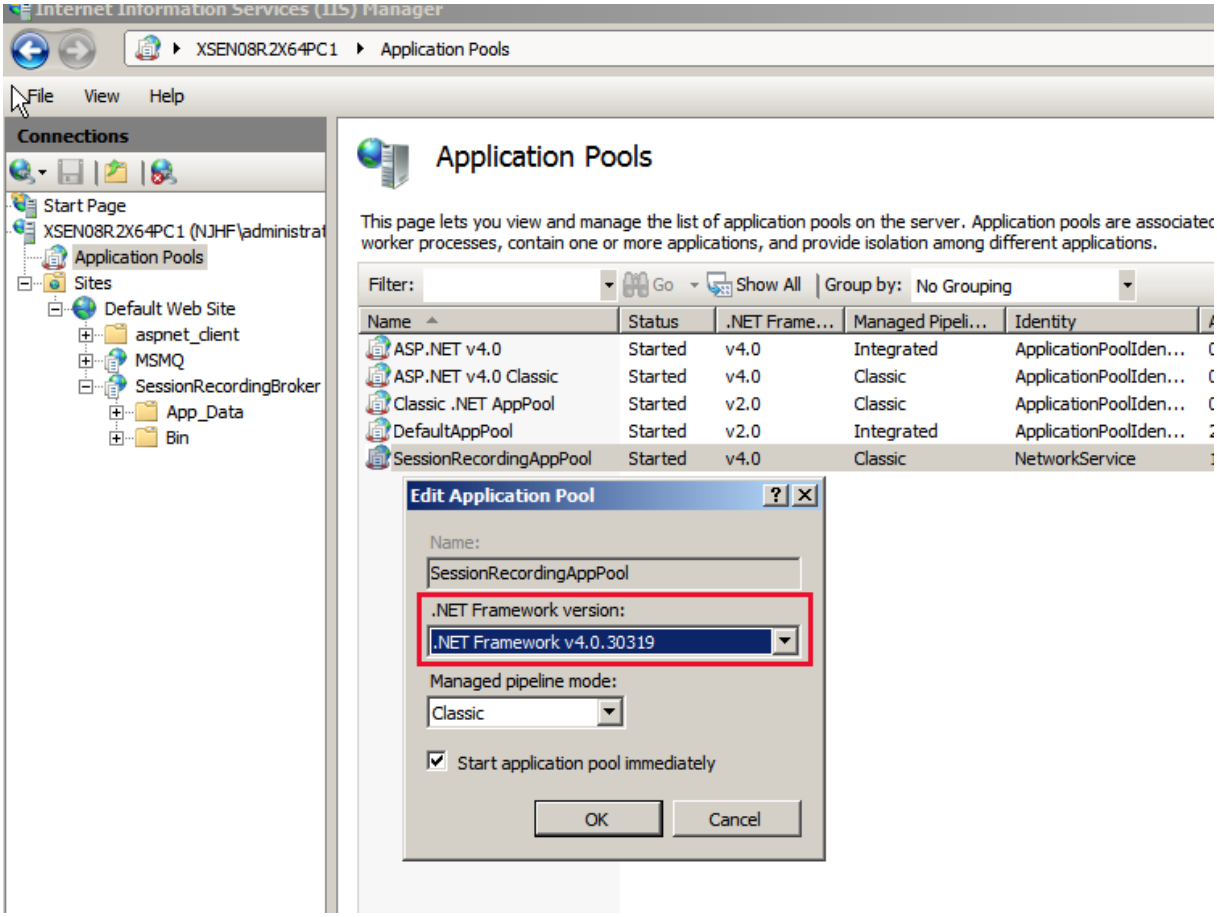
1. Si la base de données d'enregistrement de session et le serveur d'enregistrement de session sont installés sur des serveurs différents, arrêtez le service Gestionnaire de stockage d'enregistrement de session manuellement sur le serveur d'enregistrement de session, puis mettez à niveau la base de données d'enregistrement de session.
2. Assurez-vous que le broker d'enregistrement de session est exécuté avec le service IIS. Mettez à niveau le serveur d'enregistrement de session. Si la base de données d'enregistrement de session et le serveur d'enregistrement de session sont installés sur le même serveur, la base de données d'enregistrement de session doit également être mise à niveau.
3. Le service d'enregistrement de session est automatiquement reconnecté lorsque la mise à niveau du serveur d'enregistrement de session est terminée.
4. Mettez à niveau l'agent d'enregistrement de session (sur l'image principale).
5. Mettez à niveau la console de stratégie d'enregistrement de session avec ou après le serveur d'enregistrement de session.
6. Mettez à niveau le lecteur d'enregistrement de session.

Remarque : l'erreur suivante peut se produire lorsque vous mettez à niveau le composant Adminis-

tration de l'enregistrement de session sur Windows Server 2008 R2.



Dans ce cas, modifiez la « version de .NET Framework » pour « SessionRecordingAppPool » sur « .NET Framework v4 » dans IIS et effectuez à nouveau la mise à niveau.



Désinstaller l'enregistrement de session

Pour supprimer tous les composants d'enregistrement de session d'un serveur ou d'une station de travail, utilisez la capacité de désinstallation ou de suppression des programmes disponible au travers du Panneau de configuration Windows. Pour supprimer la base de données d'enregistrement de session, vous devez avoir les mêmes droits d'administrateur système SQL Server **securityadmin** et **dbcreator** que lorsque vous l'avez installée.

Pour des raisons de sécurité, la base de données de Journalisation de l'administrateur n'est pas supprimée après la désinstallation des composants.

Configurer l'enregistrement de session

February 28, 2019

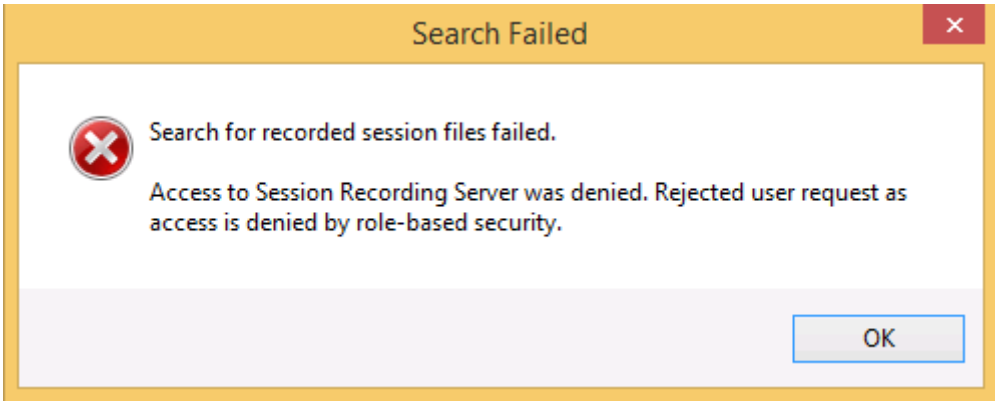
Configurer l'enregistrement de session pour lire et enregistrer des sessions

Après avoir installé les composants d'enregistrement de session, effectuez les étapes suivantes pour configurer l'enregistrement de session pour enregistrer des sessions XenApp ou XenDesktop et pour permettre aux utilisateurs de les visionner :

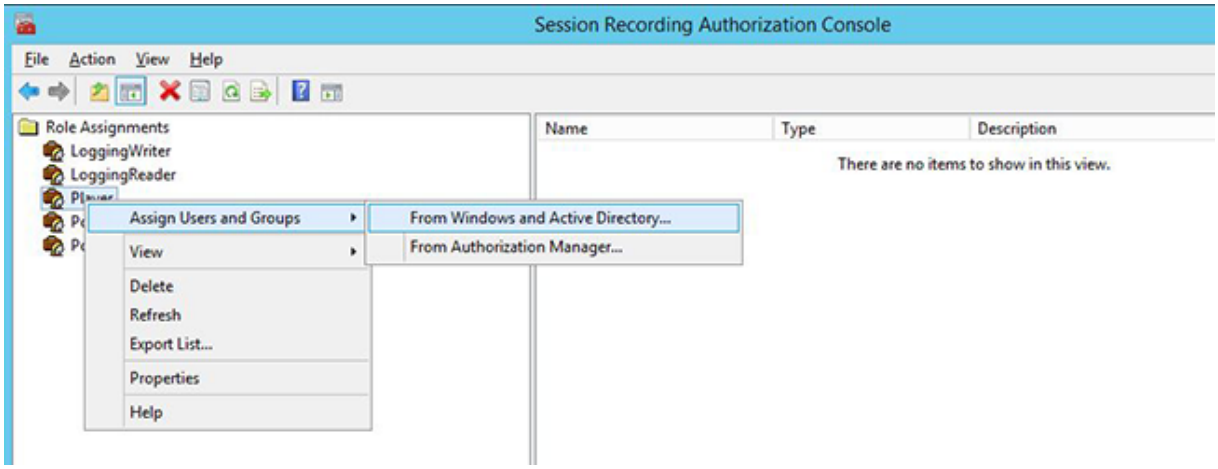
- Autorisez les utilisateurs à lire les enregistrements
- Autorisez les utilisateurs à gérer les stratégies d'enregistrement
- Paramétrez une stratégie d'enregistrement active de manière à enregistrer les sessions.
- Configurer des stratégies personnalisées
- Configurer le lecteur d'enregistrement de session pour la connexion au serveur d'enregistrement de session

Autorisez les utilisateurs à lire les sessions enregistrées

Lorsque vous installez l'enregistrement de session, aucun utilisateur n'est autorisé à lire les sessions enregistrées. Vous devez attribuer cette autorisation à chaque utilisateur, y compris l'administrateur. Un utilisateur qui n'est pas autorisé à lire des sessions enregistrées reçoit le message d'erreur suivant lorsqu'il essaye de lire une session enregistrée :



1. Ouvrez une session en tant qu'administrateur sur l'ordinateur hébergeant le serveur d'enregistrement de session.
2. Démarrez la console d'autorisation d'enregistrement de session.
3. Dans la console d'autorisation d'enregistrement de session, sélectionnez Lecteur.
4. Ajoutez les utilisateurs et les groupes que vous souhaitez autoriser à afficher les sessions enregistrées et ils apparaitront dans le volet de droite.



Autorisez les utilisateurs à gérer les stratégies d'enregistrement

Lorsque vous installez l'enregistrement de session, les administrateurs de domaine accordent par défaut l'autorisation de contrôler les stratégies d'enregistrement. Vous pouvez modifier le paramètre d'autorisation.

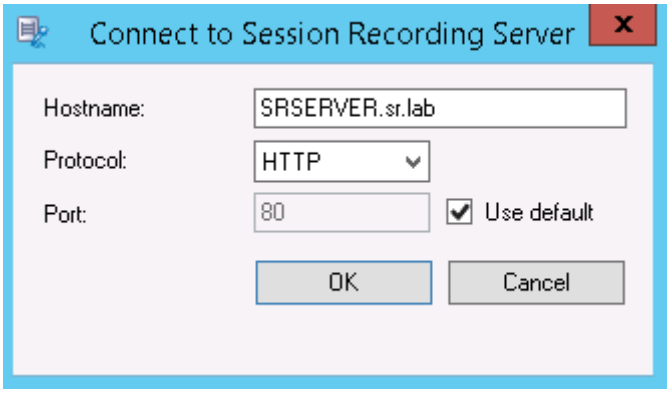
1. Ouvrez une session en tant qu'administrateur sur l'ordinateur hébergeant le serveur d'enregistrement de session.
2. Démarrez la console d'autorisation d'enregistrement de session et sélectionnez PolicyAdministrators.
3. Ajoutez les utilisateurs et les groupes pouvant administrer les stratégies d'enregistrement.

Paramétrez la stratégie d'enregistrement active de manière à enregistrer les sessions

La stratégie d'enregistrement active précise les modalités d'enregistrement des sessions sur tous les VDA ou VDI sur lesquels l'agent d'enregistrement de session est installé et connecté au serveur d'enregistrement de session. Lorsque vous installez l'enregistrement de session, la stratégie d'enregistrement active est **Ne pas enregistrer**. Les sessions ne pourront pas être enregistrées avant que vous ne changiez la stratégie d'enregistrement active.

Important : une stratégie peut contenir de multiples règles, mais une seule stratégie active peut être exécutée à la fois.

1. Ouvrez une session en tant qu'administrateur de stratégie autorisé sur le serveur sur lequel la console de stratégie d'enregistrement de session est installée.
2. Démarrez la console de stratégie d'enregistrement de session.
3. Si vous observez une fenêtre indépendante **Connexion au serveur d'enregistrement de session**, veillez à ce que le nom de l'ordinateur hébergeant le serveur d'enregistrement de session, le protocole et le port sont corrects.



4. Dans la console de stratégie d'enregistrement de session, développez **Stratégies d'enregistrement**. Les stratégies d'enregistrement disponibles lors de l'installation de l'enregistrement de session s'affichent, avec une coche indiquant la stratégie qui est active :
    - **Ne pas enregistrer**. Il s'agit de la stratégie par défaut. Si vous ne précisez pas d'autre stratégie, aucune session n'est enregistrée.
    - **Enregistrer tout le monde avec notification**. Si vous choisissez cette stratégie, toutes les sessions sont enregistrées. Une fenêtre contextuelle s'affiche pour notifier l'occurrence d'enregistrement.
    - **Enregistrer tout le monde sans notification**. Si vous choisissez cette stratégie, toutes les sessions sont enregistrées. Une fenêtre contextuelle s'affiche pour notifier l'occurrence d'enregistrement.
5. Sélectionnez la stratégie que vous souhaitez rendre active.
6. Dans la barre de menus, choisissez **Action** > **Activer la stratégie**.

L'enregistrement de session vous permet de créer votre propre stratégie d'enregistrement. Les stratégies d'enregistrement que vous créez s'affichent dans le dossier Stratégies d'enregistrement de la console de stratégie d'enregistrement de session.

Il est possible que la stratégie d'enregistrement générique ne réponde pas à vos besoins. Vous pouvez configurer des stratégies et des règles basées sur des utilisateurs, des serveurs VDA et VDI, des groupes de mise à disposition et des applications. Pour de plus amples informations sur les stratégies personnalisées, veuillez consulter la section
Créer des stratégies d'enregistrement personnalisées.

Remarque : la fonctionnalité Journalisation de l'administrateur de l'enregistrement de session vous permet de consigner les changements de stratégie d'enregistrement. Pour de plus amples informations, consultez
[Journaliser les activités d'administration].(/fr-fr/xenapp-and-xendesktop/7-15-ltsr/monitor/session-recording/administrator-logging.html)

Configurer le lecteur d'enregistrement de session

Avant qu'un lecteur d'enregistrement de session puisse lire des sessions, vous devez le configurer de manière à ce qu'il puisse se connecter au serveur d'enregistrement de session qui stocke les sessions enregistrées. Chaque lecteur d'enregistrement de session peut être configuré avec la capacité de se connecter à plusieurs serveurs d'enregistrement de session, mais ne peut se connecter qu'à un seul serveur d'enregistrement de session à la fois. Si le lecteur est configuré avec la capacité de se connecter à plusieurs serveurs d'enregistrement de session, les utilisateurs peuvent changer de serveur d'enregistrement de session auquel connecter le lecteur en cochant la case correspondante sous l'onglet **Connexions** dans **Outils** > **Options**.

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. Démarrez le lecteur d'enregistrement de session.
3. Dans la barre de menus du Lecteur d'enregistrement de session, choisissez **Outils** > **Options**.
4. Dans l'onglet **Connexions**, cliquez sur **Ajouter**.
5. Dans le champ **Nom de l'hôte**, entrez le nom ou l'adresse IP de l'ordinateur hébergeant le serveur d'enregistrement de session et sélectionnez le protocole. L'enregistrement de session est configuré par défaut pour utiliser HTTPS/SSL afin de sécuriser les communications. Si SSL n'est pas configuré, sélectionnez HTTP.
6. Pour configurer le lecteur d'enregistrement de session avec la capacité de se connecter à plusieurs serveurs d'enregistrement de session, répétez les étapes 4 et 5 pour chaque serveur d'enregistrement de session.
7. Veillez à cocher la case correspondant au serveur d'enregistrement de session auquel vous souhaitez vous connecter.

Configurer la connexion au serveur d'enregistrement de session

La connexion entre l'agent d'enregistrement de session et le serveur d'enregistrement de session est généralement configurée lorsque l'agent d'enregistrement de session est installé. Pour configurer cette connexion après l'installation de l'agent d'enregistrement de session, utilisez les propriétés de l'agent d'enregistrement de session.

1. Ouvrez une session sur le serveur sur lequel l'agent d'enregistrement de session est installé.
2. À partir du menu **Démarrer**, choisissez **Propriétés de l'Agent d'enregistrement de session**.
3. Cliquez sur l'onglet **Connexions**.
4. Dans le champ **Serveur d'enregistrement de session**, entrez le nom du serveur ou son adresse IP.
5. Dans la section **File d'attente des messages du gestionnaire de stockage d'enregistrement de session**, sélectionnez le protocole utilisé par le gestionnaire de stockage d'enregistrement de session pour communiquer et modifier le numéro de port par défaut, si nécessaire.

6. Dans le champ **Durée de validité des messages**, acceptez la valeur par défaut de 7200 secondes (deux heures) ou tapez une nouvelle valeur pour indiquer la durée en secondes pendant laquelle chaque message est conservé dans la file d'attente en cas de panne de communication. À l'issue de cette période, le message est supprimé et le fichier n'est lisible que jusqu'au point où la perte des données s'est produite.
7. Dans la section **Broker d'enregistrement de session**, sélectionnez le protocole de communication que le broker d'enregistrement de session utilise pour communiquer et modifier le numéro de port par défaut, si nécessaire.
8. À l'invite, redémarrez le **service de l'agent d'enregistrement de session** pour accepter les modifications.

Attribuer des droits d'accès aux utilisateurs

January 23, 2019

> **Important :**
>
> pour des raisons de sécurité, veillez à accorder uniquement aux utilisateurs les droits nécessaires à l'accomplissement de fonctions précises, comme l'affichage de sessions enregistrées par exemple.

Vous accordez ces privilèges aux utilisateurs de l'enregistrement de session en les attribuant à des rôles, par le biais de la console d'autorisation d'enregistrement de session sur le serveur d'enregistrement de session. Les utilisateurs de l'enregistrement de session ont trois rôles :

- **Lecteur**. Ce rôle donne le droit à l'utilisateur d'afficher des sessions XenApp enregistrées. Ce rôle n'est rattaché à aucune appartenance par défaut.
- **PolicyQuery (requête de stratégie)**. Cette option permet aux serveurs hébergeant l'agent d'enregistrement de session de demander des évaluations de stratégie d'enregistrement. Par défaut, les utilisateurs authentifiés sont membres de ce rôle.
- **PolicyAdministrator (administrateur de stratégie)**. Ce rôle donne le droit d'afficher, de créer, de modifier, de supprimer et d'activer les stratégies d'enregistrement. Par défaut, les administrateurs de l'ordinateur hébergeant le serveur d'enregistrement de session sont membres de ce rôle.

L'enregistrement de session prend en charge les utilisateurs et les groupes définis dans Active Directory.

Attribuer des rôles aux utilisateurs

1. Ouvrez une session sur l'ordinateur hébergeant le serveur d'enregistrement de session, en tant qu'administrateur ou en tant que membre du rôle d'administrateur de stratégie (Policy Admin-

istrator).
2. Démarrez la console d'autorisation d'enregistrement de session.
3. Sélectionnez le rôle que vous souhaitez attribuer aux utilisateurs.
4. Dans la barre de menus, choisissez **Action** > **Assigner des groupes et des utilisateurs Windows**.
5. Ajoutez les utilisateurs et les groupes.

Toute modification apportée à la console prend effet au cours de la mise à jour, qui se produit toutes les minutes.

Créer et activer des stratégies d'enregistrement

February 28, 2019

Utilisez la console de stratégie d'enregistrement de session pour créer et activer les stratégies qui déterminent quelles sessions sont enregistrées.

> **Important :**
>
> pour utiliser la Console de stratégie d'enregistrement de session, le Broker PowerShell Snap-in (Broker_PowerShellSnapIn_x64.msi) doit être installé. Ce composant logiciel enfichable ne peut pas être installé automatiquement par le programme d'installation. Accédez au composant logiciel enfichable dans le fichier ISO de XenApp/XenDesktop (sous \layout\image-full\x64\Citrix Desktop Delivery Controller) et suivez les instructions pour l'installer manuellement. Si vous ne respectez pas cette consigne, cela peut entraîner une erreur.

Vous pouvez activer les stratégies de système disponibles lors de l'installation de l'enregistrement de session ou créer et activer vos propres stratégies personnalisées. Les stratégies de système d'enregistrement de session appliquent une règle unique à tous les utilisateurs, à toutes les applications publiées et à tous les serveurs. Les stratégies personnalisées précisent quels utilisateurs, quelles applications publiées et quels serveurs sont enregistrés.

La stratégie active détermine quelles sessions sont enregistrées. Une seule stratégie peut être active à la fois.

Stratégies de système

L'enregistrement de session fournit ces stratégies de système :

- **Ne pas enregistrer**. Il s'agit de la stratégie par défaut. Si vous ne précisez pas d'autre stratégie, aucune session n'est enregistrée.

- **Enregistrer tout le monde avec notification**. Si vous choisissez cette stratégie, toutes les sessions sont enregistrées. Une fenêtre contextuelle s'affiche pour notifier l'occurrence d'enregistrement.
- **Enregistrer tout le monde sans notification**. Si vous choisissez cette stratégie, toutes les sessions sont enregistrées. Une fenêtre contextuelle s'affiche pour notifier l'occurrence d'enregistrement.

Les stratégies de système ne peuvent être ni modifiées, ni supprimées.

Activer une stratégie

1. Ouvrez une session sur le serveur sur lequel la console de stratégie d'enregistrement de session est installée.
2. Démarrez la console de stratégie d'enregistrement de session.
3. Si vous observez une fenêtre indépendante **Connexion au serveur d'enregistrement de session**, veillez à ce que le nom du serveur d'enregistrement de session, le protocole et le port sont corrects. Cliquez sur **OK**.
4. Dans la console de stratégie d'enregistrement de session, développez **Stratégies d'enregistrement**.
5. Sélectionnez la stratégie que vous souhaitez rendre active.
6. Dans la barre de menus, choisissez **Action** > **Activer la stratégie**.

Créer des stratégies d'enregistrement personnalisées

Lorsque vous créez votre propre stratégie, vous établissez des règles précisant pour quels utilisateurs, groupes, applications publiées et serveurs les sessions sont enregistrées. Un assistant intégré à la console de stratégie d'enregistrement de session vous aide à créer des règles. Pour obtenir la liste des applications publiées et des serveurs, vous devez disposer des droits de lecture de l'administrateur du site. Configurez ces droits sur le Delivery Controller de ce site.

Pour chaque règle que vous créez, vous spécifiez une action d'enregistrement et un critère de règle. L'action d'enregistrement s'applique aux sessions qui correspondent au critère de règle.

Pour chaque règle, choisissez une action d'enregistrement :

- **Ne pas enregistrer**. (Choisissez **Désactiver l'enregistrement de session** dans l'assistant **Règles**). Cette action d'enregistrement précise que les sessions correspondant aux critères de la règle ne sont pas enregistrées.
- **Enregistrer avec notification**. (Choisissez **Activer l'enregistrement de session avec notification** dans l'assistant **Règles**). Cette action d'enregistrement précise que les sessions correspondant aux critères de la règle sont enregistrées. Une fenêtre contextuelle s'affiche pour notifier l'occurrence d'enregistrement.

- **Enregistrer sans notification**. (Choisissez **Activer l'enregistrement de session sans notification** dans l'assistant **Règles**). Cette action d'enregistrement précise que les sessions correspondant aux critères de la règle sont enregistrées. Les utilisateurs ignorent que leurs activités sont enregistrées.

Pour chaque règle, choisissez au moins l'une des règles suivantes pour créer les critères de règle :

- **Utilisateurs ou groupes**. Crée une liste d'utilisateurs ou de groupes auxquels l'action d'enregistrement de la règle s'applique.
- **Ressources publiées**. Crée une liste d'applications ou de bureaux publiés auxquels l'action d'enregistrement de la règle s'applique. Dans l'assistant **Règles**, choisissez le ou les sites XenApp/XenDesktop sur lesquels les applications ou bureaux sont disponibles.
- **Groupes de mise à disposition ou machines**. Crée une liste de groupes de mise à disposition ou de machines auxquels l'action d'enregistrement de la règle s'applique. Dans l'assistant **Règles**, choisissez l'emplacement des groupes de mise à disposition ou machines.
- **Adresse IP ou plage d'adresses IP**. Crée une liste d'adresses IP ou des plages d'adresses IP auxquelles l'action d'enregistrement de la règle s'applique. Dans la boîte de dialogue **Sélectionner IP et plage d'adresses IP**, ajoutez une adresse IP ou une plage d'adresses IP valide pour lesquelles l'enregistrement sera activé ou désactivé.

Remarque : la console de stratégie d'enregistrement de session prend en charge la configuration de plusieurs critères au sein d'une règle unique. Lorsqu'une règle s'applique, les opérateurs logiques « ET » et « OU » sont utilisés pour calculer l'action finale. Généralement, l'opérateur « OU » est utilisé entre les éléments au sein d'un critère, et l'opérateur « ET » est quant à lui utilisé entre les critères distincts. Si le résultat est true, le moteur de stratégie d'enregistrement de session entreprend l'action de la règle. Sinon, il passe à la règle suivante et répète le processus.

Lorsque vous créez plus d'une règle dans une stratégie d'enregistrement, il est possible que certaines sessions correspondent aux critères de plusieurs de ces règles. Dans ces cas de figure, la règle ayant la plus haute priorité est celle appliquée aux sessions.

L'action d'enregistrement d'une règle en détermine la priorité :

- Les règles avec l'action **Ne pas enregistrer** ont la plus haute priorité.
- Les règles avec l'action **Enregistrer avec notification** ont la seconde plus haute priorité.
- Les règles avec l'action **Enregistrer sans notification** ont la priorité la plus faible.

Il se peut que certaines sessions ne correspondent à aucun critère de règle d'une stratégie d'enregistrement. Pour ces sessions, l'action d'enregistrement de la règle de repli des stratégies s'applique. L'action d'enregistrement de la règle de repli est toujours **Ne pas enregistrer**. La règle de repli ne peut être ni modifiée, ni supprimée.

Pour configurer des stratégies personnalisées, procédez comme suit :

1. Ouvrez une session en tant qu'administrateur de stratégie autorisé sur le serveur sur lequel la console de stratégie d'enregistrement de session est installée.

2. Démarrez la Console de stratégie d'enregistrement de session et sélectionnez **Stratégies d'enregistrement** dans le panneau gauche. Dans la barre de menus, choisissez **Action** > **Ajouter une nouvelle stratégie**.
3. Cliquez avec le bouton droit sur **Nouvelle stratégie** et sélectionnez **Ajouter une règle**.
4. Sélectionnez une option d'enregistrement : dans l'assistant **Règles**, sélectionnez **Désactiver l'enregistrement de session**, **Activer l'enregistrement de session avec notification** (ou **sans notification**), puis cliquez sur **Suivant**.
5. Sélectionnez les critères de la règle : vous pouvez choisir une option ou une combinaison d'options :
   Utilisateurs ou Groupes
   Ressources publiées
   Groupes de mise à disposition ou Machines
   Adresse IP ou Plage d'adresses IP
6. Modifiez les critères de la règle : pour modifier, cliquez sur les valeurs soulignées. Les valeurs sont soulignées en fonction des critères que vous avez choisis dans l'étape précédente.
   Remarque : si vous choisissez la valeur soulignée **Ressources publiées**, l'**adresse du site** est l'adresse IP, une adresse URL ou un nom de machine si le Controller se trouve sur un réseau local. La liste **Nom de l'application** indique le nom d'affichage.
7. Suivez les instructions de l'assistant pour terminer la configuration.

Utiliser des groupes Active Directory

L'enregistrement de session vous permet d'utiliser les groupes Active Directory lorsque vous créez des stratégies. Utiliser les groupes Active Directory au lieu d'utilisateurs individuels simplifie la création et la gestion des règles et des stratégies. Par exemple, si les utilisateurs du service financier de votre société sont réunis dans un groupe Active Directory intitulé « Finance », vous pouvez créer une règle concernant tous les membres de ce groupe en sélectionnant le groupe Finance dans l'Assistant **Règles** lors de la création de la règle.

Utilisateurs sur liste blanche

Vous pouvez créer des stratégies d'enregistrement de session qui font en sorte que certains utilisateurs de votre organisation ne sont jamais enregistrés. Cela peut se traduire par mettre ces utilisateurs en *liste blanche*. La liste blanche est utile pour les utilisateurs qui gèrent des informations relatives à la confidentialité ou lorsque votre organisation ne souhaite pas enregistrer les sessions d'une certaine classe d'employés.

Par exemple, si tous les managers d'une entreprise sont membres d'un groupe Active Directory intitulé « Cadres supérieurs », vous pouvez être faire en sorte que les sessions de ces utilisateurs ne sont jamais enregistrées en créant une règle désactivant l'enregistrement de sessions pour le groupe

Cadres supérieurs. Lorsque la stratégie contenant cette règle est active, aucune session des membres du groupe Cadres supérieurs n'est enregistrée. Les sessions des autres membres de votre organisation sont enregistrées en fonction d'autres règles de la stratégie active.

Utiliser les critères de règle Adresse IP ou plage d'adresses IP

Vous pouvez utiliser les adresses IP des machines clientes en tant que critères de correspondance de stratégie. Par exemple, si vous souhaitez enregistrer des sessions à partir de clients avec des adresses IP spécifiques ou dans une certaine plage d'adresses IP, utilisez l'assistant **Règles** pour créer une règle qui s'applique uniquement à ces clients.

Créer une nouvelle stratégie

Remarque : pour utiliser l'assistant **Règles**, vous pouvez être invité à « cliquer sur la valeur soulignée pour la modifier » lorsqu'aucune valeur soulignée ne s'affiche. Les valeurs soulignées s'affichent uniquement le cas échéant. Si aucune valeur soulignée ne s'affiche, ignorez l'étape.

1. Ouvrez une session sur le serveur sur lequel la console de stratégie d'enregistrement de session est installée.
2. Démarrez la console de stratégie d'enregistrement de session.
3. Si vous observez une fenêtre indépendante **Connexion au serveur d'enregistrement de session**, veillez à ce que le nom du serveur d'enregistrement de session, le protocole et le port sont corrects. Cliquez sur **OK**.
4. Dans la console de stratégie d'enregistrement de session, sélectionnez **Stratégies d'enregistrement**.
5. Dans le menu, choisissez **Ajouter une nouvelle stratégie**. Une stratégie intitulée **Nouvelle stratégie** s'affiche dans le volet gauche.
6. Cliquez avec le bouton droit sur la nouvelle stratégie et choisissez **Renommer** à partir du menu.
7. Entrez un nouveau nom pour la stratégie que vous allez créer et appuyez sur **Entrée** ou cliquez n'importe où hors du cadre du nouveau nom.
8. Cliquez avec le bouton droit sur la stratégie, choisissez **Ajouter une nouvelle règle** dans le menu de lancer l'assistant **Règles**.
9. Suivez les instructions pour créer les règles de cette stratégie.

Modifier une stratégie

1. Ouvrez une session sur le serveur sur lequel la console de stratégie d'enregistrement de session est installée.
2. Démarrez la console de stratégie d'enregistrement de session.

3. Si vous observez une fenêtre indépendante **Connexion au serveur d'enregistrement de session**, veillez à ce que le nom du serveur d'enregistrement de session, le protocole et le port sont corrects. Cliquez sur **OK**.
4. Dans la console de stratégie d'enregistrement de session, développez **Stratégies d'enregistrement**.
5. Sélectionnez la stratégie que vous souhaitez modifier. Les règles de cette stratégie s'affichent dans le volet droit.
6. Pour ajouter une nouvelle règle, modifier une règle ou supprimer une règle :
    - Dans la barre de menus, choisissez **Action** > **Ajouter une nouvelle règle**. Si cette stratégie est active, une fenêtre indépendante s'affiche pour demander confirmation de l'action entreprise. Utilisez l'assistant **Règles** pour créer une nouvelle règle.
    - Sélectionnez la règle que vous souhaitez modifier, cliquez avec le bouton droit de la souris et choisissez **Propriétés**. Utilisez l'assistant **Règles** pour modifier la règle.
    - Sélectionnez la règle que vous souhaitez supprimer, cliquez avec le bouton droit de la souris et choisissez **Supprimer la règle**.

Supprimer une stratégie

Remarque : vous ne pouvez pas supprimer de stratégie de système ou une stratégie active.

1. Ouvrez une session sur le serveur sur lequel la console de stratégie d'enregistrement de session est installée.
2. Démarrez la console de stratégie d'enregistrement de session.
3. Si vous observez une fenêtre indépendante **Connexion au serveur d'enregistrement de session**, veillez à ce que le nom du serveur d'enregistrement de session, le protocole et le port sont corrects. Cliquez sur **OK**.
4. Dans la console de stratégie d'enregistrement de session, développez **Stratégies d'enregistrement**.
5. Dans le volet gauche, sélectionnez la stratégie que vous souhaitez supprimer. Si la stratégie est active, vous devez en activer une autre.
6. Dans la barre de menus, choisissez **Action** > **Supprimer la stratégie**.
7. Sélectionnez **Oui** pour confirmer l'action.

Remarque : limitation concernant les sessions d'application pré-lancées :

- Si la stratégie active tente d'effectuer une correspondance avec un nom d'application, la correspondance avec les applications lancées dans la session de pré-lancement n'est pas établie, ce qui entraîne l'échec de l'enregistrement de la session.
- Si la stratégie active enregistre chaque application, lorsqu'un utilisateur ouvre la session Citrix Receiver pour Windows (au même moment où la session de pré-lancement est ouverte), une notification d'enregistrement apparaît et la session de pré-lancement (vide) et toute application lancée ultérieurement dans cette session sont enregistrées.

Pour contourner le problème, publiez les applications dans des groupes de mise à disposition séparés

en fonction de leurs stratégies d'enregistrement. N'utilisez pas de nom d'application en tant que condition d'enregistrement. Cela garantit que les sessions pré-lancées peuvent être enregistrées. Toutefois, les notifications continuent à s'afficher.

Comportement de substitution - définitions

Lorsque vous activez une stratégie, la stratégie précédemment active reste en vigueur jusqu'à la fin de la session de l'utilisateur. Toutefois, dans certains cas, la nouvelle stratégie prend effet lorsque le fichier est substitué. Les fichiers sont substitués lorsqu'ils atteignent la taille maximale. Pour plus d'informations sur la taille maximale des fichiers pour les enregistrements, consultez la section Définir la taille des fichiers pour les enregistrements.

Le tableau suivant illustre en détail les événements qui se produisent lorsque vous appliquez une nouvelle stratégie pendant qu'une session est en cours d'enregistrement et qu'une substitution a lieu :

Stratégie précédente :	Nouvelle stratégie :	Stratégie en vigueur après la substitution :
Ne pas enregistrer.	Toute autre stratégie.	Pas de modification. La nouvelle stratégie ne prend effet que lorsque l'utilisateur ouvre une nouvelle session.
Enregistrer sans notification	Ne pas enregistrer.	L'enregistrement s'arrête.
Enregistrer sans notification	Enregistrer avec notification	L'enregistrement continue et un message de notification s'affiche.
Enregistrer avec notification	Ne pas enregistrer.	L'enregistrement s'arrête.
Enregistrer avec notification	Enregistrer sans notification	L'enregistrement continue. Aucun message ne s'affiche avant que l'utilisateur ouvre une nouvelle session.

Créer des messages de notification

February 28, 2019

Si la stratégie d'enregistrement active précise que les utilisateurs sont prévenus lorsque leurs sessions sont enregistrées, une fenêtre indépendante s'ouvre et affiche un message de notification après

que les utilisateurs aient entré leurs informations d'identification. Le message de notification par défaut est `"Your activity with one or more of the programs you recently started is being recorded. If you object to this condition, close the programs."` Les utilisateurs peuvent cliquer sur **OK** pour fermer la fenêtre et pour continuer leurs sessions.

Le message de notification par défaut s'affiche dans la langue du système d'exploitation des ordinateurs hébergeant le serveur d'enregistrement de session.

Vous pouvez créer des notifications personnalisées dans les langues de votre choix ; toutefois, vous ne disposez que d'un message de notification par langue. Vos utilisateurs voient les messages de notification dans la langue correspondant à leurs paramètres locaux préférés.

Créer un nouveau message de notification

1. Ouvrez une session sur l'ordinateur exécutant le serveur d'enregistrement de session.
2. À partir du menu **Démarrer**, choisissez **Propriétés du lecteur d'enregistrement de session**.
3. Dans la fenêtre **Propriétés du serveur d'enregistrement de session**, cliquez sur l'onglet **Notifications**.
4. Cliquez sur **Ajouter**.
5. Choisissez la langue du message et tapez le nouveau message. Vous ne pouvez créer qu'un seul message par langue.

Une fois accepté et activé, le nouveau message s'affiche dans la boîte Messages de notification en langues étrangères.

Remarque : la fonctionnalité Journalisation de l'administrateur de l'enregistrement de session vous permet de consigner les changements de stratégie de serveur d'enregistrement de session. Pour de plus amples informations, consultez Journaliser les activités d'administration.

Désactiver ou activer l'enregistrement

January 23, 2019

L'installation de l'agent d'enregistrement de session s'effectue sur chaque VDA pour OS de serveur pour lequel vous souhaitez enregistrer des sessions. Chaque Agent est équipé d'un paramètre permettant d'activer les enregistrements pour le serveur sur lequel il est installé. Après l'activation de la fonction d'enregistrement, l'enregistrement de session évalue la stratégie d'enregistrement active qui détermine les sessions à enregistrer.

Lorsque vous installez l'agent d'enregistrement de session, la fonction d'enregistrement est activée. Citrix vous recommande de désactiver l'enregistrement de session sur les serveurs qui ne sont pas enregistrés, compte tenu du léger impact sur les performances au niveau du serveur, même si aucun enregistrement n'a lieu.

Désactiver ou activer l'enregistrement sur un serveur

1. Ouvrez une session sur le serveur sur lequel l'agent d'enregistrement de session est installé.
2. À partir du menu **Démarrer**, choisissez **Propriétés de l'Agent d'enregistrement de session**.
3. Sous l'option **Enregistrement de session**, sélectionnez ou effacez le contenu de la case **Activer l'enregistrement de session pour ce VDA avec OS de serveur** afin de spécifier si les sessions de ce serveur peuvent être enregistrées.
4. À l'invite, redémarrez le service de l'agent d'enregistrement de session pour accepter la modification.

Remarque : lorsque vous installez l'enregistrement de session, la stratégie active est
Ne pas enregistrer (aucune session n'est enregistrée, sur aucun serveur). Pour commencer à enregistrer, utilisez la
console de stratégie d'enregistrement de session pour activer une stratégie différente.

Activer l'enregistrement d'événement personnalisé

L'enregistrement de session vous permet d'utiliser des applications tierces pour insérer des données personnalisées (des événements) dans des sessions enregistrées. Ces événements s'affichent lorsque la session est visualisée à l'aide du lecteur d'enregistrement de session. Ils font partie du fichier de la session enregistrée et ne peuvent pas être modifiés une fois la session enregistrée.

Par exemple, un événement peut contenir le texte suivant : « Ouverture de navigateur par l'utilisateur ». Chaque fois qu'un utilisateur ouvre un navigateur pendant une session en cours d'enregistrement, le texte s'insère dans l'enregistrement à ce point. Lorsque la session est lue dans le lecteur d'enregistrement de session, le visualiseur peut localiser et compter le nombre de fois qu'un utilisateur a ouvert un navigateur en notant le nombre de marqueurs figurant dans la liste Événements et signets du lecteur d'enregistrement de session.

Pour insérer des événements personnalisés dans les enregistrements sur un serveur :

- Utilisez la fenêtre **Propriétés de l'Agent d'enregistrement de session** pour activer un paramètre sur chaque serveur dans lequel vous souhaitez insérer des événements personnalisés. Vous devez activer chaque serveur séparément. Vous ne pouvez pas activer globalement tous les serveurs d'un site.
- Générez des applications sur l'API d'enregistrement d'événements s'exécutant dans chaque session XenApp des utilisateurs (pour injecter les données dans l'enregistrement).

L'installation de l'enregistrement de session comprend une interface d'application COM (API) vous permettant d'insérer du texte provenant d'applications tierces dans un enregistrement. Vous pouvez utiliser l'API de nombreux langages de programmation, notamment Visual Basic, C++ ou C#. Pour plus d'informations, consultez l'article Citrix CTX226844. Le fichier .dll API des événements

d'enregistrement de session est installé dans le cadre de l'installation de l'enregistrement de session. Il se trouve à l'emplacement suivant : C:\Program Files\Citrix\SessionRecording\Agent\Bin\Interop.UserApi.dll.

Pour activer l'enregistrement d'événements personnalisés sur un serveur, procédez comme suit :

1. Ouvrez une session sur le serveur sur lequel l'agent d'enregistrement de session est installé.
2. À partir du menu **Démarrer**, choisissez **Propriétés de l'Agent d'enregistrement de session**.
3. Dans la fenêtre **Propriétés de l'Agent d'enregistrement de session**, cliquez sur l'onglet **Enregistrement**.
4. Sous **Enregistrement d'événement personnalisé**, cochez la case **Permettre aux applications tierces d'enregistrer des données personnalisées sur ce serveur**.

Activer ou désactiver la lecture de session active et la protection de lecture

January 23, 2019

Activer ou désactiver la lecture de session active

Avec le lecteur d'enregistrement de session, vous pouvez visualiser une session pendant son enregistrement ou après celui-ci. L'affichage d'une session en cours d'enregistrement est similaire au visionnage d'actions se déroulant en direct ; il existe toutefois un décalage d'une ou deux secondes dû à la propagation des données du serveur XenApp ou XenDesktop.

Certaines fonctionnalités ne sont pas disponibles pendant l'affichage de la session dont l'enregistrement n'est pas terminé :

- Une signature numérique ne peut pas être attribuée tant que l'enregistrement n'est pas terminé. Si la signature numérique est activée, vous pouvez afficher les sessions actives, mais elles ne sont pas signées numériquement et vous ne pouvez pas en voir les certificats avant que la session se termine.
- La protection en lecture ne peut pas s'appliquer tant que l'enregistrement n'est pas terminé. Si la protection en lecture est activée, vous pouvez afficher les sessions actives, mais elles ne sont pas cryptées tant que la session n'est pas terminée.
- Vous ne pouvez pas mettre en cache un fichier tant que l'enregistrement n'est pas terminé.

Par défaut, la lecture de session active est activée.

1. Ouvrez une session sur l'ordinateur exécutant le serveur d'enregistrement de session.
2. À partir du menu **Démarrer**, choisissez **Propriétés du lecteur d'enregistrement de session**.
3. Dans la fenêtre **Propriétés du serveur d'enregistrement de session**, cliquez sur l'onglet **Lecture**.

4. Cochez ou désélectionnez la case **Autoriser la lecture d'une session active**.

Activer ou désactiver la protection de lecture

Par mesure de sécurité, l'enregistrement de session crypte automatiquement les fichiers enregistrés avant qu'ils soient téléchargés pour être affichés dans le lecteur d'enregistrement de session. Cette protection de lecture empêche les fichiers enregistrés d'être copiés et visualisés par toute personne autre que l'utilisateur ayant téléchargé le fichier. Les fichiers ne peuvent pas être lus sur une autre station de travail ou par un autre utilisateur. Les fichiers cryptés sont identifiés par l'extension .icle ; les fichiers non cryptés sont identifiés par l'extension .icl. Les fichiers demeurent cryptés tant qu'ils résident dans le cache de la station de travail sur laquelle le lecteur d'enregistrement de session est installé, et ce jusqu'à ce qu'ils soient ouverts par un utilisateur autorisé.

