



Citrix Virtual Apps and Desktops Service

Contents

Citrix Virtual Apps and Desktops Service	3
Nouveautés	12
Problèmes connus	25
Configuration système requise	26
Vue d'ensemble de la sécurité technique	31
Méthodes de mise à disposition	36
Installer et configurer	41
Mise en route	46
Configurer des emplacements de ressources	47
Environnements de virtualisation Microsoft Azure Resource Manager	50
Environnements de virtualisation XenServer	61
Environnements de virtualisation Microsoft System Center Virtual Machine Manager	63
Environnements de virtualisation VMware	66
Environnements de virtualisation Amazon Web Services	72
Environnements de virtualisation Nutanix	80
Environnements de virtualisation Google Cloud Platform	82
Installer des Cloud Connector	91
Créer et gérer des connexions	95
Installer des VDA	107
Installer des VDA à l'aide de la ligne de commande	125
Créer des catalogues de machines	133
Déploiement rapide d'Azure	146
Créer des groupes de mise à disposition	150

Créer des groupes d'applications	157
Supprimer des composants	166
Mise à niveau	167
Imprimer	168
Technologies HDX	169
Stratégies	170
Gérer	170
Zones	171
Cache d'hôte local	182
Considérations sur le dimensionnement et la scalabilité du cache d'hôte local	192
Administration déléguée	209
Journalisation de la configuration	221
Analyse	223
Director	224
Citrix Gateway	252
Kits de développement (SDK) et API	254

Citrix Virtual Apps and Desktops Service

March 6, 2019

Introduction

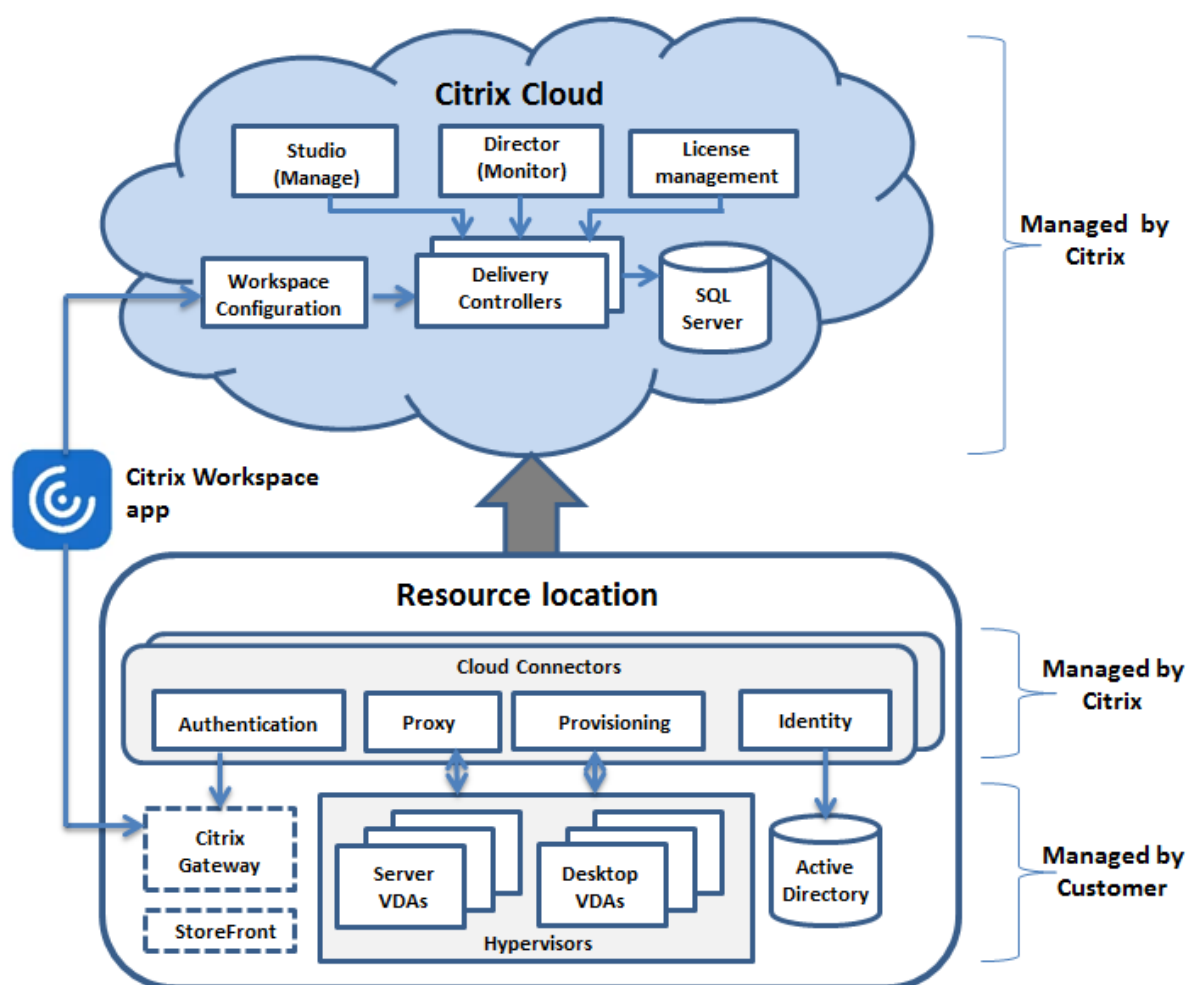
Citrix Virtual Apps and Desktops fournit des solutions de virtualisation qui confèrent au personnel informatique un contrôle des machines virtuelles, des applications et de la sécurité tout en offrant un accès à n'importe quel appareil. Les utilisateurs peuvent utiliser des applications et des bureaux indépendamment du système d'exploitation et de l'interface de l'appareil.

Citrix Virtual Apps and Desktops Service vous permet de délivrer de manière sécurisée des applications et bureaux virtuels sur n'importe quel appareil tout en laissant le gros de l'installation, la configuration, les mises à jour et la surveillance des produits à la charge de Citrix. Vous conservez un contrôle total sur les applications, les stratégies et les utilisateurs tout en offrant la meilleure expérience possible sur n'importe quel appareil.

Vous connectez vos ressources au service via Citrix Cloud Connector, qui sert de canal de communication entre Citrix Cloud et vos emplacements de ressources. Cloud Connector permet d'administrer le cloud sans nécessiter de configuration de réseau ou d'infrastructure complexe telle que des VPN ou des tunnels IPsec. Les emplacements de ressources contiennent les machines et autres ressources qui mettent à disposition des applications et des postes de travail à vos abonnés.

Qui gère quoi

Le graphique suivant illustre les composants principaux d'un déploiement de Citrix Virtual Apps and Desktops Service.

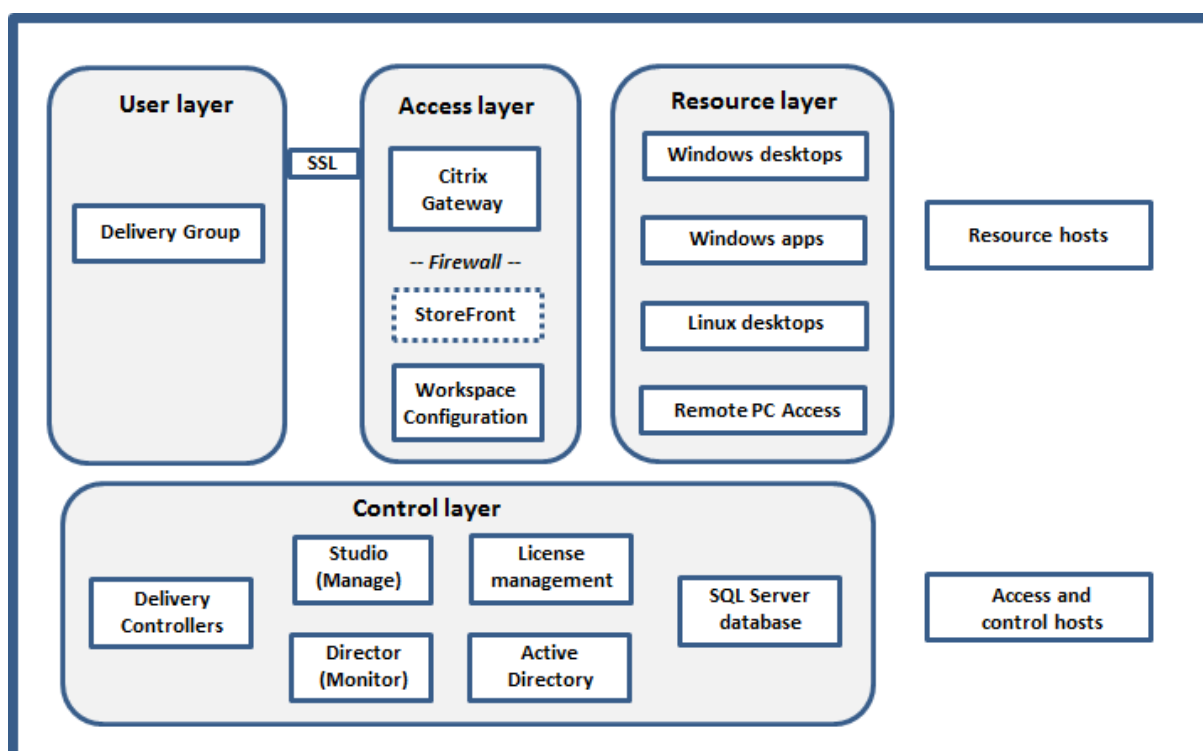


Composants

Comme illustré dans le graphique, Citrix gère les composants principaux dans Citrix Cloud. Citrix se charge également de l'installation et de la mise à niveau de ces composants. (Cela diffère d'un déploiement Citrix Virtual Apps and Desktops local, où vous êtes responsable de l'installation, de la gestion et de la mise à niveau des composants principaux).

Vos applications et bureaux résident dans un ou plusieurs emplacements de ressources. Vous installez et gérez la plupart des composants dans chaque emplacement de ressources. Les exceptions sont les Citrix Cloud Connector. Vous installez les Cloud Connector et Citrix les gère.

Le graphique suivant illustre une vue par couche des composants de Citrix Virtual Apps and Desktops Service.