Citrix vous recommande d'utiliser HTTPS pour protéger le transfert de données.

Par défaut, la protection de lecture est désactivée.

1. Ouvrez une session sur l'ordinateur exécutant le serveur d'enregistrement de session.
2. À partir du menu **Démarrer**, choisissez **Propriétés du lecteur d'enregistrement de session**.
3. Dans la fenêtre **Propriétés du serveur d'enregistrement de session**, cliquez sur l'onglet **Lecture**.
4. Cochez ou désélectionnez la case **Crypter les fichiers d'enregistrement de session téléchargés pour les lire**.

Activer et désactiver les signatures numériques

November 13, 2018

Si vous installez des certificats sur les ordinateurs sur lesquels les composants d'enregistrement de session sont installés, vous pouvez augmenter la sécurité de votre déploiement d'enregistrement de session en attribuant des signatures numériques à l'enregistrement de sessions.

Par défaut, la fonction de signature numérique est désactivée. Après avoir sélectionné le certificat utilisé pour signer les enregistrements, l'enregistrement de session accorde une autorisation d'accès en lecture au Gestionnaire de stockage d'enregistrement de session.

Activer les signatures numériques

1. Ouvrez une session sur l'ordinateur exécutant le serveur d'enregistrement de session.
2. À partir du menu **Démarrer**, choisissez **Propriétés du lecteur d'enregistrement de session**.
3. Dans la fenêtre **Propriétés du serveur d'enregistrement de session**, cliquez sur l'onglet **Signature**.

4. Recherchez le certificat qui permet la communication sécurisée entre les ordinateurs sur lesquels les composants d'enregistrement de session sont installés.

Désactiver les signatures numériques

1. Ouvrez une session sur l'ordinateur exécutant le serveur d'enregistrement de session.
2. À partir du menu **Démarrer**, choisissez **Propriétés du lecteur d'enregistrement de session**.
3. Dans la fenêtre **Propriétés du serveur d'enregistrement de session**, cliquez sur l'onglet **Signature**.
4. Cliquez sur **Effacer**.

Spécifier où les enregistrements sont stockés

November 13, 2018

Utilisez la fenêtre Propriétés du serveur d'enregistrement de session pour spécifier l'emplacement du stockage des enregistrements et l'emplacement de restauration des enregistrements restaurés pour la lecture.

Remarque : pour archiver les fichiers ou restaurer les fichiers supprimés, utilisez la commande ICLDB.

Spécifier des répertoires pour stocker les enregistrements

Par défaut, les enregistrements sont stockés dans le répertoire lecteur :**\SessionRecordings** de l'ordinateur hébergeant le serveur d'enregistrement de session. Vous pouvez changer le répertoire de stockage des enregistrements, ajouter des répertoires supplémentaires afin d'équilibrer la charge sur plusieurs volumes ou d'optimiser l'usage d'espace supplémentaire. La présence de plusieurs répertoires dans la liste indique que l'équilibrage de la charge s'applique dans les répertoires pour les enregistrements. Vous pouvez ajouter un répertoire plusieurs fois. L'équilibrage de charge passe successivement dans tous les répertoires.

1. Ouvrez une session sur l'ordinateur exécutant le serveur d'enregistrement de session.
2. À partir du menu **Démarrer**, choisissez **Propriétés du lecteur d'enregistrement de session**.
3. Dans la fenêtre **Propriétés du serveur d'enregistrement de session**, cliquez sur l'onglet **Stockage**.
4. Utilisez la liste **Répertoire de stockage des fichiers** pour gérer les répertoires dans lesquels les enregistrements sont stockés.

Après la sélection des répertoires, l'enregistrement de session accorde à son service les autorisations de contrôle total sur ces répertoires.

Vous pouvez créer des répertoires de stockage de fichier sur le lecteur local, le volume réseau SAN ou un chemin réseau UNC complet. Les lettres de lecteur mappées sur réseau ne sont pas prises en charge. N'utilisez pas l'enregistrement de session avec un serveur NAS (Network-Attached Storage), en raison des sérieux problèmes de performances et de sécurité liés à l'écriture des données d'enregistrement sur un lecteur réseau.

Spécifier un répertoire pour restaurer les enregistrements archivés pour la lecture

Par défaut, les enregistrements archivés sont restaurés sur le répertoire : **\SessionRecordingsRestore** de l'ordinateur hébergeant le serveur d'enregistrement de session. Vous pouvez changer le répertoire.

1. Ouvrez une session sur l'ordinateur exécutant le serveur d'enregistrement de session.
2. À partir du menu **Démarrer**, choisissez **Propriétés du lecteur d'enregistrement de session**.
3. Dans la fenêtre **Propriétés du serveur d'enregistrement de session**, cliquez sur l'onglet **Stockage**.
4. Dans le champ **Restaurer le répertoire des fichiers archivés**, tapez le répertoire dans lequel restaurer les enregistrements archivés.

Définir la taille des fichiers pour les enregistrements

January 23, 2019

À mesure que la taille des enregistrements augmente, les fichiers peuvent prendre plus longtemps à télécharger et réagir plus lentement lorsque vous utilisez le curseur de recherche pour naviguer pendant la lecture. Pour contrôler la taille des fichiers, spécifiez un seuil limite. Lorsque l'enregistrement atteint cette limite, l'enregistrement de session ferme le fichier et en ouvre un nouveau afin de poursuivre l'enregistrement. Cette action s'appelle une substitution.

Important : le paramètre de substitution ne s'applique pas aux sessions de bureau VDI pour XenDesktop 7.8 et l'agent d'enregistrement de session. Dans ce cas, chaque fichier d'enregistrement a une limite de taille maximale de 1 Go et les activités ne sont pas enregistrées une fois que cette limite est atteinte.

Vous pouvez préciser deux seuils pour une substitution :

- **Taille du fichier.** Lorsque le fichier atteint le nombre de méga-octets spécifié, l'enregistrement de session ferme le fichier et en ouvre un nouveau. Par défaut, les fichiers sont substitués lorsqu'ils atteignent 50 mégaoctets ; toutefois vous pouvez spécifier une limite allant de 10 mégaoctets à un gigaoctet.
- **Durée.** Lorsque la durée d'enregistrement de la session atteint le nombre d'heures précisé, le fichier se ferme et un nouveau fichier s'ouvre. Par défaut, les fichiers sont repris lorsque la durée

d'enregistrement atteint 12 heures, mais vous pouvez spécifier une limite allant de 1 heure à 24 heures.

L'enregistrement de session vérifie les deux champs afin de déterminer lequel des événements se produit en premier pour activer une substitution. Par exemple, si vous spécifiez une valeur de 17 Mo pour la taille de fichier et six heures pour la durée et que l'enregistrement atteint 17 Mo en trois heures, l'enregistrement de session réagit à la taille de fichier (17 Mo) pour fermer le fichier et en ouvrir un nouveau.

Pour éviter de créer trop de fichiers de petite taille, l'enregistrement de session ne procède à aucune substitution avant qu'une heure au moins ne se soit écoulée (il s'agit du nombre minimal que vous pouvez entrer), quelle que soit la valeur spécifiée pour la taille de fichier. L'exception à cette règle est si la taille du fichier dépasse un gigaoctet.

Définir la taille maximale des fichiers pour les enregistrements

1. Ouvrez une session sur l'ordinateur exécutant le serveur d'enregistrement de session.
2. À partir du menu **Démarrer**, choisissez **Propriétés du lecteur d'enregistrement de session**.
3. Dans la fenêtre **Propriétés du serveur d'enregistrement de session**, cliquez sur l'onglet **Substitution**.
4. Entrez un nombre entier compris entre 10 et 1024 pour spécifier la taille maximale des fichiers, en méga-octets.
5. Entrez un nombre entier compris entre 1 et 24 pour spécifier la durée maximale des enregistrements, en heures.

Journaliser les activités d'administration

January 23, 2019

La fonctionnalité Journalisation de l'administrateur d'enregistrement de session consigne les activités suivantes :

- Les modifications apportées aux stratégies d'enregistrement dans la console de stratégie d'enregistrement de session ou Citrix Director.
- Les modifications apportées aux propriétés du serveur d'enregistrement de session Citrix.
- Les téléchargements d'enregistrements dans le lecteur d'enregistrement de session.
- L'enregistrement d'une session après une requête de stratégie.
- Les tentatives non autorisées d'accès au service Journalisation de l'administrateur.

> **Avertissement :**
>
> Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Désactiver ou activer la journalisation de l'administrateur

Après l'installation, vous pouvez activer ou désactiver la fonctionnalité Journalisation de l'administrateur dans la boîte de dialogue Propriétés du serveur d'enregistrement de session.

1. Ouvrez une session en tant qu'administrateur sur le serveur sur lequel la journalisation de l'administrateur d'enregistrement de session est installée.
2. À partir du menu **Démarrer**, choisissez **Propriétés du lecteur d'enregistrement de session**.
3. Cliquez sur l'onglet **Enregistrement**.

Lorsque la journalisation de l'administrateur d'enregistrement de session est désactivée, aucune nouvelle activité n'est consignée. Vous pouvez consulter les journaux existants à partir de l'interface Web.

Lorsque le **blocage obligatoire** est activé, les activités suivantes sont bloquées si la journalisation échoue. Un événement système est également consigné avec l'ID d'événement 6001 :

- Les modifications apportées aux stratégies d'enregistrement dans la console de stratégie d'enregistrement de session ou Citrix Director.
- Les modifications apportées aux propriétés du serveur d'enregistrement de session Citrix.

L'enregistrement de session n'est pas affecté par le paramètre de blocage obligatoire.

Attribuer des droits d'accès aux utilisateurs

Pour des raisons de sécurité, veillez à accorder uniquement aux utilisateurs les droits nécessaires à l'accomplissement de fonctions précises, comme l'interrogation des journaux de la journalisation de l'administrateur.

Vous accordez ces privilèges aux utilisateurs en les attribuant à des rôles, par le biais de la console d'autorisation d'enregistrement de session sur le serveur d'enregistrement de session. La journalisation de l'administrateur est associée à deux rôles :

- **LoggingWriter**. Ce rôle donne le droit d'écrire dans les journaux de l'administrateur. Par défaut, les administrateurs locaux et le service réseau sont membres de ce rôle.

  Remarque : la modification de l'appartenance à **LoggingWriter** par défaut peut entraîner l'échec de la journalisation.

- **LoggingReader**. Ce rôle donne le droit d'interroger les journaux de l'administrateur. Ce rôle n'est rattaché à aucune appartenance par défaut.

Pour attribuer des rôles aux utilisateurs

1. En tant qu'administrateur, ouvrez une session sur l'ordinateur hébergeant le serveur d'enregistrement de session.
2. Démarrez la **console d'autorisation d'enregistrement de session**.
3. Sélectionnez le rôle que vous souhaitez attribuer aux utilisateurs.
4. Dans la barre de menus, choisissez **Action** > **Assigner des groupes et des utilisateurs Windows**.
5. Ajouter des utilisateurs et des groupes.

Toute modification apportée à la console prend effet au cours de la mise à jour, qui se produit toutes les minutes.

Configurer un compte de service de la journalisation de l'administrateur

Par défaut, la journalisation de l'administrateur est exécutée en tant qu'application Web dans Internet Information Services (IIS) et son identité est Service réseau. Pour améliorer le niveau de sécurité, vous pouvez modifier l'identité de l'application Web vers un compte de service ou un compte de domaine spécifique.

1. En tant qu'administrateur, ouvrez une session sur l'ordinateur hébergeant le serveur d'enregistrement de session.
2. Dans le Gestionnaire des services Internet, cliquez sur **Pools d'applications**.
3. Dans **Pools d'applications**, cliquez avec le bouton droit sur **SessionRecordingLoggingAppPool**, et choisissez **Paramètres avancés**.
4. Modifiez l'attribut **identité** pour le compte que vous voulez utiliser.
5. Accordez au compte l'autorisation **db_owner** pour la base de données **CitrixSessionRecordingLogging** dans Microsoft SQL Server.
6. Accordez au compte le droit en lecture pour la clé de registre sur **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix**

Désactiver ou activer la journalisation d'actions d'enregistrement

Par défaut, la journalisation de l'administrateur consigne chaque action d'enregistrement de session une fois que la requête de stratégie est terminée. Cela peut générer une grande quantité d'entrées. Pour améliorer les performances et économiser le stockage, désactivez ce type de journalisation dans le registre.

1. En tant qu'administrateur, ouvrez une session sur l'ordinateur hébergeant le serveur d'enregistrement de session.
2. Ouvrez l'éditeur de registre.
3. Accédez à **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server**.
4. Définissez la valeur de **EnableRecordingActionLogging** sur :

   0 : désactive la journalisation des actions d'enregistrement

   1 : active la journalisation des actions d'enregistrement

Interroger les données de la journalisation de l'administrateur

L'enregistrement de session fournit une interface Web permettant d'interroger tous les journaux d'administrateur.

Sur l'ordinateur hébergeant le serveur d'enregistrement de session :

1. À partir du menu **Démarrer**, choisissez **Enregistrement de session > Journalisation de l'administrateur**.
2. Entrez les informations d'identification d'un utilisateur **LoggingReader**.

Sur d'autres ordinateurs :

1. Ouvrez un navigateur Web et accédez à la page Web pour Journalisation de l'administrateur.

   Pour HTTPS : `https://servername/SessionRecordingLoggingWebApplication/`, où *servername* correspond au nom de l'ordinateur hébergeant le serveur d'enregistrement de session.

   Pour HTTP : `http://servername/SessionRecordingLoggingWebApplication/`, où *servername* correspond au nom de l'ordinateur hébergeant le serveur d'enregistrement de session.

2. Entrez les informations d'identification d'un utilisateur **LoggingReader**.

Installer l'enregistrement de session avec une haute disponibilité de base de données

February 28, 2019

L'enregistrement de session prend en charge les solutions suivantes pour la haute disponibilité de base de données basée sur Microsoft SQL Server. Les bases de données peuvent basculer automatiquement lorsque le matériel ou le logiciel d'un serveur SQL Server principal échoue, ce qui garantit que l'enregistrement de session continue à fonctionner comme prévu.

- Groupes de disponibilité AlwaysOn

La fonctionnalité Groupes de disponibilité AlwaysOn est une solution de haute disponibilité et de récupération d'urgence qui offre une alternative pour la mise en miroir de base de données. Introduite dans SQL Server 2012, cette fonctionnalité maximise la disponibilité d'un ensemble de bases de données utilisateur pour une entreprise. Les Groupes de disponibilité AlwaysOn nécessitent que les instances SQL Server résident les nœuds WSFC (Windows Server Failover Clustering). Pour plus d'informations, veuillez consulter l'article https://msdn.microsoft.com/en-us/library/hh510230.

- Mise en cluster SQL Server

La technologie de mise en cluster SQL de Microsoft permet à un serveur d'assurer automatiquement la reprise des tâches et des responsabilités du serveur en échec. Toutefois, cette solution est complexe à mettre en place et le basculement automatique est généralement plus lent qu'avec les autres méthodes, comme la mise en miroir de la base de données SQL Server. Pour plus d'informations, veuillez consulter l'article https://msdn.microsoft.com/en-us/library/ms189134.aspx.

- Mise en miroir de base de données SQL Server

La mise en miroir de base de données garantit qu'un basculement automatique se produit en quelques secondes si le serveur de base de données actif échoue. Cette solution est plus coûteuse que les deux autres solutions car des licences complètes de SQL Server sont requises sur chaque serveur de base de données. Vous ne pouvez pas utiliser l'édition SQL Server Express dans un environnement de mise en miroir. Pour plus d'informations, veuillez consulter l'article https://msdn.microsoft.com/en-us/library/ms189852.aspx.

Méthodes d'installation de l'enregistrement de session avec une haute disponibilité de base de données

Pour installer l'enregistrement de session avec une haute disponibilité de base de données, suivez l'une des procédures suivantes :

- Commencez par installer les composants du serveur d'enregistrement de session, puis configurez une haute disponibilité de base de données pour les bases de données créées.
  Vous pouvez installer les composants d'administration d'enregistrement de session avec les bases de données configurées pour être installées sur l'instance de SQL Server préparée, puis configurer une haute disponibilité de base de données pour les bases de données créées.
  - Pour les groupes de disponibilité AlwaysOn et la mise en cluster, vous devez manuellement définir le nom de l'instance SQL Server sur le nom de l'écouteur du groupe de disponibilité ou du réseau SQL Server dans HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\Sr
  - Pour la mise en miroir de base de données, vous devez ajouter manuellement les partenaires de basculement pour les bases de données dans HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Sma et HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\LoggingDatabaseFailoverPartner.

- Commencez par configurer une haute disponibilité de base de données pour des bases de données vides, puis installez les composants d'administration d'enregistrement de session.
  Vous pouvez créer deux bases de données vides en tant que base de données d'enregistrement de session et base de données de journalisation de l'administrateur dans l'instance de SQL Server principale attendue et configurer la haute disponibilité. Entrez le nom de l'instance SQL Server lors de l'installation des composants du serveur d'enregistrement de session :
  - Pour utiliser la solution Groupes de disponibilité AlwaysOn, entrez le nom de votre écouteur de groupe de disponibilité.
  - Pour utiliser la solution de mise en miroir de base de données, entrez le nom de votre SQL Server principal.
  - Pour utiliser la solution de mise en cluster, entrez le nom du réseau de votre SQL Server.

Afficher les enregistrements

November 13, 2018

Utilisez le lecteur d'enregistrement de session pour afficher, rechercher et créer des signets pour les sessions XenApp et XenDesktop enregistrées.

Si les sessions sont enregistrées avec la fonctionnalité de lecture active, vous pouvez afficher les sessions en cours de progression, avec un retard de quelques secondes, ainsi que les sessions terminées.

Les sessions dont la durée ou la taille de fichier sont supérieures aux limites configurées par votre administrateur d'enregistrement de session apparaissent dans plusieurs fichiers de session.

Remarque : un administrateur d'enregistrement de session doit accorder aux utilisateurs le droit d'accéder aux sessions des VDA pour OS de serveur. Si l'accès aux sessions vous est refusé, contactez votre administrateur d'enregistrement de session.

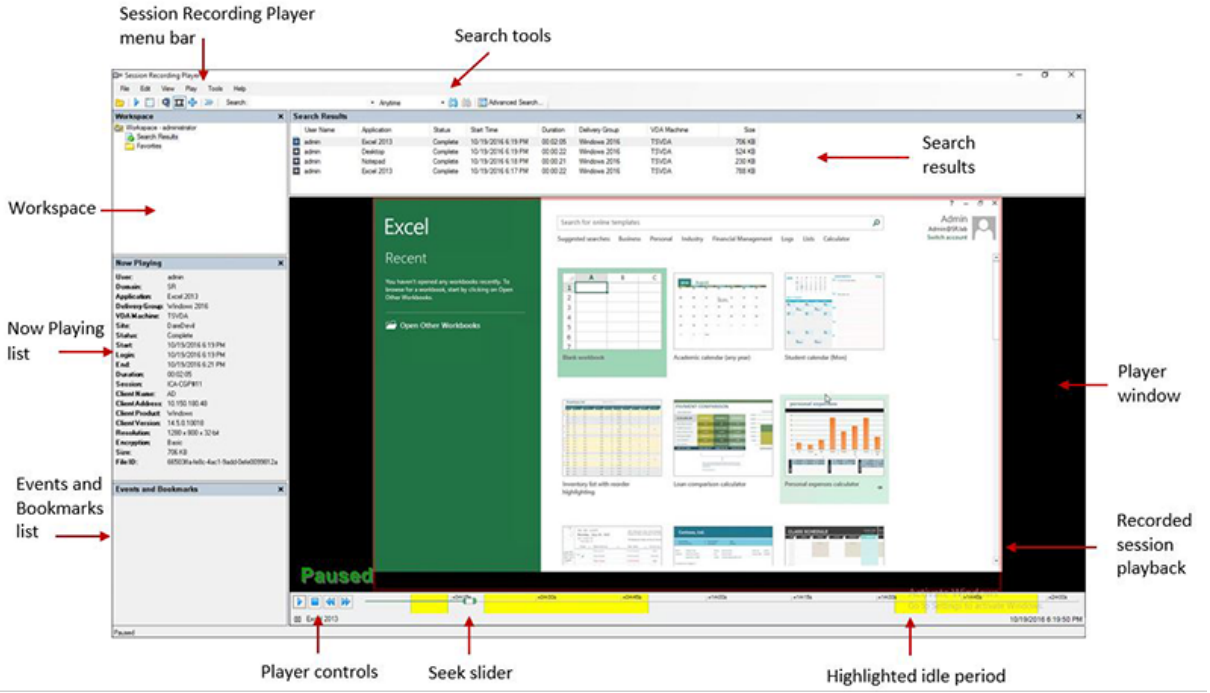
Lorsque le lecteur d'enregistrement de session est installé, l'administrateur d'enregistrement de session établit généralement une connexion entre le lecteur d'enregistrement de session et le serveur d'enregistrement de session. Si cette connexion n'est pas établie, vous êtres invité à l'établir à l'occasion de la première recherche de fichiers. Pour plus d'informations sur ce sujet, contactez votre administrateur d'enregistrement de session.

Lancer le lecteur d'enregistrement de session

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.

   Le lecteur d'enregistrement de session s'affiche.

Cette illustration montre le lecteur d'enregistrement de session avec des légendes indiquant ses principaux éléments. Les fonctions de ces éléments sont décrites au fil des articles suivants.



Afficher ou masquer les éléments de fenêtre

Le lecteur d'enregistrement de session possède des éléments de fenêtre que vous activez et désactivez.

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Dans la barre de menu du **lecteur d'enregistrement de session**, choisissez **Affichage**.
4. Choisissez les éléments que vous souhaitez afficher. La sélection d'un élément en entraîne l'affichage immédiat. Un élément sélectionné est indiqué par la case correspondante cochée.

Changer de serveurs d'enregistrement de session

Si l'administrateur d'enregistrement de session paramètre votre lecteur d'enregistrement de session avec la capacité de se connecter à plusieurs serveurs d'enregistrement de session, vous pouvez sélectionner le serveur d'enregistrement de session auquel le lecteur d'enregistrement de session se connecte. Le lecteur d'enregistrement de session ne peut se connecter qu'à un seul serveur d'enregistrement de session à la fois.

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Dans la barre de menus du **lecteur d'enregistrement de session**, choisissez **Outils** > **Options** > **Connexions**.
4. Sélectionnez le serveur d'enregistrement de session auquel vous connecter.

Ouvrir et lire des enregistrements

February 28, 2019

Vous pouvez utiliser trois méthodes différentes pour ouvrir des enregistrements de session dans le lecteur d'enregistrement de session :

- Faites une recherche à l'aide du lecteur d'enregistrement de session. Les sessions enregistrées correspondant aux critères de recherche s'affichent dans la zone des résultats de la recherche.
- Accédez aux fichiers de session enregistrée directement sur votre disque dur local ou sur un lecteur partagé.
- Accédez aux fichiers de session enregistrée à partir d'un dossier Favoris.

Lorsque vous ouvrez un fichier enregistré sans signature numérique, un message d'avertissement s'affiche pour vous indiquer que l'origine et l'intégrité du fichier n'ont pas été vérifiées. Si vous avez confiance dans l'intégrité du fichier, cliquez sur **Oui** dans la fenêtre d'avertissement pour ouvrir le fichier.

Remarque : la fonctionnalité Journalisation de l'administrateur de l'enregistrement de session vous permet de consigner les téléchargements d'enregistrement dans le lecteur d'enregistrement de session. Pour de plus amples informations, consultez Journaliser les activités d'administration.

Ouvrir et lire un enregistrement dans la zone de résultats de la recherche

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Effectuez une recherche rapide.
4. Si la zone des résultats de la recherche n'est pas visible, sélectionnez **Résultats de la recherche** dans le volet Espace de travail.
5. Dans la zone des résultats de la recherche, sélectionnez la session que vous souhaitez lire.
6. Effectuez une des actions suivantes :
    - Double-cliquez sur la session.
    - Cliquez avec le bouton droit et sélectionnez **Propriétés**.

- Dans la barre de menu du **lecteur d'enregistrement de session**, choisissez **Lecture** > **Vitesse de lecture**.

Ouvrir et lire un enregistrement en accédant au fichier

Le nom d'un fichier de session enregistrée commence par i_, suivi d'un identifiant alphanumérique de fichier unique, suivi d'une extension de fichier .icl et .icle : L'extension .icl indique les enregistrements sans protection en lecture, et l'extension .icle indique les enregistrements avec protection en lecture. Les fichiers de sessions enregistrées sont enregistrés dans un dossier incorporant la date à laquelle les sessions ont été enregistrées. Par exemple, le fichier d'une session enregistrée le 22 décembre 2014, est enregistré dans le chemin de dossier 2014\12\22.

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Effectuez une des actions suivantes :
   - Dans la barre de menus du **lecteur d'enregistrement de session**, choisissez **Fichier** > **Ouvrir** et recherchez le fichier.
   - À l'aide de Windows Explorer, naviguez jusqu'au fichier et glissez-déplacez le fichier dans la fenêtre **Lecteur**.
   - À l'aide de Windows Explorer, naviguez jusqu'au fichier et double-cliquez dessus.
   - Si vous avez créé des favoris dans le volet Espace de travail, sélectionnez **Favoris** et ouvrez le fichier à partir de la zone Favoris de la même manière que vous ouvrez des fichiers à partir de la zone de résultats de recherche.

Utiliser des favoris

Créer des dossiers Favoris vous permet d'accéder rapidement à des enregistrements que vous visionnez fréquemment. Ces dossiers Favoris répertorient des fichiers de sessions enregistrées qui sont stockés sur votre station de travail ou sur un lecteur réseau. Vous pouvez importer et exporter ces fichiers vers d'autres stations de travail et partager ces dossiers avec d'autres utilisateurs du lecteur d'enregistrement de session.

Remarque : seuls les utilisateurs disposant des droits d'accès au lecteur d'enregistrement de session peuvent télécharger les fichiers de sessions enregistrées associés aux dossiers Favoris. Pour plus d'informations sur les droits d'accès, veuillez contacter votre administrateur d'enregistrement de session.

Pour créer un sous-dossier Favoris :

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.

2. À partir du menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Dans la fenêtre **Lecteur d'enregistrement de session**, sélectionnez le dossier **Favoris** de votre volet Espace de travail.
4. Dans la barre de menus, choisissez **Fichier** > **Dossier** > **Nouveau dossier**. Un nouveau dossier apparaît sous le dossier **Favoris**.
5. Tapez le nom du dossier, puis appuyez sur **Entrer** ou cliquez n'importe où pour accepter le nouveau nom.

Vous pouvez utiliser les autres options qui s'affichent dans le menu
Fichier > **Dossier** pour supprimer, renommer, copier, importer et exporter les dossiers.

Lire des sessions enregistrées

January 23, 2019

Après avoir ouvert une session enregistrée dans le lecteur d'enregistrement de session, vous pouvez parcourir les sessions enregistrées en utilisant les méthodes suivantes :

- Utilisez les contrôles du lecteur pour lire, arrêter, mettre en pause et pour augmenter ou réduire la vitesse de lecture.
- Utilisez le curseur de recherche pour avancer ou reculer.

Si vous avez inséré des marqueurs dans l'enregistrement ou si la session enregistrée contient des événements personnalisés, vous pouvez aussi naviguer directement dans la session jusqu'à ces marqueurs et événements.

Remarque :

- un second pointeur de souris peut apparaître pendant la lecture d'une session enregistrée. Le deuxième pointeur s'affiche dans l'enregistrement lorsque l'utilisateur navigue dans Internet Explorer, puis clique sur une image qui était à l'origine plus grande que l'écran, mais avait été automatiquement réduite par Internet Explorer. Bien qu'un seul pointeur apparaisse au cours de la session, deux peuvent apparaître pendant la lecture.
- Cette version de l'enregistrement de session ne prend pas en charge l'accélération multimédia SpeedScreen pour XenApp ou le paramètre de stratégie de réglage de la qualité Flash pour XenApp. Lorsque cette option est activée, la lecture affiche un carré noir.
- L'enregistrement de session ne peut pas enregistrer la vidéo provenant de la webcam Lync lors de l'utilisation du pack d'optimisation HDX RealTime.
- Lors de l'enregistrement d'une session avec une résolution supérieure ou égale à 4 096 x 4 096, des fragments peuvent apparaître dans l'apparence de l'enregistrement.
- Vous ne pouvez pas enregistrer les sessions de bureau Windows 7 correctement lorsque **Mode graphique d'ancienne génération** est activé par la stratégie de site XenDesktop et **Mise en cache sur le disque** est activé par la stratégie Citrix Receiver pour Windows. Ces

enregistrements affichent un écran noir.
Pour résoudre ce problème, désactivez la **Mise en cache sur le disque** avec un objet de stratégie de groupe sur les machines sur lesquelles vous avez installé Citrix Receiver pour Windows. Pour plus d'informations sur la désactivation de **Mise en cache sur le disque**, voir CTX123169.

- Enregistrement de session ne prend pas en charge le mode d'affichage Framehawk. Les sessions en mode d'affichage Framehawk ne peuvent pas être enregistrées ni lues correctement. Les sessions enregistrées dans le mode d'affichage Framehawk peuvent ne pas contenir les activités de session.

Utiliser les contrôles du lecteur

Vous pouvez cliquer sur les contrôles du lecteur dans la partie inférieure de la fenêtre Lecteur ou y accéder en choisissant **Lecture** dans la barre de menu du **lecteur d'enregistrement de session**. Utilisez les contrôles du lecteur pour effectuer les opérations suivantes :

Contrôle du lecteur	Fonction
	Lit le fichier de session sélectionné.
	Suspend la lecture.
	Arrête la lecture. Si vous cliquez sur **Arrêter**, puis **Lire**, l'enregistrement reprend au début du fichier.
	Réduit la vitesse de lecture actuelle jusqu'à un quart minimum de la vitesse normale.
	Double la vitesse de lecture actuelle jusqu'à 32 fois maximum la vitesse normale.

Utiliser le curseur de recherche

Utilisez le curseur de recherche situé dans la partie inférieure de la fenêtre Lecteur pour sauter directement à une position différente dans la session enregistrée. Vous pouvez faire glisser le curseur de recherche jusqu'au point de l'enregistrement que vous souhaitez afficher ou vous pouvez cliquer n'importe où sur la barre du curseur pour vous déplacer dans cette direction.

Vous pouvez aussi utiliser les touches clavier suivantes pour contrôler le curseur de recherche :

Clé	Action de recherche
Accueil	Recherche depuis le début.
Fin	Recherche jusqu'à la fin.
Flèche droite	Recherche en avant (cinq secondes).
Flèche gauche	Recherche en arrière (cinq secondes).
Déplacement de la roulette de la souris d'un cran vers le bas	Recherche en avant (15 secondes).
Déplacement de la roulette de la souris d'un cran vers le haut	Recherche en arrière (15 secondes).
Ctrl + Flèche droite	Recherche en avant (30 secondes).
Ctrl + Flèche gauche	Recherche en arrière (30 secondes).
Pg suiv.	Recherche en avant (une minute).
Pg préc.	Recherche en arrière (une minute).
Ctrl + Déplacement de la roulette de la souris d'un cran vers le bas	Recherche en avant (90 secondes).
Ctrl + Déplacement de la roulette de la souris d'un cran vers le haut	Recherche en arrière (90 secondes).
Ctrl + Page suivante	Recherche en avant (six minutes).
Ctrl + Page précédente	Recherche en arrière (six minutes).

Pour régler la vitesse du curseur de recherche : dans la barre de menu du **lecteur d'enregistrement de session**, choisissez **Outils** > **Options** > **Lecteur** et faites glisser le curseur pour augmenter ou réduire le délai de réponse de la recherche. Un temps de réponse plus rapide sollicite plus de mémoire. La réponse peut être lente en fonction de la taille des enregistrements et du matériel de votre ordinateur.

Modifier la vitesse de lecture

Vous pouvez paramétrer le lecteur d'enregistrement de session pour une lecture en incréments exponentiels allant d'un quart à 32 fois la vitesse de lecture normale.

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Dans la barre de menu du **lecteur d'enregistrement de session**, choisissez **Lecture** > **Vitesse de lecture**.

4. Choisissez une option de vitesse.

La vitesse s'adapte immédiatement. Un nombre indiquant la vitesse, augmentée ou réduite, s'affiche sous les contrôles de la fenêtre du lecteur. Le texte indiquant le taux exponentiel s'affiche rapidement en vert dans la fenêtre Lecteur.

Afficher les périodes d'inactivité des sessions enregistrées

Les périodes d'inactivité d'une session enregistrée sont les parties pendant lesquelles aucune action n'a lieu. Le lecteur d'enregistrement de session peut indiquer les périodes d'inactivité des sessions enregistrées lors de la lecture. L'option par défaut est **Activé**.

Notez que les périodes d'inactivité ne sont pas affichées lors de la lecture de sessions actives à l'aide du lecteur d'enregistrement de session.

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Dans la barre de menu du **Lecteur d'enregistrement de session**, choisissez **Affichage** > **Périodes inactives** et cochez ou décochez la case.

Ignorer les espaces sans action

Le mode de consultation rapide vous permet de régler le lecteur d'enregistrement de session de manière à sauter les parties de sessions enregistrées pendant lesquelles aucune action n'a lieu. Ce réglage permet de gagner du temps pour visionner l'enregistrement ; cependant, il ne permet pas d'ignorer les séquences animées comme les mouvements de souris, les clignotements de curseur ou les horloges affichées et leurs aiguilles en mouvement.

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Dans la barre de menu du **lecteur d'enregistrement de session**, choisissez **Lecture** > **Mode de consultation rapide**.

L'option passe de l'état activée à désactivée et vice-versa. Chaque fois que vous le choisissez, le statut s'affiche rapidement en vert dans la fenêtre Lecteur.

Utiliser des événements et des signets

November 13, 2018

Vous pouvez utiliser les événements et les signets pour vous aider à naviguer à travers les sessions enregistrées.

Les événements sont insérés dans les sessions pendant l'enregistrement de celles-ci, à l'aide de l'API d'événements et d'une application tierce. Les événements sont enregistrés comme faisant partie du fichier de session. Vous ne pouvez pas les supprimer ou les modifier à l'aide du lecteur d'enregistrement de session.

Les signets sont des marqueurs que vous insérez dans une session enregistrée au cours de la lecture de la session à l'aide du lecteur d'enregistrement de session. Une fois insérés, les signets sont associés à la session enregistrée jusqu'à ce que vous les supprimiez, mais ils ne sont pas enregistrés comme faisant partie du fichier de session. Les signets sont stockés sous forme de fichiers « .iclb » distincts dans le dossier en cache **Signets** sur le lecteur d'enregistrement de session, par exemple, C:\Users\SpecificUser\AppData\Local\Citrix\SessionRecording\Player\Bookmarks, avec les mêmes noms de fichier que les fichiers d'enregistrement « .icl ». Si vous souhaitez lire un fichier d'enregistrement contenant des signets sur un autre lecteur, copiez les fichiers « .iclb » dans le dossier en cache **Signets** sur ce lecteur. Par défaut, chaque signet est accompagné de l'étiquette Signet, mais vous pouvez changer ce nom pour le texte d'annotation de votre choix (avec une limite maximale de 128 caractères).

Les événements et signets s'affichent sous forme de points dans la partie inférieure de la fenêtre Lecteur. Les événements sont représentés par des points jaunes, les signets par des points bleus. Déplacer la souris sur ces points permet d'afficher le texte de l'étiquette qui leur est associé. Vous pouvez aussi afficher les événements et les signets dans la liste **Événements et signets** du lecteur d'enregistrement de session. Ils s'affichent dans cette liste avec leur étiquette et l'heure de la session enregistrée à laquelle ils apparaissent, dans l'ordre chronologique.

Vous pouvez utiliser les événements et les signets pour vous aider à naviguer à travers les sessions enregistrées. En allant à un événement ou un signet, vous pouvez atteindre directement le point de la session enregistrée où l'événement ou signet a été inséré.

Afficher les événements et les signets dans la liste

La liste **Événements et signets** contient les événements et les signets insérés dans la session enregistrée en cours de lecture. Elle peut afficher les événements, les signets seulement ou elle peut afficher les deux.

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Déplacez le pointeur de la souris dans la zone de la liste **Événements et signets** et cliquez avec le bouton droit pour afficher le menu.

4. Choisissez **Afficher les événements seulement**, **Afficher les signets seulement** ou **Afficher tout**.

Insérer un signet

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Commencez la lecture de la session enregistrée à laquelle vous souhaitez ajouter un signet.
4. Déplacez le curseur de recherche sur le point d'insertion souhaité pour le signet.
5. Déplacez le pointeur de la souris dans la zone de la fenêtre Lecteur et cliquez avec le bouton droit pour afficher le menu.
6. Ajoutez un signet avec l'étiquette **Signet** par défaut ou créez une annotation :
    - Pour ajouter un signet avec l'étiquette **Signet** par défaut, choisissez **Ajouter un signet**.
    - Pour ajouter un signet avec un texte descriptif que vous créez, choisissez **Ajouter une annotation**. Entrez le texte de l'étiquette que vous souhaitez attribuer au signet, d'une longueur maximale de 128 caractères. Cliquez sur **OK**.

Ajouter ou modifier une annotation

Après avoir créé un signet, vous pouvez y ajouter une annotation ou en modifier une.

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Commencez la lecture de la session enregistrée contenant le signet.
4. Assurez-vous que la liste des événements et des signets affiche des signets.
5. Sélectionnez le signet dans la liste **Événements et signets** et cliquez avec le bouton droit pour afficher le menu.
6. Choisir **Modifier l'annotation**.
7. Dans la fenêtre qui apparaît, tapez la nouvelle annotation et cliquez sur **OK**.

Supprimer un signet

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Commencez la lecture de la session enregistrée contenant le signet.
4. Assurez-vous que la liste des événements et des signets affiche des signets.

5. Sélectionnez le signet dans la liste Événements et signets et cliquez avec le bouton droit pour afficher le menu.
6. Choisissez **Supprimer**.

Aller à un événement ou un signet

Aller à un événement ou un signet conduit le lecteur d'enregistrement de session à aller au point de la session enregistrée où l'événement ou le signet a été inséré.

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Commencez à lire un enregistrement de session contenant des événements ou des signets.
4. Allez à un événement ou un signet.
    - Dans la partie inférieure de la fenêtre du lecteur, cliquez sur le point représentant l'événement ou le signet que vous souhaitez consulter.
    - Dans la liste **Événements et signets**, double-cliquez sur un élément pour vous y rendre. Pour accéder à l'événement ou au favori suivant, sélectionnez-le dans la liste, cliquez dessus avec le bouton droit de la souris pour afficher le menu, puis choisissez **Rechercher jusqu'au signet**.

Modifier l'affichage de la lecture

January 23, 2019

Certaines options vous permettent de modifier le mode d'affichage des sessions enregistrées dans la fenêtre Lecteur. Vous pouvez faire un panoramique et mettre à l'échelle l'image, afficher la lecture en mode plein écran, afficher la fenêtre Lecteur dans une fenêtre séparée et afficher une bordure rouge autour de la session enregistrée pour la différencier de l'arrière-plan du lecteur.

Afficher la fenêtre Lecteur en plein écran

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Dans la barre de menu du **lecteur d'enregistrement de session**, choisissez **Afficher** > **Lecteur en plein écran**.
4. Pour revenir à la taille originale, appuyez sur Échap ou F11.

Afficher la fenêtre Lecteur dans une fenêtre séparée

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Dans la barre de menu du **lecteur d'enregistrement de session**, choisissez **Affichage** > **Lecteur dans une fenêtre séparée**. Une nouvelle fenêtre s'affiche ; elle contient la fenêtre Lecteur. Vous pouvez faire glisser et redimensionner la fenêtre.
4. Pour incorporer la fenêtre Lecteur dans la fenêtre principale, choisissez **Affichage** > **Lecteur dans une fenêtre séparée** ou appuyez sur **F10**.

Mettre l'écran de lecture de session à l'échelle de la fenêtre Lecteur

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Dans la barre de menu du **lecteur d'enregistrement de session**, choisissez **Lecture** > **Panorama et mise à l'échelle** > **Mise à l'échelle**.
    - **Mise à l'échelle (rendu rapide)** rétrécit les images tout en fournissant une bonne qualité. Les images sont créées plus rapidement qu'avec l'option Haute qualité, mais les images et le texte ne sont pas aussi nets. Utilisez cette option si vous avez des problèmes de performances en utilisant le mode Haute qualité.
    - **Mise à l'échelle (haute qualité)** rétrécit les images tout en fournissant une haute qualité. L'emploi de cette option peut se traduire par plus de lenteur dans la création des images qu'avec l'option Rendu rapide.

Réaliser un panorama de l'image

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Dans la barre de menu du **lecteur d'enregistrement de session**, choisissez **Lecture** > **Panorama et mise à l'échelle** > **Panorama**. Le pointeur se transforme en main et une représentation de l'écran en taille réduite s'affiche dans le coin supérieur droit de la fenêtre Lecteur.
4. Faites glisser l'image. La représentation de taille réduite indique où vous vous trouvez dans l'image.
5. Pour arrêter le panorama, choisissez l'une des options de mise à l'échelle.

Afficher une bordure rouge autour de l'enregistrement de session

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Dans la barre de menus du **Lecteur d'enregistrement de session**, choisissez **Outils** > **Options** > **Lecteur**.
4. Sélectionnez la case **Afficher le pourtour de l'enregistrement de la session**.
   Conseil : si la case **Afficher le pourtour de l'enregistrement de session** n'est pas cochée, vous pouvez afficher temporairement le pourtour rouge en cliquant sur le bouton gauche de la souris et en le maintenant enfoncé pendant que le pointeur se trouve dans la fenêtre du lecteur.

Mettre en cache des fichiers de session enregistrée

February 28, 2019

Chaque fois que vous ouvrez un fichier de session enregistrée, le lecteur d'enregistrement de session télécharge le fichier de l'emplacement de stockage des enregistrements. Si vous téléchargez les mêmes fichiers régulièrement, vous pouvez gagner du temps en mettant les fichiers en cache sur votre station de travail. Les fichiers mis en cache sont stockés sur votre station de travail dans ce dossier :

userprofile**AppData\Local\Citrix\SessionRecording\Player\Cache**

Vous pouvez spécifier la quantité d'espace disque utilisée pour le cache. Lorsque les enregistrements atteignent le volume d'espace disque spécifié, l'enregistrement de session supprime les enregistrements les plus anciens et les moins utilisés pour faire de la place aux nouveaux enregistrements. Vous pouvez vider le cache à tout moment pour libérer de l'espace disque.

Activer la mise en cache

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Dans la barre de menus du **Lecteur d'enregistrement de session**, choisissez **Outils** > **Options** > **Cache**.
4. Cochez la case **Mettre en cache les fichiers téléchargés sur la machine locale**.
5. Si vous souhaitez limiter le volume d'espace disque utilisé pour la mise en cache, cochez la case **Limiter le volume d'espace disque utilisable** et faites glisser le curseur ou entrez le nombre de mégaoctets à utiliser pour le cache.
6. Cliquez sur **OK**.