L'application Citrix Workspace est installée sur les machines utilisateur et d'autres points de terminaison, tels que des bureaux virtuels. L'application Citrix Workspace offre aux utilisateurs un accès sécurisé, rapide et en libre-service aux documents, applications et bureaux à partir de tout appareil, y compris les smartphones, tablettes et PC. L'application Citrix Workspace 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 de l'application Citrix Workspace, l'application Citrix Workspace pour HTML5 offre une connexion via un navigateur Web compatible HTML5.

Composants de Citrix Cloud

Citrix installe et gère les composants suivants dans Citrix Cloud.

Delivery Controller

Le Delivery Controller est le composant de couche de commande centralisée dans un déploiement. Les services du Controller communiquent via les Cloud Connector dans chaque emplacement de ressources pour :

- Distribuer des applications et bureaux.
- Authentifier et gérer l'accès des utilisateurs.
- Établir les connexions entre les utilisateurs et leurs applications et bureaux virtuels.
- Optimiser l'utilisation des connexions et en équilibrer la charge.

- Savoir 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. Cela inclut la gestion de l'état des bureaux, leur démarrage ou arrêt à la demande en fonction de la configuration administrative.

Les données provenant des services Controller sont stockées dans la base de données du site Microsoft SQL Server. Un déploiement utilise également une base de données de journalisation de la configuration, ainsi qu'une base de données de surveillance utilisée par Director.

Lorsque le Citrix Cloud est hébergé sur Microsoft Azure, SQL Server sur les VM Azure (IaaS) est pris en charge. La base de données Azure SQL (PaaS) n'est pas prise en charge.

Gestion des licences Citrix

La fonctionnalité de gestion des licences communique avec le Controller pour gérer les licences de chaque session utilisateur et allouer les fichiers de licences. L'administrateur du client n'a pas besoin de configurer ou de gérer quoi que ce soit en ce qui concerne les licences. Cette tâche est effectuée automatiquement dans Citrix Cloud.

Citrix Studio

Studio est la console de gestion que vous utilisez pour configurer et gérer les connexions, les catalogues de machines et les groupes de mise à disposition. Studio démarre lorsque vous sélectionnez **Gérer** dans la console Citrix Cloud.

Citrix Director

Director 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. Les affichages incluent :

- Données de session en temps réel à partir du Broker Service dans le Controller, qui comprennent des données de l'agent broker dans le VDA.
- Données historiques provenant du service Monitoring dans le Controller.
- Données sur le trafic HDX (également appelé trafic ICA).

Director affiche ces données lorsque vous sélectionnez **Surveiller** dans la console Citrix Cloud.

Configuration de l'espace de travail

Depuis la configuration de Workspace dans Citrix Cloud, vous pouvez :

- Spécifier les services intégrés à Citrix Workspace.
- Personnaliser l'URL que vos abonnés utilisent pour accéder à leur espace de travail.
- Personnaliser l'apparence des espaces de travail des abonnés, tels que les logos, la couleur et les préférences.
- Indiquer comment les abonnés s'authentifient auprès de leur espace de travail, par exemple en utilisant Active Directory ou Azure Active Directory.
- Spécifier la connectivité externe des emplacements de ressources utilisés par vos abonnés.

Citrix StoreFront

Citrix StoreFront est le prédécesseur de Citrix Workspace et est utilisé dans les déploiements sur site. Il offre plusieurs fonctionnalités similaires à Citrix Workspace, notamment l'accès des abonnés aux applications et bureaux, l'authentification et d'autres données sur les abonnés garantissant une expérience cohérente sur tous les appareils.

Dans un déploiement de service, vous pouvez éventuellement installer des serveurs StoreFront dans des emplacements de ressources. Le fait de disposer de magasins locaux peut aider à fournir des applications et des postes de travail pendant les pannes de réseau.

Citrix Gateway

Lorsque les utilisateurs se connectent en dehors du pare-feu d'entreprise, Citrix Virtual Apps and Desktops peut utiliser la technologie Citrix Gateway pour sécuriser les connexions avec le protocole TLS. L'appliance virtuelle Citrix Gateway ou VPX est une appliance SSL VPN déployée dans la DMZ (zone démilitarisée). Il fournit un point d'accès sécurisé unique via le pare-feu d'entreprise.

Bien que Citrix installe et gère Citrix Gateway dans Citrix Cloud, vous pouvez également installer Citrix Gateway dans les emplacements de ressources.

Composants dans les emplacements de ressources

Un emplacement de ressources contient les ressources requises pour fournir des services à vos abonnés (utilisateurs). Vous pouvez gérer ces ressources à partir de Citrix Cloud. Les emplacements de ressources contiennent des ressources différentes selon les services Citrix Cloud que vous utilisez et les services que vous souhaitez fournir à vos utilisateurs.

Pour interagir avec Citrix Cloud, chaque emplacement de ressources a besoin de Cloud Connector et d'un accès à un domaine Microsoft Active Directory.

Dans un déploiement Citrix Virtual Apps and Desktops Service, un emplacement de ressources contient des éléments provenant de la couche d'accès et de la couche de ressources :

- Cloud Connector
- Contrôleur de domaine Active Directory
- Virtual Delivery Agents (VDA)
- Hyperviseurs qui provisionnent des VDA et stockent leurs données, s'ils sont utilisés
- Citrix Gateway (facultatif)
- Serveurs StoreFront (facultatif)

Cloud Connector

Chaque emplacement de ressources contient au moins un Cloud Connector (deux ou plus sont recommandés pour assurer la redondance). Un Cloud Connector est le canal de communication entre les composants dans le Citrix Cloud et les composants dans l'emplacement de ressources. Dans l'emplacement de ressources, le Cloud Connector sert de proxy pour le Delivery Controller dans Citrix Cloud.

Vous installez les Cloud Connector à partir de la console Citrix Cloud. Citrix gère et met à jour les Cloud Connector automatiquement.