Purger les caches

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Dans la barre de menus du **Lecteur d'enregistrement de session**, choisissez **Outils** > **Options** > **Cache**.
4. Cochez la case **Mettre en cache les fichiers téléchargés sur la machine locale**.
5. Dans le lecteur d'enregistrement de session, choisissez **Outils** > **Options** > **Cache**.
6. Cliquez sur **Purger le cache**, puis sur **OK** pour confirmer l'action.

Rechercher des enregistrements

January 23, 2019

Le lecteur d'enregistrement de session vous permet d'effectuer des recherches rapides et avancées et de spécifier des options s'appliquant à toutes les recherches. Le résultat des recherches s'affiche dans la zone Résultats de la recherche du lecteur d'enregistrement de session.

> **Remarque :**
>
> Pour afficher toutes les sessions enregistrées disponibles, jusqu'au nombre maximum de sessions pouvant s'afficher dans une recherche, effectuez une recherche sans spécifier de paramètre de recherche précis.

Effectuer une recherche rapide

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Définissez vos critères de recherche :
   - Entrez un critère de recherche dans le champ **Rechercher**.
   - Faites glisser le pointeur de la souris sur l'étiquette **Rechercher** pour afficher une liste de paramètres à utiliser à titre indicatif.
   - Cliquez sur la flèche à droite du champ **Rechercher** pour afficher le texte des 64 dernières recherches que vous avez effectuées.
   - Utilisez la liste déroulante située à droite du champ **Rechercher** pour sélectionner une période ou une durée spécifiant quand la session a été enregistrée.
4. Cliquez sur l'icône binoculaire à droite de la liste déroulante pour lancer la recherche.

Effectuer une recherche avancée

Les recherches avancées peuvent prendre jusqu'à 20 secondes pour renvoyer des résultats contenant plus de 150 000 entités. Citrix vous recommande d'utiliser des critères de recherche plus précis comme une plage de dates ou un utilisateur afin de réduire le nombre de résultats.

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. À partir du menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Dans la fenêtre **Lecteur d'enregistrement de session**, cliquez sur **Recherche avancée** dans la barre d'outils ou choisissez **Outils** > **Recherche avancée**.
4. Définissez vos critères de recherche dans les onglets de la boîte de dialogue **Recherche avancée** :
   - **Commun** vous permet de faire une recherche par domaine ou autorité de compte, par site, groupe, VDA pour OS de serveur, application ou identificateur de fichier.
   - **Date/Heure** vous permet de faire une recherche en fonction de la date, du jour de la semaine et de l'heure.
   - **Événements** vous permet de rechercher des événements définis par Citrix et personnalisés qui sont insérés dans les sessions.
   - **Autre** vous permet de faire une recherche par nom de session, nom de client, adresse de client et durée d'enregistrement. Cet onglet vous permet aussi de spécifier, pour cette recherche, le nombre maximum de résultats affichés et d'inclure ou d'exclure les fichiers archivés.
     À mesure que vous précisez les critères de recherche, la requête que vous créez s'affiche dans le volet situé au bas de la boîte de dialogue.
5. Cliquez sur **Recherche** pour lancer la recherche.

   vous pouvez enregistrer et récupérer les requêtes de recherche avancée. Cliquez sur **Enregistrer** dans la boîte de dialogue **Recherche avancée** pour enregistrer la requête actuelle. Cliquez sur **Ouvrir** dans la boîte de dialogue **Recherche avancée** pour extraire une requête enregistrée. Les requêtes sont enregistrées sous forme de fichiers avec l'extension .isq.

Paramétrer les options de recherche

Les options de recherche du lecteur d'enregistrement de session vous permettent de limiter le nombre maximum d'enregistrements de sessions qui s'affichent dans les résultats de la recherche et de spécifier si ces résultats peuvent inclure les fichiers de sessions archivés.

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.

2. À partir du menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Dans la barre de menus du **lecteur d'enregistrement de session**, choisissez **Outils** > **Options** > **Recherche**.
4. Dans le champ **Nombre maximum de résultats à afficher**, tapez le nombre de résultats de recherche que vous souhaitez afficher. Un maximum de 500 résultats peuvent être affichés.
5. Pour définir si les fichiers archivés doivent ou non être inclus dans les recherches, sélectionnez ou désélectionnez **Inclure les fichiers archivés**.

Résolution des problèmes de l'enregistrement de session

January 23, 2019

Les informations de dépannage contenues dans ce chapitre contiennent des solutions à certains problèmes éventuels que vous pourriez rencontrer pendant et après l'installation des composants de l'enregistrement de session :

- échecs de connexion entre composants ;
- échecs d'enregistrement de sessions ;
- problèmes avec le lecteur d'enregistrement de session ou la console de stratégie d'enregistrement de session ;
- problèmes avec votre protocole de communication.

> **Avertissement :**
>
> Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

L'agent d'enregistrement de session ne peut pas se connecter

Lorsque l'agent d'enregistrement de session ne peut pas se connecter, le message d'événement **Détection d'exception pendant l'envoi du message d'interrogation au broker d'enregistrement de session** est journalisé, suivi du texte d'exception. Le texte d'exception donne les raisons de l'échec de la connexion. Ces raisons sont les suivantes :

- **La connexion sous-jacente a été fermée. Impossible d'établir une relation de confiance pour le canal sécurisé SSL/TLS.** Cette exception signifie que le serveur d'enregistrement de session utilise un certificat signé par une autorité de certification (CA) à laquelle le serveur sur lequel l'agent d'enregistrement de session réside ne fait pas confiance, ou n'a pas de certificat CA. Le certificat peut aussi avoir expiré ou peut avoir été révoqué.

Résolution : vérifiez que le certificat CA correct est installé sur le serveur hébergeant l'agent d'enregistrement de session ou utilisez une CA de confiance.

- **Le serveur distant a renvoyé une erreur : (403) interdit.** Il s'agit d'une erreur HTTPS standard qui s'affiche lorsque vous tentez de vous connecter en utilisant HTTP (protocole non sécurisé). L'ordinateur hébergeant le serveur d'enregistrement de session rejette la connexion car il n'accepte que les connexions sécurisées.

  Solution : utilisez les propriétés de l'agent d'enregistrement de session pour modifier le protocole de l'agent d'enregistrement de session vers **HTTPS**.

Le broker d'enregistrement de session a renvoyé une erreur inconnue lors de l'évaluation d'une requête de stratégie d'enregistrements. Code d'erreur 5 (accès refusé). Veuillez consulter le journal des événements sur le serveur d'enregistrement de session pour plus de détails. Cette erreur se produit lorsque les sessions démarrent et qu'une requête pour une évaluation de stratégie d'enregistrement est faite. L'erreur est le résultat de la suppression du groupe Utilisateurs authentifiés (il s'agit du membre par défaut) du rôle Requête de stratégie de la console d'autorisation d'enregistrement de session.

Résolution : ajoutez à nouveau le groupe Utilisateurs authentifiés à ce rôle ou ajoutez chaque serveur hébergeant chaque agent d'enregistrement de session au rôle PolicyQuery.

La connexion sous-jacente a été fermée. Une connexion qui devait être maintenue active a été fermée par le serveur. Cette erreur signifie que le serveur d'enregistrement de session est en panne, ou qu'il est indisponible pour accepter les requêtes. IIS est peut-être déconnecté ou a redémarré, ou le serveur entier peut être déconnecté.

Solution : vérifiez que le serveur d'enregistrement de session est démarré, que IIS est en cours d'exécution sur le serveur et que le serveur est connecté au réseau.

Échec de l'installation des composants du serveur d'enregistrement de session

L'installation des composants du serveur d'enregistrement de session échoue avec les codes d'erreur 2503

vérifiez la liste de contrôle d'accès (ACL) du dossier C:\windows\Temp pour vous assurer que Utilisateurs et groupes locaux ont un accès en écriture à ce dossier. Si ce n'est pas le cas, ajoutez manuellement les autorisations en écriture.

Le serveur d'enregistrement de session ne peut pas se connecter à la base de données d'enregistrement de session

Lorsque le serveur d'enregistrement de session ne peut pas se connecter à la base de données d'enregistrement de session, il est possible qu'un message similaire aux suivants s'affiche :

Source de l'événement :

Une erreur liée au réseau ou à une instance spécifique s'est produite lors de l'établissement d'une connexion à SQL Server. Cette erreur s'affiche avec l'ID 2047 dans le journal des événements Applications de l'observateur d'événements de l'ordinateur hébergeant le serveur d'enregistrement de session.

Description Gestionnaire de stockage d'enregistrement de session Citrix : Détection d'exception pendant l'établissement de connexion à la base de données. Cette erreur s'affiche dans le journal des événements Applications de l'observateur d'événements de l'ordinateur hébergeant le serveur d'enregistrement de session.

Impossible de se connecter au serveur d'enregistrement de session. Veuillez vérifier que le serveur d'enregistrement de session fonctionne. Ce message d'erreur apparaît lorsque vous lancez la console de stratégie d'enregistrement de session.

Résolution :

- L'édition Express de Microsoft SQL Server 2008 R2, Microsoft SQL Server 2012, Microsoft SQL Server 2014 ou Microsoft SQL Server 2016 est installée sur un serveur autonome et ne possède pas les services ou paramètres appropriés configurés pour l'enregistrement de session. Sur le serveur, le protocole TCP/IP doit être activé et le service SQL Server doit fonctionner. Veuillez consulter la documentation Microsoft pour des informations sur l'activation de ces paramètres.
- Lors de l'installation de l'enregistrement de session (option Administration), des informations incorrectes ont été fournies pour le serveur et la base de données. Désinstallez la base de données d'enregistrement de session et réinstallez-la, en fournissant les informations correctes.
- Le serveur de la base de données d'enregistrement de session est en panne. Vérifiez que le serveur est connecté.
- L'ordinateur hébergeant le serveur d'enregistrement de session ou celui hébergeant le serveur de la base de données d'enregistrement de session ne peut pas résoudre le nom de domaine complet ou le nom NetBIOS de l'autre. Utilisez la commande ping pour vérifier que les noms peuvent être résolus.
- Vérifiez la configuration du pare-feu sur la base de données d'enregistrement de session pour vous assurer que les connexions du serveur SQL Server sont autorisées. Pour plus d'informations, veuillez consulter l'article Microsoft sur https://msdn.microsoft.com/en-us/library/cc646023.aspx.

La connexion a échoué pour l'utilisateur 'NT_AUTHORITY\ANONYMOUS LOGON'. Ce message d'erreur signifie que les services sont journalisés incorrectement en tant que .\administrator.

Résolution : redémarrez les services en tant qu'utilisateur système local et redémarrez les services SQL.

Les sessions ne sont pas enregistrées

Si l'enregistrement de vos sessions applicatives échoue, commencez par vérifier le journal d'application dans l'observateur d'événements du VDA pour OS de serveur exécutant l'agent d'enregistrement de session et le serveur d'enregistrement de session. Il peut vous fournir des informations de diagnostic importantes.

Si les sessions ne sont pas enregistrées, les problèmes suivants peuvent en être la cause :

- **Connectivité des composants et certificats.** Si les composants d'enregistrement de session ne peuvent pas communiquer entre eux, cela peut entraîner l'échec des enregistrements de sessions. Pour résoudre les problèmes d'enregistrement, vérifiez que tous les composants sont configurés correctement de manière à pointer vers les ordinateurs corrects et que tous les certificats sont valides et installés correctement.
- **Environnements de domaine non Active Directory.** L'enregistrement de session est conçu pour être exécuté dans un environnement de domaine Microsoft Active Directory. Si vous n'évoluez pas dans un environnement Active Directory, vous pouvez avoir des difficultés d'enregistrement. Veillez à ce que tous les composants d'enregistrement de session sont exécutés sur des ordinateurs membres d'un domaine Active Directory.
- **Le partage de session entre en conflit avec la stratégie active.** L'enregistrement de session fait correspondre la stratégie active à la première application publiée qu'un utilisateur ouvre. Toute application suivante ouverte au cours de la même session continue d'observer la stratégie en vigueur pour la première application. Pour empêcher le partage de session d'entrer en conflit avec la stratégie active, publiez les applications en conflit sur des VDA pour OS de serveur distincts.
- **L'enregistrement n'est pas activé.** Par défaut, l'installation de l'agent d'enregistrement de session sur un VDA pour OS de serveur permet d'activer le serveur pour la fonction d'enregistrement. L'enregistrement n'aura pas lieu avant qu'une stratégie d'enregistrement active soit configurée pour le permettre.
- **La stratégie d'enregistrement active n'autorise pas l'enregistrement.** Pour qu'une session soit enregistrée, la stratégie d'enregistrement active doit permettre l'enregistrement des sessions pour l'utilisateur, du serveur ou de l'application publiée.
- **Les services d'enregistrement de session ne sont pas exécutés.** Pour que les sessions soient enregistrées, le service de l'agent d'enregistrement de session doit être exécuté sur un VDA pour OS de serveur et le service Gestionnaire de stockage d'enregistrement de session doit s'exécuter sur l'ordinateur hébergeant le serveur d'enregistrement de session.
- **MSMQ n'est pas configuré.** Si MSMQ n'est pas configuré correctement sur le serveur exécutant l'agent d'enregistrement de session et sur le serveur d'enregistrement de session, des problèmes d'enregistrement peuvent se produire.

Impossible d'afficher la lecture de session active

Si vous rencontrez des difficultés lors de l'affichage d'enregistrements avec le lecteur d'enregistrement de session, le message d'erreur suivant peut s'afficher :

Échec du téléchargement du fichier de la session enregistrée. La lecture de session active n'est pas autorisée. Le serveur est configuré de manière à interdire cette fonctionnalité. Cette erreur indique que le serveur est configuré pour interdire l'action.

Résolution : dans **Propriétés du serveur d'enregistrement de session**, choisissez l'onglet **Lecture** et cochez la case **Autoriser la lecture d'une session active**.

Les enregistrements sont endommagés ou incomplets

- Si les enregistrements sont endommagés ou incomplets lors de leur affichage à l'aide du lecteur d'enregistrement de session, vous pouvez également voir des avertissements dans les journaux d'événements de l'agent d'enregistrement de session.

  Source de l'événement : Gestionnaire de stockage d'enregistrement de session Citrix

  Description : perte de données lors de l'enregistrement du fichier <nom du fichier icl>

  Cela se produit généralement lorsque Machine Creation Services (MCS) ou Provisioning Services est utilisé pour créer les VDA avec une image principale configurée et que Microsoft Message Queuing (MSMQ) est installé. Dans ce cas, les VDA ont les mêmes QMId pour MSMQ.

  Pour résoudre ce problème, créez un QMId unique pour chaque VDA. Pour plus d'informations, veuillez consulter l'étape 8 dans la section **Installer l'agent d'enregistrement de session** sous Installer, mettre à niveau et désinstaller un enregistrement de session.

- Le lecteur d'enregistrement de session peut signaler une erreur interne avec ce message : **« Le fichier lu indique qu'une erreur système interne (code d'erreur : {0}) s'est produite pendant l'enregistrement d'origine. Le fichier peut toujours être lu jusqu'au niveau où l'erreur d'enregistrement s'est produite.**» lors de la lecture d'un nouveau fichier d'enregistrement.

  Cette erreur est généralement causée par une taille de tampon insuffisante de l'agent d'enregistrement de session lors de l'enregistrement de sessions gourmandes en ressources graphiques.

  Pour contourner le problème, définissez la valeur de registre HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Sma sur un niveau plus élevé dans l'agent d'enregistrement de session, puis redémarrez la machine.

Le test de connexion de l'instance de base de données a échoué lors de l'installation du composant Base de données d'enregistrement de session ou Serveur d'enregistrement de session

Lorsque vous installez la base de données d'enregistrement de session ou le serveur d'enregistrement de session, le test de la connexion échoue avec le message d'erreur **Échec du test de la connexion à la base de données. Corrigez le nom de l'instance de base de données**, et ce, même si le nom de l'instance de base de données est correct.

Dans ce cas, vérifiez que l'utilisateur actuel dispose de l'autorisation de rôle SQL Server public pour éviter l'échec pour cause d'autorisation insuffisante.

Journalisation de l'administrateur

Dans Windows Server 2008 R2 SP1, avant d'installer la fonctionnalité de journalisation d'administrateur, installez **Fonctionnalités .NET Framework 3.5** > **Services WCF** > **Activation HTTP**, puis installez .Net Framework 4.5 ou une version ultérieure. Assurez-vous que vous n'installez pas ces deux fonctionnalités dans l'ordre inverse. Si vous ne respectez pas cette exigence, la journalisation de l'administrateur peut ne pas fonctionner comme prévu. Vous pouvez rencontrer des blocages lors d'une tentative de modification des configurations d'enregistrement de session à l'aide de la console des propriétés du serveur ou d'une tentative de mise à jour des stratégies d'enregistrement de session avec la journalisation obligatoire activée.

Pour résoudre ce problème :

1. Ouvrez le gestionnaire IIS (Internet Information Services) et accédez au nœud **Pools d'applications**.
2. Cliquez avec le bouton droit sur **SessionRecordingLoggingAppPool** et ouvrez la boîte de dialogue **Paramètres de base**.
3. Modifiez la version .NET Framework vers .NET Framework v4.0.

Vérifier les connexions des composants

January 23, 2019

Pendant l'installation de l'enregistrement de session, il se peut que les composants ne se connectent pas à d'autres. Tous les composants communiquent avec le serveur d'enregistrement de session (broker). Par défaut, le broker (un composant IIS) est sécurisé à l'aide du certificat du site Web IIS par défaut. Si un composant ne peut pas se connecter au serveur d'enregistrement de session, il est possible que les tentatives de connexion des autres composants échouent également.

L'agent d'enregistrement de session et le serveur d'enregistrement de session (gestionnaire de stockage et broker) journalisent les erreurs de connexion dans le journal des événements des applications, dans l'observateur d'événements de l'ordinateur hébergeant le serveur d'enregistrement de session, alors que la console de stratégie d'enregistrement de session et le lecteur d'enregistrement de session affichent des messages d'erreur de connexion à l'écran lorsque les connexions échouent.

Vérifier que l'agent d'enregistrement de session est connecté

1. Ouvrez une session sur le serveur sur lequel l'agent d'enregistrement de session est installé.
2. À partir du menu **Démarrer**, choisissez **Propriétés de l'Agent d'enregistrement de session**.
3. Dans la boîte de dialogue **Propriétés de l'agent d'enregistrement de session**, cliquez sur l'onglet **Connexions**.
4. Vérifiez que la valeur Serveur d'enregistrement de session est le nom de serveur correct de l'ordinateur hébergeant le serveur d'enregistrement de session.
5. Vérifiez que le serveur choisi pour la valeur Serveur d'enregistrement de session peut être contacté par votre VDA pour OS de serveur.

Remarque : recherchez des erreurs et des avertissements dans le journal des événements de l'application.

Vérifier que le serveur d'enregistrement de session est connecté

Avertissement : l'utilisation de l'Éditeur du Registre peut entraîner de sérieux problèmes et nécessiter la réinstallation du système d'exploitation. Citrix ne peut garantir la résolution des problèmes résultant d'une utilisation incorrecte de l'éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil.

1. Ouvrez une session sur l'ordinateur exécutant le serveur d'enregistrement de session.
2. Ouvrez l'éditeur de registre.
3. Accédez à HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server.
4. Vérifiez que la valeur de **SmAudDatabaseInstance** réfère correctement à la base de données d'enregistrement de session que vous avez installée sur votre instance SQL Server.

Vérifier que la base de données d'enregistrement de session est connectée

1. À l'aide d'un outil de gestion SQL, ouvrez votre instance SQL contenant la base de données d'enregistrement de session que vous avez installée.
2. Ouvrez les autorisations de sécurité de la base de données d'enregistrement de session.

3. Vérifiez que le compte d'ordinateur d'enregistrement de session a accès à la base de données. Par exemple, si l'ordinateur hébergeant le serveur d'enregistrement de session a pour nom **SsRecSrv** dans le domaine MIS, le compte d'ordinateur de votre base de données doit être configuré ainsi : **MIS\SsRecSrv$**. Cette valeur est configurée au cours de l'installation de la base de données d'enregistrement de session.

Tester la connectivité IIS

Tester les connexions au site IIS du serveur d'enregistrement de session avec un navigateur Web pour accéder à la page Web du broker d'enregistrement de session peut vous aider à déterminer si les problèmes de communication éventuels entre les composants de l'enregistrement de session proviennent d'une mauvaise configuration de protocole, de problèmes de certification ou de problèmes au niveau du broker d'enregistrement de session.

Pour vérifier la connectivité IIS avec l'agent d'enregistrement de session :

1. Ouvrez une session sur le serveur sur lequel l'agent d'enregistrement de session est installé.
2. Lancez un navigateur Web et entrez l'adresse suivante :
   - Pour HTTPS : `https://servername/SessionRecordingBroker/RecordPolicy.rem?wsdl`, où *nomserveur* correspond au nom de l'ordinateur hébergeant le serveur d'enregistrement de session.
   - Pour HTTP : `http://servername/SessionRecordingBroker/RecordPolicy.rem?wsdl`, où *nomserveur* correspond au nom de l'ordinateur hébergeant le serveur d'enregistrement de session.
3. Si vous êtes invité à vous authentifier par NT LAN Manager (NTLM), connectez-vous avec un compte d'administrateur de domaine.

Pour vérifier la connectivité IIS avec le lecteur d'enregistrement de session :

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. Lancez un navigateur Web et entrez l'adresse suivante :
   - Pour HTTPS : `https://servername/SessionRecordingBroker/Player.rem?wsdl`, où *nomserveur* correspond au nom de l'ordinateur hébergeant le serveur d'enregistrement de session.
   - Pour HTTP : `http://servername/SessionRecordingBroker/Player.rem?wsdl`, où *nomserveur* correspond au nom de l'ordinateur hébergeant le serveur d'enregistrement de session.
3. Si vous êtes invité à vous authentifier par NT LAN Manager (NTLM), connectez-vous avec un compte d'administrateur de domaine.

Pour vérifier la connectivité IIS avec la console de stratégie d'enregistrement de session :

1. Ouvrez une session sur le serveur sur lequel la console de stratégie d'enregistrement de session est installée.
2. Lancez un navigateur Web et entrez l'adresse suivante :
   - Pour HTTPS : `https://servername/SessionRecordingBroker/PolicyAdministration.rem?wsdl`, où *nomserveur* correspond au nom de l'ordinateur hébergeant le serveur d'enregistrement de session.
   - Pour HTTP : `http://servername/SessionRecordingBroker/PolicyAdministration.rem?wsdl`, où *nomserveur* correspond au nom de l'ordinateur hébergeant le serveur d'enregistrement de session.
3. Si vous êtes invité à vous authentifier par NT LAN Manager (NTLM), connectez-vous avec un compte d'administrateur de domaine.

Si votre navigateur affiche un document au format XML, cela permet de vérifier que l'ordinateur exécutant la console de stratégie d'enregistrement de session s'est connecté au serveur d'enregistrement de session à l'aide du protocole configuré.

Dépanner les problèmes de certificat

Si le protocole de communication que vous utilisez est HTTPS, l'ordinateur hébergeant le serveur d'enregistrement de session doit être configuré avec un certificat de serveur. Toutes les connexions de composant au serveur d'enregistrement de session doivent posséder un certificat racine d'autorité de certification (CA). Sans cela, les tentatives de connexion entre les différents composants échoueront.

Vous pouvez tester vos certificats en accédant à la page Web du broker d'enregistrement de session, de la même manière que vous le feriez pour tester la connectivité IIS. Si vous pouvez accéder à la page XML de chaque composant, cela signifie que les certificats sont configurés correctement.

Voici quelques situations courantes pour lesquelles les émissions de certificats perturbent les connexions :

- **Certificats non valides ou manquants.** Si le serveur exécutant l'agent d'enregistrement de session n'a pas de certificat racine pouvant faire confiance au certificat de serveur, et qu'il ne peut pas faire confiance et se connecter au serveur d'enregistrement de session sur le protocole HTTPS, la connexion échoue. Vérifiez que tous les composants font confiance au certificat du serveur d'enregistrement de session.
- **Nom incohérent.** Si le certificat de serveur attribué à l'ordinateur hébergeant le serveur d'enregistrement de session est créé avec un nom de domaine complet (FQDN), tous les composants se connectant doivent utiliser le nom de domaine complet lors de la connexion au serveur d'enregistrement de session. Si un nom NetBIOS est utilisé, configurez les composants avec un nom NetBIOS pour le serveur d'enregistrement de session.
- **Certificats expirés.** Si un certificat de serveur est expiré, la connectivité au serveur d'enregistrement de session via le protocole HTTPS échoue. Veuillez vérifier que le certi-

ficat de serveur attribué à l'ordinateur hébergeant le serveur d'enregistrement de session est valide et qu'il n'est pas arrivé à expiration. Si le même certificat est utilisé pour la signature numérique des enregistrements de session, le journal des événements de l'ordinateur hébergeant le serveur d'enregistrement de session produira des messages d'erreur indiquant que le certificat a expiré ou des messages d'avertissement lorsqu'il arrive à expiration.

Échec de la recherche d'enregistrements à l'aide du lecteur

January 23, 2019

Si vous rencontrez des difficultés lors de la recherche d'enregistrements avec le lecteur d'enregistrement de session, les messages d'erreur suivants peuvent s'afficher :

- **Échec de la recherche des fichiers de session enregistrée. Le nom de serveur distant n'a pas pu être résolu : nomserveur. nomserveur** est le nom du serveur auquel le lecteur d'enregistrement de session tente de se connecter. Le lecteur d'enregistrement de session ne peut pas contacter le serveur d'enregistrement de session. Il existe deux raisons possibles : un nom de serveur tapé incorrectement ou le DNS ne peut pas résoudre le nom du serveur.

  Résolution : dans la barre de menu du lecteur, choisissez **Outils** > **Options** > **Connexions** et vérifiez que le nom du serveur dans la liste **Serveurs d'enregistrement de session** est correct. S'il est correct, exécutez la commande ping dans une invite de commande afin de vérifier s'il est possible de résoudre le nom. Lorsque le serveur d'enregistrement de session est en panne ou hors ligne, le message d'erreur d'échec de recherche des fichiers de session enregistrés est **Impossible de contacter le serveur distant**.

- **Impossible de contacter le serveur distant.** Cette erreur se produit lorsque le serveur d'enregistrement de session est en panne ou déconnecté.

  Résolution : vérifiez que le serveur d'enregistrement de session est connecté.

- **Accès refusé.** Une erreur d'accès refusé se produit si l'utilisateur n'a pas obtenu d'autorisation de recherche et de téléchargement de fichiers de session enregistrée.

  Résolution : attribuez le rôle Lecteur à l'utilisateur à l'aide de la console d'autorisation d'enregistrement de session.

- **Accès refusé lorsque le rôle Lecteur est attribué.** Cette erreur se produit lorsque vous installez le lecteur d'enregistrement de session sur la même machine que le serveur d'enregistrement de session, et que vous avez activé la fonction UAC. Lorsque vous attribuez au groupe d'utilisateurs Administrateurs du domaine ou Administrateurs le rôle Lecteur, un administrateur non intégré qui est inclus dans ce groupe peut échouer à la vérification basée sur le rôle lors de la recherche de fichiers d'enregistrement avec le lecteur d'enregistrement de session.

  Résolutions :

  - Exécuter le lecteur d'enregistrement de session en tant qu'administrateur.
  - Attribuer à des utilisateurs spécifiques le rôle Lecteur plutôt qu'à l'ensemble du groupe.
  - Installer le lecteur d'enregistrement de session sur une machine distincte de celle du serveur d'enregistrement de session.

- **Échec de la recherche des fichiers de session enregistrée. La connexion sous-jacente a été fermée. Impossible d'établir une relation de confiance pour le canal sécurisé SSL/TLS.** Cette exception est causée par le serveur d'enregistrement de session, qui utilise un certificat signé par une CA auquel la machine cliente ne fait pas confiance ou pour lequel elle n'a pas de certificat CA.

  Résolution : installez le certificat CA correct ou de confiance sur la station de travail sur laquelle le lecteur d'enregistrement de session est installé.

- **Le serveur distant a renvoyé une erreur : (403) interdit.** Il s'agit d'une erreur HTTPS standard qui se produit lorsque vous tentez de vous connecter en utilisant HTTP (protocole non sécurisé). Le serveur rejette la connexion parce qu'il est configuré par défaut pour n'accepter que les connexions sécurisées.

  Résolution : dans la barre de menus du **lecteur d'enregistrement de session**, choisissez **Outils** > **Options** > **Connexions**. Sélectionnez le serveur dans la liste **Serveurs d'enregistrement de session**, puis cliquez sur **Modifier**. Changez le protocole de **HTTP** à **HTTPS**.

Résolution des problèmes MSMQ

Si un message de notification s'affiche mais que l'utilisateur ne peut pas trouver les enregistrements après avoir effectué une recherche dans le lecteur d'enregistrement de session, il y a un problème avec MSMQ. Vérifiez que la file d'attente est connectée au serveur d'enregistrement de session (gestionnaire de stockage). Utilisez un navigateur Web pour tester les connexions afin d'identifier des erreurs de connexion éventuelles (si vous utilisez HTTP ou HTTPS pour votre protocole de communication MSMQ).

Pour vérifier que la file d'attente est connectée :

1. Ouvrez une session sur le serveur hébergeant l'agent d'enregistrement de session et afficher les files d'attente sortantes.
2. Vérifiez que la file d'attente de l'ordinateur hébergeant le serveur d'enregistrement de session indique un état connecté.
   - Si l'état indiqué est **En attente de connexion**, que la file d'attente contient des messages et que le protocole est HTTP ou HTTPS (selon le protocole sélectionné dans l'onglet **Connexions** de la boîte de dialogue **Propriétés de dialogue de l'agent d'enregistrement de session**), effectuez les opérations de l'étape 3.

- Si l'état indique **connecté** et qu'aucun message ne se trouve dans la file d'attente, il peut y avoir un problème sur le serveur hébergeant le serveur d'enregistrement de session. Ignorez l'étape 3 et effectuez l'étape 4.

3. Si la file d'attente contient des messages, ouvrez un navigateur Web et entrez l'adresse suivante :

   - Pour HTTPS : `https://servername/msmq/private$/CitrixSmAudData`, où *nom-serveur* correspond au nom de l'ordinateur hébergeant le serveur d'enregistrement de session.
   - Pour HTTP : `http://servername/msmq/private$/CitrixSmAudData`, où *nom-serveur* correspond au nom de l'ordinateur hébergeant le serveur d'enregistrement de session.

   Si la page renvoie une erreur telle que **Le serveur n'accepte que les connexions sécurisées**, changez le protocole MSMQ figurant dans la liste **Propriétés de l'agent d'enregistrement de session** pour HTTPS. Si la page fait état d'un problème avec le certificat de sécurité du site Web, il se peut qu'il y ait un problème avec une relation d'approbation pour le canal sécurisé TLS. Dans ce cas, installez le certificat CA correct, ou utilisez une CA de confiance.

4. Si la file d'attente ne contient pas de message, ouvrez une session sur l'ordinateur hébergeant le serveur d'enregistrement de session et affichez les files d'attente privées. Sélectionnez **citrixsmauddata**. Si la file d'attente contient des messages (colonne Nombre de messages), vérifiez que le service StorageManager de l'enregistrement de session a démarré. S'il ne l'est pas, redémarrez le service.

Changer de protocole de communication

January 23, 2019

Pour des raisons de sécurité, Citrix déconseille d'utiliser HTTP comme protocole de communication. L'installation de l'enregistrement de session est configurée pour utiliser le mode HTTPS. Pour utiliser HTTP au lieu de HTTPS, vous devez modifier plusieurs paramètres.

Utiliser HTTP comme protocole de communication

1. Connectez-vous à l'ordinateur hébergeant le serveur d'enregistrement de session et désactivez les connexions sécurisées pour Session Recording Broker dans IIS.
2. Changez le paramètre du protocole de HTTPS à HTTP dans **Propriétés de l'agent d'enregistrement de session** sur chaque serveur sur lequel l'Agent d'enregistrement de session est installé :

a) Ouvrez une session sur chaque serveur sur lequel l'agent d'enregistrement de session est installé.
b) À partir du menu **Démarrer**, choisissez **Propriétés de l'Agent d'enregistrement de session**.
c) Dans la boîte de dialogue **Propriétés de l'Agent d'enregistrement de session**, choisissez l'onglet **Connexions**.
d) Dans la zone **Broker d'enregistrement de session**, sélectionnez **HTTP** dans la liste déroulante **Protocole** et choisissez **OK** pour accepter la modification. Si vous êtes invité à redémarrer le service, choisissez **Oui**.

3. Modifiez le paramètre de protocole de HTTPS à HTTP dans les paramètres du lecteur d'enregistrement de session :
   a) Ouvrez une session sur chaque poste de travail sur lequel le lecteur d'enregistrement de session est installé.
   b) À partir du menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
   c) Dans la barre de menu **Lecteur d'enregistrement de session**, choisissez **Outils** > **Options** > **Connexions**, sélectionnez le serveur et choisissez **Modifier**.
   d) Sélectionnez **HTTP** dans la liste déroulante **Protocole** et cliquez deux fois sur **OK** pour accepter le changement et quitter la boîte de dialogue.
4. Changez le paramètre de protocole de HTTPS à HTTP dans la console d'enregistrement de session:
   a) Ouvrez une session sur le serveur sur lequel la console de stratégie d'enregistrement de session est installée.
   b) À partir du menu **Démarrer**, choisissez **Console de stratégie d'enregistrement de session**.
   c) Sélectionnez **HTTP** dans la liste déroulante **Protocole** et cliquez sur **OK** pour vous connecter. Si la connexion est établie, ce paramètre est mémorisé lorsque vous lancez la console de stratégie d'enregistrement de session la fois suivante.

Rétablir HTTPS en tant que protocole de communication

1. Connectez-vous à l'ordinateur hébergeant le serveur d'enregistrement de session et activez les connexions sécurisées pour Broker d'enregistrement de session dans IIS.
2. Changez le paramètre du protocole de HTTP à HTTPS dans chaque boîte de dialogue **Propriétés de l'agent d'enregistrement de session** :
   a) Ouvrez une session sur chaque serveur sur lequel l'agent d'enregistrement de session est installé.
   b) À partir du menu **Démarrer**, choisissez **Propriétés de l'Agent d'enregistrement de session**.
   c) Dans la boîte de dialogue **Propriétés de l'Agent d'enregistrement de session**, choisissez

l'onglet **Connexions**.

d) Dans la zone **Broker d'enregistrement de session**, sélectionnez **HTTPS** dans la liste déroulante **Protocole** et choisissez **OK** pour accepter la modification. Si vous êtes invité à redémarrer le service, choisissez **Oui**.

3. Modifiez le paramètre de protocole de HTTP à HTTPS dans les paramètres du lecteur d'enregistrement de session :
   a) Ouvrez une session sur chaque poste de travail sur lequel le lecteur d'enregistrement de session est installé.
   b) À partir du menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
   c) Dans la barre de menu **Lecteur d'enregistrement de session**, choisissez **Outils** > **Options** > **Connexions**, sélectionnez le serveur et choisissez **Modifier**.
   d) Sélectionnez **HTTPS** dans la liste déroulante **Protocole** et cliquez deux fois sur **OK** pour accepter le changement et quitter la boîte de dialogue.
4. Modifiez le paramètre de protocole de HTTP à HTTPS dans les paramètres de la console de stratégie d'enregistrement de session :
   a) Ouvrez une session sur le serveur sur lequel la console de stratégie d'enregistrement de session est installée.
   b) À partir du menu **Démarrer**, choisissez **Console de stratégie d'enregistrement de session**.
   c) Sélectionnez **HTTPS** dans la liste déroulante **Protocole** et cliquez sur **OK** pour vous connecter. Si la connexion est établie, ce paramètre est mémorisé lorsque vous lancez la console de stratégie d'enregistrement de session la fois suivante.

Gérer vos enregistrements de base de données

February 28, 2019

L'utilitaire de base de données de journalisation ICA (ICLDB) est un utilitaire de ligne de commande pour base de données utilisé pour la manipulation des éléments de base de données constitués d'enregistrements de sessions. Cet utilitaire est installé en même temps que l'enregistrement de session dans le répertoire lecteur:\Program Files\Citrix\SessionRecording\Server\Bin du serveur hébergeant le logiciel Serveur d'enregistrement de session.

Tableau de référence rapide

Le tableau suivant contient la liste des commandes et des options disponibles avec l'utilitaire ICLDB. Tapez les commandes en utilisant le format suivant :

icldb [version | locate | dormant | import | archive | remove | removeall] command-options [/l] [/f] [/s] [/?]

> **Remarque :**
>
> des instructions plus détaillées sont disponibles dans l'aide associée à l'utilitaire. Pour y accéder à partir d'une ligne de commande, tapez **icldb /?** dans le répertoire du lecteur :**\Program Files\Citrix\SessionRecording\Server\Bin**. Pour accéder à l'aide de commandes spécifiques, tapez **icldb *command* /?**.

Commande	Description
archive	Permet d'archiver les fichiers d'enregistrement de session plus anciens que la période de rétention spécifiée. Utilisez cette commande pour archiver les fichiers.
dormant	Cette commande permet d'afficher ou de compter les fichiers d'enregistrement de session considérés comme dormants. Les fichiers dormants sont des enregistrements de session incomplets en raison d'une perte de données. Utilisez cette commande pour vérifier si vous suspectez une perte de données. Vous pouvez vérifier si les fichiers d'enregistrement de session deviennent dormants pour l'intégralité de la base de données ou si s'il ne s'agit que des enregistrements effectués pendant un certain nombre de jours, d'heures ou de minutes.
import	Permet d'importer les fichiers d'enregistrement de session dans la base de données d'enregistrement de session. Utilisez la commande pour reconstituer la base de données si vous perdez les enregistrements de la base de données. Vous pouvez également utiliser la commande pour fusionner des bases de données (si vous avez deux bases de données, vous pouvez importer les fichiers de l'une des bases de données).

Commande	Description
locate	Permet de localiser et d'afficher le chemin complet vers un fichier d'enregistrement de session en utilisant l'identificateur de fichier comme critère. Utilisez cette commande lorsque vous cherchez l'emplacement d'un fichier d'enregistrement de session. Il s'agit aussi d'une manière de vérifier si la base de données est à jour par rapport à un fichier spécifique.
la	Permet de supprimer les références à des fichiers d'enregistrement de session de la base de données. Utilisez cette commande (prudemment) pour nettoyer la base de données. Spécifiez la période de rétention à utiliser comme critères. Vous pouvez également supprimer le fichier physique associé.
removeall	Cette commande supprime toutes les références aux fichiers d'enregistrement de session de la base de données d'enregistrement de session et rétablit l'état d'origine de la base de données. Les fichiers physiques ne sont pas supprimés ; il est toutefois impossible de les rechercher dans le lecteur d'enregistrement de session. Utilisez cette commande (prudemment) pour nettoyer la base de données. Les références supprimées ne peuvent être rétablies qu'en effectuant une restauration à partir des fichiers de sauvegarde.
version	Cette commande permet d'afficher la version du schéma de la base de données d'enregistrement de session.
/l	Cette commande enregistre les résultats et les erreurs dans le journal des événements Windows.

Commande	Description
/f	Cette commande force l'exécution de la commande sans invites.
/s	Cette commande supprime le message de copyright.
/?	Cette commande affiche l'aide des commandes.

Archiver les anciens fichiers d'enregistrement de session

Pour maintenir un niveau adéquat de capacité de disque disponible dans les emplacements de stockage des enregistrements, archivez régulièrement les fichiers d'enregistrement de session. Les intervalles d'archivage diffèrent en fonction de la quantité d'espace disque disponible et de la taille typique des fichiers d'enregistrement de session. Les fichiers d'enregistrement de session doivent dater de plus de deux jours à compter de la date de début avant de pouvoir être archivés. Cette règle vise à empêcher l'archivage d'enregistrements en direct avant qu'ils soient terminés.

Deux méthodes sont disponibles lorsque vous archivez des enregistrements de session. L'enregistrement de base de données pour un fichier d'enregistrement de session peut être mis à jour vers le statut d'archivage tant que le fichier d'enregistrement de session reste à l'emplacement de stockage de l'enregistrement. Cette méthode peut être utilisée pour réduire les résultats de la recherche dans le lecteur. L'autre méthode consiste à mettre à jour l'enregistrement de la base de données d'un fichier d'enregistrement de session vers le statut archivé et à déplacer le fichier depuis l'emplacement de stockage de l'enregistrement vers un autre emplacement afin de le sauvegarder sur un autre support. Lorsque l'utilitaire ICLDB déplace les fichiers d'enregistrement de session, ceux-ci sont déplacés vers le répertoire spécifié, dans lequel la structure de dossiers d'origine, année/mois/jour, n'existe plus.

L'enregistrement de session dans la base de données d'enregistrement de session contient deux champs associés à l'archivage : l'heure d'archivage représentant la date et l'heure actuelles d'archivage d'un enregistrement de session ; la note d'archivage, une note textuelle facultative pouvant être ajoutée par l'administrateur lors de l'archivage. Les deux champs indiquent qu'un enregistrement de session a été archivé et l'heure d'archivage.

Dans le lecteur d'enregistrement de session, tous les enregistrements de session archivés indiquent l'état Archivé, ainsi que la date et l'heure de l'archivage. Les enregistrements de session archivés peuvent toujours être lus si les fichiers n'ont pas été déplacés. Si un fichier d'enregistrement de session a été déplacé lors de l'archivage, une erreur de fichier introuvable est affichée. Le fichier d'enregistrement de session doit être restauré avant que la session ne puisse être lue. Pour restaurer un enregistrement de session, indiquez à l'administrateur l'identifiant de fichier et l'heure d'archivage

de l'enregistrement de la session à partir de la boîte de dialogue Propriétés d'enregistrement du Lecteur d'enregistrement de session. La restauration de fichiers archivés est abordée plus loin dans la section Restaurer les fichiers d'enregistrement de session.

La commande **archive** de l'utilitaire ICLDB a plusieurs paramètres qui sont décrits comme suit :

- **/RETENTION:<jours>** - Période de rétention, en jours, des enregistrements de session. Les enregistrements plus anciens que le nombre de jours spécifié sont marqués comme archivés dans la base de données d'enregistrement de session. La période de rétention doit être un nombre entier supérieur ou égal à 2 jours.
- **/LISTFILES** – Répertorie le chemin complet et le nom des fichiers d'enregistrement de la session au fur et à mesure de leur archivage. Paramètre facultatif.
- **/MOVETO:<répertoire>** - Répertoire dans lequel vous déplacez physiquement les fichiers d'enregistrement de session archivés. Le répertoire spécifié doit exister. Paramètre facultatif. Si aucun répertoire n'est spécifié, les fichiers restent dans leur emplacement de stockage d'origine.
- **/NOTE:<note>** - note de texte ajoutée à l'enregistrement de la base de données pour chaque enregistrement de session archivé. Assurez-vous que la note est entourée de guillemets. Paramètre facultatif.
- **/L** - Enregistre les résultats et les erreurs dans le journal des événements Windows du nombre de fichiers d'enregistrement de session archivés. Paramètre facultatif.
- **/F** – Cette commande force l'exécution de la commande sans invites. Paramètre facultatif.

Pour archiver des enregistrements de session dans la base de données d'enregistrement de session et déplacer physiquement les fichiers d'enregistrement de session

1. Ouvrez une session en tant qu'administrateur local sur le serveur sur lequel le serveur d'enregistrement de session est installé.
2. Démarrez une invite de commande.
3. Passez du répertoire de travail actuel au répertoire Bin du chemin d'installation du serveur d'enregistrement de session (<chemin d'installation du serveur d'enregistrement de session>/Server/Bin).
4. Exécutez la commande **ICLDB ARCHIVE /RETENTION:<jours> /LISTFILES /MOVETO:<répertoire> /NOTE:<note> /L** où **jours** est la durée de rétention des fichiers d'enregistrement de session, **répertoire** est le répertoire dans lequel les fichiers d'enregistrement de session archivés sont déplacés, et **note** est la note de texte ajoutée à l'enregistrement de la base de données pour chaque fichier d'enregistrement de session archivé. Entrez **Y** pour confirmer l'archivage.