Virtual Delivery Agents (VDA)

Chaque machine physique ou virtuelle qui met à disposition des applications et des bureaux doit disposer d'un VDA. Le VDA s'enregistre auprès d'un Cloud Connector. Après l'enregistrement, les connexions sont établies à partir de ces ressources vers les utilisateurs. Les VDA établissent et gèrent la connexion entre la machine et l'appareil de l'utilisateur et appliquent toute stratégie qui a été configurée pour la session.

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

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.

Dans cette documentation, le mot « VDA » fait référence à l'agent ainsi qu'à la machine sur laquelle il est installé.

Hyperviseurs et services de cloud

Un hyperviseur ou service de cloud contient les VDA qui hébergent des applications et bureaux.

Pour provisionner des machines virtuelles qui mettent à disposition des applications et des bureaux, vous pouvez utiliser :

- Machine Creation Services : la technologie MCS est intégrée à Studio et accessible automatiquement via la console Cloud Citrix. MCS crée des copies d'une image principale pour créer et provisionner des machines virtuelles.
- Citrix Provisioning (anciennement Provisioning Services) : la technologie Citrix Provisioning transmet une image principale aux machines utilisateur. Citrix Provisioning ne nécessite pas d'hyperviseur, vous pouvez donc provisionner des machines physiques.
- Un autre outil de provisioning de votre choix.

Bien que la plupart des déploiements utilisent des hyperviseurs, vous n'en avez pas besoin si :

- Vos applications et bureaux sont hébergés sur des machines physiques.
- Vous utilisez Citrix Provisioning pour provisionner des VM.
- Vous souhaitez déployer Remote PC Access, ce qui permet aux employés d'accéder à distance à leurs PC physiques.

Active Directory

Bien que n'étant pas un composant Citrix, Microsoft Active Directory est requis pour l'authentification et autorisation dans n'importe quel déploiement. L'infrastructure Kerberos dans Active Directory est utilisée pour garantir l'authenticité et la confidentialité des communications avec Citrix Cloud.

Éléments qui facilitent la mise à disposition de bureaux et d'applications

Dans le cadre de la mise à disposition d'applications et de bureaux auprès d'utilisateurs dans un environnement de production, vous configurez les éléments suivants.

Connexion hôte

Une connexion hôte permet la communication entre les composants dans le plan de contrôle (Citrix Cloud) et les VDA dans un hyperviseur ou service de cloud. Spécifications relatives à la connexion :

- Adresse et informations d'identification pour accéder à l'hôte
- Outils à utiliser pour créer des VM
- Méthode de stockage et machines à utiliser pour le stockage
- Réseau que les VM vont utiliser

Catalogue de machines

Un catalogue de machines est une collection de machines physiques ou virtuelles qui ont le même type de système d'exploitation : serveur ou bureau.

Si vous utilisez des machines virtuelles, vous pouvez créer une image principale (également appelée modèle) sur l'hyperviseur ou le service de cloud, et installer un VDA sur l'image principale. Vous pouvez également installer des applications sur l'image principale, si vous souhaitez qu'elles apparaissent sur toutes les machines créées à partir de cette image et ne pas les virtualiser. Ensuite, vous créez un catalogue à l'aide d'un outil Citrix (MCS ou Citrix Provisioning) ou de vos propres outils. Avec les outils Citrix, le processus de création de catalogue provisionne des machines virtuelles identiques à celles de cette image.

Si vous utilisez vos propres outils pour provisionner des VM, ou si vous utilisez des machines physiques, le processus de création de catalogue ajoute ces machines au catalogue.

Pour plus de détails techniques sur les outils Citrix Provisioning, consultez la section [Gestion des images Citrix Virtual Apps and Desktops](#).

Groupe de mise à disposition

Un groupe de mise à disposition spécifie :

- Une ou plusieurs machines sur un catalogue de machines.
- Si vous le souhaitez, les utilisateurs qui sont autorisés à accéder à ces machines. Vous pouvez également spécifier les utilisateurs via la console Citrix Cloud.
- Si vous le souhaitez, les applications et bureaux auxquels les utilisateurs peuvent accéder. Vous pouvez également spécifier les applications via la console Citrix Cloud.