Pour archiver des enregistrements de session dans la base de données d'enregistrement de session uniquement

1. Ouvrez une session en tant qu'administrateur local sur le serveur sur lequel le serveur d'enregistrement de session est installé.
2. Démarrez une invite de commande.
3. Passez du répertoire de travail actuel au répertoire Bin du chemin d'installation du serveur d'enregistrement de session (<chemin d'installation du serveur d'enregistrement de session>/Server/Bin).
4. Exécutez la commande **ICLDB ARCHIVE /RETENTION:<jours> /LISTFILES /NOTE:<note> /L** où **jours** est la durée de rétention des fichiers d'enregistrement de session et **note** est la note de texte ajoutée à l'enregistrement de la base de données pour chaque enregistrement de session archivé. Entrez **Y** pour confirmer l'archivage.

Restaurer les fichiers d'enregistrement de session

La restauration des fichiers d'enregistrement de session est requise lorsque vous souhaitez afficher un enregistrement de session archivé dans la base de données d'enregistrement de session et que le fichier a été déplacé de l'emplacement de stockage de l'enregistrement. Les enregistrements de session archivés qui n'ont pas été déplacés depuis l'emplacement de stockage des enregistrements pendant l'archivage sont toujours accessibles dans le lecteur d'enregistrement de session.

Deux méthodes sont disponibles pour restaurer les fichiers d'enregistrement de session qui ont été déplacés. Copiez le fichier d'enregistrement de session requis dans le répertoire de restauration des fichiers archivés ou importez-le dans la base de données d'enregistrement de session à l'aide de l'utilitaire ICLDB. Citrix recommande la première méthode de restauration des fichiers d'enregistrement de session archivés. Supprimez les fichiers archivés copiés dans le répertoire de restauration lorsque vous n'en avez plus besoin.

Le broker d'enregistrement de session utilise le **répertoire de restauration pour fichiers archivés** lorsqu'un fichier d'enregistrement de session est introuvable dans son emplacement de stockage d'origine. Cela se produit lorsque le lecteur d'enregistrement de session demande la lecture d'un fichier d'enregistrement de session. Le broker d'enregistrement de session tente d'abord de trouver le fichier d'enregistrement de session dans l'emplacement de stockage d'origine. Si le fichier n'est pas trouvé dans l'emplacement de stockage d'origine, le broker vérifie ensuite le **répertoire de restauration pour fichiers archivés**. Si le fichier est présent dans le répertoire de restauration, le broker l'envoie au lecteur d'enregistrement de session pour le lire. Sinon, si le fichier n'est pas trouvé, le broker envoie une erreur de fichier non trouvé au lecteur d'enregistrement de session.

L'importation de fichiers d'enregistrement de session archivés à l'aide de l'utilitaire ICLDB met à jour la base de données d'enregistrement de session avec les informations d'enregistrement de session

provenant du fichier d'enregistrement de session, y compris un nouveau chemin de stockage pour le fichier. L'utilisation de l'utilitaire ICLDB pour importer un fichier d'enregistrement de session archivé ne le déplace pas vers son emplacement de stockage d'origine lors de l'enregistrement de la session.

Remarque : l'heure d'archivage et la note d'archivage sont effacées dans la base de données d'enregistrement de session d'un fichier importé. Par conséquent, lors de la prochaine exécution de la commande d'archivage ICLDB, le fichier d'enregistrement de session importé peut être à nouveau archivé.

La commande d'importation ICLDB est utile pour importer un grand nombre de fichiers d'enregistrement de session archivés, réparer ou mettre à jour des données d'enregistrement de session incorrectes ou manquantes dans la base de données d'enregistrement de session, ou déplacer des fichiers d'enregistrement de session d'un emplacement de stockage vers un autre emplacement sur le serveur d'enregistrement de session. La commande **import** de l'ICLDB peut également être utilisée pour remplir la base de données d'enregistrement de session avec des enregistrements de session après l'exécution de la commande ICLDB **removeall**.

La commande **import** de l'utilitaire ICLDB a plusieurs paramètres qui sont décrits comme suit :

- **/LISTFILES** – Répertorie le chemin complet et le nom des fichiers d'enregistrement de la session au fur et à mesure de leur importation. Paramètre facultatif.
- **/RECURSIVE** - Recherche dans tous les sous-répertoires les fichiers d'enregistrement de session. Paramètre facultatif.
- **/L** - Enregistre les résultats et les erreurs dans le journal des événements Windows du nombre de fichiers d'enregistrement de session importés. Paramètre facultatif.
- **/F** – Cette commande force l'exécution de la commande sans invites. Paramètre facultatif.

Pour restaurer des fichiers d'enregistrement de session à l'aide du répertoire de restauration des fichiers archivés

1. Ouvrez une session en tant qu'administrateur local sur le serveur sur lequel le serveur d'enregistrement de session est installé.
2. Dans les propriétés du lecteur d'enregistrement de session, déterminez l'ID de fichier et l'heure d'archivage du fichier d'enregistrement de session archivé.
3. Localisez le fichier d'enregistrement de session dans vos sauvegardes à l'aide de l'ID de fichier spécifié dans les propriétés du lecteur d'enregistrement de session. Chaque enregistrement de session a le nom de fichier **i_<IDFichier>**.icl, où IDFichier est l'ID du fichier d'enregistrement de session.
4. Copiez le fichier d'enregistrement de session de votre sauvegarde dans le répertoire de restauration pour fichiers archivés. Pour déterminer le répertoire de restauration pour fichiers archivés

:

a) À partir du menu **Démarrer**, choisissez **Démarrer** > **Tous les programmes** > **Citrix** > **Propriétés du lecteur d'enregistrement de session**.

b) Dans la fenêtre Propriétés du serveur d'enregistrement de session, sélectionnez l'onglet **Stockage**. Le répertoire de restauration actuel apparaît dans le champ **Répertoire de restauration pour les fichiers archivés**.

Pour restaurer des fichiers d'enregistrement de session à l'aide de la commande d'importation ICLDB

1. Ouvrez une session en tant qu'administrateur local sur le serveur sur lequel le serveur d'enregistrement de session est installé.
2. Démarrez une invite de commande.
3. Passez du répertoire de travail actuel au répertoire Bin du chemin d'installation du serveur d'enregistrement de session (<chemin d'installation du serveur d'enregistrement de session>/Server/Bin).
4. Vous pouvez au choix :
   - Exécutez la commande **ICLDB IMPORT /LISTFILES /RECURSIVE /L <répertoire>** où **répertoire** est le nom d'un ou de plusieurs répertoires, séparés par un espace, contenant des fichiers d'enregistrement de session. Entrez **Y** pour confirmer l'importation.
   - Exécutez la commande **ICLDB IMPORT /LISTFILES /L <fichier>** où **fichier** est le nom d'un ou de plusieurs fichiers d'enregistrement de session, séparés par un espace. Des caractères génériques peuvent être utilisés pour spécifier des fichiers d'enregistrement de session. Entrez **Y** pour confirmer l'importation.

Journalisation de la configuration

November 13, 2018

La journalisation de la configuration capture les modifications apportées à la configuration du site et les activités administratives effectuées sur la base de données. Vous pouvez utiliser le contenu consigné pour :

- diagnostiquer et résoudre les problèmes après que des modifications sont apportées à la configuration ; le journal fournit une arborescence hiérarchique ;
- assister la gestion des modifications et suivre les configurations ;
- signaler les activités administratives.

Vous définissez les préférences de journalisation de la configuration, afficher les journaux de configuration et générer des rapports HTML et CSV à partir de Citrix Studio. Vous pouvez filtrer les affichages des journaux de configuration par plages de dates et selon les résultats de recherche en texte intégral. La journalisation obligatoire, lorsqu'elle est activée, empêche les modifications de la configuration à moins qu'elles puissent être journalisées. Avec des autorisations appropriées, vous pouvez supprimer des entrées dans le journal de configuration. Vous ne pouvez pas utiliser la fonction de journalisation de la configuration pour modifier le contenu du journal.

La journalisation de la configuration utilise un SDK PowerShell et le service de journalisation de la configuration. Le service de journalisation de la configuration s'exécute sur chaque Controller dans le site ; si un Controller échoue, le service sur un autre Controller traite automatiquement les demandes de journalisation.

Par défaut, la fonction de journalisation de la configuration est activée, et utilise la base de données qui est créée lorsque vous créez le site (la base de données de configuration de site). Vous pouvez spécifier un emplacement différent pour la base de données. La base de données de journalisation de la configuration prend en charge les mêmes fonctions haute disponibilité que la base de données de configuration de site.

L'accès à la journalisation de la configuration est contrôlé via l'administration déléguée, avec les autorisations Modifier les préférences de journalisation et Afficher les journaux de configuration.

Les journaux de configuration sont localisés lorsqu'ils sont créés. Par exemple, un journal créé en anglais sera lue en anglais, quels que soient les paramètres régionaux du lecteur.

Qu'est-ce qui est journalisé

Les modifications de configuration et les activités administratives initiées depuis Studio, Director et des scripts PowerShell sont journalisées. Les exemples de modifications apportées à la configuration journalisées comprennent l'utilisation de (création, modification, suppression des affectations) :

- Catalogues de machines
- Groupes de mise à disposition (y compris la modification des paramètres de gestion de la puissance)
- Rôles et étendues de l'administrateur
- Ressources et connexions de l'hôte
- Stratégies Citrix au travers de Studio

Exemples de modifications administratives journalisées :

- Gestion de la puissance d'une machine virtuelle ou d'un bureau utilisateur
- Envoi d'un message à un utilisateur par Studio ou Director

Les opérations suivantes ne sont pas enregistrées :

- Opérations autonomes telles que la mise sous tension de la gestion du pool de machines virtuelles.
- Actions de stratégie implémentées au travers de la console de gestion des stratégies de groupe (GPMC) ; utilisez les outils Microsoft pour afficher des journaux de ces actions.
- Les modifications effectuées via le Registre, accès direct à la base de données, ou à partir de sources autres que Studio, Director ou PowerShell.
- Lorsque le déploiement est initialisé, la journalisation de la configuration est disponible lorsque la première instance du service de journalisation de la configuration s'enregistre auprès du service de configuration. Par conséquent, les premières étapes de configuration ne sont pas journalisées (par exemple, lorsque le schéma de base de données est obtenu et appliqué, lors de l'initialisation d'un hyperviseur).

Gérer la journalisation de la configuration

Par défaut, la journalisation de la configuration utilise la base de données qui est créée lorsque vous créez un site (également connu sous le nom de base de données de configuration de site). Citrix vous recommande d'utiliser un autre emplacement pour la base de données de journalisation de configuration (et la base de données de surveillance) pour les raisons suivantes :

- La stratégie de sauvegarde de la base de données de journalisation de la configuration est susceptible d'être différente de celle de la stratégie de sauvegarde de la base de données de configuration de site.
- Le volume de données collectées pour la journalisation de la configuration (et le service de surveillance) peut avoir un impact négatif sur l'espace disponible pour la base de données de configuration de site.
- Elle partage le point de défaillance unique pour les trois des bases de données.

Remarque : les éditions de produit qui ne prennent pas en charge la journalisation de la configuration ne disposent pas d'un nœud Journalisation dans Studio.

Activer/désactiver la journalisation de la configuration et la journalisation obligatoire

Par défaut, la journalisation de la configuration est activée et la journalisation obligatoire est désactivée.

1. Sélectionnez **Journalisation** dans le volet de navigation Studio.
2. Sélectionnez **Préférences** dans le volet Actions. La boîte de dialogue Journalisation de la configuration contient des informations de base de données et indique si la journalisation de la configuration et la journalisation obligatoire sont activées ou désactivées.
3. Sélectionnez l'action souhaitée :

Pour activer la journalisation de la configuration, sélectionnez le bouton radio **Activer**. C'est le réglage par défaut. S'il est impossible d'écrire sur la base de données, les informations de journalisation sont ignorées, mais l'opération se poursuit.

Pour désactiver la journalisation de la configuration, sélectionnez le bouton radio **Désactiver**. Si la journalisation était préalablement activée, les journaux existants restent lisibles avec le SDK PowerShell.

Pour activer la journalisation obligatoire, sélectionnez le bouton radio **Empêcher les modifications à la configuration du site lorsque la BDD n'est pas disponible**. Aucune modification de la configuration ou activité administrative ne sera enregistrée (contrairement à la normale) à moins qu'elle puisse être écrite dans la base de données de journalisation de la configuration. Vous pouvez activer la journalisation obligatoire uniquement lorsque la journalisation de la configuration est activée, c'est-à-dire lorsque le bouton radio **Activer** est sélectionné. Si le service de journalisation de la configuration échoue, et que la haute disponibilité n'est pas utilisée, la journalisation obligatoire est utilisée. Dans de tels cas, les opérations qui seraient normalement enregistrées ne le sont pas.

Pour désactiver la journalisation obligatoire, sélectionnez le bouton radio **Autoriser modifications de la configuration du site lorsque la BDD n'est pas disponible**. Les modifications de configuration et les activités administratives sont autorisées, même si la base de données utilisée pour la journalisation de la configuration est inaccessible. C'est le réglage par défaut.

Pour modifier l'emplacement de la base de données de journalisation de la configuration

Remarque : vous ne pouvez pas modifier l'emplacement de la base de données lorsque la journalisation obligatoire est activée, car la modification de l'emplacement inclut un bref intervalle qui ne peut pas être enregistré.

1. Créez un serveur de base de données, à l'aide d'une version SQL Server prise en charge.
2. Sélectionnez **Journalisation** dans le volet de navigation Studio.
3. Sélectionnez **Préférences** dans le volet Actions.
4. Dans la boîte de dialogue Préférences de journalisation, sélectionnez **Modifier la base de données de journalisation**.
5. Dans la boîte de dialogue Changer la base de données de journalisation, spécifiez l'emplacement du serveur contenant le nouveau serveur de base de données. Les formats valides sont répertoriés dans l'article Bases de données.
6. Pour autoriser Studio pour créer la base de données, cliquez sur **OK**. Lorsque vous y êtes invité, cliquez sur **OK** et la base de données sera créée automatiquement. Studio tente d'accéder à la base de données à l'aide des informations d'identification de l'utilisateur de Studio ; si la tentative échoue, vous êtes invité à entrer les informations d'identification de l'utilisateur de la base de données. Studio télécharge ensuite le schéma de base de données vers la base de

données. (Les informations d'identification ne sont conservées que lors de la création de la base de données.)

7. Pour créer la base de données manuellement, cliquez sur **Générer script de base de données**. Le script généré comprend des instructions pour la création manuelle de la base de données. Assurez-vous que la base de données est vide et qu'au moins un utilisateur est autorisé à accéder et modifier la base de données avant le chargement du schéma.

Les données journalisation de la configuration ne sont pas importées vers la nouvelle base de données. Les journaux ne peuvent pas être regroupés pour les deux bases de données lors de la récupération des journaux. La première entrée du journal dans la nouvelle base de données de journalisation de la configuration indique qu'une modification a été apportée dans une base de données, mais elle n'identifie pas la base de données précédente.

Afficher le contenu du journal de configuration

Lorsque vous effectuez des modifications de configuration et des activités administratives, les opérations de haut niveau créées par Studio et Director sont affichées dans la partie supérieure du panneau central dans Studio. Une opération de haut niveau se traduit par un ou plusieurs appels de service et de SDK, qui sont des opérations de bas niveau. Lorsque vous sélectionnez une opération de haut niveau dans le panneau supérieur du milieu, le panneau inférieur central affiche les opérations de bas niveau.

Si une opération échoue avant la fin de l'opération, l'opération de journalisation peut ne pas être effectuée dans la base de données ; par exemple, un enregistrement de début n'aura pas d'enregistrement de fin correspondant. Dans de tels cas, le journal indique qu'il manque des informations. Lorsque vous affichez les journaux basés en fonction de plages de temps, les journaux incomplets sont affichés si les données dans les journaux correspondent aux critères. Par exemple, si tous les journaux des cinq derniers jours sont demandés et qu'un journal existe avec une heure de début dans les cinq derniers jours, mais sans date de fin, il est inclus.

Lors de l'utilisation d'un script pour appeler des applets de commande PowerShell, si vous créez une opération de bas niveau sans spécifier une opération de haut niveau parente, la journalisation de la configuration va créer une opération de haut niveau de substitution.

Pour afficher le contenu du journal de configuration, sélectionnez **Journalisation** dans le panneau de navigation. Par défaut, l'affichage dans le panneau central affiche le contenu du journal par ordre chronologique (la plus récente des entrées en premier), en les séparant par date.

Pour filtrer l'affichage par	Effectuez cette action
Résultats de la recherche	Entrez le texte dans la zone Rechercher en haut du panneau central. L'affichage filtré inclut le nombre de résultats de la recherche. Pour revenir à l'affichage de la journalisation standard, désactivez le texte dans la zone Rechercher.
En-tête de la colonne	Cliquez sur un en-tête de colonne pour trier l'affichage par ce champ.
Une plage de dates	Sélectionnez un intervalle dans la zone de liste déroulante en regard de la zone Rechercher en haut du panneau central.

Générer des rapports

Vous pouvez générer des rapports au format CSV et HTML contenant les données du journal de la configuration.

- Le rapport CSV contient toutes les données de journalisation à partir d'un intervalle de temps spécifié. La hiérarchie des données dans la base de données est aplatie dans un seul tableau CSV. Aucun aspect des données n'a la priorité dans le fichier. Aucune mise en forme n'est utilisée, les données sont donc inintelligibles. Le fichier (appelé sur MyReport) contient les données dans un format lisible. Les fichiers CSV sont souvent utilisés pour l'archivage des données ou en tant que source de données pour un outil de création de rapports ou de manipulation de données tel que Microsoft Excel.
- Le rapport HTML fournit un formulaire lisible des données de journalisation pour un intervalle de temps spécifié. Il fournit une vue structurée et navigable pour la vérification des modifications. Un rapport HTML se compose de deux fichiers appelés Résumé et Détails. Le fichier Résumé répertorie les opérations de haut niveau : moment auquel chaque opération se produit, personne qui réalise l'opération et le résultat. Si vous cliquez sur un lien Détails en regard de chaque opération, vous êtes amené aux opérations de bas niveau dans le fichier Détails, qui fournit des informations supplémentaires.

Pour générer un rapport du journal de configuration, sélectionnez **Journalisation** dans le panneau de navigation de Studio, puis sélectionnez **Créer un rapport personnalisé** dans le volet Actions.

- Sélectionnez la plage de dates pour le rapport.
- Sélectionnez le format du rapport : CSV, HTML ou les deux.
- Naviguez jusqu'à l'emplacement où le rapport doit être enregistré.

Supprimer le contenu du journal de configuration

Pour supprimer le journal de configuration, vous devez posséder certaines permissions d'administration déléguée et de base de données SQL Server.

- **Administration déléguée :** vous devez disposer d'un rôle Administration déléguée qui permet la lecture de la configuration du déploiement. Le rôle d'administrateur complet intégré dispose de cette autorisation. Les options En lecture seule ou Gérer doivent être sélectionnées dans la catégorie Autres permissions pour un rôle personnalisé.

  Pour créer une copie de sauvegarde des données de journalisation de la configuration avant de les supprimer, les options En lecture seule ou Gérer doivent également être sélectionnées dans la catégorie Permissions de journalisation pour le rôle personnalisé.

- **Base de données SQL Server :** vous devez disposer d'une connexion au serveur SQL avec la permission de supprimer des enregistrements de la base de données. Il existe deux façons de procéder :

  - Utiliser une connexion à une base de données SQL Server avec un rôle de serveur sysadmin, ce qui vous permet d'effectuer toute activité sur le serveur de base de données. Les rôles de serveur serveradmin ou setupadmin vous permettent d'effectuer des opérations de suppression.
  - Si votre déploiement requiert une sécurité supplémentaire, utilisez une connexion de base de données non-sysadmin mappée sur un utilisateur de base de données qui est autorisé à supprimer des enregistrements de la base de données.

    1. Dans SQL Server Management Studio, créez une connexion SQL Server avec un rôle de serveur autre que « sysadmin ».
    2. Mappez la connexion sur un utilisateur dans la base de données ; SQL Server crée automatiquement un utilisateur dans la base de données avec le même nom que la connexion.
    3. Dans l'appartenance au rôle de base de données, spécifiez au moins un des membres de rôle pour la base de données utilisateur : ConfigurationLoggingSchema_ROLE ou dbowner.

    Pour de plus amples informations, consultez la documentation de SQL Server Management Studio.

Pour supprimer les journaux de configuration :

1. Sélectionnez **Journalisation** dans le volet de navigation Studio.
2. Sélectionnez **Supprimer les journaux** dans le volet Actions.
3. Vous êtes invité à indiquer si vous voulez créer une sauvegarde des journaux avant de les supprimer. Si vous choisissez de créer une copie de sauvegarde, naviguez jusqu'à l'emplacement

où l'archive de sauvegarde doit être enregistrée. La sauvegarde va être créée en tant que fichier CSV.

Une fois les journaux de configuration effacés, la suppression du journal est la première activité consignée dans le journal vide. Cette entrée fournit des informations sur la personne qui a supprimé les journaux et la date à laquelle ils ont été supprimés.

Journaux d'événements

January 23, 2019

Les articles suivants contiennent des listes et des descriptions des événements qui peuvent être consignés par les services XenApp et XenDesktop.

Ces informations ne sont pas complètes ; consultez les articles de chaque fonctionnalité pour plus d'informations sur les événements.

Événements Citrix Broker Service (HTML)

Événements SDK Citrix FMA Service (HTML)

Événements Citrix Configuration Service (HTML)

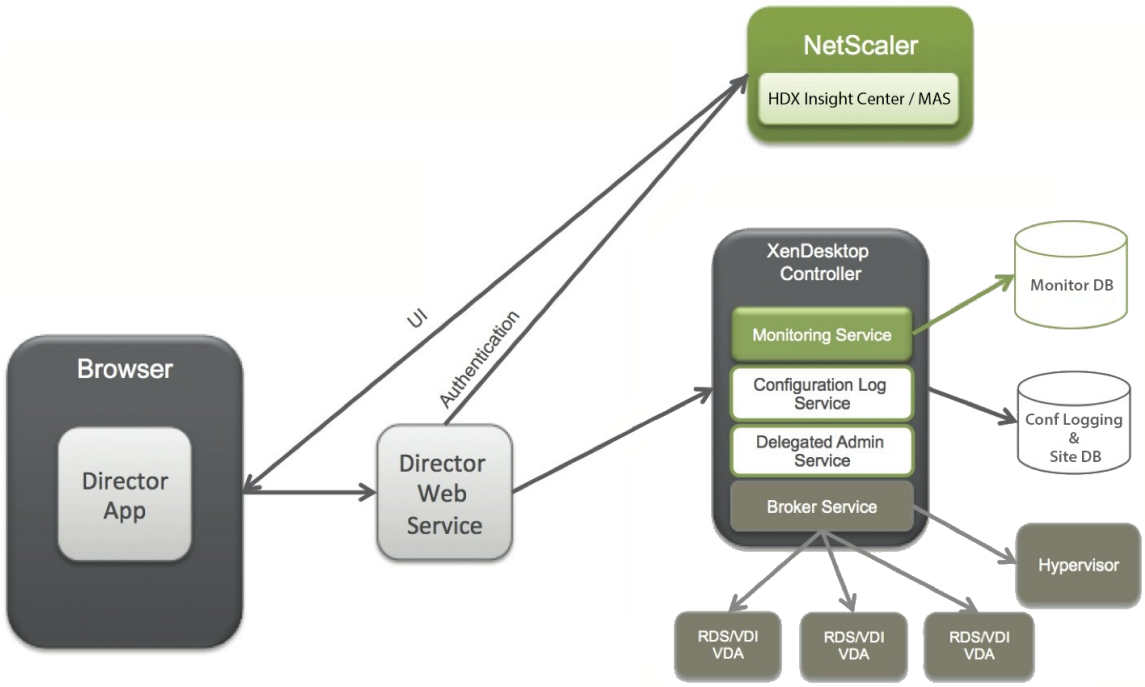
Événements Citrix Delegated Administration Service (HTML)

Director

November 13, 2018

À propos de Director

Director est une console de surveillance et de résolution des problèmes pour XenApp et XenDesktop.



Director peut accéder :

- Aux données en temps réel à partir de l'agent Broker à l'aide d'une console unifiée, intégrée à Analytics, Performance Manager et Network Inspector.
  - Analytics est une solution de gestion des performances permettant d'assurer l'intégrité et la capacité à monter en charge qui offre des tendances historiques et une analyse réseau ; elle est optimisée par NetScaler Insight Center ou NetScaler MAS pour identifier les goulots d'étranglement dus au réseau dans votre environnement XenApp ou XenDesktop.
- Aux données d'historiques stockées dans la base de données Monitor pour accéder à la base de données de journalisation de la configuration.
- Aux données ICA provenant de NetScaler Gateway à l'aide de NetScaler Insight Center ou NetScaler MAS.
  - À la visibilité du gain dans l'expérience des utilisateurs pour les applications et les bureaux virtuels, et les utilisateurs pour XenApp ou XenDesktop.
  - Effectuez une corrélation des données réseau avec les données d'application et les mesures en temps réel pour une résolution des problèmes effective.
  - Intégration à l'outil d'analyse XenDesktop 7 Director.
- Les données Personal vDisk qui offrent une surveillance au moment de l'exécution des données affichent une allocation de base et donnent aux administrateurs du bureau d'assistance la possibilité de réinitialiser le Personal vDisk (pour n'être utilisé qu'en dernier recours).
  - L'outil de ligne de commande de CtxPvdDiag.exe est utilisé pour collecter les informations de journalisation dans un fichier pour la résolution des problèmes.

Director utilise un tableau de bord de résolution des problèmes qui offre un contrôle d'intégrité en

temps réel et historique du site XenApp ou XenDesktop. Cette fonctionnalité vous permet d'afficher les défaillances en temps réel, ce qui permet de vous faire une meilleure idée des problèmes rencontrés par les utilisateurs.

Pour plus d'informations sur la compatibilité des fonctionnalités de Director avec les Delivery Controller (DC), les VDA et tout autre composant dépendant, consultez la section Tableau de compatibilité des fonctionnalités.

Vues de l'interface

Director offre différentes vues de l'interface adaptées aux administrateurs particuliers. Les permissions du produit déterminent ce qui est affiché et les commandes disponibles.

Par exemple, les administrateurs du bureau d'assistance voient une interface adaptée aux tâches du personnel d'assistance technique. Director permet aux administrateurs du bureau d'assistance de rechercher l'utilisateur signalant un problème et afficher les activités associées à cet utilisateur, tels que l'état des applications et des processus de l'utilisateur. Ils peuvent résoudre des problèmes rapidement en effectuant des actions telles que la fermeture d'une application ou d'un processus qui ne répond pas, l'observation d'opérations sur la machine de l'utilisateur, le redémarrage de la machine ou la réinitialisation du profil utilisateur.

Inversement, les administrateurs complets peuvent voir et gérer l'ensemble du site et peuvent réaliser des commandes pour plusieurs utilisateurs et machines. Le tableau de bord fournit une vue d'ensemble des aspects clés d'un déploiement, tel que l'état des sessions, les ouvertures de session des utilisateurs et l'infrastructure d'un site. Les informations sont mises à jour toutes les minutes. Si des problèmes surviennent, des détails apparaissent automatiquement sur le nombre et le type d'échec.

Déployer et configurer Director

Director est installé par défaut en tant que site Web sur le Delivery Controller. Pour les composants pré-requis et d'autres détails, consultez la documentation relative à la configuration système requise pour cette version.

Cette version de Director n'est pas compatible avec les déploiements XenApp antérieurs à la version 6.5 ou les déploiements XenDesktop antérieurs à la version 7.

Lorsque Director est utilisé dans un environnement contenant plus d'un site, assurez-vous de synchroniser les horloges du système sur tous les serveurs sur lesquels les Controller, Director et autres composants principaux sont installés. Sinon, il se peut que les sites ne s'affichent pas correctement dans Director.

Conseil : si vous souhaitez surveiller les sites XenApp 6.5 en plus des sites XenApp 7.5 ou XenDesktop 7.x, Citrix vous recommande d'installer Director sur un autre serveur que celui qui est utilisé par la console Director pour surveiller les sites XenApp 6.5.

Important : pour protéger la sécurité des noms d'utilisateur et des mots de passe envoyés en texte brut via le réseau, Citrix recommande vivement d'autoriser les connexions Director utilisant uniquement HTTPS, et non pas HTTP. Certains outils peuvent lire le texte brut des noms d'utilisateur et des mots de passe dans des paquets réseau HTTP (non cryptés), ce qui peut créer un risque de sécurité pour les utilisateurs.

Pour configurer des autorisations

Pour ouvrir une session sur Director, les administrateurs disposant de permissions pour Director doivent être des utilisateurs de domaine Active Directory et disposer des droits suivants :

- Droits de lecture dans toutes les forêts Active Directory à parcourir (voir Configuration avancée).
- Les rôles d'administrateur délégué configuré (voir Administration déléguée et Director).
- Pour observer les utilisateurs, les administrateurs doivent être configurés à l'aide d'une stratégie de groupe Microsoft pour l'Assistance à distance Windows. De plus :
  - Lors de l'installation de VDA, assurez-vous que la fonction Assistance à distance de Windows est activée sur toutes les machines utilisateur (sélectionnée par défaut).
  - Lorsque vous installez Director sur un serveur, assurez-vous que l'Assistance à distance est installée (sélectionnée par défaut). Toutefois, elle est désactivée sur le serveur par défaut. La fonction ne doit pas être activée pour Director pour obtenir de l'aide auprès des utilisateurs. Citrix vous recommande de laisser la fonctionnalité désactivée pour améliorer la sécurité sur le serveur.
  - Pour permettre aux administrateurs d'initier l'assistance à distance Windows, vous devez leur attribuer les permissions nécessaires à l'aide des paramètres de stratégie de groupe Microsoft correspondants pour l'assistance à distance. Pour plus d'informations, reportez-vous à l'article CTX127388 : How to Enable Remote Assistance for Desktop Director (Comment activer l'assistance à distance pour Desktop Director).
- Pour les machines utilisateur avec VDA antérieure à 7.0, une configuration supplémentaire est requise. Voir Configurer les permissions pour VDA antérieurs à XenDesktop 7.

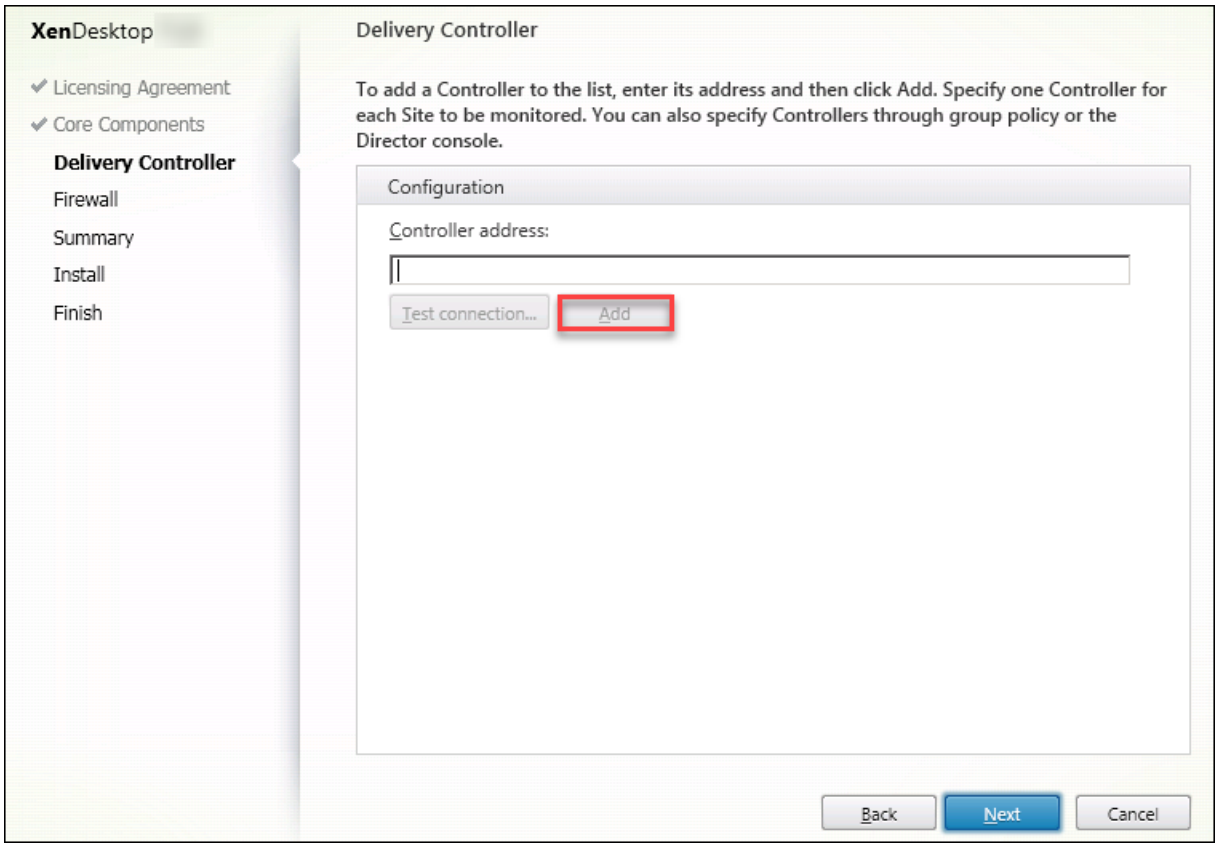
Installer Director

Installez Director à l'aide du programme d'installation ISO du produit complet pour XenApp et Desktop, qui vérifie la présence de composants pré-requis, installe les composants manquants, configure le site Web Director et effectue la configuration de base. La configuration par défaut fournie par le programme d'installation ISO convient aux déploiements classiques. Si Director n'a pas été inclus au

cours de l'installation, utilisez le programme d'installation ISO pour ajouter Director. Pour ajouter des composants supplémentaires, réexécutez le programme d'installation ISO et sélectionnez les composants à installer. Pour plus d'informations sur l'utilisation du programme d'installation ISO, consultez Installer les composants principaux dans la documentation relative à l'installation. Citrix vous recommande d'effectuer l'installation à l'aide du programme d'installation ISO du produit uniquement, et non pas le fichier MSI.

Lorsque Director est installé sur le Controller, il est automatiquement configuré avec localhost comme adresse de serveur, et Director communique avec le Controller local par défaut.

Pour installer Director sur un serveur dédié qui est distant par rapport à un Controller, vous êtes invité à entrer l'adresse FQDN ou IP d'un Controller.



Remarque : cliquez sur **Ajouter** pour ajouter le Controller à surveiller.

Par défaut, Director communique avec ce Controller spécifié. Spécifiez une seule adresse de Controller pour chaque site que vous surveillez. Director découvre automatiquement tous les autres Controller du même site et retourne vers ces Controller en cas d'échec du Controller spécifié.

Remarque : Director n'équilibre pas les charges entre les Controller.

Pour sécuriser les communications entre le navigateur et le serveur Web, Citrix recommande de mettre en œuvre TLS sur le site Web IIS qui héberge Director. Pour plus d'informations, reportez-vous à la documentation de Microsoft IIS. La configuration Director n'est pas requise pour activer TLS.

Installer Director pour XenApp 6.5

Pour installer Director pour XenApp 6.5, procédez comme suit : En général, Director est installé sur un ordinateur autre que celui utilisé pour les Controller XenApp.

1. Installez Director à partir du support d'installation de XenApp. Si Director est déjà installé pour XenDesktop, ignorez cette étape et passez à l'étape suivante.
2. Utilisez la console Gestionnaire des services Internet (IIS) sur chaque serveur Director pour mettre à jour la liste des adresses de serveur XenApp dans les paramètres de l'application comme indiqué dans la section **Pour ajouter des sites à Director** dans Configuration avancée. Vous devez fournir l'adresse de serveur d'un Controller par site XenApp : les autres Controller du site XenApp sont alors utilisés automatiquement en cas de basculement. Director n'équilibre pas les charges entre les Controller.
   Important : pour les adresses XenApp, pensez à bien utiliser le paramètre Service.AutoDiscoveryAddressesXA et non le paramètre par défaut Service.AutoDiscoveryAddresses.
3. Le programme d'installation du fournisseur WMI de Director se trouve dans le dossier **Support\DirectorWMIProvider** sur le DVD. Installez-le sur tous les serveurs XenApp appropriés (Controller et travailleurs sur lesquels les sessions sont en cours d'exécution).
   Si **winrm** n'est pas configuré, exécutez la commande **winrm qc**.
4. Configurez chaque serveur de tâches XenApp pour accepter les requêtes WinRM comme indiqué dans la rubrique Configurer des autorisations.
5. Configurez une exception de pare-feu pour le port 2513, utilisé pour la communication entre Director et XenApp.
6. Pour sécuriser les communications entre le navigateur et le serveur Web, Citrix recommande de mettre en œuvre TLS sur le site Web IIS qui héberge Director.
   Pour plus d'informations, reportez-vous à la documentation de Microsoft IIS. Pour activer TLS, aucune configuration n'est requise dans Director.

Remarque : pour autoriser Director à localiser toutes les tâches XenApp dans la batterie, vous devez ajouter une zone DNS inversée pour les sous-réseaux dans lesquels les serveurs XenApp résident sur les serveurs DNS utilisés par la batterie de serveurs.

Ouvrir une session sur Director

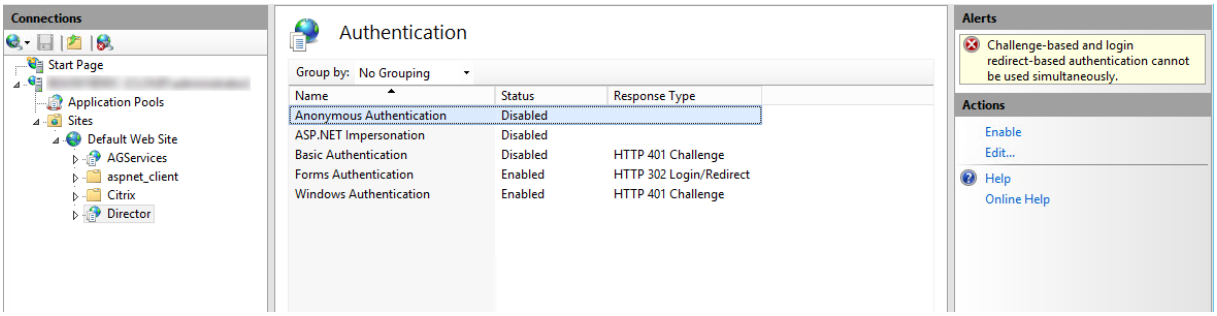
Le site Web Director se trouve à l'adresse https ou `http://<ServerFQDN>/Director`.

Si l'un des sites d'un déploiement multisite est arrêté, l'ouverture de session pour Director nécessite un peu plus de temps lorsqu'il tente de se connecter au site qui est arrêté.

Utiliser Director avec l'authentification Windows intégrée

Avec l'authentification Windows intégrée, les utilisateurs appartenant à un domaine disposent d'un accès direct à Director sans avoir à saisir de nouveau leurs informations d'identification dans la page d'ouverture de session Director. Configuration requise pour l'utilisation de l'authentification Windows intégrée et de Director :

- Activez l'authentification Windows intégrée sur le site Web IIS qui héberge Director. Lorsque vous installez Director, l'authentification anonyme et l'authentification par formulaire sont activées. Pour utiliser l'authentification Windows intégrée et Director, désactivez l'authentification anonyme et activez l'authentification Windows. L'authentification par formulaire doit rester activée pour l'authentification des utilisateurs sans domaine.
  1. Démarrez le gestionnaire IIS.
  2. Accédez à **Sites** > **Site Web par défaut** > **Director**.
  3. Sélectionnez **Authentification**.
  4. Cliquez avec le bouton droit sur **Authentification Anonyme** et sélectionnez **Désactiver**.
  5. Cliquez avec le bouton droit sur **Authentification Windows** et sélectionnez **Activer**.



- Configurez l'autorisation de délégation Active Directory pour la machine Director. Cette étape est requise uniquement si Director et le Delivery Controller sont installés sur des machines distinctes.
  1. Sur la machine Active Directory, ouvrez la console de gestion Active Directory.
  2. Dans la console de gestion Active Directory, accédez à **Nom de domaine** > **Ordinateurs**. Sélectionnez la machine Director.
  3. Cliquez avec le bouton droit et sélectionnez **Propriétés**.
  4. Dans Propriétés, sélectionnez l'onglet **Délégation**.
  5. Sélectionnez l'option **Approuver cet ordinateur pour la délégation à tous les services (Kerberos uniquement)**.
- Le navigateur qui est utilisé pour accéder à Director doit prendre en charge l'authentification Windows intégrée. Cela peut nécessiter des étapes de configuration supplémentaires dans Firefox et Chrome. Pour plus d'informations, reportez-vous à la documentation relative au navigateur.
- Le service de surveillance Monitoring Service doit exécuter Microsoft .NET Framework 4.5.1 ou

une version ultérieure prise en charge répertoriée dans la section Configuration système requise pour Director. Pour plus d'informations, veuillez consulter la section Configuration système requise.

Lorsqu'un utilisateur ferme sa session sur Director ou à l'expiration de la session, la page d'ouverture de session s'affiche. À partir de la page de connexion, l'utilisateur peut définir le type d'authentification sur **Ouverture de session automatique** ou **Informations d'identification utilisateur**.

Collecte de données d'utilisation par Google Analytics
Le Service Director utilise Google Analytics pour collecter anonymement des données d'utilisation après l'installation de Director. Des statistiques et des informations sur l'utilisation de la page Tendances et de ses onglets sont collectées. La collecte des données est activée par défaut lors de l'installation Director.
Pour désactiver la collecte de données Google Analytics, modifiez la clé de Registre HKEY_LOCAL_MACHINE\Softwa sur la machine où Director est installé, comme décrit dans la section Installer et mettre à niveau les outils d'analyse de Citrix Insight Services.

Remarque : la clé de Registre HKEY_LOCAL_MACHINE\Software\Citrix\MetaInstall contrôle la collecte de données d'utilisation par Citrix Insight Services ainsi que Google Analytics. Toute modification de la valeur de la clé affecte la collecte par les deux services.