Mise à disposition d'applications et de bureaux

Les [méthodes de mise à disposition](#) décrivent les choix disponibles pour fournir des applications et des postes de travail aux utilisateurs.

Accord de niveau de service

Citrix Virtual Apps and Desktops service (le Service) utilise les meilleures pratiques de l'industrie pour proposer un service cloud de taille appropriée et un haut degré de disponibilité du service.

Pour plus d'informations sur l'engagement de Citrix concernant la disponibilité des services Citrix Cloud, consultez le [contrat de niveau de service](#).

Les performances par rapport à cet objectif peuvent être contrôlées de manière continue sur <https://status.cloud.com>.

Limitations

Le calcul de cet objectif de niveau de Service n'inclut pas la perte de disponibilité pour les raisons suivantes :

- Le client n'a pas respecté les exigences de configuration du service documentées sur <https://docs.citrix.com>.
- Composant non géré par Citrix, y compris, mais sans s'y limiter, les composants suivants : machines physiques et virtuelles contrôlées par le client, systèmes d'exploitation installés et entretenus par le client, équipement réseau ou autre matériel installé et contrôlé par le client ; paramètres de sécurité, stratégies de groupe et autres stratégies de configuration définies et contrôlés par le client ; défaillances du fournisseur de cloud public, défaillances du fournisseur de services Internet ou autres défaillances externes au contrôle de Citrix.
- Interruption de service pour des raisons indépendantes de la volonté de Citrix, y compris une catastrophe naturelle, une guerre, des actes de terrorisme, action gouvernementale.

Plus d'informations

- [Diagrammes Citrix Virtual Apps and Desktops Service](#)
- [Architecture de référence et méthodes de déploiement de Citrix Virtual Apps and Desktops Service](#)
- [Vue d'ensemble de la sécurité technique](#)
- [Comment fonctionnent les déploiements typiques](#)
- [Ports réseau](#)
- [Avis de tiers](#)
- [Configuration système requise](#)

Fonctionnalités

- [Technologies HDX](#)
- [Remote PC Access](#) : permet aux utilisateurs d'ouvrir une session à distance depuis n'importe quel emplacement sur un PC physique au bureau.
- [Publier du contenu](#) : permet de publier une application qui est simplement une URL ou un chemin UNC vers une ressource
- [Server VDI](#) : permet de mettre à disposition un bureau depuis un système d'exploitation de serveur pour un utilisateur unique

Mise en route

Pour savoir comment installer et configurer votre déploiement, consultez la section [Installer et configurer](#). Ce résumé vous guide à travers les étapes principales du processus et offre des liens vers des descriptions détaillées.

Nouveautés

March 8, 2019

L'un des objectifs de Citrix est d'offrir de nouvelles fonctionnalités et des mises à jour de produits aux clients de Citrix Virtual Apps and Desktops Service dès qu'elles sont disponibles. Les nouvelles versions étant plus avantageuses, il est important que vous en profitiez le plus rapidement possible. Des mises à jour sont déployées sur le service environ toutes les 3 semaines.

Ce processus est transparent pour l'utilisateur. Les mises à jour initiales sont uniquement appliquées aux sites Citrix internes pour être ensuite graduellement appliquées aux environnements des clients. La mise à disposition des mises à jour de façon incrémentielle permet de garantir la qualité des produits et de maximiser la disponibilité.

Pour plus d'informations sur le contrat de niveau de service dans le cadre de l'évolutivité et la disponibilité des services dans le cloud, consultez [Contrat de niveau de service](#). Pour contrôler les interruptions de service et la maintenance planifiée, consultez le [tableau de bord de l'état de service](#).

Virtual Delivery Agents (VDA) : les VDA pour machines Windows sont généralement publiés en même temps que le produit Citrix Virtual Apps and Desktops sur site.