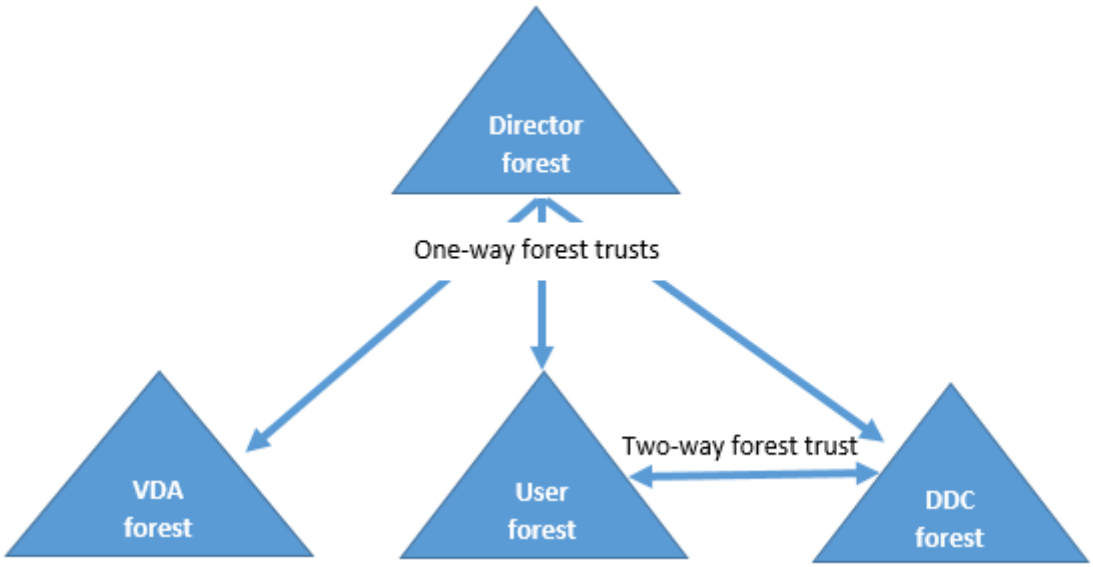
Configuration avancée

November 13, 2018

Director peut prendre en charge les environnements multi-forêts multiples dans lesquels les utilisateurs, les Domain Delivery Controller (DDC), les VDA et les Director se trouvent dans différentes forêts. Cela nécessite une configuration appropriée de relations d'approbation parmi les forêts et paramètres de configuration.

Configuration recommandée pour Director pour qu'il fonctionne dans un environnement multi-forêts

Il est recommandé de configurer des relations d'approbation de forêts bilatérales parmi les forêts avec authentification à l'échelle du domaine.



La relation d'approbation à partir de la console Director vous permet de résoudre les problèmes dans les sessions utilisateur, les VDA et les contrôleurs de domaine situés dans des forêts différentes.

La configuration avancée requise pour Director pour la prise en charge de plusieurs forêts est contrôlée au travers de paramètres définis dans le Gestionnaire des services Internet (IIS).

Important : lorsque vous modifiez un paramètre dans les services IIS, le service Director redémarre automatiquement et ferme la session des utilisateurs.

Pour configurer les paramètres avancés à l'aide des services IIS :

1. Ouvrez la console du Gestionnaire des services Internet Information Services (IIS).
2. Accédez au site Web Director sous le site Web par défaut.
3. Cliquez deux fois sur **Paramètres d'application**.
4. Cliquez deux fois sur un paramètre pour le modifier.

Director utilise Active Directory pour rechercher des utilisateurs et accéder à des informations supplémentaires sur ces utilisateurs ou leur machine. Par défaut, Director recherche le domaine ou la forêt dans lequel ou laquelle :

- le compte d'administrateur est membre ;
- le serveur Web Director est membre (si différent).

Director tente d'effectuer des recherches au niveau de la forêt à l'aide du catalogue global Active Directory. Si vous ne disposez pas de permissions vous permettant d'effectuer des recherches au niveau de la forêt, la recherche porte uniquement sur le domaine.

Pour rechercher des données dans un domaine ou une forêt Active Directory distincts, vous devez spécifier explicitement les domaines ou les forêts à parcourir. Configurez le paramètre suivant :

```
Connector.ActiveDirectory.Domains = (utilisateur),(serveur)
```


La valeur des attributs utilisateur et serveur représentent les domaines de l'utilisateur Director (l'administrateur) et du serveur Director respectivement.

Pour autoriser les recherches dans un autre domaine ou une autre forêt, ajoutez le nom du domaine à la liste comme indiqué dans l'exemple suivant :

```
Connector.ActiveDirectory.Domains = (utilisateur),(serveur),\<domaine1
    \>,\<domaine2\> |
```

Pour chaque domaine de la liste, Director tente d'effectuer des recherches au niveau de la forêt. Si vous ne disposez pas de permissions vous permettant d'effectuer des recherches au niveau de la forêt, la recherche porte uniquement sur le domaine.

Remarque : dans un environnement comportant plusieurs forêts, Director n'affiche pas les détails de sessions des utilisateurs d'autres forêts qui ont été attribués au groupe de mise à disposition XenDesktop à l'aide du groupe local de domaine.

Ajouter des sites à Director

Si Director est déjà installé, configurez-le pour qu'il fonctionne avec plusieurs sites. Pour ce faire, utilisez la console Gestionnaire des services Internet (IIS) sur chaque serveur Director pour mettre à jour la liste des adresses de serveurs dans les paramètres de l'application.

Ajoutez l'adresse d'un Controller pour chaque site au paramètre suivant :

```
Service.AutoDiscoveryAddresses = SiteAController,SiteBController
```

où *SiteAController* et *SiteBController* correspondent aux adresses Delivery Controllers de deux sites différents.

Pour les sites XenApp 6.5, ajoutez l'adresse d'un Controller pour chaque batterie XenApp au paramètre suivant :

```
Service.AutoDiscoveryAddressesXA = FarmAController,FarmBController
```

où *FarmAController* et *FarmBController* correspondent aux adresses des Controller XenApp de deux batteries différentes.

Pour les sites XenApp 6.5, il existe une autre méthode pour ajouter un Controller à une batterie XenApp :

```
DirectorConfig.exe /xenapp FarmControllerName
```


Désactiver la visibilité des applications en cours d'exécution dans le Gestionnaire d'activités

Par défaut, le Gestionnaire d'activité de Director affiche une liste de toutes les applications en cours d'exécution pour la session d'un utilisateur. Ces informations peuvent être consultées par les administrateurs qui ont accès à la fonctionnalité Gestionnaire d'activité de Director. Pour les rôles d'administrateur délégué, ceci comprend l'administrateur complet, l'administrateur du groupe de mise à disposition et l'administrateur du bureau d'assistance.

Pour protéger la confidentialité des utilisateurs et les applications qu'ils sont en cours d'exécution, vous pouvez désactiver l'onglet Applications afin qu'il arrête de répertorier les applications en cours d'exécution.

Avertissement : la modification incorrecte du Registre peut entraîner des problèmes graves pouvant nécessiter la réinstallation de votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

1. Sur le VDA, modifiez la clé de registre située à l'adresse HKEY_LOCAL_MACHINE\Software\Citrix\Director\Task
   Par défaut, la clé est définie sur 1. Modifiez la valeur sur 0, ce qui signifie que les informations ne sont pas collectées depuis le VDA et par conséquent ne sont pas affichées dans le Gestionnaire d'activités.
2. Sur le serveur sur lequel Director est installé, modifiez le paramètre qui contrôle la visibilité des applications en cours d'exécution. Par défaut, la valeur est true, ce qui permet de voir les applications en cours d'exécution dans l'onglet Applications. Modifiez la valeur sur false, ce qui désactive cette visibilité. Cette option affecte uniquement le gestionnaire d'activité dans Director et non le VDA.

   Modifiez la valeur du paramètre suivant :

   ```
   1 UI.TaskManager.EnableApplications = false
   ```

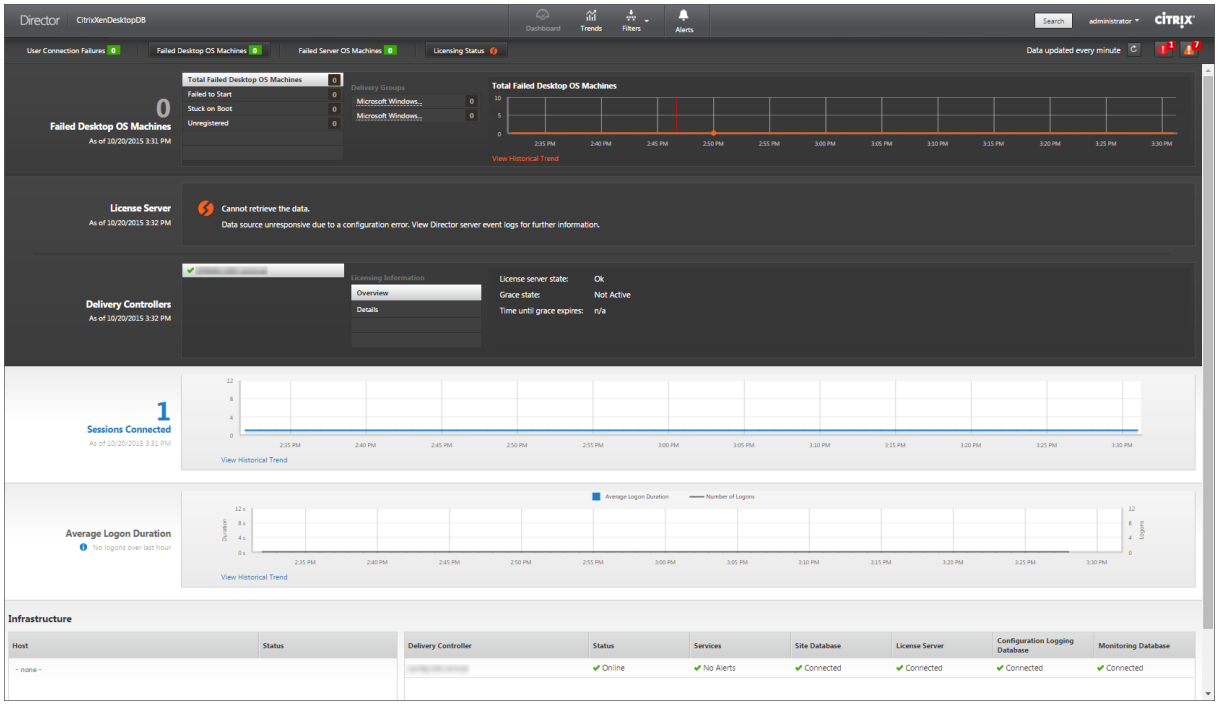
Important : pour désactiver l'affichage des applications en cours d'exécution, Citrix vous recommande d'effectuer ces modifications pour vous assurer que les données ne sont pas affichées dans le Gestionnaire d'activités.

Surveiller les déploiements

February 28, 2019

Surveiller les sites

Avec une permission d'administrateur complet, lorsque vous ouvrez Director, le Tableau de bord fournit un emplacement centralisé permettant de surveiller l'intégrité et l'utilisation d'un site.



S'il n'existe actuellement aucune erreur et qu'aucune erreur ne s'est produite au cours des dernières 60 minutes, les panneaux ne s'affichent pas. Lorsqu'il existe des erreurs, le panneau d'échec spécifique s'affiche automatiquement.

Remarque : en fonction des licences de votre organisation et des privilèges de l'administrateur, certaines options ou fonctionnalités risquent de ne pas être disponibles.

Panneau	Description
Échecs de connexion utilisateur	Échecs de connexion lors des dernières 60 minutes. Cliquez sur les catégories situées en regard du nombre total pour afficher les métriques pour ce type d'échec. Dans la table suivante, ce nombre est réparti par groupe de mise à disposition. Échecs de connexion inclut les erreurs causées par les limites d'application qui sont atteintes. Pour de plus amples informations sur les limites d'application, consultez la section Applications.

Panneau	Description
Machines avec OS de bureau en échec ou Machines avec OS de serveur en échec	Nombre total d'échecs dans les dernières 60 minutes réparties par groupes de mise à disposition. Échecs répartis par types, y compris les échecs de démarrage, bloqués au démarrage, et non enregistrés. Pour les machines avec OS de serveur, les erreurs comprennent également le moment où les machines atteignent une charge maximale.
Statut de la licence	Les alertes du serveur de licences affichent des alertes envoyées par le serveur de licences et les actions requises pour la résolution des alertes. Requiert le serveur de licences 11.12.1 ou version ultérieure. Les alertes Delivery Controller affichent les détails de l'état des licences comme elles sont vues par le Controller et sont envoyées par le Controller. Requiert un Controller pour XenApp 7.6 ou XenDesktop 7.6 ou version ultérieure. Vous pouvez définir le seuil des alertes dans Studio.
Session(s) connectée(s)	Sessions connectées sur tous les groupes de mise à disposition pour les dernières 60 minutes.
Durée moyenne de l'ouverture de session	Données d'ouverture de session pour les dernières 60 minutes. Le nombre important sur la gauche est la durée moyenne d'ouverture de session sur l'heure en cours. Les données d'ouverture de session pour les VDA antérieurs à XenDesktop 7.0 ne sont pas incluses dans cette moyenne. Pour de plus amples informations, consultez la section Diagnostiquer les problèmes de connexion utilisateur.

Panneau	Description
Infrastructure.	Dresse la liste de l'infrastructure de votre site – hôtes et Controller. Pour l'infrastructure de XenServer ou VMware, vous pouvez afficher les alertes de performance. Par exemple, vous pouvez configurer XenCenter pour générer des alertes de performances lorsque l'utilisation de l'UC, E/S réseau ou E/S disque dépasse un seuil spécifié sur un serveur ou une machine virtuelle géré(e). Par défaut, l'intervalle de répétition d'alerte est de 60 minutes, mais vous pouvez le configurer. Pour de plus amples informations, accédez à XenServer version actuelle ; consultez la section XenCenter Performance Alerts dans le Guide de l'administrateur de Citrix XenServer (en anglais).

Remarque : l'absence d'icône pour une mesure donnée indique que cette mesure n'est pas prise en charge par le type de l'hôte utilisé. Par exemple, aucune information d'intégrité n'est disponible pour les hôtes System Center Virtual Machine Manager (SCVMM), AWS et CloudStack.

Continuez à résoudre les problèmes à l'aide de ces options (qui sont répertoriées ci-dessous) :

- Contrôler l'alimentation de la machine utilisateur
- Empêcher les connexions aux machines

Contrôler des sessions

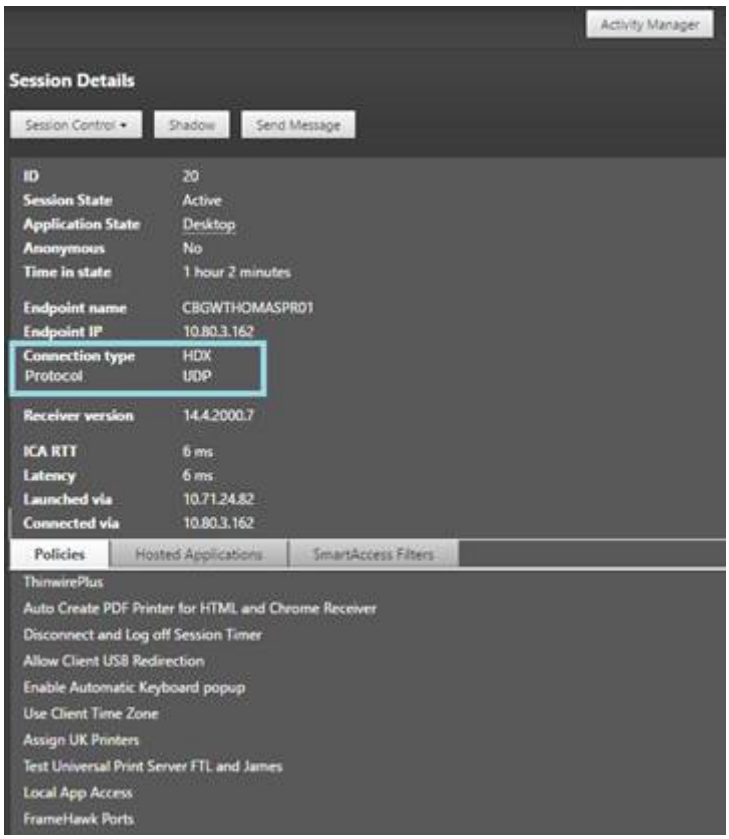
Si une session devient déconnectée, elle reste active et ses applications continuent d'être exécutées, mais la machine cliente ne communique plus avec le serveur.

Action	Description
Afficher la machine ou la session actuellement connectée de l'utilisateur	À partir des vues Gestionnaire d'activités et Détails de l'utilisateur, affichez la machine ou la session actuellement connectée de l'utilisateur et une liste de toutes les machines et des sessions auxquelles cet utilisateur a accès. Pour accéder à cette liste, cliquez sur l'icône de sélection de session dans la barre de titre utilisateur. Pour plus d'informations, consultez la section Restaurer les sessions.
Afficher le nombre total de sessions déconnectées sur tous les groupes de mise à disposition	Dans le tableau de bord, dans le volet Sessions connectées, affichez le nombre total de sessions connectées sur tous les groupes de mise à disposition pendant les 60 dernières minutes. Puis cliquez sur le nombre total, qui ouvre la vue Filtres, où vous pouvez afficher les données de session graphiques basées sur les groupes de mise à disposition sélectionnés et les plages et l'utilisation au travers des groupes de mise à disposition.[](/fr-fr/xenapp-and-xendesktop/7-15-ltsr/director/troubleshooting-applications.html)
Mettre fin aux sessions inactives	La vue Filtres de session affiche des données relatives à toutes les sessions actives. Filtrez les sessions en fonction de l'utilisateur associé, du groupe de mise à disposition, de l'état de la session et du temps d'inactivité supérieur à un seuil spécifié. Dans la liste filtrée, sélectionnez les sessions à fermer. Pour obtenir davantage d'informations, veuillez consulter la section [Résolution des problèmes d'applications].(/fr-fr/xenapp-and-xendesktop/7-15-ltsr/director/troubleshooting-applications.html)

Action	Description
Afficher les données sur une période plus longue	Dans la vue Tendances, sélectionnez l'onglet Sessions pour afficher des données d'utilisation plus spécifiques pour les sessions connectées et déconnectées sur une période de temps plus longue (nombre total de sessions antérieur aux 60 dernières minutes). Pour afficher ces informations, cliquez sur **Afficher les tendances historiques**.

Remarque : si la machine utilisateur exécute un Virtual Delivery Agent (VDA) d'ancienne génération, telle qu'un VDA antérieur à la version 7 ou un Linux VDA, Director ne peut pas afficher d'informations complètes sur la session. Un message s'affiche indiquant que les informations ne sont pas disponibles.

Affichez le protocole de transport utilisé pour le type de connexion HDX associé à la session en cours dans le panneau Détails de session. Ces informations sont disponibles pour les sessions lancées sur des VDA 7.13 ou version ultérieure.



- Pour le type de connexion **HDX** :

  - Le protocole affiché est **UDP**, si EDT est utilisé pour la connexion HDX.
  - Le protocole affiché est **TCP**, si TCP est utilisé pour la connexion HDX.
- Pour le type de connexion **RDP**, le protocole affiché est **S.O.**.

Lorsque le transport adaptatif est configuré, le protocole de transport de la session bascule dynamiquement entre EDT (via UDP) et TCP, selon les conditions de réseau. Si la session HDX ne peut pas être établie à l'aide d'EDT, elle utilise le protocole TCP.

Pour plus d'informations sur la configuration du transport adaptatif, consultez la section Transport adaptatif.

Filtrer les données pour résoudre les échecs

Lorsque vous cliquez sur des nombres sur le tableau de bord ou que vous sélectionnez un filtre pré défini depuis le menu Filtres, la vue Filtres s'ouvre pour afficher les données basées sur la machine sélectionnée ou le type d'échec.

Les filtres prédéfinis ne peuvent être modifiés, mais vous pouvez enregistrer un filtre pré défini en tant que filtre personnalisé puis le modifier. De plus, vous pouvez créer des vues de filtres personnalisés de machines, de connexions, de sessions et d'instances d'applications sur tous les groupes de mise à disposition.

1. Sélectionner une vue :
   - **Machines**. Sélectionnez des machines avec OS de bureau ou des machines avec OS de serveur. Ces vues illustrent le nombre de machines configurées. L'onglet Machines avec OS de serveur comprend également l'index de calculateur de charge, qui indique la distribution des compteurs de performances et les info-bulles du nombre de sessions si vous survolez le lien avec la souris.
   - **Sessions**. Vous pouvez également afficher le nombre de sessions depuis la vue Sessions. Utilisez les mesures de délai d'inactivité pour identifier les sessions qui restent inactives au-delà d'une période de temps donnée.
   - **Connexions**. Filtrez les connexions par différentes périodes de temps, y compris les 60 dernières minutes, les dernières 24 heures ou les derniers 7 jours.
   - **Instances d'application**. Cette vue affiche les propriétés de toutes les instances d'application sur les VDA d'OS de serveur et de bureau. Les mesures de délai d'inactivité de session sont disponibles pour les instances d'application sur les VDA d'OS de serveur.
2. Pour **Filtrer par**, sélectionnez le critère.
3. Utilisez les onglets supplémentaires pour chaque vue, selon vos besoins, pour terminer le filtre.
4. Sélectionnez des colonnes supplémentaires, selon vos besoins, pour résoudre plus de problèmes.
5. Enregistrez votre filtre et attribuez-lui un nom.

6. Pour accéder aux filtres de plusieurs serveurs Director, stockez les filtres sur un dossier partagé accessible à partir de ces serveurs :
   - Le dossier partagé doit avoir des autorisations Modifier pour les comptes sur le serveur Director.
   - Les serveurs Director doivent être configurés pour accéder au dossier partagé. Pour ce faire, exécutez **Gestionnaire des services Internet**. Dans **Sites > Site Web par défaut > Director> Paramètres de l'application**, modifiez le paramètre **Service.UserSettingsPath** pour qu'il reflète le chemin d'accès UNC du dossier partagé.
7. Pour ouvrir le filtre plus tard, depuis le menu Filtres, sélectionnez le type de filtre (Machines, Sessions, Connexions ou Instances d'application), puis sélectionnez le filtre enregistré.
8. Si nécessaire, pour les vues **Machines** ou **Connexions**, utilisez les commandes de puissance pour toutes les machines que vous sélectionnez dans la liste filtrée. Pour la vue Sessions, utilisez les commandes ou l'option de session pour envoyer des messages.
9. Dans les vues **Machines** et **Connexions**, cliquez sur **Raison de l'échec** pour une machine ou une connexion en échec afin d'obtenir une description détaillée de l'échec et des actions recommandées pour résoudre le problème. Les raisons de l'échec et les actions recommandées pour des défaillances de machines et de connexion sont disponibles dans le Citrix Director 7.12 Failure Reasons Troubleshooting Guide.
10. Dans la vue **Machines**, cliquez sur le lien du nom d'une machine pour accéder à la page **Détails de la machine** correspondante. Cette page affiche les détails de la machine, fournit des contrôles de l'alimentation, affiche les graphiques de CPU, de mémoire, de surveillance des disques et de surveillance des GPU. Cliquez aussi sur **Afficher utilisation historique** pour afficher les tendances d'utilisation des ressources pour la machine. Pour obtenir davantage d'informations, veuillez consulter la section Dépanner les machines.
11. Dans la vue **Instances d'application**, triez ou filtrez en fonction d'un **temps d'inactivité** supérieur à une période de temps donnée. Sélectionnez les instances d'application inactives à fermer. La fin de session ou la déconnexion d'une instance d'application met fin à toutes les instances de l'application actives dans la même session. Pour obtenir davantage d'informations, veuillez consulter la section Résolution des problèmes d'applications.

    Remarque : la page de filtre des instances d'application et les mesures de délai d'inactivité dans les pages de filtre des sessions sont disponibles si Director, les Delivery Controller et les VDA sont à la version 7.13 ou ultérieure.

Contrôler les tendances historiques sur un site

La vue Tendances accède aux informations de tendances d'historique pour les sessions, les échecs de connexion, les échecs de machines, les performances d'ouverture de session, l'évaluation de charge, la gestion de la capacité, l'utilisation de la machine, l'utilisation des ressources et l'analyse du réseau pour chaque site. Pour trouver ces informations, cliquez sur le menu **Tendances**.

Cette fonctionnalité d'exploration vous permet de naviguer au travers des diagrammes de tendances en effectuant un zoom avant sur une période de temps (en cliquant sur un point de données dans le diagramme) et en effectuant un éclatement pour afficher les détails associés avec la tendance. Elle vous permet de mieux comprendre les détails des personnes ou éléments affecté(e)s par les tendances affichées.

Pour modifier l'étendue par défaut de chaque graphique, appliquez un filtre différent aux données.

Choisissez une période de temps pendant laquelle vous souhaitez utiliser les informations de tendances historiques ; la période de temps disponible dépend de votre déploiement de Director comme suit :

- des rapports de tendance pour l'année écoulée (365 jours) sont disponibles sur les sites sous licence Platinum ;
- des rapports de tendance pour le mois écoulé (31 jours) sont disponibles sur les sites sous licence Enterprise ;
- des rapports de tendance pour la semaine écoulée (7 jours) sont disponibles sur les sites sans licence Platinum et Enterprise.

Remarque :

- Dans tous les déploiements de Director, les informations de tendances Sessions, Échecs et Performances d'ouverture de session sont présentées sous forme de graphiques et de tableaux lorsque la période de temps est définie sur Mois dernier (**se terminant maintenant**) ou une période plus courte. Lorsque la période de temps est définie sur Mois dernier avec une date de fin personnalisée ou Année dernière, les informations de tendance sont disponibles sous forme de graphiques, mais pas de tableaux.
- Les valeurs par défaut de rétention de nettoyage des données de tendances par Monitoring Service sont disponibles dans la section Granularité de données et rétention. Les clients sur sites avec licence Platinum peuvent modifier la rétention de nettoyage sur leur nombre de jours de rétention désirés.

Tendances disponibles

Afficher les tendances des sessions : dans l'onglet Sessions, sélectionnez le groupe de mise à disposition et la période de temps pour afficher des informations plus détaillées sur le nombre de sessions simultanées.

Afficher les tendances pour les échecs de connexion : depuis l'onglet Échecs, sélectionnez la connexion, le type de machine, le type d'échec, le groupe de mise à disposition et la période de temps pour afficher un graphique contenant des informations plus détaillées sur les échecs de connexion utilisateur sur votre site.

Afficher les tendances des échecs de machine : depuis l'onglet Machines avec OS de bureau défectueuses ou Machines avec OS serveur, sélectionnez le type de défaillance, le groupe de mise à disposition et la période de temps pour afficher un graphique contenant des informations plus détaillées sur les échecs de machine sur votre site.

Afficher les tendances pour les performances d'ouverture de session : dans l'onglet Performances d'ouverture de session, sélectionnez le groupe de mise à disposition et la période de temps pour afficher un graphique contenant des informations plus détaillées sur la durée d'ouverture de session de l'utilisateur sur votre site et si le nombre d'ouvertures de session affecte les performances. Cette vue affiche également la durée moyenne des phases d'ouverture de session, telles que la durée de la négociation et la durée de démarrage de la machine virtuelle.
Ces données sont spécifiques aux ouvertures de session des utilisateurs et ne comprennent pas les utilisateurs essayant de se reconnecter à des sessions déconnectées.
Le tableau en dessous du diagramme affiche la Durée de connexion par session utilisateur. Vous pouvez choisir les colonnes à afficher et trier le rapport en fonction de n'importe colonne.
Pour de plus amples informations, consultez la section Diagnostiquer les problèmes de connexion utilisateur.

Afficher les tendances pour l'évaluation de charge : dans l'onglet Index de calculateur de charge, affichez un graphique contenant des informations plus détaillées sur la charge distribuée entre les machines avec OS de serveur. Les options de filtre de ce graphique incluent le groupe de mise à disposition ou la machine avec OS de serveur dans un groupe de mise à disposition, la machine avec OS de serveur (disponible uniquement si la machine avec OS de serveur d'un groupe de mise à disposition a été sélectionnée), et la plage.

Afficher l'utilisation des applications hébergées : la disponibilité de cette fonctionnalité dépend de la licence de votre organisation.
À partir de l'onglet Gestion de la capacité, sélectionnez l'onglet Utilisation des applications hébergées, sélectionnez le groupe de mise à disposition et la période de temps pour visualiser un graphique affichant la période d'utilisation simultanée maximale et une table affichant l'utilisation de l'application. À partir de la table affichant l'utilisation de l'application, vous pouvez choisir une application spécifique pour voir les détails et une liste des utilisateurs qui utilisent, ou ont utilisé l'application.

Afficher l'utilisation des OS de bureau et de serveur : la vue Tendances affiche l'utilisation des OS de bureau par site et par groupe de mise à disposition. Lorsque vous sélectionnez Site, l'utilisation est indiquée par groupe de mise à disposition. Lorsque vous sélectionnez Groupe de mise à disposition, l'utilisation est indiquée par utilisateur.
La vue Tendances affiche également l'utilisation des OS de serveur par site, par groupe de mise à disposition et par machine. Lorsque vous sélectionnez Site, l'utilisation est indiquée par groupe de mise à disposition. Lorsque vous sélectionnez Groupe de mise à disposition, l'utilisation est indiquée par machine et par utilisateur. Lorsque Machine est sélectionné, l'utilisation est indiquée par utilisateur.

Afficher l'utilisation de machine virtuelle : à partir de l'onglet Utilisation de machine, sélectionnez Machines avec OS de bureau ou Machines avec OS de serveur pour obtenir une vue en temps réel de votre utilisation des machines virtuelles, ce qui vous permet d'évaluer rapidement les besoins en capacité de votre site.
Disponibilité d'OS de bureau : affiche l'état actuel des machines avec OS de bureau (VDI) par disponibilité pour la totalité du site ou un groupe de mise à disposition spécifique.
Disponibilité d'OS de serveur : affiche l'état actuel des machines avec OS de serveur par disponibilité pour la totalité du site ou un groupe de mise à disposition spécifique.

Afficher l'utilisation des ressources : à partir de l'onglet Utilisation des ressources, sélectionnez Machines avec OS de bureau ou Machines avec OS de serveur pour afficher les tendances historiques d'utilisation d'UC et de mémoire et les données E/S par seconde et latence de disque pour chaque machine VDI afin de mieux planifier les capacités.
Cette fonctionnalité requiert la **version 7.11** ou ultérieure de Delivery Controller et de VDA.
Les graphiques affichent des données d'UC moyenne, de mémoire moyenne, de nombre moyen d'E/S par seconde, de latence de disque et de sessions simultanées maximales. Vous pouvez accéder aux détails de la machine et afficher des données et des graphiques pour les 10 processus consommant le plus d'UC. Filtrez par groupe de mise à disposition et période. Les graphiques pour CPU, utilisation de la mémoire et sessions simultanées maximum sont disponibles pour les 2 dernières heures, les dernières 24 heures, les 7 derniers jours, le dernier mois et la dernière année. Les graphiques de nombre moyen d'E/S par seconde et de latence de disque sont disponibles pour les dernières 24 heures, le dernier mois et la dernière année.

Remarques :

- Le paramètre de stratégie Surveillance, Activer le suivi des processus, doit être défini sur « Autorisé » pour collecter et afficher les données dans le tableau des 10 processus les plus utilisés sur la page Utilisation historique des machines. Par défaut, la stratégie est définie sur « Interdite ». Toutes les données d'utilisation des ressources sont collectées par défaut. Ce comportement peut être désactivé en utilisant le paramètre de stratégie Activer le suivi des ressources. Le tableau sous les graphiques affiche les données d'utilisation des ressources par machine.
- Nbre moyen d'E/S par seconde indique les moyennes quotidiennes. E/S par seconde max. est calculé comme la moyenne la plus élevée d'E/S pour la période sélectionnée. (Le nombre moyen d'E/S par seconde est la moyenne d'E/S par seconde collectée au cours de l'heure sur le VDA).

Afficher les données d'analyse du réseau : la disponibilité de cette fonctionnalité dépend de la licence de votre organisation et vos permissions d'administrateur. Cette fonctionnalité requiert la **version 7.11** ou ultérieure de Delivery Controller.

Dans l'onglet Réseau, surveillez votre analyse réseau, qui fournit une vue contextuelle utilisateur, application et bureau du réseau. Grâce à cette fonctionnalité, Director fournit des analyses avancées du

trafic ICA dans votre déploiement via les rapports HDX Insight de NetScaler Insight Center ou NetScaler MAS. Pour de plus amples informations, consultez la section Configurer l'analyse réseau.

Afficher les échecs applicatifs : l'onglet Échecs applicatifs affiche les échecs associés aux applications publiées sur les VDA.

Cette fonctionnalité requiert la **version 7.15** ou ultérieure de Delivery Controller et de VDA. Les VDA avec OS de bureau exécutant Windows Vista ou version ultérieure, et les VDA avec OS de serveur exécutant Windows Server 2008 et versions ultérieures sont pris en charge.
Pour plus d'informations, consultez la section Détection des défaillances applicatives.

Par défaut, seuls les échecs applicatifs de VDA avec OS de serveur sont détectés. Vous pouvez configurer la détection des échecs applicatifs à l'aide de stratégies de surveillance. Pour plus d'informations, veuillez consulter la section [Paramètres de stratégie Surveillance]. (/fr-fr/xenapp-and-xendesktop/7-15-ltsr/policies/reference/virtual-delivery-agent-policy-settings/monitoring-policy-settings.html)

Créer des rapports personnalisés : l'onglet Rapports personnalisés offre une interface utilisateur pour générer des rapports personnalisés contenant des données en temps réel et des données historiques provenant de la base de données de surveillance sous forme de tableau.

Cette fonctionnalité requiert la **version 7.12** ou ultérieure de Delivery Controller.

À partir de la liste des requêtes de rapport personnalisé enregistrées précédemment, vous pouvez cliquer sur **Exécuter** pour exporter le rapport au format CSV, cliquer sur **Copier OData** pour copier et partager la requête OData correspondante, ou cliquer sur **Modifier** pour modifier la requête.
Vous pouvez créer une requête de rapport personnalisé basée sur les machines, les connexions, les sessions, ou les instances d'application. Spécifiez les conditions de filtrage à l'aide de champs tels que la machine, le groupe de mise à disposition ou la période de temps. Spécifiez les colonnes supplémentaires requises dans votre rapport personnalisé. L'aperçu affiche un exemple des données du rapport. L'enregistrement de la requête de rapport personnalisé l'ajoute à la liste des requêtes enregistrées.

Vous pouvez créer un rapport personnalisé basé sur une requête OData copiée. Pour ce faire, sélectionnez l'option Requête OData et collez la requête OData copiée. Vous pouvez enregistrer la requête résultante pour l'exécuter ultérieurement.

Les icônes de drapeaux sur le graphique indiquent des actions ou événements significatifs pour cette période spécifique. Placez le pointeur sur un drapeau et cliquez pour obtenir la liste des événements ou actions.

Remarques :

- les données d'ouverture de session de la connexion HDX ne sont pas collectées pour les VDA antérieurs à la version 7. Pour les VDA antérieurs, les données du graphique sont affichées en tant que 0.
- Les groupes de mise à disposition supprimés dans Citrix Studio sont disponibles pour sélection dans les filtres de tendances Director jusqu'à ce que les données y afférent soient nettoyées.

La sélection d'un groupe de mise à disposition supprimé affiche des graphiques pour les données disponibles entrant dans le cadre de la période de rétention des données. Toutefois, les tableaux n'affichent aucune donnée.

- Si vous déplacez une machine contenant des sessions actives d'un groupe de mise à disposition à un autre, les tableaux **Utilisation des ressources et Indice de calculateur de charge** du nouveau groupe de mise à disposition affichent les mesures consolidées des anciens et des nouveaux groupes de mise à disposition.

Exporter des rapports

Vous pouvez exporter les données sur les tendances pour générer des rapports d'utilisation et de gestion de la capacité. L'exportation prend en charge les formats de rapport PDF, Excel et CSV. Les rapports aux formats PDF et Excel contiennent les tendances représentées sous la forme de graphiques et de tableaux. Les rapports au format CSV contiennent des données tabulaires pouvant être traitées pour générer des vues ou être archivées.

Pour exporter un rapport :

1. Accédez à l'onglet **Tendances**.
2. Définissez les critères de filtrage et la période, puis cliquez sur **Appliquer**. Le graphique et le tableau des tendances sont renseignés avec les données.
3. Cliquez sur **Exporter** et entrez le nom et le format du rapport.

Director génère le rapport en fonction des critères de filtre que vous avez sélectionnés. Si vous modifiez les critères de filtre, cliquez sur **Appliquer** avant de cliquer sur **Exporter**.

Remarque : l'exportation d'une grande quantité de données entraîne une augmentation significative de la consommation de mémoire et d'UC pour le serveur Director, le Delivery Controller et les serveurs SQL. Le nombre d'opérations d'exportation simultanées et le volume de données qui peuvent être exportées sont définis sur les limites par défaut permettant d'obtenir les meilleures performances d'exportation.

Limites d'exportation prises en charge

Les rapports PDF et Excel exportés contiennent des graphiques complets pour les critères de filtre sélectionnés. Toutefois, les données tabulaires de tous les formats de rapport sont tronquées au-delà des limites par défaut sur le nombre de lignes ou d'enregistrements dans le tableau. Le nombre de données pris en charge par défaut est défini en fonction du format du rapport.

Vous pouvez modifier la valeur par défaut en configurant les paramètres d'application Director dans Internet Information Services (IIS).

Format de rapport	Nombre d'enregistrements pris en charge par défaut	Champs dans les paramètres d'application Director	Nombre maximal d'enregistrements pris en charge
PDF	500	UI.ExportPdfDrilldownL	5000
Excel	100,000	UI.ExportExcelDrilldownLimit	100,000
CSV	100 000 (10 000 000 dans l'onglet Sessions)	UI.ExportCsvDrilldownL	100,000

Pour modifier la limite du nombre d'enregistrements que vous pouvez exporter :

1. Ouvrez la console du gestionnaire IIS.
2. Accédez au site Web Director sous le site Web par défaut.
3. Cliquez deux fois sur **Paramètres d'application**.
4. Modifiez le champ ou ajoutez un nouveau champ.

L'ajout de ces valeurs de champ dans Paramètres d'application remplace les valeurs par défaut.

Avertissement : la définition de valeurs de champ supérieures au nombre maximal d'enregistrements pris en charge peut avoir un impact sur les performances d'exportation et n'est pas prise en charge.

Gestion des erreurs

Cette section explique comment gérer les erreurs que vous pourriez rencontrer lors de l'opération d'exportation.

- **Director a expiré**

Cette erreur peut se produire en raison de problèmes de réseau ou d'utilisation élevée des ressources sur le serveur Director ou par le service de surveillance.

Le délai d'expiration par défaut est de 100 secondes. Pour augmenter le délai d'expiration du service Director, définissez la valeur du champ **Connector.DataServiceContext.Timeout dans** les paramètres d'application Director dans Internet Information Services (IIS) :

1. Ouvrez la console du gestionnaire IIS.
2. Accédez au site Web Director sous le site Web par défaut.
3. Cliquez deux fois sur **Paramètres d'application**.
4. Modifiez la valeur **Connector.DataServiceContext.Timeout**.

- **Le service de surveillance a expiré**

Cette erreur peut se produire en raison de problèmes de réseau ou d'utilisation élevée des ressources sur le serveur SQL ou par le service de surveillance.

Pour augmenter le délai d'expiration du service de surveillance, exécutez les commandes PowerShell suivantes sur le Delivery Controller :

```
asnp Citrix.*
Get-MonitorConfiguration
Set-MonitorConfiguration -MonitorQueryTimeoutSeconds <délai d'
   expiration>
```

- **Opérations d'exportation ou d'aperçu max. simultanées en cours**

Director prend en charge une seule instance d'exportation ou d'aperçu. Si vous recevez une erreur concernant les **opérations d'exportation ou d'aperçu simultanées maximales**, attendez avant d'effectuer la prochaine opération d'exportation.

Il est possible d'augmenter le nombre d'opérations d'exportation ou d'aperçu simultanées, mais cela peut avoir un impact sur les performances de Director et n'est pas prise en charge :

1. Ouvrez la console du gestionnaire IIS.
2. Accédez au site Web Director sous le site Web par défaut.
3. Cliquez deux fois sur **Paramètres d'application**.
4. Modifiez la valeur **UI.ConcurrentExportLimit**.

- **Espace disque insuffisant dans Director**

Chaque opération d'exportation requiert un maximum de 2 Go d'espace disque disponible dans le dossier temporaire de Windows. Réessayez d'exporter après avoir libéré de l'espace ou ajouté de l'espace disque sur le serveur Director.

Contrôler les corrections à chaud

Pour afficher les corrections à chaud installées sur un VDA de machine (physique ou VM) spécifique, choisissez la vue Détails de la machine.

Contrôler les états d'alimentation de la machine utilisateur

Pour contrôler l'état des machines que vous sélectionnez dans Director, utilisez les options de Contrôle de l'alimentation. Ces options sont disponibles pour les machines avec système d'exploitation de bureau, mais pas pour les machines avec système d'exploitation de serveur.

Remarque : cette fonctionnalité n'est pas disponible pour les machines physiques utilisant Remote PC Access.

Commande	Fonction
Redémarrer	Effectue une fermeture (en douceur) ordonnée de la VM, et tous les processus en cours d'exécution sont arrêtés individuellement avant le redémarrage de la VM. Par exemple, sélectionnez les machines qui s'affichent dans Director en tant que « n'a pas réussi à démarrer » et utilisez cette commande pour les redémarrer.
Forcer le redémarrage	Redémarre la VM sans tenter d'effectuer de procédure de fermeture. Cette commande ne fonctionne de la même manière que lorsque vous débranchez un serveur physique puis le rebranchez et le redémarrez à nouveau.
Fermeture	Effectue une fermeture (en douceur) ordonnée de la VM ; tous les processus en cours d'exécution sont arrêtés individuellement.
Forcer la fermeture	Arrête la VM sans effectuer tout d'abord une procédure de fermeture. Cette commande fonctionne de la même manière que lorsque vous débranchez un serveur physique. Il est possible que tous les processus en cours d'exécution ne soient pas arrêtés, et vous risquez de perdre des données si vous arrêtez la VM de cette manière.
Suspendre	Permet de suspendre une VM en cours d'exécution dans son état actuel et stocke cet état dans un fichier sur le référentiel de stockage par défaut. Cette option vous permet de fermer le serveur hôte de la VM et plus tard, après le redémarrage, reprendre la VM, le retourner à son état d'origine en cours d'exécution.
Reprendre	Reprend une VM suspendue et restaure l'état en cours d'exécution d'origine.

Commande	Fonction
Démarrer	Démarre une VM lorsqu'elle est désactivée (également appelé un démarrage à froid).

Si les actions du contrôle de l'alimentation échouent, placez le curseur de la souris sur l'alerte et un message contextuel s'affiche avec des détails sur l'échec.

Empêcher les connexions aux machines

Utiliser le mode maintenance pour empêcher de nouvelles connexions temporairement lorsque l'administrateur approprié effectue des tâches de maintenance sur l'image.

Lorsque vous activez le mode maintenance sur les machines, aucune nouvelle connexion n'est autorisée jusqu'à ce que vous la désactiviez. Si la session des utilisateurs est actuellement ouverte, le mode maintenance prend effet dès que les sessions de tous les utilisateurs sont fermées. Pour les utilisateurs qui ne ferment pas leur session, envoyez un message les informant que les machines vont être arrêtées à un certain moment, et utilisez les commandes d'alimentation pour forcer la fermeture des machines.

1. Sélectionnez la machine dans la vue Détails de l'utilisateur ou un groupe de machines dans la vue Filtres.
2. Sélectionnez le mode Maintenance et activez l'option.

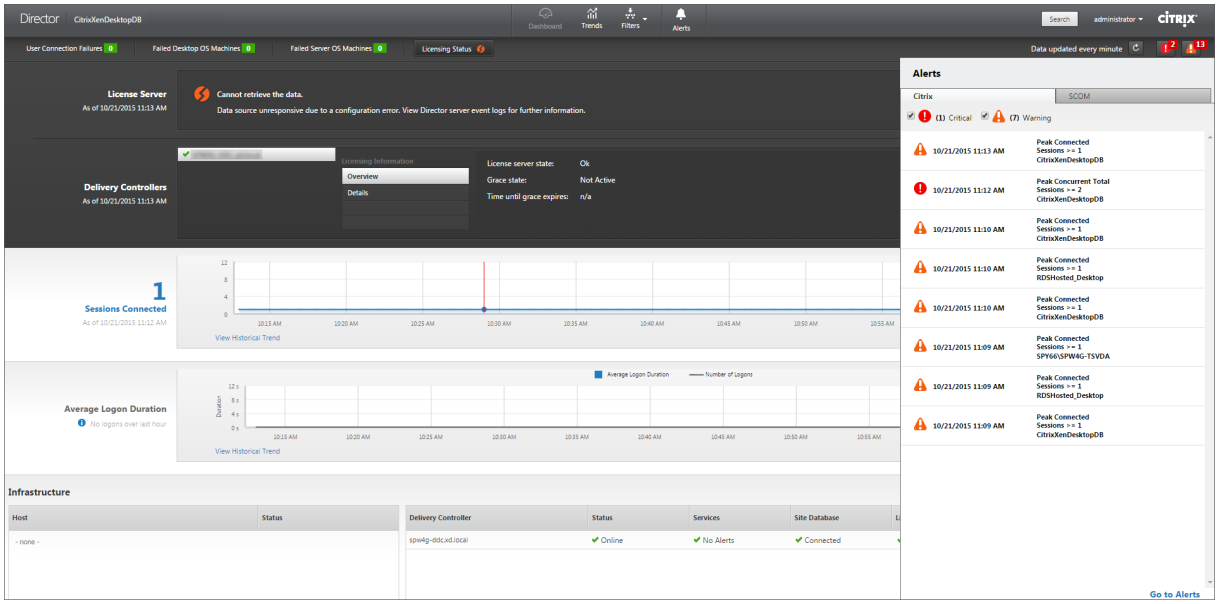
Si un utilisateur essaie de se connecter à un bureau affecté lors qu'il se trouve en mode maintenance, un message s'affiche indiquant que le bureau est actuellement non disponible. Aucune nouvelle connexion ne peut être effectuée tant que vous n'aurez pas désactivé le mode maintenance.

Alertes et notifications

February 28, 2019

Surveiller les alertes

Les alertes sont affichées dans Director sur le tableau de bord et dans d'autres vues de haut niveau avec des symboles d'avertissement et d'alerte critique. Des alertes sont disponibles pour les sites sous licence **Platinum**. Les alertes sont mises à jour automatiquement toutes les minutes ; vous pouvez également mettre à jour les alertes à la demande.

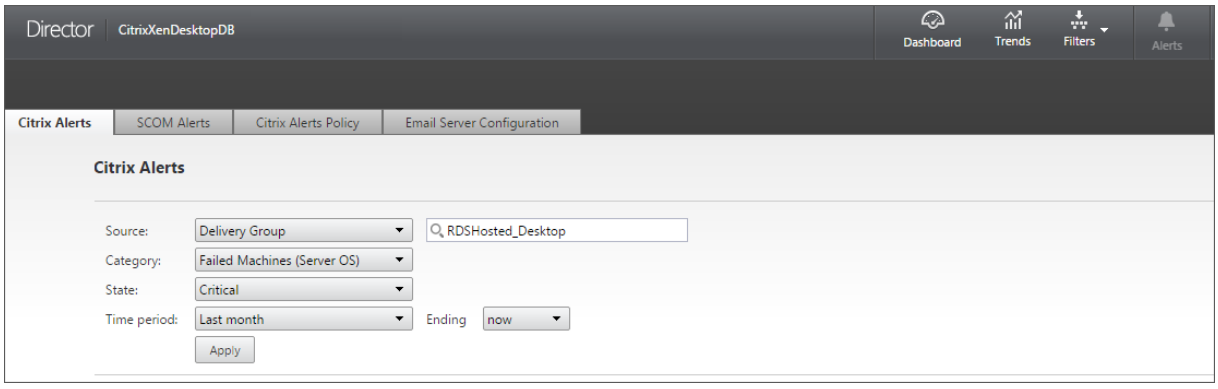


Une alerte d'avertissement (triangle de couleur ambre) indique que le seuil d'avertissement d'une condition a été atteint ou dépassé.

Une alerte critique (cercle rouge) indique que le seuil critique d'une condition a été atteint ou dépassé.

Vous pouvez afficher des informations plus détaillées sur les alertes en sélectionnant une alerte dans la barre latérale, en cliquant sur le lien **Aller aux alertes** dans le bas de la barre latérale ou en sélectionnant **Alertes** dans le haut de la page de Director.

Dans la vue Alertes, vous pouvez filtrer et exporter les alertes. Par exemple, les machines défectueuses avec OS de serveur pour un groupe de mise à disposition spécifique sur le dernier mois, ou toutes les alertes pour un utilisateur spécifique. Pour de plus amples informations, consultez la section Exporter des rapports.



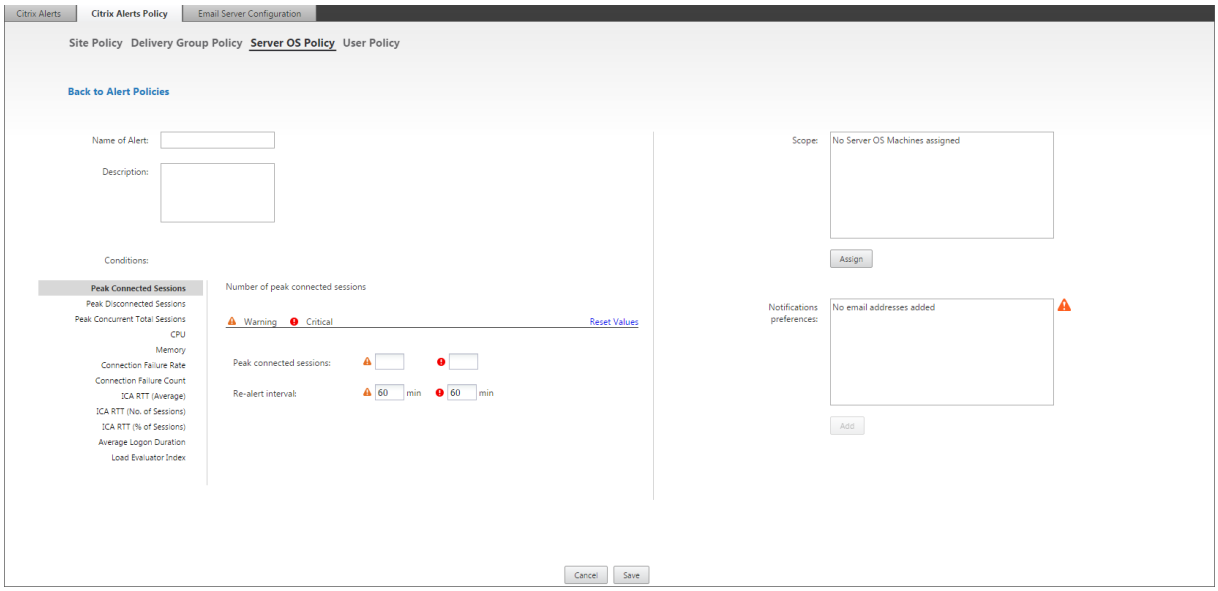
Alertes Citrix. Les alertes Citrix sont des alertes que vous pouvez surveiller dans Director provenant de composants Citrix. Vous pouvez configurer les alertes Citrix dans Director sous **Alertes** > **Stratégies d'alerte Citrix**. Dans le cadre de la configuration, vous pouvez définir l'envoi par e-mail de notifications à des individus et des groupes lorsque les alertes dépassent les seuils que vous avez définis. Vous pouvez configurer la notification en tant que webhooks Octoblu, ou également en tant

qu'interruptions SNMP. Pour de plus amples informations sur la configuration des alertes Citrix, consultez la section Créer des stratégies d'alerte.

Alertes SCOM. Les alertes SCOM affichent des informations provenant de Microsoft System Center 2012 Operations Manager (SCOM) pour fournir une indication plus complète de l'intégrité et des performances du centre de données de Director. Pour de plus amples informations, consultez la section Alertes SCOM.

Le nombre d'alertes affiché en regard des icônes d'alertes avant que vous développiez la barre latérale représente la somme totale des alertes Citrix et SCOM.

Créer des stratégies d'alerte



Pour créer une nouvelle stratégie d'alerte, par exemple pour générer une alerte lorsqu'un ensemble spécifique de critères concernant le nombre de sessions est rempli :

1. Accédez à **Alertes** > **Stratégies d'alerte Citrix** et sélectionnez, par exemple, Stratégie d'OS de serveur.
2. Cliquez sur **Create**.
3. Fournissez un nom et une description pour la stratégie, puis définissez les conditions qui doivent être remplies pour que l'alerte soit déclenchée. Par exemple, spécifiez le nombre d'alertes d'avertissement et d'alertes critiques pour Sessions connectées maximales, Sessions déconnectées maximales et Total des sessions simultanées maximales. La valeur définie pour les alertes d'avertissement ne doit pas être supérieure à la valeur des alertes critiques. Pour de plus amples informations, consultez Conditions des stratégies d'alertes.
4. Définissez le paramètre Intervalle de répétition d'alerte. Si les conditions pour l'alerte sont toujours présentes, l'alerte est de nouveau déclenchée à cet intervalle et, si elle est configurée dans

la stratégie, une notification par e-mail est générée. Une alerte ignorée ne génère pas de notification par e-mail à l'intervalle de répétition d'alerte.

5. Définissez l'étendue. Par exemple, sélectionnez un groupe de mise à disposition spécifique.
6. Dans les préférences de notification, spécifiez les personnes qui doivent être notifiées par e-mail lorsque l'alerte est déclenchée. Vous devez spécifier un serveur de messagerie dans l'onglet **Configuration du serveur de messagerie** pour définir les préférences de notification par e-mail dans les stratégies d'alertes.
7. Cliquez sur **Enregistrer**.

Pour de plus amples informations sur la configuration de webhooks Octoblu, veuillez consulter la section Configurer des stratégies d'alerte avec des webhooks Octoblu.

Pour de plus amples informations sur la configuration d'interruptions SNMP, veuillez consulter la section Configurer des stratégies d'alerte avec des interruptions SNMP.

La création d'une stratégie comprenant plus de 20 groupes de mise à disposition dans l'étendue peut prendre environ 30 secondes. Un compteur s'affiche durant cette période.

La création de plus de 50 stratégies pour un maximum de 20 groupes de mise à disposition uniques (total de 1 000 cibles au maximum) peut entraîner une réponse plus rapide (environ 5 secondes).

Le déplacement d'une machine contenant des sessions actives d'un groupe de mise à disposition à un autre peut déclencher des alertes de groupe de mise à disposition erronées qui sont définies à l'aide des paramètres de la machine.

Conditions de stratégies d'alerte

Condition de stratégie d'alerte	Description et actions recommandées
Sessions connectées max.	Nombre de sessions connectées max. Vérifier la vue Tendances de session dans Director pour les sessions connectées maximales. S'assurer qu'il y a suffisamment de capacité pour gérer la charge de session. Ajouter des machines si nécessaire.
Sessions déconnectées max.	Nombre de sessions déconnectées max. Vérifier la vue Tendances de session dans Director pour les sessions déconnectées maximales. S'assurer qu'il y a suffisamment de capacité pour gérer la charge de session. Ajouter des machines si nécessaire. Fermer les sessions déconnectées si nécessaire.

Condition de stratégie d'alerte	Description et actions recommandées
Total des sessions simultanées max.	Nombre de sessions simultanées max. Vérifier la vue Tendances de session dans Director pour les sessions simultanées maximales. S'assurer qu'il y a suffisamment de capacité pour gérer la charge de session. Ajouter des machines si nécessaire. Fermer les sessions déconnectées si nécessaire.
UC	Pourcentage d'utilisation d'UC. Identifier les processus ou les ressources consommant de l'UC. Arrêter le processus si nécessaire. L'arrêt du processus entraîne la perte des données non enregistrées. Si tout fonctionne comme prévu, ajouter des ressources d'UC dans le futur. **Remarque :** le paramètre de stratégie Activer le suivi des ressources est autorisé par défaut pour le contrôle des compteurs de performances de l'UC et de la mémoire sur les machines avec des VDA. Si ce paramètre de stratégie est désactivé, les alertes avec conditions d'UC et de mémoire ne seront pas déclenchées. Pour plus d'informations, veuillez consulter la section Stratégie Surveillance.

Condition de stratégie d'alerte	Description et actions recommandées
Mémoire	Pourcentage d'utilisation de la mémoire. Identifier les processus ou les ressources consommant de la mémoire. Arrêter le processus si nécessaire. L'arrêt du processus entraîne la perte des données non enregistrées. Si tout fonctionne comme prévu, ajouter plus de mémoire dans le futur. **Remarque :** le paramètre de stratégie Activer le suivi des ressources est autorisé par défaut pour le contrôle des compteurs de performances de l'UC et de la mémoire sur les machines avec des VDA. Si ce paramètre de stratégie est désactivé, les alertes avec conditions d'UC et de mémoire ne seront pas déclenchées. Pour plus d'informations, veuillez consulter la section Paramètres de stratégie Surveillance.
Taux d'échecs de connexion	Pourcentage d'échecs de connexion au cours de la dernière heure. Calculé en fonction du nombre total d'échecs de tentatives de connexions. Vérifier la vue Tendance des défaillances dans Director pour les événements consignés dans le journal de configuration. Déterminer si les applications ou bureaux sont accessibles.
Nombre d'échecs de connexion	Nombre d'échecs de connexion au cours de la dernière heure. Vérifier la vue Tendance des défaillances dans Director pour les événements consignés dans le journal de configuration. Déterminer si les applications ou bureaux sont accessibles.

Condition de stratégie d'alerte	Description et actions recommandées
RTT ICA (moyenne)	Durée moyenne de la boucle ICA Vérifier la répartition du RTT ICA dans NetScaler HDX Insight pour déterminer la cause. Si NetScaler n'est pas disponible, vérifier le RTT ICA et la latence dans la vue Détails utilisateur de Director et déterminer s'il s'agit d'un problème de réseau ou d'un problème XD/XA. Pour de plus amples informations, consultez la documentation de NetScaler Insight Center, Use Cases: HDX Insight.
RTT ICA (nbre de sessions)	Nombre de sessions qui dépassent la durée seuil de la boucle ICA. Vérifier dans NetScaler HDX Insight le nombre de sessions avec un RTT ICA élevé. Pour de plus amples informations, consultez la documentation de NetScaler Insight Center, HDX Insight Reports. Si NetScaler n'est pas disponible, collaborer avec l'équipe du réseau pour déterminer la cause.
RTT ICA (% de sessions)	Pourcentage de sessions qui dépassent la durée moyenne des boucles ICA. Vérifier dans NetScaler HDX Insight le nombre de sessions avec un RTT ICA élevé. Pour de plus amples informations, consultez la documentation de NetScaler Insight Center, HDX Insight Reports. Si NetScaler n'est pas disponible, collaborer avec l'équipe du réseau pour déterminer la cause.
RTT ICA (utilisateur)	Durée de la boucle ICA qui est appliquée aux sessions lancées par l'utilisateur spécifié. L'alerte est déclenchée si le RTT ICA est supérieur à la valeur de seuil dans au moins une session.

Condition de stratégie d'alerte	Description et actions recommandées
Machines défectueuses (OS de bureau)	Nombre de machines défectueuses avec OS de bureau. Les échecs peuvent se produire pour diverses raisons comme indiqué dans les vues Tableau de bord et Filtres de Director. Exécuter les diagnostics Citrix Scout pour déterminer la cause. Pour de plus amples informations, consultez la section Résoudre les problèmes utilisateur.
Machines défectueuses (OS de serveur)	Nombre de machines défectueuses avec OS de serveur. Les échecs peuvent se produire pour diverses raisons comme indiqué dans les vues Tableau de bord et Filtres de Director. Exécuter les diagnostics Citrix Scout pour déterminer la cause.
Durée moyenne de l'ouverture de session	Durée moyenne des ouvertures de session au cours de la dernière heure. Vérifier le tableau de bord de Director pour obtenir des mesures à jour sur la durée des ouvertures de session. Les ouvertures de session peuvent prendre plus de temps si un grand nombre d'utilisateurs ouvrent une session pendant une courte période. Vérifier la ligne de base et le détail des ouvertures de session pour déterminer la cause. Pour de plus amples informations, consultez la section Diagnostiquer les problèmes de connexion utilisateur.
Durée d'ouverture de session (Utilisateur)	Durée des ouvertures de session au cours de la dernière heure pour l'utilisateur spécifié.
Indice de calculateur de charge	Valeur de l'indice de calculateur de charge pour les 5 dernières minutes. Vérifier dans Director s'il existe des machines avec OS de serveur connaissant un pic de charge (charge max.). Afficher le tableau de bord (échecs) et le rapport de tendances de l'indice de calculateur de charge.

Configurer des stratégies d'alerte avec des webhooks Octoblu

Outre les notifications par e-mail, vous pouvez configurer des stratégies d'alerte avec des webhooks Octoblu pour initier des services IoT.

Remarque : cette fonctionnalité requiert la version 7.11 ou ultérieure de Delivery Controller.

Les services IoT qui peuvent utiliser les alertes incluent l'envoi de notifications SMS au personnel d'assistance ou l'intégration avec des plates-formes de résolution d'incident personnalisées pour aider au suivi des notifications.

Vous pouvez configurer une stratégie d'alerte avec un rappel HTTP ou un HTTP POST à l'aide d'applets de commande PowerShell. Elles prennent désormais en charge les webhooks.

Pour de plus amples informations sur la création d'un nouveau workflow Octoblu et l'obtention de l'adresse URL de webhook correspondante, consultez la plateforme des développeurs Octoblu.

Pour configurer une adresse URL de webhook Octoblu pour une nouvelle stratégie ou une stratégie existante, utilisez les applets de commande PowerShell suivantes.

Créer une nouvelle stratégie d'alertes avec une URL de webhook :

```
$policy = New-MonitorNotificationPolicy -Name <nom stratégie> -
    Description <description stratégie> -Enabled $true -Webhook <URL de
    webhook>
```

Ajouter une adresse URL de webhook à une stratégie d'alerte :

```
Set-MonitorNotificationPolicy - Uid <ID stratégie> -Webhook <URL de
    webhook>
```

Pour de plus amples informations sur les commandes PowerShell, utilisez l'aide de PowerShell, par exemple :

```
Get-Help  <Set-MonitorNotificationPolicy>
```

Pour de plus amples informations sur la configuration des stratégies d'alerte à l'aide de PowerShell, consultez la section Director 7.7 : Gestion et configuration d'alertes et de notifications à l'aide de PowerShell dans Concepts avancés.

Les notifications générées à partir de la stratégie d'alerte déclenchent le webhook avec un appel POST à l'adresse URL du webhook. Le message POST contient les informations de notification au format JSON :

```
{
 "NotificationId" : <Notification Id>,

```



```
4  "Target" : <Notification Target Id>,
5
6  "Condition" : <Condition that was violated>,
7
8  "Value" : <Threshold value for the Condition>,
9
10 "Timestamp": <Time in UTC when notification was generated>,
11
12 "PolicyName": <Name of the Alert policy>,
13
14 "Description": <Description of the Alert policy>,
15
16 "Scope" : <Scope of the Alert policy>,
17
18 "NotificationState": <Notification state critical, warning, healthy or
      dismissed>,
19
20 "Site" : <Site name> }
```

Configurer des stratégies d'alerte avec des interruptions SNMP

Lorsqu'une alerte configurée avec une interruption SNMP est déclenchée, le message d'interruption SNMP correspondant est transféré à l'écouteur du réseau configuré pour être traitée. Les alertes Citrix prennent en charge les interruptions SNMP version 2 et ultérieure. Actuellement, le message d'interruption peut être envoyé à un seul écouteur.

Remarque : cette fonctionnalité requiert la version 7.12 ou ultérieure de Delivery Controller.

Pour configurer des interruptions SNMP, utilisez les applets de commande PowerShell suivantes :

- Obtenir la configuration actuelle du serveur SNMP :

```
1  Get-MonitorNotificationSnmpServerConfiguration
```

- Définir la configuration du serveur pour SNMP version 2 :

```
1  Set-MonitorNotificationSnmpServerConfiguration -ServerName <IP
       serveur> -PortNumber <ID port> -SnmpSender <nom expéditeur> -
       CommunityString public -Protocol V2
```

- Définir la configuration du serveur pour SNMP version 3 :

```
1  $authpass = "<authentication password>" | ConvertTo-SecureString
       -AsPlainText -Force
```



```
$privpass = "<Privacy password>" | ConvertTo-SecureString -
    AsPlainText -Force
Set-MonitorNotificationSnmpServerConfiguration -ServerName <
    Server IP> -PortNumber <Port ID> -SnmpSender <Sender name> -
    EngineId <Engine Id> -AuthPassword $authpass -PrivPassword
    $privpass -PrivPasswordProtocol <Privacy password protocol> -
    AuthPasswordProtocol <Authentication password protocol> -
    Protocol V3
```

- Activer l'interruption SNMP pour une stratégie d'alerte existante :

```
Set-MonitorNotificationPolicy -IsSnmpEnabled $true -Uid <ID stratégie>
```

- Créer une nouvelle stratégie d'alerte avec une configuration d'interruption SNMP :

```
$policy = New-MonitorNotificationPolicy -Name <nom stratégie> -
    IsSnmpEnabled $true -Description <description stratégie> -
    Enabled $true
```

La structure des OID dans les messages d'interruption SNMP provenant de Director est la suivante : **1.3.6.1.4.1.3845.100.1.*<UID>***
Ici, ***<UID>*** est généré en série pour chaque stratégie d'alerte définie dans Director. Les OID sont donc propres à chaque environnement utilisateur.

- Utilisez **1.3.6.1.4.1.3845.100.1** pour filtrer tous les messages d'interruption provenant de Director.
- Utilisez **1.3.6.1.4.1.3845.100.1.*<UID>*** pour filtrer et gérer les messages d'interruption pour des alertes spécifiques.

Utilisez l'applet de commande suivante pour obtenir les UID pour les stratégies d'alerte définies dans votre environnement :

```
Get-MonitorNotificationPolicy
```

Vous pouvez transférer les interruptions SNMP vers SCOM. Pour ce faire, configurez SCOM avec le Delivery Controller pour écouter les messages d'interruption.

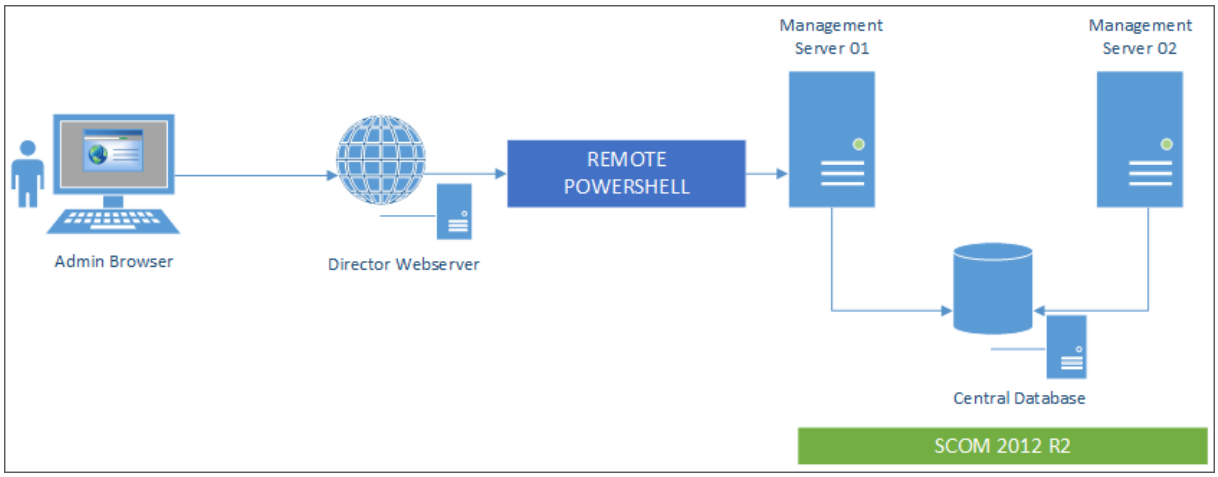
Configurer l'intégration d'alertes SCOM

L'intégration de SCOM avec Director vous permet de visualiser des alertes provenant de SCOM sur le tableau de bord et dans d'autres vues de haut niveau dans Director.

Les alertes SCOM s'affichent à l'écran, ainsi que les alertes Citrix. Vous pouvez accéder aux alertes SCOM et en afficher les détails depuis l'onglet SCOM dans la barre latérale.

Vous pouvez afficher l'historique des alertes depuis un mois, trier, filtrer et exporter les informations filtrées dans des rapports aux formats CSV, Excel et PDF. Pour de plus amples informations, consultez la section Exporter des rapports.

L'intégration de System Center Operations Manager (SCOM) utilise PowerShell 3.0 à distance ou une version plus récente pour interroger les données du serveur d'administration de System Center Operations Manager et maintient une connexion runspace permanente dans la session Director de l'utilisateur. Le serveur Director et le serveur SCOM doivent disposer de la même version de PowerShell.



La configuration requise pour l'intégration de SCOM est la suivante :

- Windows Server 2012 R2
- System Center 2012 R2 Operations Manager
- PowerShell 3.0 ou version ulétrieure (la version de PowerShell doit être la même sur le serveur Director et le serveur SCOM)
- UC quadruple cœur avec 16 Go de RAM (recommandé)
- Un serveur d'administration principal pour System Center Operations Manager doit être configuré dans le fichier web.config de Director. Vous pouvez le faire à l'aide de l'outil DirectorConfig.

Remarque :

- Citrix recommande que le compte d'administrateur de Director soit configuré en tant que rôle d'opérateur de SCOM de façon à ce qu'il puisse obtenir des informations d'alertes complètes dans Director. Si cela n'est pas possible, un compte d'administrateur SCOM peut être configuré dans le fichier web.config à l'aide de l'outil DirectorConfig.
- Citrix vous recommande de ne pas configurer plus de 10 administrateurs Director par serveur d'administration SCOM afin d'assurer des performances optimales.

Sur le serveur Director :

1. Tapez **Enable-PSRemoting** pour activer la communication à distance PowerShell.

2. Ajoutez le serveur d'administration SCOM à la liste TrustedHosts. Ouvrez une invite PowerShell et exécutez les commandes suivantes :

   a) Obtenez la liste TrustedHosts.

```
Get-Item WSMAN:\localhost\Client\TrustedHosts
```

```
1. Ajoutez le nom de domaine complet du serveur d'administration SCOM
   à la liste TrustedHosts. \<Old Values\> représente l'ensemble
   existant d'entrées renvoyées depuis l'applet de commande Get-Item.
```

```
Set-Item WSMAN:\localhost\Client\TrustedHosts -Value "<FQDN SCOM
    Management Server>,<Old Values>"
```

1. Configurez SCOM à l'aide de l'outil DirectorConfig.

```
C:\inetpub\wwwroot\Director\tools\DirectorConfig.exe /configscom
```

Sur le serveur d'administration SCOM :

1. Attribuez les administrateurs Director à un rôle d'administrateur SCOM.

   a) Ouvrez la console d'administration SCOM et accédez à **Administration** > **Sécurité** > **Rôles utilisateur**.

   b) Dans Rôles utilisateur, vous pouvez créer un nouveau rôle utilisateur ou modifier un rôle existant. Il existe quatre catégories de rôles d'opérateur SCOM qui définissent la nature de l'accès aux données SCOM. Par exemple, un opérateur en lecture seule ne voit pas le panneau Administration et ne peut détecter ou gérer les règles, comptes ou machines. Un rôle d'opérateur est un rôle d'administrateur complet.

   Remarque : les opérations suivantes ne sont pas disponibles si un administrateur de Director se voit attribuer un rôle non opérateur :

   - Si plusieurs serveurs d'administration ont été configurés et que le serveur d'administration principal n'est pas disponible, l'administrateur de Director ne peut pas se connecter au serveur d'administration secondaire. Le serveur d'administration principal est le serveur configuré dans le fichier web.config de Director, qui est le même serveur que celui spécifié avec l'outil DirectorConfig à l'étape 3 ci-dessus. Les serveurs d'administration secondaires sont des serveurs d'administration homologues du serveur principal.
   - Lors du filtrage des alertes, l'administrateur de Director ne peut pas rechercher l'origine de l'alerte. Cette opération requiert une autorisation de niveau opérateur.

   c) Pour modifier un rôle utilisateur, cliquez avec le bouton droit sur le rôle, puis cliquez sur **Propriétés**.

d) Dans la boîte de dialogue Propriétés du rôle, vous pouvez ajouter ou supprimer des administrateurs Director pour ce rôle utilisateur.

2. Ajoutez les administrateurs Director au groupe Utilisateurs de gestion à distance sur le serveur d'administration SCOM. Ceci permet aux administrateurs Director d'établir une connexion PowerShell distante.
3. Tapez **Enable-PSRemoting** pour activer la communication à distance PowerShell.
4. Définissez les limites des propriétés WS-Management :

   a) Modifiez MaxConcurrentUsers :

   Dans l'interface de ligne de commande :

   ```
   winrm set winrm/config/winrs @{
    MaxConcurrentUsers = "20" }
   ```

   Dans PS :

   ```
   Set -Item WSMan:\localhost\Shell\MaxConcurrentUsers 20
   ```

   b) Modifiez MaxShellsPerUser :

   Dans l'interface de ligne de commande :

   ```
   winrm set winrm/config/winrs @{
    MaxShellsPerUser="20" }
   ```

   Dans PS :

   ```
   Set-Item WSMan:\localhost\Shell\MaxShellsPerUser 20
   ```

   c) Modifiez MaxMemoryPerShellMB :

   Dans l'interface de ligne de commande :

   ```
   winrm set winrm/config/winrs @{
    MaxMemoryPerShellMB="1024" }
   ```

   Dans PS :

   ```
   Set -Item WSMan:\localhost\Shell\MaxMemoryPerShellMB 1024
   ```

5. Pour vous assurer que l'intégration de SCOM fonctionne dans les environnements de domaine mixtes, définissez l'entrée de registre suivante.

   Chemin : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

   Clé : LocalAccountTokenFilterPolicy

Type : DWord

Valeur : 1

Avertissement : la modification incorrecte du Registre peut entraîner des problèmes graves pouvant nécessiter la réinstallation de votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de cet outil. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Une fois que l'intégration de SCOM est configurée, il se peut que le message suivant s'affiche : « Impossible d'obtenir les dernières alertes de SCOM. Consultez les journaux d'événements du serveur Director pour plus d'informations. » Les journaux d'événements du serveur permettent d'identifier et de corriger le problème. Causes potentielles :

- Perte de connectivité réseau sur la machine Director ou SCOM.
- Le service SCOM n'est pas disponible ou trop occupé pour répondre.
- Échec de l'autorisation en raison d'une modification des autorisations de l'utilisateur configuré.
- Une erreur dans Director lors du traitement des données SCOM.
- Version de PowerShell différente entre Director et le serveur SCOM.

Administration déléguée et Director

November 13, 2018

L'administration déléguée utilise trois concepts : les administrateurs, les rôles et les étendues. Les permissions sont basées sur un rôle administrateur et l'étendue de ce rôle. Par exemple, un administrateur peut affecter un rôle d'administrateur du bureau d'assistance où l'étendue implique la responsabilité des utilisateurs à un site uniquement.

Pour de plus amples informations sur la création d'administrateurs délégués, veuillez consulter le document Administration déléguée.

Les permissions d'administration déterminent l'interface Director présentée aux administrateurs et les tâches à effectuer. Les permissions déterminent :

- Les vues auxquelles l'administrateur peut accéder, collectivement nommées vue.
- Les bureaux, les machines et les sessions que l'administrateur peut afficher et interagir avec.
- Les commandes de l'administrateur peut effectuer, telles que l'observation d'une session de l'utilisateur ou l'activation du mode maintenance.

Les rôles et les permissions intégrés déterminent également la manière d'utilisation de Director par les administrateurs :

Rôle Administrateur	Permissions de Director
Administrateur complet	Possède un accès complet à toutes les vues et peut effectuer toutes les commandes, y compris l'observation d'une session utilisateur, l'activation du mode maintenance et l'exportation des données des tendances.
Administrateur de groupe de mise à disposition	Possède un accès complet à toutes les vues et peut effectuer toutes les commandes, y compris l'observation d'une session utilisateur, l'activation du mode maintenance et l'exportation des données des tendances.
Administrateur en lecture seule	Peut accéder à toutes les vues et afficher tous les objets dans les étendues spécifiées ainsi que les informations globales. Peut télécharger des rapports à partir de canaux HDX et peut exporter les données de Tendances à l'aide de l'option Exporter dans la vue Tendances. Ne peut exécuter des commandes ou modifier quoi que ce soit dans les vues.
Administrateur du service d'assistance	Peut accéder uniquement aux vues Bureau d'assistance et Détails de l'utilisateur et peut afficher uniquement des objets que l'administrateur est autorisé à gérer. Peut observer une session utilisateur et exécuter des commandes pour cet utilisateur. Peut effectuer les opérations du mode maintenance. Peut utiliser les options de contrôle de l'alimentation pour les machines avec OS de bureau. Impossible d'accéder aux vues Tableau de bord, Tendances, Alertes ou Filtres. Ne peut utiliser les options de contrôle de l'alimentation pour les machines avec OS de serveur.
Administrateur du catalogue de machines	Aucun accès. Cet administrateur n'est pas pris en charge pour Director et ne peut pas afficher les données. Cet utilisateur peut accéder à la page Détails de machine (recherche machine).

Rôle Administrateur	Permissions de Director
Administrateur d'hôte	Aucun accès. Cet administrateur n'est pas pris en charge pour Director et ne peut pas afficher les données.

Pour configurer les rôles personnalisés pour les administrateurs Director

Dans Studio, vous pouvez également configurer des rôles spécifiques à Director, personnalisés pour correspondre plus étroitement aux besoins de votre organisation et déléguer des permissions de manière plus flexible. Par exemple, vous pouvez limiter le rôle d'administrateur du Bureau d'assistance intégré afin que cet administrateur ne puisse pas fermer de sessions.

Si vous créez un rôle personnalisé avec les permissions Director, vous devez également donner à ce rôle d'autres permissions génériques :

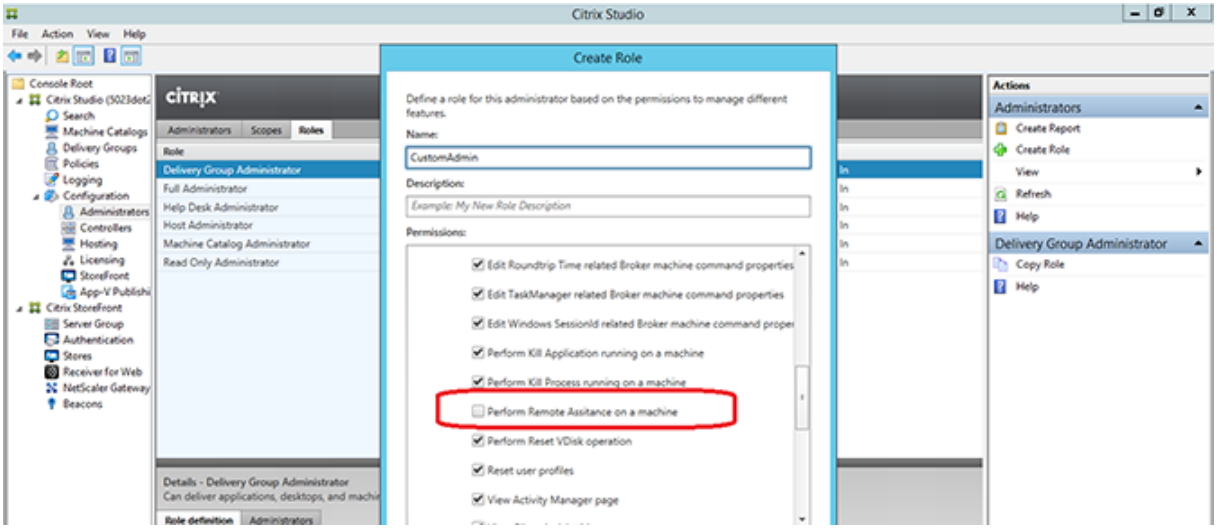
- Permissions pour le Delivery Controller de se connecter à Director : au minimum un accès en lecture seule au nœud Administrateur
- Permissions pour les groupes de mise à disposition pour afficher les données liées à ces groupes de mise à disposition dans Director, un accès en lecture seule au minimum.

Éventuellement, vous pouvez créer un rôle personnalisé en copiant un rôle existant et inclure des permissions supplémentaires pour différentes vues. Par exemple, vous pouvez copier le rôle du Bureau d'assistance et inclure des permissions pour afficher les pages Tableau de bord ou Filtres.

Sélectionnez les permissions de Director pour le rôle personnalisé, y compris :

- Arrêter l'application en cours d'exécution sur une machine
- Arrêter le processus en cours d'exécution sur une machine
- Intervenir à distance sur une machine
- Effectuer des réinitialisations d'opérations vDisk
- Réinitialiser les profils utilisateur
- Afficher la page des détails du client
- Afficher la page du tableau de bord
- Afficher la page Filtres
- Afficher la page Détails de la machine
- Afficher la page des tendances
- Afficher la page des détails utilisateur

Dans cet exemple, l'observation (Effectuer une intervention à distance sur une machine) est désactivée.



Une permission peut dépendre d'autres permissions pour pouvoir s'appliquer sur l'interface utilisateur. Par exemple, la sélection de la permission **Arrêter l'application en cours d'exécution sur une machine** active la fonctionnalité **Arrêter l'application** uniquement dans les panneaux sur lesquels le rôle a la permission. Vous pouvez sélectionner les permissions de panneau suivantes :

- Afficher la page Filtres
- Afficher la page des détails utilisateur
- Afficher la page Détails de la machine
- Afficher la page des détails du client

En outre, depuis la liste des permissions pour d'autres composants, prenez en compte ces permissions des groupes de mise à disposition :

- Activer/désactiver le mode de maintenance d'une machine via l'appartenance à un groupe de mise à disposition
- Réaliser des opérations d'alimentation sur les machines de bureau Windows via l'appartenance à un groupe de mise à disposition
- Réaliser la gestion de session sur les machines via l'appartenance à un groupe de mise à disposition

Sécuriser le déploiement de Director

January 23, 2019

Cet article dresse la liste des domaines susceptibles d'avoir un impact sur la sécurité du système lors du déploiement et de la configuration de Director.

Configurer Microsoft Internet Information Services (IIS)

Vous pouvez configurer Director avec une configuration IIS limitée. Veuillez noter qu'il ne s'agit pas de la configuration IIS par défaut.

Extensions de nom de fichier

Vous pouvez interdire les extensions de nom de fichier non répertoriées.

Director requiert ces extensions de nom de fichier dans le Filtrage des demandes :

- .aspx
- .css
- .html
- .js
- .png
- .svc

Director requiert les verbes HTTP suivants dans le Filtrage des demandes : Vous pouvez interdire les verbes non répertoriés.

- GET
- POST
- HEAD

Director ne requiert pas ce qui suit :

- Filtres ISAPI
- Extensions ISAPI
- Programmes CGI
- Programmes FastCGI

Important :

- Director requiert l'approbation Confiance totale. Ne définissez pas le niveau de confiance .NET global sur Élevé ou Moyen.
- Director gère un pool d'applications distinct. Pour modifier les paramètres de Director, sélectionnez le site Director et modifiez-le.

Configurer les droits des utilisateurs

Lorsque Director est installé, le droit d'ouverture de session Ouvrir une session en tant que service et les privilèges Ajuster les quotas de mémoire pour un processus, Générer des audits de sécurité et Remplacer un jeton de niveau processus sont accordés à ses pools d'applications. Il s'agit d'un comportement d'installation normal lorsque des pools d'applications sont créés.

Vous n'avez pas besoin de changer ces droits d'utilisateur. Ces privilèges ne sont pas utilisés par Director et sont automatiquement désactivés.

Communications Director

Dans un environnement de production, Citrix vous recommande d'utiliser Internet Protocol Security (IPsec) ou le protocole HTTPS pour sécuriser le transfert des données entre Director et vos serveurs. IPsec est un ensemble d'extensions standard du protocole Internet qui garantit des communications authentifiées et cryptées avec intégrité des données et protection contre la relecture. IPsec étant un ensemble de protocoles de couches réseau, les protocoles d'un niveau plus élevé peuvent l'utiliser sans modification. HTTPS utilise les protocoles Transport Layer Security (TLS) pour fournir un cryptage puissant des données.

Remarque :

- Citrix vous recommande de ne pas autoriser les connexions non sécurisées à Director dans un environnement de production.
- Les communications sécurisées en provenance de Director requièrent une configuration séparée pour chaque connexion.
- Le protocole SSL n'est pas recommandé. Utilisez plutôt le protocole TLS plus sécurisé.
- Vous devez sécuriser les communications à NetScaler à l'aide de TLS, et non IPsec.

Pour sécuriser les communications entre Director et les serveurs XenApp et XenDesktop (pour le suivi et la création de rapports), reportez-vous à la section Sécurisation de l'accès aux données.

Pour sécuriser les communications entre Director et NetScaler (pour NetScaler Insight), reportez-vous à la section Configurer l'analyse réseau.

Pour sécuriser les communications entre Director et le serveur de licences, reportez-vous à la section Sécuriser la console License Administration Console.

Séparation de la sécurité de Director

Si vous déployez des applications Web dans le même domaine Web (nom de domaine et de port) que Director, tout risque ayant trait à la sécurité dans ces applications Web peut potentiellement réduire la sécurité de votre déploiement Director. Lorsqu'un degré plus important de séparation de la sécurité est nécessaire, Citrix recommande de déployer Director dans un domaine Web distinct.

Configurer les permissions pour VDA antérieurs à XenDesktop 7

November 14, 2018

Si les utilisateurs possèdent des VDA antérieurs à XenDesktop 7, Director complète les informations sur le déploiement avec des données en temps réel sur l'état et des métriques via Windows Remote Management (WinRM).

En outre, utilisez cette procédure pour configurer WinRM pour une utilisation avec Remote PC dans XenDesktop 5.6 Feature Pack 1.

Par défaut, seuls les administrateurs locaux de la machine de bureau (c'est-à-dire, généralement, les administrateurs de domaine et autres utilisateurs privilégiés) disposent des permissions nécessaires pour afficher les données en temps réel.

Pour plus d'informations sur l'installation et la configuration de WinRM, veuillez consulter l'article CTX125243.

Pour autoriser d'autres utilisateurs à afficher les données en temps réel, vous devez leur accorder les permissions correspondantes. Par exemple, supposez qu'il existe plusieurs utilisateurs Director (HelpDeskUserA, HelpDeskUserB, etc) qui appartiennent au groupe de sécurité Active Directory appelé HelpDeskUsers. Le groupe a été attribué au rôle d'administrateur du bureau d'assistance dans Studio, leur offrant les permissions Delivery Controller requises. Toutefois, le groupe doit également pouvoir accéder aux informations de la machine de bureau.

Pour fournir l'accès nécessaire, vous pouvez configurer les permissions requises de l'une des façons suivantes :

- Accorder des permissions aux utilisateurs de Director (modèle d'usurpation d'identité)
- Accorder des permissions au service Director (modèle de sous-système autorisé)

Pour accorder des permissions aux utilisateurs de Director (modèle d'usurpation d'identité)

Par défaut, Director utilise le modèle d'usurpation d'identité : la connexion WinRM à la machine de bureau est établie en utilisant l'identité de l'utilisateur Director. C'est donc l'utilisateur qui doit disposer des permissions appropriées sur le bureau.