- Pour plus d'informations sur les nouvelles fonctionnalités VDA et HDX, consultez les articles [Nouveautés](#) et [Problèmes connus](#) pour le produit Citrix Virtual Apps and Desktops sur site actuel.
- Pour plus d'informations sur les plates-formes de VDA et les fonctionnalités qui ne sont plus prises en charge, consultez la section [Fin de prise en charge](#). Cet article inclut également les plates-formes et les fonctionnalités qui ne seront plus prises en charge dans une version ultérieure (par exemple, les systèmes d'exploitation prenant en charge l'installation de VDA).

Février 2019

Fonctionnalités nouvelles et améliorées

Surveillance des alertes d'hyperviseur. Les alertes de Citrix Hypervisor et VMware vSphere sont désormais affichées dans l'onglet **Surveiller > Alertes** pour vous aider à surveiller les états et paramètres suivants de l'intégrité de l'hyperviseur :

- Utilisation UC

- Utilisation de mémoire
- Utilisation du réseau
- Connexion d'hyperviseur non disponible
- Utilisation du disque (vSphere uniquement)
- État de l'alimentation ou de la connexion de l'hôte (vSphere uniquement)

Pour plus d'informations, consultez la section Surveillance des alertes d'hyperviseur dans [Alertes et notifications](#).

Communications via les versions TLS antérieures. Pour améliorer la sécurité de Citrix Virtual Apps and Desktops Service, Citrix bloquera toute communication via TLS (Transport Layer Security) 1.0 et 1.1 à compter du 15 mars 2019 et autorisa uniquement les communications TLS 1.2. Pour plus d'informations, consultez la section [Version TLS](#). Pour obtenir des instructions supplémentaires, consultez le document [CTX247067](#).

Groupes d'applications. 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. (La fonction Restriction de balise n'est actuellement pas disponible.) Pour plus d'informations, consultez la section [Créer des groupes d'applications](#).

Performances d'ouverture de session - Détails du profil. Le panneau **Durée de connexion** de la page **Détails de l'utilisateur** sur l'onglet **Surveiller** contient désormais des informations sur les détails de la phase de chargement du profil du processus de connexion. Les détails du profil fournissent des informations utiles sur les profils utilisateur de la session en cours, qui peuvent aider les administrateurs à résoudre les problèmes de charge de profil. Une info-bulle contenant les informations de profil utilisateur suivantes est affichée :

- Nombre de fichiers
- Taille du profil
- Nombre de fichiers volumineux

Une analyse détaillée fournit des informations sur les dossiers individuels, leur taille et le nombre de fichiers. Cette fonctionnalité est disponible sur la version 1811 ou ultérieure des VDA. Pour de plus amples informations, consultez la section [Diagnostiquer les problèmes de connexion utilisateur](#).

Intégrité des licences Microsoft RDS. L'onglet Surveiller affiche l'état de la licence Microsoft RDS (Remote Desktop Services) sur le panneau **Détails de la machine** de la page Détails de la machine et Détails de l'utilisateur pour les machines avec OS de serveur. Un message approprié s'affiche sur l'état de la licence. Vous pouvez survoler l'icône d'information pour voir plus de détails. Pour plus d'informations, consultez la section Intégrité des licences Microsoft RDS dans [Dépanner les machines](#).

Analyse d'application. Cette fonctionnalité automatise l'évaluation de l'intégrité des applications virtuelles publiées sur un site.

Pour lancer l'analyse d'application :

- Sur une ou plusieurs machines de point de terminaison, installez Citrix Application Probe Agent.
- Configurez Citrix Application Probe Agent avec les informations d'identification de Citrix Workspace et Citrix Virtual Apps and Desktops Service.
- Configurez les applications à analyser, les machines de point de terminaison sur lesquelles exécuter l'analyse et l'heure d'analyse planifiée dans l'onglet **Surveiller** > **Configuration** de Citrix Virtual Apps and Desktops Service.

L'agent teste le lancement des applications sélectionnées via Citrix Workspace et indique les résultats de l'analyse dans l'onglet **Surveiller** de Citrix Virtual Apps and Desktops Service.

- Les résultats sont affichés sur la page Applications (données des dernières 24 heures) et la page **Tendances** > **Résultats de l'analyse d'application**.
- Les résultats incluent l'historique des analyses, ainsi que l'étape où l'échec d'analyse s'est produit : Accessibilité de Workspace, Authentification de Workspace, Énumération de Workspace, Téléchargement ICA ou Lancement d'applications.