Vous pouvez configurer ces permissions de deux manières (décrites dans ce document) :

1. Ajouter des utilisateurs au groupe d'administrateurs locaux sur la machine de bureau.
2. Accorder aux utilisateurs les permissions spécifiques requises par Director. Cette option permet d'éviter de transmettre les permissions administratives de Director aux utilisateurs (par exemple, le groupe HelpDeskUsers) sur la machine.

Pour accorder des permissions au service Director (modèle de sous-système autorisé)

Au lieu d'accorder aux utilisateurs Director des permissions sur les machines de bureaux, vous pouvez configurer Director de sorte qu'il établisse les connexions WinRM à l'aide d'une identité de service et

accorder à cette identité de service uniquement les permissions nécessaires.

Avec ce modèle, les utilisateurs Director ne sont pas autorisés à passer eux-mêmes des appels WinRM. Ils peuvent uniquement accéder aux données à l'aide de Director.

Le regroupement d'applications Director des services IIS est configuré pour être exécuté comme identité de service. Par défaut, il s'agit du compte virtuel APPPOOL\Director. Lorsque vous établissez des connexions à distance, ce compte apparaît en tant que compte d'ordinateur Active Directory du serveur, par exemple MonDomaine\ServeurDirector$. Vous devez configurer ce compte avec les permissions nécessaires.

Si plusieurs sites Web Director sont déployés, vous devez placer chaque compte d'ordinateur du serveur Web dans un groupe de sécurité Active Directory configuré avec les permissions appropriées.

Pour configurer Director pour utiliser l'identité de service pour WinRM au lieu de l'identité de l'utilisateur, configurez le paramètre suivant, comme décrit dans Configuration avancée :

```
1 Service.Connector.WinRM.Identity = Service
```

Vous pouvez configurer ces permissions de l'une des façons suivantes :

1. Ajouter le compte de service au groupe d'administrateurs locaux sur la machine de bureau.
2. Accorder au compte de service les permissions spécifiques requises par Director (décrit ci-après). Cette option évite d'accorder au compte de service l'ensemble des permissions administratives sur la machine.

Pour attribuer des permissions à un utilisateur ou à un groupe spécifique

Les permissions suivantes sont requises pour que Director puisse accéder aux informations relatives à la machine de bureau via WinRM :

- Permissions de lecture et d'exécution dans WinRM RootSDDL
- Permissions sur l'espace de nom WMI :
  - root/cimv2 - accès distant
  - root/citrix - accès distant
  - root/RSOP - accès distant et exécution
- Membre de ces groupes locaux :
  - Utilisateurs de type contrôle des performances
  - Lecteurs de journaux d'événements

L'outil ConfigRemoteMgmt.exe, utilisé pour accorder automatiquement des permissions, est disponible sur le support d'installation dans les dossiers x86\Virtual Desktop Agent et x64\Virtual Desktop Agent et sur le support d'installation dans le dossier C:\inetpub\wwwroot\Director\tools. Vous devez accorder des permissions à tous les utilisateurs Director.

Pour accorder des permissions à un groupe de sécurité, utilisateur, compte d'ordinateur Active Directory, ou pour des actions telles que celles qui consistent à Mettre fin à l'application et Mettre fin au processus, exécutez l'outil avec les privilèges d'administration à partir d'une invite de commande qui utilise les arguments suivants :

```
ConfigRemoteMgmt.exe /configwinrmuser domain\name
```

où name correspond au compte du groupe de sécurité, de l'utilisateur ou de l'ordinateur.

Pour accorder les permissions nécessaires à un groupe de sécurité d'utilisateur :

```
ConfigRemoteMgmt.exe /configwinrmuser domain\HelpDeskUsers
```

Pour accorder les permissions à un compte d'ordinateur spécifique :

```
ConfigRemoteMgmt.exe /configwinrmuser domain\DirectorServer$
```

Pour les actions Mettre fin au processus, Mettre fin à l'application et Observer :

```
ConfigRemoteMgmt.exe /configwinrmuser domain\name /all
```

Pour accorder des permissions à un groupe d'utilisateurs :

```
ConfigRemoteMgmt.exe /configwinrmuser domain\HelpDeskUsers /all
```

Pour afficher l'aide de l'outil :

```
ConfigRemoteMgmt.exe
```

Configurer l'analyse réseau

January 23, 2019

Remarque : la disponibilité de cette fonctionnalité dépend de la licence de votre organisation et de vos permissions d'administrateur.

Director s'intègre à NetScaler Insight Center ou NetScaler MAS pour offrir une analyse de réseau et une gestion des performances :

- L'analyse de réseau tire parti des rapports HDX Insight de NetScaler Insight Center ou NetScaler MAS pour fournir une vue contextuelle des applications et des bureaux du réseau. Avec cette fonctionnalité, Director offre une analyse avancée du trafic ICA dans votre déploiement.
- La gestion des performances fournit un archivage des données d'historique ainsi que des rapports de tendance. Avec la conservation de l'historique des données par rapport à l'évaluation

en temps réel, vous pouvez créer des rapports de tendance, y compris des tendances de capacité et d'intégrité.

Après avoir activé cette fonctionnalité dans Director, les rapports HDX Insight fournissent des informations supplémentaires à Director :

- L'onglet Réseau de la page Tendances affiche des effets de latence et de bande passante pour les applications, les bureaux et les utilisateurs sur l'ensemble du déploiement.
- La page Détails de l'utilisateur affiche des informations spécifiques à la latence et à la bande passante pour une session utilisateur particulière.

Limitations :

- Durée des boucles de session ICA (RTT) affiche les données correctement pour Receiver pour Windows 3.4 ou version ultérieure et Receiver pour Mac 11.8 ou version ultérieure. Pour les versions antérieures de ces Receiver, les données ne s'affichent pas correctement.
- Dans la vue Tendances, les données d'ouverture de session de connexion HDX ne sont pas collectées pour les VDA antérieurs à la version 7. Pour les VDA antérieurs, les données du graphique sont affichées en tant que 0.

Pour activer l'analyse de réseau, vous devez installer et configurer NetScaler Insight Center ou NetScaler MAS dans Director. Director requiert NetScaler MAS version 11.1 Build 49.16 ou une version ultérieure. Insight Center et MAS sont des appliances virtuelles exécutées sur Citrix XenServer. À l'aide de l'analyse de réseau, Director communique et rassemble les informations relatives à votre déploiement.

Pour plus d'informations, veuillez consulter la documentation Netscaler MAS.

1. Sur le serveur sur lequel Director est installé, situez l'outil de ligne de commande DirectorConfig dans C:\inetpub\wwwroot\Director\tools, et exécutez-le avec le paramètre /confignetscaler dans une invite de commande.
2. Lorsque vous y êtes invité, entrez le nom de la machine (FQDN ou adresse IP) NetScaler Insight Center ou NetScaler MAS, le nom d'utilisateur, le mot de passe, le type de connexion HTTP ou HTTPS et choisissez l'intégration à NetScaler Insight ou NetScaler MAS.
3. Pour vérifier les modifications, fermez votre session et rouvrez-la.

Résoudre les problèmes utilisateur

February 28, 2019

Utilisez la vue **Assistance** de Director (page **Gestionnaire d'activités**) pour afficher des informations sur l'utilisateur :

- Vérifiez les détails sur l'ouverture de session de l'utilisateur, la connexion et les applications.

- Observez la machine de l'utilisateur.
- Enregistrez la session ICA.
- Résolvez le problème avec les actions recommandées dans le tableau suivant, et, si nécessaire, informez l'administrateur du problème.

Conseils de dépannage

Problème utilisateur	Suggestions
L'ouverture de session prend beaucoup de temps ou échoue par intermittence ou de manière répétée	Diagnostiquer les problèmes de connexion utilisateur
L'application est lente ou ne répond pas	Résoudre les échecs applicatifs
La connexion a échoué	Restaurer les connexions aux bureaux
La session est lente ou ne répond pas	Restaurer les sessions
Enregistrer des sessions	Enregistrer des sessions
La vidéo est lente ou de qualité médiocre	Exécuter des rapports système sur le canal HDX

Remarque : pour vous assurer que la machine n'est pas en mode de maintenance, à partir de la vue Détails de l'utilisateur, vérifiez le panneau Détails de la machine.

Astuces de recherche

Lorsque vous tapez le nom de l'utilisateur dans le champ Rechercher, Director recherche des utilisateurs dans Active Directory pour les utilisateurs de tous les sites configurés pour prendre en charge Director.

Lorsque vous entrez un nom de machine à plusieurs utilisateurs dans le champ Rechercher, Director affiche les Détails de la machine pour la machine spécifiée.

Lorsque vous entrez un nom de point de terminaison dans le champ Rechercher, Director utilise les sessions authentifiées (anonymes) et non authentifiées connectées à un point de terminaison spécifique, qui permet de résoudre des sessions non authentifiés. Assurez-vous que les noms de points de terminaison sont uniques pour activer la résolution des problèmes des sessions non authentifiées.

Les résultats de la recherche incluent également les utilisateurs qui ne sont pas connectés ou attribués à une machine.

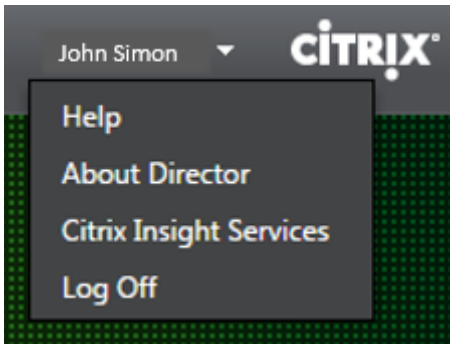
- Les recherches ne sont pas sensibles à la casse.

- Les entrées partielles produisent une liste de correspondances possibles.
- Lorsque vous entrez les premières lettres d'un nom en deux parties (nom d'utilisateur, nom de famille et prénom ou nom d'affichage), en les séparant par un espace, les résultats comprennent les correspondances pour les deux chaînes. Par exemple, si vous tapez jo rob, les résultats peuvent inclure des chaînes telles que « John Robertson » ou Robert, Jones.

Pour revenir à la page d'accueil, cliquez sur le logo Director.

Accéder à Citrix Insight Services

Vous pouvez accéder à Citrix Insight Services (CIS) à partir de la liste déroulante Utilisateur dans Director pour accéder à des informations de diagnostic supplémentaires. Les données disponibles dans CIS sont fournies à partir de sources telles que Call Home et Citrix Scout.



Charger des informations de dépannage pour le support technique Citrix

Exécutez Citrix Scout à partir d'un Delivery Controller ou d'un VDA pour capturer les points de données clés et les traces Citrix Diagnostic Facility (CDF) pour dépanner les ordinateurs sélectionnés. Scout offre la possibilité de charger des données en toute sécurité vers la plate-forme CIS pour aider l'assistance technique de Citrix à résoudre les problèmes. L'assistance technique de Citrix utilise la plate-forme CIS pour réduire la durée de résolution des problèmes signalés par les clients.

Scout est installé avec les composants XenApp ou XenDesktop. En fonction de la version de Windows, Scout s'affiche dans le menu Démarrer de Windows ou l'écran d'accueil lorsque vous installez ou mettez à niveau vers XenDesktop 7.1, XenDesktop 7.5, XenApp 7.5, XenDesktop 7.6, XenApp 7.6, XenDesktop 7.7 ou XenApp 7.7.

Pour démarrer Scout, à partir du menu Démarrer ou de l'écran d'accueil, sélectionnez Citrix > Citrix Scout.

Pour plus d'informations sur l'utilisation et la configuration Scout, et accéder aux questions fréquemment posées, consultez l'article CTX130147.

Envoyer des messages aux utilisateurs

November 13, 2018

À partir de Director, envoyez un message à un utilisateur qui est connecté à une ou plusieurs machines. Par exemple, utilisez cette fonctionnalité pour envoyer des notifications immédiates sur des actions administratives telles que la maintenance de bureau imminente, les fermetures de session et les redémarrages de machine et les réinitialisations de profil.

1. Dans la vue Gestionnaire d'activités, sélectionnez l'utilisateur, puis cliquez sur Détails.
2. Dans la vue Détails de l'utilisateur, situez le panneau Détails de session, puis cliquez sur Envoyer un message.
3. Tapez votre message d'informations dans les champs Objet et Message, puis cliquez sur Envoyer.

Si le message n'est pas envoyé avec succès, un message de confirmation s'affiche dans Director. Si la machine de l'utilisateur est connectée, le message s'affiche.

Si le message n'est pas envoyé avec succès, un message d'erreur s'affiche dans Director. Résoudre le problème en fonction du message d'erreur. Lorsque vous avez terminé, tapez le sujet et le texte du message et cliquez sur Réessayer.

Restaurer les sessions

November 13, 2018

Si une session devient déconnectée, elle reste active et ses applications continuent d'être exécutées, mais la machine cliente ne communique plus avec le serveur.

Dans la vue Détails de l'utilisateur, résolvez les échecs de session dans le panneau Détails de la session. Vous pouvez afficher les détails de la session en cours, indiquée par l'ID de session.

Action	Description
Arrêter les applications ou processus qui ne répondent pas	Cliquez sur l'onglet Applications. Sélectionnez toute application qui ne répond pas et cliquez sur Fermer l'application. Sélectionnez également un processus correspondant qui ne répond pas et cliquez sur Arrêter le processus. Mettez également fin aux processus qui consomment une quantité de mémoire ou de ressources UC anormalement élevée, ce qui peut rendre le processeur inutilisable.

Action	Description
Déconnecter la session Windows	Cliquez sur Contrôle de la session, puis sélectionnez Déconnecter. Cette option est uniquement disponible pour les machines avec OS de serveur avec broker. Pour les sessions sans broker, l'option est désactivée.
Fermer la session de l'utilisateur	Cliquez sur Contrôle de la session, puis sélectionnez Fermer la session.

Pour tester la session, l'utilisateur peut essayer de la rouvrir. Vous pouvez également observer l'utilisateur pour surveiller plus étroitement cette session.

Remarque : si les machines utilisateur exécutent des Virtual Delivery Agent (VDA) antérieurs à la version 7, Director ne peut pas afficher d'informations complètes sur la session, et affiche à la place un message indiquant que les informations ne sont pas disponibles. Ces messages peuvent apparaître dans la page
Détails de l'utilisateur et
Gestionnaire d'activités.

Réinitialiser un Personal vDisk

February 28, 2019

Avertissement : lorsque vous réinitialisez le disque, les paramètres par défaut sont rétablis et toutes leurs données sont supprimées, y compris les applications. Les données de profil sont conservées, sauf si vous avez modifié le Personal vDisk par défaut (de redirection des profils depuis le lecteur C:), ou si vous ne disposez pas d'une solution de profil tierce.

Pour effectuer la réinitialisation, la machine possédant le Personal vDisk doit être en cours d'exécution ; cependant, l'utilisateur n'a pas besoin d'être connecté.

Cette option est uniquement disponible pour les machines avec OS de bureau ; elle est désactivée pour les machines avec OS de serveur.

1. Dans la vue Bureau d'assistance, choisissez la machine avec OS de bureau ciblée.
2. À partir de cette vue ou dans le panneau de personnalisation de la vue Détails de l'utilisateur, cliquez sur Réinitialiser un Personal vDisk.
3. Cliquez sur Réinitialiser. Un message d'avertissement s'affiche indiquant à l'utilisateur que sa session va être fermée. La session de l'utilisateur est fermée (s'il en avait ouvert une) et la machine redémarre.

Si l'opération de réinitialisation est réussie, la valeur du champ Statut Personal vDisk dans le panneau de personnalisation de la vue Détails de l'utilisateur est En cours d'exécution. Si la réinitialisation échoue , un X rouge à droite de la valeur En cours d'exécution s'affiche. Lorsque vous pointez sur ce X, les informations relatives à l'erreur s'affichent.

Exécuter des rapports système sur le canal HDX

February 28, 2019

Dans la vueDétails de l'utilisateur, vérifiez le statut des canaux HDX sur la machine de l'utilisateur dans le
panneau HDX. Ce panneau est disponible uniquement si la machine utilisateur est connectée à l'aide de HDX.

Si un message s'affiche indiquant que les informations ne sont pas disponibles actuellement, patientez une minute afin que la page s'actualise, ou sélectionnez le bouton Actualiser. Les données HDX nécessitent un peu plus de temps pour être mises à jour que d'autres données.

Cliquez sur une icône d'erreur ou d'avertissement pour plus d'informations.

Conseil : vous pouvez afficher des informations sur les autres canaux dans la même boîte de dialogue en cliquant sur les flèches gauche situées dans le coin gauche de la barre de titre.

Les rapports du système de canal HDX sont principalement utilisés par le support technique Citrix pour résoudre davantage de problèmes.

1. Dans le panneau HDX, cliquez sur Télécharger le rapport système.
2. Vous pouvez afficher ou enregistrer le fichier de rapport .xml.
    - Pour afficher le fichier .xml, cliquez sur Ouvrir. Le fichier .xml s'affiche dans la même fenêtre que l'application Director.
    - Pour enregistrer le fichier .xml, cliquez sur Enregistrer. La fenêtre Enregistrer sous s'affiche, vous invitant à entrer un emplacement sur la machine Director dans lequel télécharger le fichier.

Observer les utilisateurs

November 13, 2018

À partir de Director, utilisez la fonctionnalité d'observation utilisateur pour afficher et travailler directement sur la machine virtuelle ou la session d'un utilisateur. L'utilisateur doit être connecté à la machine que vous souhaitez observer. Vérifiez ceci en vérifiant le nom de la machine dans la barre de titre utilisateur.

1. Dans la vue Détails de l'utilisateur, sélectionnez la session utilisateur.
2. Activer l'observation pour la session utilisateur sélectionnée :
    - Pour la surveillance de machine, dans la vue Gestionnaire d'activités, cliquez sur Observer.
    - Pour la surveillance de session, dans la vue Détails de l'utilisateur, situez le panneau Détails de la session et cliquez sur Observer.
3. Une fois que la connexion s'initialise, une boîte de dialogue vous invite à ouvrir ou enregistrer le fichier .msrcincident.
4. Ouvrez le fichier d'incident avec la Visionneuse de l'Assistance à distance, si elle n'est pas déjà sélectionnée par défaut. Une invite de confirmation s'affiche sur la machine utilisateur.
5. Demandez à l'utilisateur de cliquer sur Oui pour démarrer la machine ou le partage de session.

Pour un contrôle supplémentaire, demandez à l'utilisateur de partager le contrôle du clavier et de la souris.

Optimiser les navigateurs Microsoft Internet Explorer pour l'observation

Configurez votre navigateur Microsoft Internet Explorer pour ouvrir automatiquement le fichier Assistance à distance Microsoft téléchargé (.msra) à l'aide du le client Assistance à distance.

Pour ce faire, vous devez activer le paramètre Demander confirmation pour les téléchargements de fichiers dans l'éditeur de stratégie de groupe :

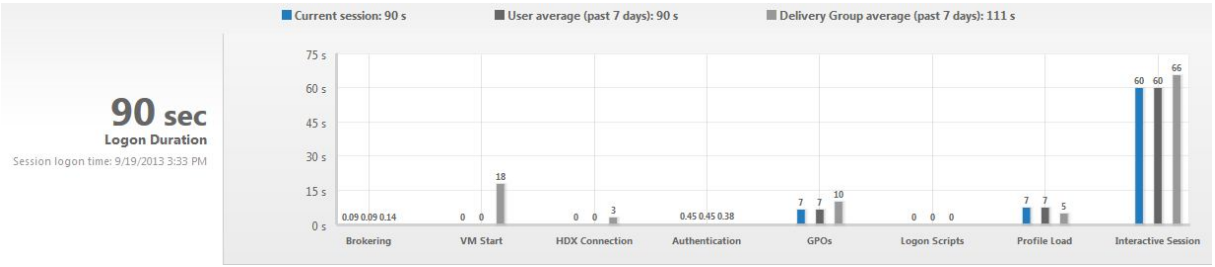
Configuration ordinateur > Modèles d'administration > Composants Windows > Internet Explorer > Panneau de configuration Internet > Page Sécurité > Zone Internet > Demander confirmation pour les téléchargements de fichiers.

Cette option est activée par défaut pour les sites de la zone d'intranet locale. Si le site Director est en dehors de la zone intranet locale, vous pouvez ajouter manuellement le site à la zone.

Diagnostiquer les problèmes de connexion utilisateur

November 13, 2018

Utilisez les données de durée d'ouverture de session pour résoudre les problèmes d'ouverture de session des utilisateurs. Dans la vue Détails de l'utilisateur, la durée est affichée sous la forme d'une valeur numérique en dessous de laquelle l'heure d'ouverture de session est affichée ainsi qu'un graphique des phases du processus d'ouverture de session.



Lorsque les utilisateurs ouvrent une session sur XenApp et XenDesktop, Monitor Service suit les phases du processus d'ouverture de session depuis la connexion de l'utilisateur à partir de Citrix Receiver jusqu'au moment où le bureau est prêt à être utilisé. Le nombre élevé sur la gauche est la durée totale d'ouverture de session et il est calculé en combinant la durée nécessaire à l'établissement de la connexion et à l'obtention d'un bureau à partir du Delivery Controller avec le temps nécessaire pour authentifier et ouvrir la session sur un bureau virtuel. Les informations de durée sont présentées en secondes (ou fractions de secondes) dans l'heure locale du navigateur Web de l'administrateur.

Utilisez ces étapes générales pour résoudre les problèmes d'ouverture de session :

1. Dans la vue **Détails de l'utilisateur**, résolvez l'état d'ouverture de session à l'aide du panneau Durée de l'ouverture de session.
   - Si l'utilisateur ouvre une session, l'affichage indique le processus d'ouverture de session.
   - Si l'utilisateur est actuellement connecté, le panneau Durée de l'ouverture de session affiche le temps qu'il a fallu à l'utilisateur pour se connecter à la session en cours.
2. Examinez les phases du processus d'ouverture de session.

Phases du processus d'ouverture de session	Description
Négociation des connexions	Durée requise pour décider quel bureau à attribuer à l'utilisateur.
Démarrage de VM	Si la session requiert le démarrage d'une machine, durée requise pour démarrer la machine virtuelle.
Connexion HDX	Durée requise pour effectuer les étapes permettant d'établir la connexion HDX du client vers la machine virtuelle.
Authentification	Durée requise pour effectuer l'authentification sur la session distante.
GPO	Si des paramètres de stratégie de groupe sont activés sur les machines virtuelles, durée requise pour appliquer les objets de stratégie de groupe.

Phases du processus d'ouverture de session	Description
Scripts de connexion	Si des scripts de connexion sont configurés pour la session, durée requise pour l'exécution des scripts de connexion.
Chargement profil	Si des paramètres de profil sont configurés pour l'utilisateur ou la machine virtuelle, durée requise pour charger le profil utilisateur.
Session interactive	Durée requise pour transférer le contrôle du clavier et de la souris à l'utilisateur après chargement du profil utilisateur. De toutes les phases du processus d'ouverture de session, il s'agit généralement de la durée la plus longue. Elle est calculée comme suit : **Durée de session interactive = heure à laquelle le bureau est prêt (EventId 1000 sur le VDA) - heure à laquelle le profil utilisateur est chargé (EventId 2 sur le VDA)**.

La durée totale d'ouverture de session n'est pas la somme exacte de ces phases. Par exemple, certaines phases se produisent en parallèle, et dans certaines phases, un traitement supplémentaire se produit pouvant entraîner une durée d'ouverture de session plus longue que la somme.

Remarque : le graphique Durée d'ouverture de session affiche les phases d'ouverture de session en secondes. Toutes les valeurs de durée inférieures à une seconde sont affichées en tant que fraction de seconde. Les valeurs supérieures à une seconde sont arrondies à la demi-seconde la plus proche. Le graphique a été conçu pour afficher la valeur la plus élevée de l'axe Y en tant que 200 secondes. Toute valeur supérieure à 200 secondes est montrée avec la valeur réelle affichée au-dessus de la barre.

Conseils de dépannage

Pour identifier les valeurs inattendues ou inhabituelles dans le graphique, comparez la durée requise lors de chaque phase de la session en cours avec la durée moyenne pour cet utilisateur au cours des sept derniers jours, et avec la durée moyenne de tous les utilisateurs dans ce groupe de mise à disposition au cours des sept derniers jours.

Faites remonter le problème si nécessaire. Par exemple, si le démarrage de la machine virtuelle est lent, le problème peut provenir de l'hyperviseur, vous pouvez donc en informer l'administrateur de l'hyperviseur. Ou, si la durée de négociation est lente, vous pouvez adresser ce problème à l'administrateur de site pour vérifier l'équilibrage de charge sur le Delivery Controller.

Examinez les différences inhabituelles, notamment :

- Barres d'ouverture de session manquantes
- Écart important entre la durée actuelle et la durée moyenne de cet utilisateur. Causes potentielles :
  - Une nouvelle application a été installée.
  - Une mise à jour du système d'exploitation s'est produite.
  - Des modifications ont été apportées à la configuration.
  - La taille du profil utilisateur est élevée. Dans ce cas, le temps de chargement du profil sera élevé.
- Écart important entre le nombre d'ouvertures de session de l'utilisateur (actuel et durée moyenne) et la durée moyenne du groupe de mise à disposition.

Si nécessaire, cliquez sur **Redémarrer** pour observer le processus d'ouverture de session de l'utilisateur pour résoudre les problèmes, tels que Démarrage de VM ou Négociation.

Enregistrer des sessions

November 13, 2018

Vous pouvez enregistrer les sessions ICA à l'aide des contrôles d'enregistrement de session sur l'écran **Détails de l'utilisateur** et **Détails de la machine** dans Director. Cette fonctionnalité est disponible pour les clients de sites **Platinum**.

Pour configurer l'enregistrement de session sur Director à l'aide de l'outil DirectorConfig, consultez la section **Configurer Director pour utiliser le serveur d'enregistrement de session** dans Installer, mettre à niveau et désinstaller un enregistrement de session.
Les contrôles d'enregistrement de session sont disponibles dans Director uniquement si l'utilisateur connecté dispose du droit de modifier les stratégies d'enregistrement de session. Ce droit peut être défini sur la Console d'autorisation d'enregistrement de session, comme décrit dans Créer et activer des stratégies d'enregistrement.
Remarque : les modifications apportées aux paramètres d'enregistrement de session depuis Director ou la Console de stratégie d'enregistrement de session prennent effet à partir de la session ICA suivante.

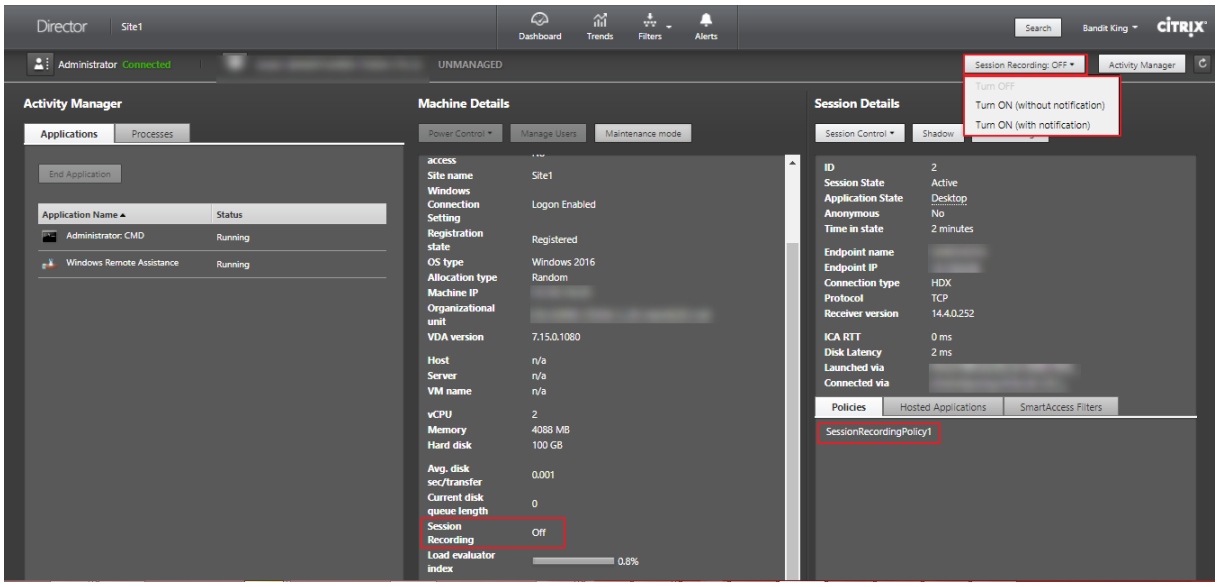
Contrôles d'enregistrement de session dans Director

Vous pouvez activer l'enregistrement de session pour un utilisateur spécifique sur l'écran **Gestionnaire d'activités** ou **Détails de l'utilisateur**. Les sessions suivantes sont enregistrées pour cet utilisateur spécifique sur tous les serveurs pris en charge.

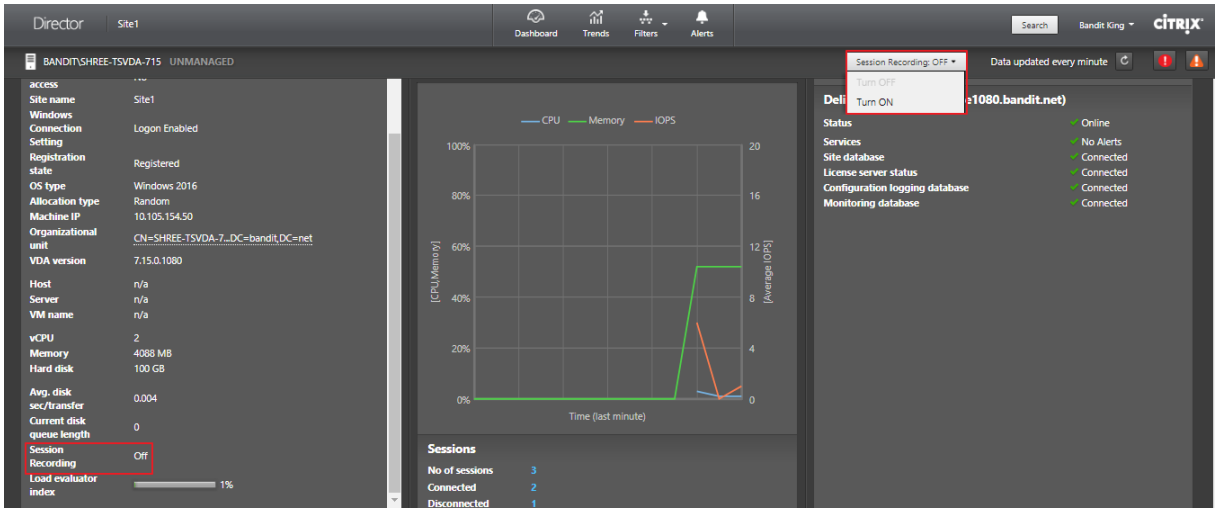
Vous pouvez :

- Activer (avec notification) : l'utilisateur est notifié de l'enregistrement de la session lorsqu'il ouvre une session ICA.
- Activer (sans notification) : la session est enregistrée de façon silencieuse sans notifier l'utilisateur.
- Désactiver : désactive l'enregistrement des sessions pour l'utilisateur.

Le panneau Stratégies affiche le nom de la stratégie d'enregistrement de session active.



Vous pouvez activer l'enregistrement de session pour une machine spécifique à partir de la page Détails de la machine. Les sessions suivantes sur la machine seront enregistrées. Le panneau Détails de la machine affiche l'état de la stratégie d'enregistrement de session pour la machine.



Restaurer les connexions aux bureaux

February 28, 2019

Dans Director, vérifiez le statut de connexion de l'utilisateur pour la machine courante dans la barre de titre utilisateur.

Si la connexion au bureau a échoué, l'erreur qui est la cause de l'échec est affichée et peut vous aider à résoudre le problème.

Action	Description
Assurez-vous que la machine n'est pas en mode de maintenance.	Sur la page Détails de l'utilisateur, assurez-vous que le mode maintenance est désactivé.
Redémarrer la machine de l'utilisateur	Sélectionnez la machine et cliquez sur Redémarrer. Utilisez cette option si la machine de l'utilisateur ne répond pas ou ne parvient pas à se connecter, comme lorsque la machine utilise une quantité élevée de ressources UC, ce qui peut rendre le processeur inutilisable.

Résoudre les échecs applicatifs

February 28, 2019

Dans la vue **Gestionnaire d'activités**, cliquez sur l'onglet **Applications**. Vous pouvez afficher toutes les applications sur toutes les machines auxquelles cet utilisateur a accès, y compris les applications locales et hébergées pour la machine actuellement connectée ainsi que l'état actuel de chaque.

Remarque : si l'onglet Applications est grisé, contactez un administrateur avec les permissions nécessaires à l'activation de l'onglet.

La liste contient uniquement ces applications qui ont été lancée dans la session.

Pour les machines avec OS de serveur et les machines avec OS de bureau, les applications sont répertoriées pour chaque session déconnectée. Si l'utilisateur n'est pas connecté, aucune application n'est affichée.

Action	Description
Arrêter l'application qui ne répond pas	Choisissez l'application qui ne répond pas et cliquez sur Fermer l'application. Lorsque l'application est arrêtée, demandez à l'utilisateur de la démarrer à nouveau.
Arrêter les processus qui ne répondent pas	Si vous avez les permissions requises, cliquez sur l'onglet Processus. Sélectionnez un processus lié à l'application ou qui utilise une quantité importante de ressources UC ou de mémoire, et cliquez sur Mettre fin au processus. Toutefois, si vous ne possédez pas les permissions nécessaires pour mettre fin au processus, une tentative d'arrêt d'un processus échouera.
Redémarrer la machine de l'utilisateur	Pour les machines avec OS de bureau, pour la session sélectionnée, cliquez sur Redémarrer. Éventuellement, à partir de la vue de Détails de machine, utilisez la puissance des contrôles pour arrêter ou redémarrer la machine. Demandez aux utilisateurs de rouvrir une session afin que vous puissiez vérifier de nouveau l'application. Pour les machines avec OS de serveur, l'option de redémarrage n'est pas disponible. Au lieu de cela, fermez la session de l'utilisateur et laissez l'utilisateur rouvrir une session.
Placer la machine en mode de maintenance	Si l'image de la machine nécessite une maintenance, telle que l'installation d'un correctif ou d'autres mises à jour, placez la machine en mode de maintenance. Dans la vue Détails de machine, cliquez sur Détails et activez l'option du mode de maintenance. Informez l'administrateur du problème.

Réinitialiser un profil utilisateur

November 13, 2018

Avertissement : si un profil est réinitialisé, bien que les dossiers et les fichiers de l'utilisateur soient enregistrés et copiés dans le nouveau profil, la plupart des données de profil utilisateur sont supprimées (par exemple, le Registre est réinitialisé et les paramètres d'application peuvent être supprimés).

1. À partir de Director, recherchez l'utilisateur dont vous voulez réinitialiser le profil et sélectionnez la session de cet utilisateur.
2. Cliquez sur **Réinitialiser le profil**.
3. Demandez à l'utilisateur de fermer toutes ses sessions.
4. Demandez à l'utilisateur de rouvrir une session. Les dossiers et fichiers qui ont été enregistrés depuis le profil de l'utilisateur sont copiés dans le nouveau profil.
   Important : si l'utilisateur possède des profils sur des plates-formes multiples (telles que Windows 8 et Windows 7), demandez à l'utilisateur de rouvrir une session tout d'abord sur le même bureau ou application que l'utilisateur a signalé comme un problème. Ceci garantit que le profil approprié est réinitialisé.
   Si le profil est un profil utilisateur Citrix, le profil est déjà réinitialisé lorsque le bureau de l'utilisateur s'affiche. Si le profil est un profil itinérant Microsoft, la restauration du dossier est peut-être toujours en cours d'exécution pendant un court instant. L'utilisateur doit rester connecté jusqu'à ce que la restauration soit terminée.

Remarque : les étapes précédentes supposent que vous utilisiez XenDesktop (VDA de bureau). Si vous utilisez XenApp (VDA de serveur), vous devez être connecté pour réinitialiser le profil. L'utilisateur doit ensuite se déconnecter et se reconnecter pour terminer la réinitialisation du profil.

Si le profil n'est pas correctement réinitialisé (par exemple, l'utilisateur ne peut pas correctement ouvrir une session à nouveau sur la machine ou certains fichiers sont manquants), vous devez manuellement restaurer le profil d'origine.

Les dossiers (et leurs fichiers) provenant du profil de l'utilisateur sont enregistrés et copiés vers le nouveau profil. Ils sont copiés dans l'ordre indiqué :

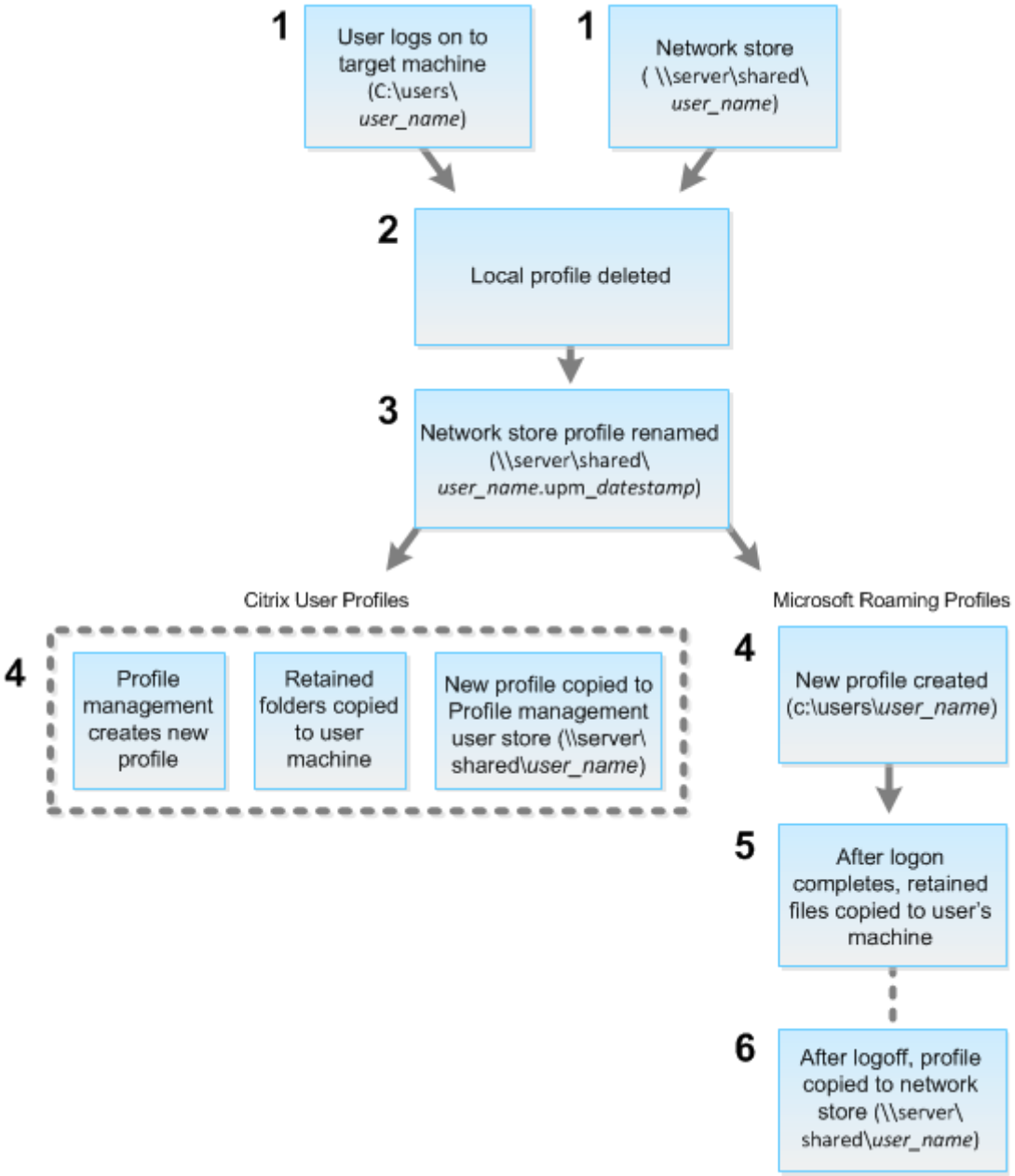
- Bureau
- Cookies
- Favoris
- Documents
- Images
- Musique
- Vidéos

Remarque : dans Windows 8 ou version ultérieure, les cookies ne sont pas copiés lorsque les profils sont réinitialisés.

Comment les profils réinitialisés sont traités

Tout profil utilisateur Citrix ou profil itinérant Microsoft peut être réinitialisé. Lorsque l'utilisateur ferme sa session et que vous sélectionnez la commande de réinitialisation (dans Director ou en utilisant le kit de développement PowerShell), Director identifie d'abord le profil utilisateur en cours d'utilisation et délivre une commande de réinitialisation appropriée. Director reçoit les informations au travers de Profile Management, y compris les informations sur la taille, le type et la durée d'ouverture de session du profil.

Ce diagramme illustre le processus qui suit la connexion de l'utilisateur.



1. La commande de réinitialisation émise par Director spécifie le type de profil. Le service Profile Management, tente ensuite de réinitialiser un profil de ce type et recherche le partage réseau approprié (magasin de l'utilisateur). Si l'utilisateur est traité par Profile Management, mais reçoit une commande de profil itinérant, elle est rejetée (et vice versa).
2. Si un profil local est présent, il est supprimé.
3. Le profil réseau est renommé.
4. L'action suivante dépend du fait que le profil en cours de réinitialisation est un profil utilisateur Citrix ou un profil itinérant Microsoft.
    - Pour les profils utilisateur Citrix, le nouveau profil est créé à l'aide des règles d'importation de Profile Management, et les dossiers sont copiés dans le profil réseau, et l'utilisateur peut ouvrir une session normalement. Si un profil itinérant est utilisé pour la réinitialisation, tous les paramètres de registre du profil itinérant sont conservés dans le profil de réinitialisation.
      Remarque : vous pouvez configurer Profile Management de manière à ce qu'un profil modèle remplace le profil itinérant, si nécessaire.
    - Pour les profils itinérants Microsoft, un nouveau profil est créé par Windows, et lorsque l'utilisateur ouvre une session, les dossiers sont copiés vers la machine utilisateur. Lorsque l'utilisateur ferme une session, le profil est copié sur le magasin réseau.

Pour restaurer un profil manuellement après un échec de réinitialisation

1. Demandez à l'utilisateur de fermer toutes ses sessions.
2. Supprimez le profil local s'il en existe un.
3. Recherchez le dossier archivé sur le partage réseau contenant la date et l'heure ajoutées au nom du dossier, le dossier avec une extension .upm_horodatage.
4. Supprimez le nom de profil courant ; c'est-à-dire, celui sans extension upm_horodatage.
5. Renommez le dossier archivé en utilisant le nom de profil d'origine. En d'autres termes, supprimez l'extension d'horodatage. Vous avez retourné le profil à son état d'origine, pré-réinitialisation.

Résolution des problèmes d'applications

November 13, 2018

Surveillance des applications en temps réel

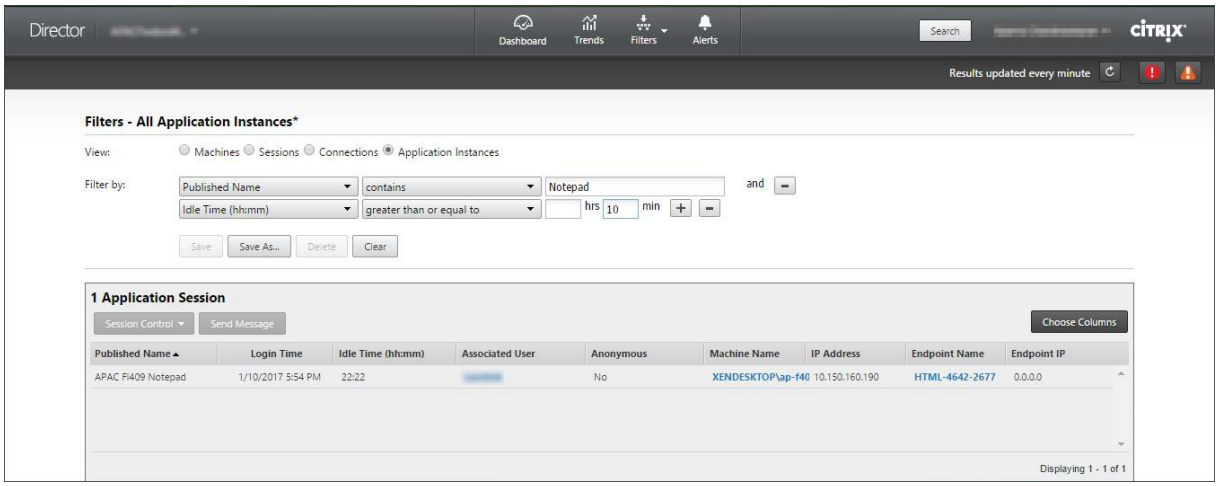
Vous pouvez résoudre les problèmes d'applications et de sessions à l'aide de la mesure de délai d'inactivité pour identifier les instances qui restent inactives au-delà d'une durée spécifique.

Le secteur de la santé, dans lequel les employés partagent les licences d'application, représente un cas d'utilisation typique pour la résolution de problèmes d'applications. En effet, vous devez mettre fin aux instances d'applications et aux sessions inactives pour purger l'environnement XenApp et XenDesktop, pour reconfigurer les serveurs avec problèmes de performances, ou pour gérer et mettre à niveau les applications.

La page de filtre **Instances d'application** répertorie toutes les instances d'application sur les VDA d'OS de serveur et de bureau. Les mesures de délai d'inactivité associées sont affichées pour les instances d'application sur VDA d'OS de serveur qui sont inactives depuis au moins 10 minutes.

Remarque : les mesures Instances d'application sont disponibles sur les sites de toutes les éditions de licence.

Utilisez ces informations pour identifier les instances d'application qui restent inactives au-delà d'une période de temps spécifique et mettez fin à la session ou déconnectez-les en fonction des besoins. Pour ce faire, sélectionnez **Filtres > Instances d'application** et sélectionnez un filtre pré-enregistré ou choisissez **Toutes les instances d'application** et créez votre propre filtre.

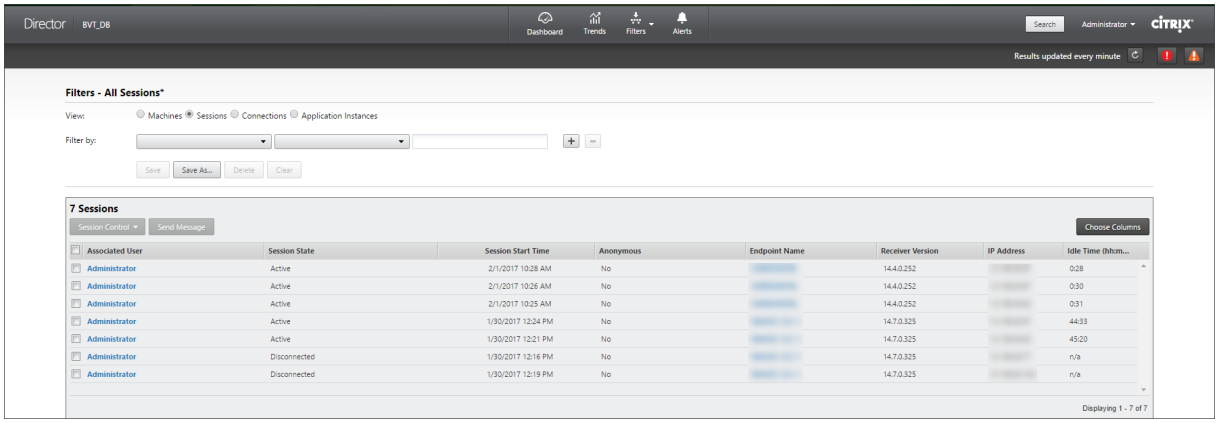


Voici un exemple de filtre. Comme critère **Filtrer par**, choisissez **Nom publié** (de l'application) et **Durée d'inactivité**. Définissez ensuite la **durée d'inactivité** sur **supérieur ou égal à** un délai spécifique et enregistrez le filtre pour une éventuelle réutilisation. Dans la liste filtrée, sélectionnez les instances d'application. Sélectionnez l'option pour envoyer des messages ou à partir du menu déroulant **Contrôle de la session**, choisissez **Fermer la session** ou **Déconnecter** pour mettre fin aux instances.

Remarque : la fermeture de session ou la déconnexion d'une instance d'application ferme ou déconnecte la session en cours, ce qui entraîne l'arrêt de toutes les instances d'application qui appartiennent à la même session.

Vous pouvez identifier les sessions inactives dans la page de filtre **Sessions** à l'aide des informations d'état de session et de mesure de durée d'inactivité de session. Triez selon la colonne **Délai d'inactivité** ou définissez un filtre pour identifier les sessions qui restent inactives au-delà d'une

durée spécifique. Le délai d'inactivité est indiqué pour les sessions sur VDA d'OS de serveur qui sont inactives depuis au moins 10 minutes.



Le **délai d'inactivité** s'affiche en tant que **N/A** lorsque l'instance de la session ou de l'application

- n'a pas été inactive pendant plus de 10 minutes,
- est démarrée sur un VDA d'OS de bureau, ou
- est démarrée sur un VDA exécutant la version 7.12 ou antérieure.

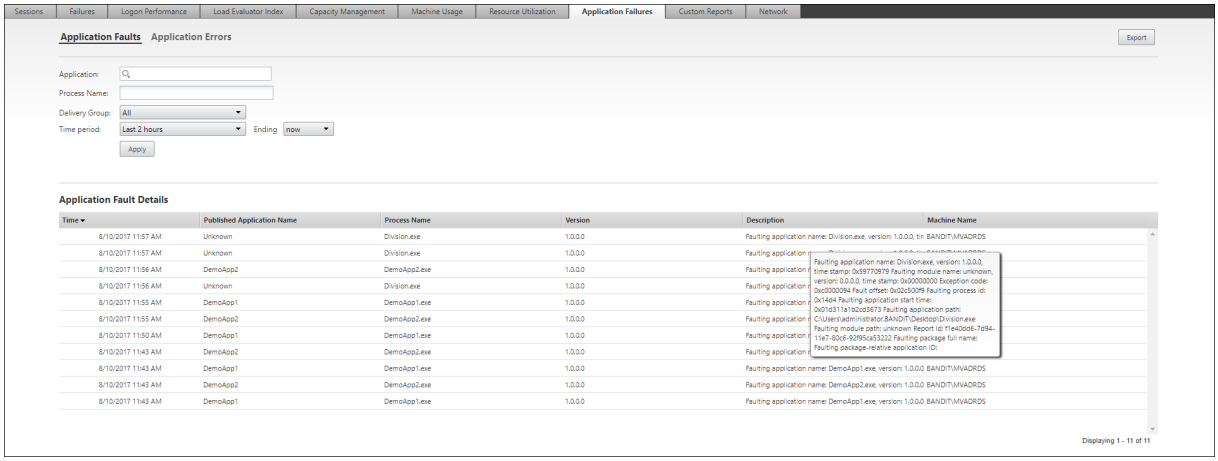
Historique de détection des défaillances applicatives

L'onglet **Tendances** -> **Échecs applicatifs** affiche les échecs associés aux applications publiées sur les VDA.

Les tendances d'échecs applicatifs sont disponibles pour les 2 dernières heures, 24 dernières heures, 7 derniers jours et le dernier mois pour les sites sous licence Platinum et Enterprise. Elles sont disponibles pour les 2 dernières heures, 24 dernières heures et 7 derniers jours pour les autres types de licence. Les échecs applicatifs qui sont consignés dans l'Observateur d'événements avec la source « Erreurs applicatives » seront surveillés. Cliquez sur **Exporter** pour générer des rapports aux formats CSV, Excel ou PDF

Les paramètres de rétention de nettoyage pour la détection des échecs applicatifs, GroomApplicationErrorsRetentionDays et GroomApplicationFaultsRetentionDays, sont configurés sur un jour par défaut pour les sites avec licence Platinum et non-Platinum. Vous pouvez modifier ce paramètre à l'aide de la commande PowerShell :

```
1 *Set-MonitorConfiguration -\<nom de paramétre\> \<valeur\>*
```

Les échecs sont affichés en tant que **Défaillances applicatives** ou **Erreurs applicatives** en fonction de leur niveau de gravité. L'onglet Défaillances applicatives affiche les échecs associés à la perte de données ou de fonctionnalité. Les erreurs applicatives indiquent des problèmes qui ne sont pas immédiats ; ils indiquent des conditions qui peuvent entraîner des problèmes futurs.

Vous pouvez filtrer les échecs selon les paramètres **Nom de l'application publiée**, **Nom du processus** ou **Groupe de mise à disposition** et **Période**. Le tableau affiche le code d'erreur ou d'incident et une brève description de l'échec. La description détaillée de l'échec s'affiche en tant qu'info-bulle.

Remarque : le nom de l'application publiée est affiché comme « Inconnu » lorsque le nom de l'application correspondante ne peut pas être déterminé. Cela se produit généralement lorsqu'une application publiée échoue dans une session de bureau, ou lorsqu'elle échoue en raison d'une exception non prise en charge causée par un exécutable dépendant.

Par défaut, seuls les échecs d'applications hébergées sur des VDA avec OS de serveur sont détectés. Vous pouvez modifier les paramètres de détection dans les stratégies de groupe de surveillance : Activer la détection des défaillances applicatives et Activer la détection des défaillances applicatives sur les VDA d'OS de bureau et Liste des applications exclues de la détection des défaillances. Pour de plus amples informations, consultez la section Stratégies pour la détection des défaillances applicatives dans Paramètres de stratégie Surveillance.

Dépanner les machines

November 13, 2018

Dans la vue **Filtres** > **Machines**, sélectionnez **Machines avec OS de bureau** ou **Machines avec OS de serveur** pour voir les machines configurées sur le site. L'onglet Machines avec OS de serveur comprend l'indice de calculateur de charge, qui indique la distribution des compteurs de performances et les info-bulles du nombre de sessions si vous survolez le lien avec la souris.

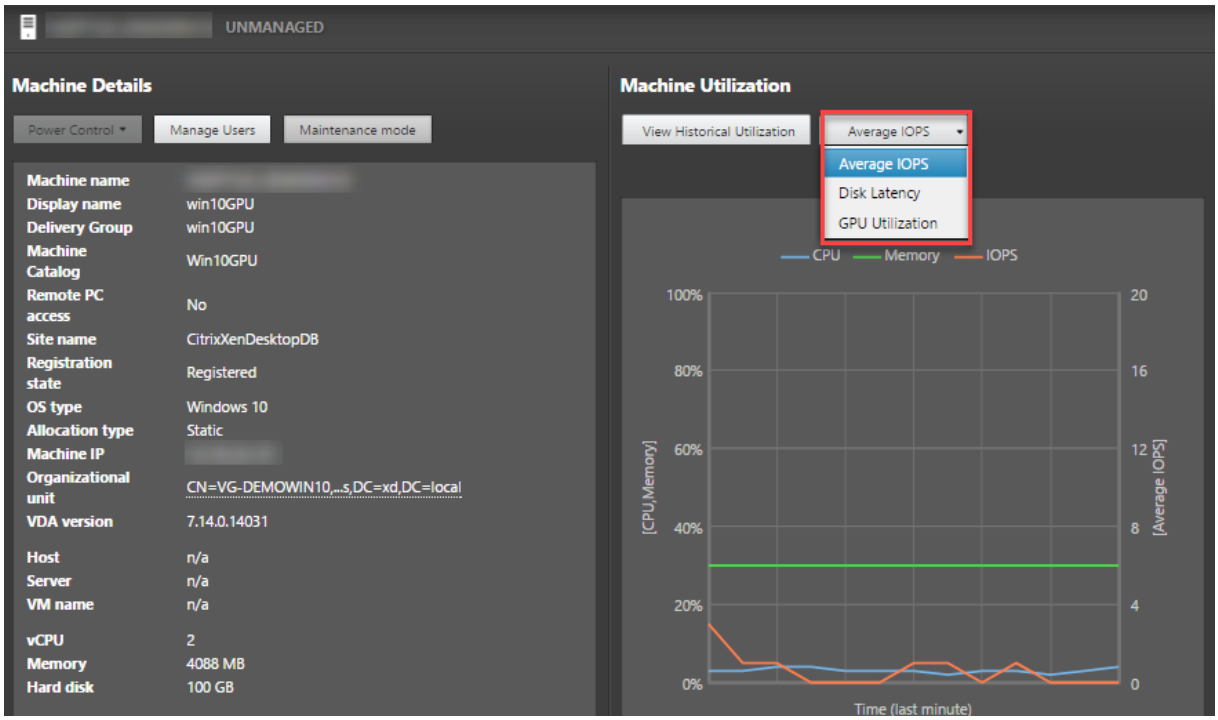
Cliquez sur **Raison de l'échec** pour une machine en échec afin d'obtenir une description détaillée de l'échec et des actions recommandées pour résoudre le problème. Les raisons de l'échec et les actions recommandées pour des défaillances de machines et de connexion sont disponibles dans le Citrix Director 7.12 Failure Reasons Troubleshooting Guide.

Cliquez sur le lien du nom d'une machine pour accéder à la page **Détails de la machine**. La page Détails de la machine présente les détails de la machine, les détails de l'infrastructure, et les détails des correctifs appliqués sur la machine. Le panneau **Utilisation de machine** affiche les graphiques d'utilisation de machine.

Utilisation des ressources en temps réel par machine

Le panneau **Utilisation de machine** affiche des graphiques montrant l'utilisation en temps réel du CPU et de la mémoire. En outre, les graphiques de surveillance de GPU et de disque sont disponibles pour les sites avec Delivery Controller et VDA version **7.14** ou ultérieure.

Les graphiques de surveillance de disque, les nombres moyens d'E/S par seconde et la latence du disque sont des mesures importantes de performance qui vous aident à surveiller et à résoudre les problèmes liés aux disques VDA. Le graphique Nbre moyen d'E/S par seconde affiche le nombre moyen de lectures et d'écritures sur un disque. Sélectionnez **Latence de disque** pour afficher un graphique du délai entre une requête de données et son retour à partir du disque, mesuré en millisecondes.



Sélectionnez **Utilisation du GPU** pour afficher le pourcentage d'utilisation du GPU, de la mémoire du GPU et de l'encodeur et du décodeur afin de résoudre les problèmes liés au GPU sur des VDA avec

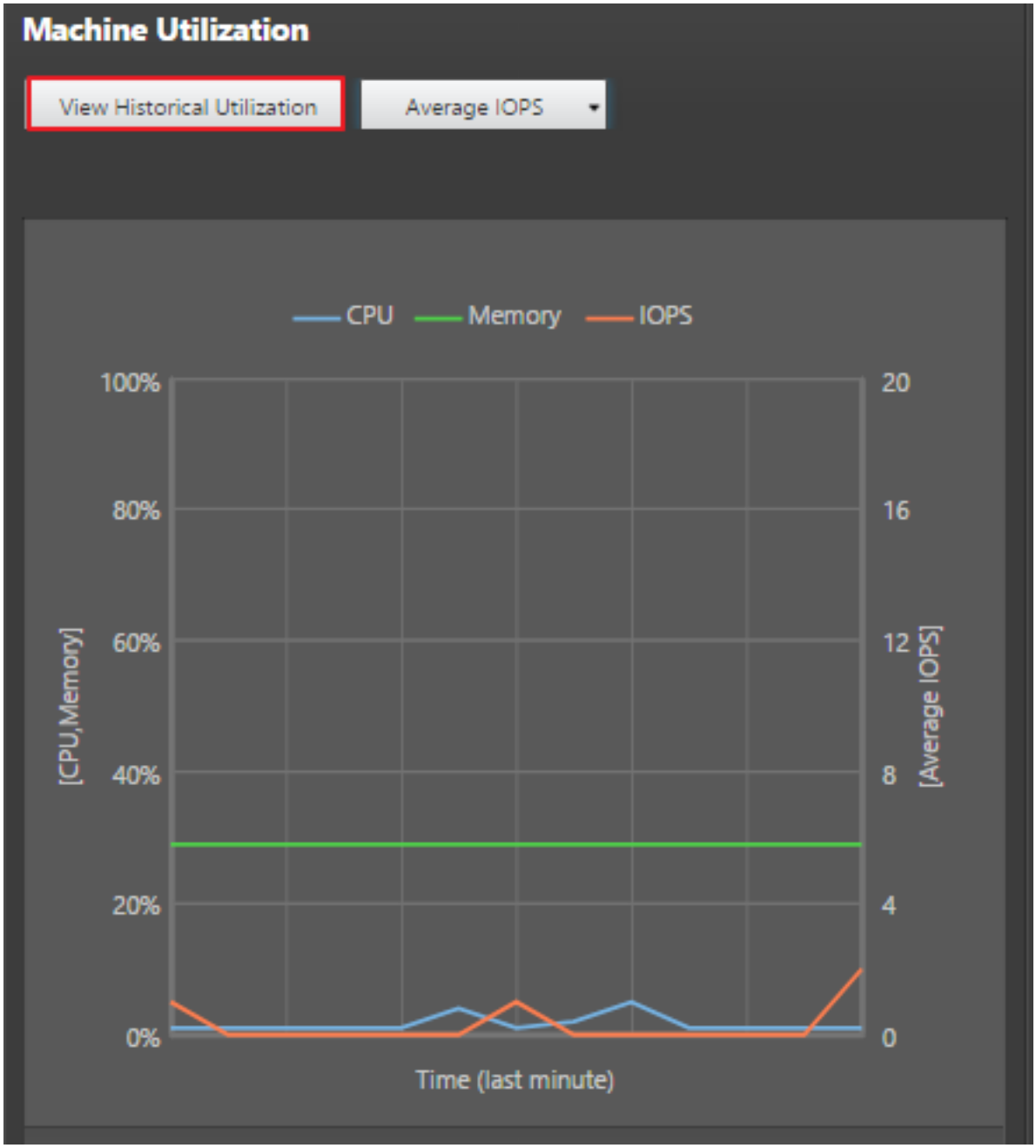
OS de bureau ou de serveur. Les graphiques Utilisation du GPU sont disponibles uniquement sur les VDA exécutant Windows 64 bits, avec GPU NVIDIA Tesla M60 et un pilote d'affichage version 369.17 ou version ultérieure.
HDX 3D Pro doit être activé sur le VDA pour que ce dernier puisse proposer l'accélération GPU. Pour de plus amples informations, consultez les sections Accélération GPU pour OS de bureau Windows et Accélération GPU pour OS de serveur Windows.
Lorsqu'un VDA accède à plusieurs GPU, le graphique d'utilisation affiche la moyenne des mesures de GPU collectées à partir des GPU individuels. Les mesures GPU sont collectées pour le VDA complet et non pour des processus individuels.

Utilisation des ressources historiques par machine

Dans le panneau **Utilisation de machine**, cliquez sur **Afficher utilisation historique** pour afficher l'historique d'utilisation des ressources sur la machine sélectionnée.
Les graphiques d'utilisation comprennent les compteurs de performance critiques de CPU, de mémoire, de sessions simultanées maximales, de nombre moyen d'E/S par seconde et de latence du disque.

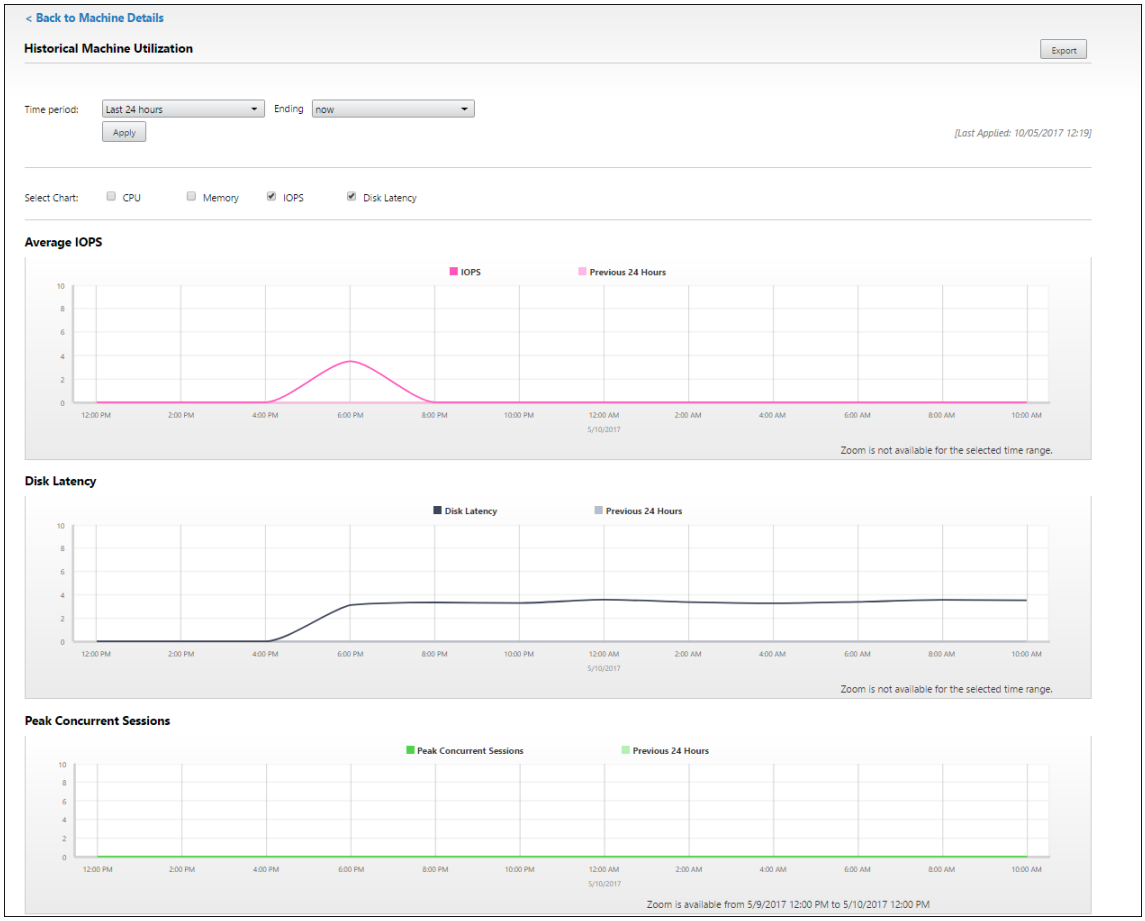
Remarque : le paramètre de stratégie Surveillance, **Activer le suivi des processus**, doit être défini sur Autorisé pour collecter et afficher les données dans le tableau des 10 processus les plus utilisés sur la page Utilisation historique des machines. La collecte n'est pas autorisée par défaut.

Les données d'utilisation de l'UC et de la mémoire, du nombre moyen d'E/S par seconde et de latence de disque sont collectées par défaut. Vous pouvez désactiver la collecte à l'aide du paramètre de stratégie **Activer le suivi des ressources**.



1. Dans le panneau **Utilisation de machine** de la vue de **Détails de machine**, sélectionnez **Afficher utilisation historique**. Cette action ouvre la page **Utilisation historique des machines**.
2. Définissez la **période d'affichage** : 2 dernières heures, 24 dernières heures, 7 derniers jours, dernier mois ou dernière année.
   Remarque : les données de nombre moyen d'E/S par seconde et d'utilisation de latence de disque sont disponibles uniquement pour les 24 dernières heures, le dernier mois et l'année se terminant. L'heure de fin personnalisée n'est pas prise en charge.
3. Cliquez sur **Appliquer** et sélectionnez les graphiques requis.

4. Placez le pointeur de la souris sur les différentes sections du graphique pour afficher de plus amples informations sur la période sélectionnée.



   Par exemple, si vous sélectionnez les **2 dernières heures**, la période de référence correspond aux 2 heures avant l'intervalle sélectionné. Affichez la tendance d'UC, de mémoire et de session au cours des 2 dernières heures et de la période de référence.
   Si vous sélectionnez **Mois dernier**, la période de référence est le mois précédent. Sélectionnez cette option pour afficher le nombre moyen d'E/S par seconde et la latence de disque au cours du dernier mois et la période de référence.

5. Cliquez sur **Exporter** pour exporter les données d'utilisation des ressources pendant la période sélectionnée. Pour de plus amples informations, consultez la section Exporter des rapports dans Surveiller les déploiements.

6. Sous les graphiques, le tableau dresse la liste des 10 processus utilisant le plus d'UC ou de mémoire. Vous pouvez trier par colonne pour la durée sélectionnée : nom de l'application, nom d'utilisateur, ID de session, utilisation moyenne et max. de l'UC et utilisation moyenne et max. de la mémoire. Les colonnes E/S par seconde et Latence de disque ne peuvent pas être triées.

   Remarque : l'ID de session pour les processus système s'affiche en tant que « 0000 ».

7. Pour afficher les tendances historiques de consommation de ressources d'un processus particulier, accédez aux détails d'un des 10 processus les plus utilisés.

Tableau de compatibilité des fonctionnalités

January 23, 2019

Dans chaque site, bien que vous puissiez utiliser des versions antérieures de VDA ou de Delivery Controller, certaines fonctionnalités de la version la plus récente de Director risquent de ne pas être disponibles. En outre, la disponibilité des fonctionnalités dépend de l'édition de la licence du site. Citrix vous recommande d'installer les mêmes versions pour Director, Delivery Controller et VDA.

Remarque : après avoir mis à niveau un Delivery Controller, vous êtes invité à mettre à niveau le site lorsque vous ouvrez Studio. Pour plus d'informations, veuillez consulter la section **Séquence de mise à niveau** dans Mettre un déploiement à niveau.

Le tableau ci-dessous dresse la liste des fonctionnalités de Director et de la version minimale des Delivery Controller (DC), VDA et autres composants dépendants requis ainsi que l'édition de la licence.

Version de Director	Fonctionnalité	Dépendances - version min requise	Édition
7.15	Détection des défaillances applicatives	DC 7.15 et VDA 7.15	Toutes
7.14	Résolution des problèmes centrée sur les applications	DC 7.13 et VDA 7.13	Toutes
7.14	Contrôle des disques	DC 7.14 et VDA 7.14	Toutes
7.14	Suivi GPU	DC 7.14 et VDA 7.14	Toutes
7.13	Protocole de transport sur le panneau Détails de la session	DC 7.x et VDA 7.13	Toutes
7.12	Descriptions claires des échecs de connexion et de machine	DC 7.12 et VDA 7.x	Toutes

Version de Director	Fonctionnalité	Dépendances - version min requise	Édition
7.12	Optimisation des données historiques disponibles dans l'édition Enterprise	DC 7.12 et VDA 7.x	Entreprise
7.12	Rapports personnalisés	DC 7.12 et VDA 7.x	Platinum
7.12	Automatiser les notifications Director avec des interruptions SNMP	DC 7.12 et VDA 7.x	Platinum
7.11	Rapports d'utilisation des ressources	DC 7.11 et VDA 7.11	Toutes
7.11	Alertes étendues pour les conditions CPU, mémoire et RTT ICA	DC 7.11 et VDA 7.11	Platinum
7.11	Amélioration de l'exportation des rapports	DC 7.11 et VDA 7.x	Toutes
7.11	Automatiser les notifications Director avec Citrix Octoblu	DC 7.11 et VDA 7.x	Platinum
7.11	Intégration avec NetScaler MAS	DC 7.11, VDA 7.x et MAS version 11.1 Build 49.16	Platinum
7.9	Répartition de la durée d'ouverture de session	DC 7.9 et VDA 7.x	Toutes
7.7	Analyse et alertes proactives	DC 7.7 et VDA 7.x	Platinum
7.7	Intégration SCOM	DC 7.7, VDA 7.x, SCOM 2012 R2 et PowerShell 3.0	Platinum

Version de Director	Fonctionnalité	Dépendances - version min requise	Édition
7.7	Intégration de l'authentification Windows	DC 7.x et VDA 7.x	Toutes
7.7	Utilisation des OS de bureau et de serveur	DC 7.7 et VDA 7.x	Platinum
7.6.300	Prise en charge du canal virtuel Framehawk	DC 7.6 et VDA 7.6	Toutes
7.6.200	Intégration d'enregistrement de session	DC 7.6 et VDA 7.x	Platinum
7	Intégration de HDX Insight	DC 7.6, VDA 7.x et NetScaler Insight Center	Platinum

Granularité de données et rétention

January 23, 2019

Agrégation des valeurs de données

Le service Monitor collecte les données, notamment l'utilisation de la session utilisateur, les détails des performances de l'ouverture de session utilisateur, les détails de l'équilibrage de charge de la session, et les informations de connexion et d'échec de machine. Les données sont agrégées différemment en fonction de leur catégorie. La compréhension de l'agrégation des valeurs de données présentées à l'aide de l'API OData Method est critique à l'interprétation des données. Par exemple :

- Les sessions connectées et les échecs de machine se produisent sur une période de temps. Ils sont donc exposés comme valeurs maximales sur une période de temps.
- La durée d'ouverture de session est une mesure de durée, par conséquent elle est exposée en tant que moyenne sur une période de temps.
- Le nombre d'ouvertures de session et les échecs de connexion représentent des nombres d'occurrences sur une période de temps, et par conséquent sont exposés en tant que sommes sur une période de temps.

Évaluation des données simultanées

Les sessions doivent se chevaucher pour être considérées comme simultanées. Toutefois, lorsque l'intervalle de temps est de 1 minute, toutes les sessions de cette minute (si elles se chevauchent ou non) sont considérées comme simultanées, la taille de l'intervalle est si petite que la surcharge de performances impliquée dans le calcul de la précision ne vaut pas la valeur ajoutée. Si les sessions se produisent dans la même heure, mais pas dans la même minute, elles ne sont pas considérées comme se chevauchant.

Corrélation de tables de synthèse avec des données brutes

Le modèle de données représente des métriques de deux manières différentes :

- Les tables de synthèse représentent des vues des mesures détaillées de l'agrégation par minute, heure et jour.
- Les données brutes représentent des événements individuels ou l'état actuel de l'objet suivi dans la session, la connexion, l'application et autres objets.

Lorsque vous tentez de corréler les données dans les appels API ou dans le modèle de données lui-même, il est important de bien comprendre les concepts et les limitations suivantes :

- **Aucune données de synthèse pour les intervalles partiels.** Des résumés de métriques sont conçus pour répondre aux besoins de tendances historiques sur de longues périodes. Les métriques sont agrégées dans la table de synthèse pour effectuer des intervalles. Il y aura pas de données de synthèse pour un intervalle partiel au début (les plus anciennes données disponibles) de la collection de données ni à la fin. Lorsque vous affichez les agrégations d'une journée (intervalle = 1 440), ceci signifie que la premier et le dernier jour incomplet ne possède pas de données. Bien que des données brutes puissent exister pour des intervalles partiels, elles ne seront jamais synthétisées. Vous pouvez déterminer le premier et le dernier intervalle d'agrégation pour une granularité de données particulière en extrayant les valeurs minimales et maximales de SummaryDate pour une table de synthèse particulière. La colonne SummaryDate représente le début de l'intervalle. La colonne Granularité représente la durée de l'intervalle pour les données agrégées.
- **Corrélation par heure.** Les métriques sont agrégées dans la table de synthèse pour terminer les intervalles comme décrit ci-dessus. Ils peuvent être utilisés pour les tendances historiques, mais les événements bruts peuvent être plus actifs dans l'état de ce qui a été résumé pour l'analyse de tendances. Toute comparaison temporelle de synthèse des données brutes doit prendre en compte le fait qu'aucune donnée de synthèse pour les intervalles partiels susceptibles de se produire ou pour le début et la fin de la période de temps.
- **Événements manqués et latents.** Les mesures qui sont agrégées dans la table de synthèse peuvent être légèrement inexactes si les événements sont manqués ou latents pour la période d'agrégation. Bien que le service Monitor tente de conserver un état courant précis, il ne

retourne pas dans le temps pour recalculer l'agrégation dans les tables de synthèse pour les événements manqués ou latents.

- **Haute disponibilité de connexion.** Lors de la haute disponibilité de connexion, il existera des espaces dans les données de synthèse du nombre de connexions actives, mais les instances de session seront toujours en cours d'exécution dans les données brutes.
- **Périodes de rétention des données.** Les données des tables de synthèse sont conservées sur un programme de nettoyage différent du programme des données brutes d'événement. Il se peut que les données soient manquantes, car elles ont été effacées depuis les tables de données de synthèse ou brutes. Les périodes de rétention peuvent également différer pour différentes granularités de données de synthèse. Les données de granularité inférieures (en minutes) sont nettoyées plus rapidement que les données de granularité supérieures (en jours). Si des données sont manquantes dans une granularité à cause du nettoyage, elles peuvent être détectées dans une meilleure granularité. Étant donné que les appels API retournent uniquement la granularité demandée, l'absence de réception de données pour un niveau de granularité ne signifie pas que les données n'existent pas pour une meilleure granularité pour la même période.
- **Fuseaux horaires.** Les métriques sont stockées avec des horodatages UTC. Les tables de synthèse sont regroupées sur des limites de fuseau horaire. Pour les zones qui ne se trouvent pas dans les limites horaires, il se peut qu'il existe une différence pour laquelle les données sont agrégées.

Granularité et rétention

La granularité des données agrégées récupérées par Director est une fonction de la période de temps (T) demandée. Les règles sont les suivantes :

- 0 < T <= 1 heure utilise une granularité minute par minute
- 0 < T <= 30 jours utilise une granularité heure par heure
- T > 31 jours utilise une granularité jour par jour

Les données requises qui ne proviennent pas de données agrégées proviennent de la session brute et des informations de connexion. Ces données ont tendance à croître rapidement, et par conséquent, disposent de leur propre paramètre de nettoyage. Le nettoyage garantit que seules les données appropriées sont conservées à long terme. Cela garantit de meilleures performances tout en conservant la granularité nécessaire pour la création de rapports. Les clients sur sites avec licence Platinum peuvent modifier la rétention de nettoyage sur leur nombre de jours de rétention désirés, sinon, la valeur par défaut est utilisée.

Pour accéder aux paramètres, exécutez les commandes PowerShell suivantes sur le Delivery Controller :

```
asnp Citrix.*
 Get-MonitorConfiguration
```



```
Set-MonitorConfiguration -<setting name> <value>
```

Les paramètres suivants sont utilisés pour contrôler le nettoyage :

	Nom du paramètre	Nettoyage affecté	Valeur par défaut Platinum (jours)	Valeur par défaut non Platinum (jours)
1	GroomSessionsRe	Rétention des enregistrements de session et de connexion après la fermeture de session	90	7
2.	GroomFailuresRetentionDays	Enregistrements MachineFail-ureLog et ConnectionFail-ureLog	90	7
3	GroomLoadIndexe	Enregistrements LoadIndex	90	7
4	GroomDeletedRetentionDays	Les entités Machine, Catalog, DesktopGroup et Hypervisor qui possèdent un LifecycleState « Supprimé ». Cette opération supprime également tout enregistrement Session, SessionDetail, Summary, Failure ou LoadIndex.	90	7

	Nom du paramètre	Nettoyage affecté	Valeur par défaut Platinum (jours)	Valeur par défaut non Platinum (jours)
5	GroomSummaries	Enregistrements DesktopGroup-Summary, FailureLogSum-mary et LoadIndexSum-mary. Données agrégées : granularité quotidienne.	90	7
6	GroomMachineHotfixLogRetentionDays	Durée de conservation à chaud appliquées aux machines VDA et Controller	90	90
7	GroomMinuteRete	Données agrégées : granularité par minute	3	3
8	GroomHourlyRetentionDays	Données agrégées : granularité horaire	32	7
9	GroomApplication	Historique des instances d'application	90	0
10	GroomNotificationLogRetentionDays	Enregistrements de journal de notification	90	
11	GroomResourceUs	Données d'utilisation des ressources : données brutes	1	1

	Nom du paramètre	Nettoyage affecté	Valeur par défaut Platinum (jours)	Valeur par défaut non Platinum (jours)
12	GroomResourceUsageMinutesDataRetentionDays	Données de synthèse d'utilisation des ressources : granularité par minute	7	7
13	GroomResourceUsageHourlyDataRetentionDays	Données de synthèse d'utilisation des ressources : granularité par heure	30	7
14	GroomResourceUsageDailyDataRetentionDays	Données de synthèse d'utilisation des ressources : granularité par jour	90	7
15	GroomProcessUsageRawDataRetentionDays	Données d'utilisation des processus : données brutes	1	1
16	GroomProcessUsageMinutesDataRetentionDays	Données d'utilisation des processus : granularité par minute	3	3
17	GroomProcessUsageHourlyDataRetentionDays	Données d'utilisation des processus : granularité par heure	7	7

	Nom du paramètre	Nettoyage affecté	Valeur par défaut Platinum (jours)	Valeur par défaut non Platinum (jours)
18	GroomProcessUsageRawDataRetentionDays	Données d'utilisation des processus : granularité par jour	30	7
19	GroomSessionMet	Données de mesure de session	7	7
20	GroomMachineMetricDataRetentionDays	Données de mesure de machine	3	3
21	GroomMachineMe	Données de synthèse de mesure de machine	90	7
22	GroomApplicationErrorsRetentionDays	Données d'erreur d'application	1	1
.	GroomApplication	Données d'échec d'application	1	1

Avertissement : la modification des valeurs de la base de données du service Monitor nécessite le redémarrage du service pour que les nouvelles valeurs prennent effet. Vous êtes invités à apporter des modifications à la base de données du service Monitor uniquement avec l'assistance de Citrix.

Notes sur la rétention de nettoyage :

- Sites sous licence Platinum : vous pouvez mettre à jour les paramètres de rétention de nettoyage ci-dessus et spécifier le nombre de jours que vous souhaitez.
  - Exception : GroomApplicationErrorsRetentionDays et GroomApplicationFaultsRetention-Days sont limités à 31 jours. GroomProcessUsageRawDataRetentionDays est limité à 1 jour.
- Sites sous licence Enterprise : la rétention de nettoyage est limitée à 31 jours pour tous les paramètres.
- Tous les autres sites : la rétention de nettoyage est limitée à 7 jours pour tous les paramètres.

La conservation de données pendant de longues périodes aura les conséquences suivantes sur la taille

des tables :

- **Données horaires.** Si les données horaires sont autorisées à rester dans la base de données pour un maximum de deux années, un site de 1 000 groupes de mise à disposition peut influencer la croissance de la base de données comme suit :

  1 000 groupes de mise à disposition x 24 heures/jour x 365 jours/an x 2 ans = 17 520 000 lignes de données. L'impact sur les performances d'une telle quantité importante de données dans les tables d'agrégation est significatif. Étant donné que les données du tableau de bord sont tirées de cette table, la configuration requise sur le serveur de base de données peut être importante. Il se peut que des quantités excessives de données aient un impact dramatique sur les performances.

- **Données de session et d'événement.** Ce sont les données collectées chaque fois qu'une session est démarrée et qu'une connexion/reconnexion est effectuée. Pour un site important (100 000 utilisateurs), ces données vont s'accroître très rapidement. Par exemple, l'équivalent de deux ans de tables rassemblerait plus d'un To de données nécessitant une base de données d'entreprise de haut au niveau.

Kits de développement (SDK) et API

November 13, 2018

Plusieurs kits de développement et API sont disponibles avec cette version. Pour plus d'informations, veuillez consulter la documentation pour développeurs. À partir de là, vous pouvez accéder à des informations de programmation pour :

- Delivery Controller
- Monitor Service OData
- StoreFront

Le kit de développement de stratégie de groupe Citrix vous permet d'afficher et de configurer les paramètres et les filtres de stratégie de groupe. Il utilise un fournisseur PowerShell pour créer un lecteur virtuel qui correspond aux paramètres et filtres de la machine et de l'utilisateur. Le fournisseur apparaît sous forme d'extension de New-PSDrive. Pour utiliser le kit de développement de stratégie de groupe, soit Studio soit le kit de développement XenDesktop doit être installé. Consultez la section Kit de développement de stratégie de groupe pour de plus amples informations.

SDK Delivery Controller

Le kit de développement logiciel comprend un certain nombre de composants logiciels enfichables PowerShell installés automatiquement par l'assistant d'installation lorsque vous installez les composants Delivery Controller ou Studio.

Autorisations : vous devez exécuter le shell ou le script avec une identité disposant de droits d'administration Citrix. Bien que les membres du groupe d'administrateurs locaux du Controller disposent automatiquement de privilèges d'administration complets pour permettre l'installation de XenApp ou XenDesktop, Citrix vous recommande, pour un fonctionnement normal, de créer des administrateurs Citrix avec les droits appropriés, plutôt que d'utiliser le compte des administrateurs locaux. Si vous exécutez Windows Server 2008 R2, vous devez exécuter le shell ou le script en tant qu'administrateur Citrix, et non en tant que membre du groupe des administrateurs locaux.

Pour accéder aux applets de commande et les exécuter :

1. Démarrez un shell dans PowerShell : ouvrez Studio, sélectionnez l'onglet **PowerShell** et cliquez sur **Lancer PowerShell**.
2. Pour utiliser les applets de commande du kit de développement dans des scripts, définissez la stratégie d'exécution dans PowerShell. Pour plus d'informations sur la stratégie d'exécution PowerShell, veuillez consulter votre documentation Microsoft.
3. Ajoutez les composants enfichables dont vous avez besoin à l'environnement PowerShell en utilisant l'applet de commande **Add -PSSnapin** dans la console Windows PowerShell.

V1 et V2 indiquer la version du composant logiciel enfichable (les composants logiciels enfichables XenDesktop 5 sont à la version 1 ; les composants logiciels enfichables XenDesktop 7 sont à la version 2. Par exemple, pour installer les composants logiciels enfichables XenDesktop 7, tapez Add-PSSnapin Citrix.ADIdentity.Admin.V2). Pour importer tous les applets de commande, tapez : Add-PSSnapin Citrix.*.Admin.V*

Une fois que les composants logiciels enfichables ont été ajoutés, vous pouvez accéder aux applets de commande et à l'aide associée.

REMARQUE : pour consulter l'aide de l'applet de commande PowerShell XenApp et XenDesktop :

1. À partir de la console PowerShell, ajoutez les composants logiciels enfichables Citrix : Add – PSSnapin.*.Admin.V*.
2. Suivez les instructions fournies dans PowerShell Integrated Scripting Environment (ISE).

Kit de développement de stratégie de groupe

Pour utiliser le kit de développement de stratégie de groupe, soit Studio soit le kit de développement XenDesktop doit être installé.

Pour ajouter le SDK de stratégie de groupe, tapez **Add-PSSnapin citrix.common.grouppolicy**. (Pour accéder à l'aide, tapez : **help New-PSDrive -path localgpo:/**)

Pour créer un lecteur virtuel et le charger de paramètres, tapez : **New-PSDrive <*Paramètres standard*> [-PSProvider] CitrixGroupPolicy -Controller <*chaîne*>** où la chaîne de Controller correspond au nom de domaine complet d'un Controller du site auquel vous voulez vous connecter et à partir duquel vous voulez charger les paramètres.

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States