Le rapport d'échec est envoyé par courrier électronique aux adresses configurées. Vous pouvez planifier l'exécution de vos analyses d'application pendant les heures creuses sur plusieurs emplacements géographiques et utiliser les résultats pour résoudre les problèmes liés aux applications provisionnées, aux machines d'hébergement ou aux connexions avant que les utilisateurs ne les rencontrent. Pour plus d'informations, voir [Analyse d'application](#).

Janvier 2019

Fonctionnalités nouvelles et améliorées

Administration déléguée avec étendue personnalisée. La surveillance prend désormais en charge l'étendue personnalisée grâce à des rôles d'administrateur délégué intégrés. Pour plus d'informations sur les rôles intégrés disponibles pour la surveillance et comment les affecter, consultez [Rôles d'administrateur délégué](#).

Décembre 2018

- La date après laquelle Citrix bloquera toute communication via TLS (Transport Layer Security) 1.0 et 1.1 est passée au 31 janvier 2019 (au lieu du 31 décembre 2018). Pour plus de détails, voir [Fin de prise en charge des versions TLS](#).

Novembre 2018

Fonctionnalités nouvelles et améliorées

- **Données historiques de machine disponibles à l'aide de l'API OData** : données historiques suivantes contenant des analyses de machine sont désormais disponibles via l'API OData. Ces données sont collectées toutes les heures et rassemblées pour la journée.
 - Nombre de machines sous tension (pour les machines avec gestion de l'alimentation)
 - Nombre de machines enregistrées
 - Nombre de machines en mode maintenance
 - Nombre total de machines

Les données sont agrégées pour la période pendant laquelle le service de surveillance est en cours d'exécution. Pour plus d'informations sur l'utilisation de l'API OData et des exemples, voir [Citrix Monitor Service 7 1808](#). Le schéma de base de données est disponible dans [Schéma de Monitor Service](#).

- **Performances d'ouverture de session - Détails de la session interactive** : le panneau Durée de connexion de la vue Détails de l'utilisateur et Détails de la session contient des informations sur la phase Session interactive du processus de connexion. Le temps nécessaire pour chacune des trois sous-phases (Pre-userinit, Userinit et Shell) est affiché dans la barre de session interactive sous la forme d'une info-bulle. Cela permet un dépannage plus précis de cette phase de la connexion. Le délai cumulé entre les sous-phases et un lien vers la documentation sont également fournis. Cette fonctionnalité est disponible sur Delivery Controller version 7 1808 ou version ultérieure. La barre de détail Session interactive affiche uniquement la durée de la session en cours. Pour de plus amples informations, consultez la section [Diagnostiquer les problèmes de connexion utilisateur](#).
- **Performances d'ouverture de session - Détails GPO** : le panneau Durée de connexion de la vue Détails de l'utilisateur et de la session contient la durée des objets de stratégie de groupe (GPO). Il s'agit du temps total nécessaire pour appliquer les objets de stratégie de groupe sur la machine virtuelle au cours du processus d'ouverture de session. À présent, vous pouvez voir les détails de chaque stratégie appliquée selon les CSE (extensions côté client) sous forme d'info-bulle dans la barre GPO. Pour chaque application de stratégie, le détail affiche l'état et le temps nécessaire. Ces informations supplémentaires facilitent le dépannage et la résolution des problèmes impliquant une durée de GPO élevée. Les durées indiquées dans le détail représentent uniquement la durée du traitement des CSE et ne correspondent pas à la durée totale du GPO. Cette fonctionnalité est disponible sur Delivery Controller version 7 1808 ou version ultérieure. Pour de plus amples informations, consultez la section [Diagnostiquer les problèmes de connexion utilisateur](#).

Corrections

Les requêtes de rapport personnalisé enregistrées durant la surveillance ne sont pas disponibles après une mise à niveau du Cloud. [DNA-23420]

Octobre 2018

Fonctionnalités nouvelles et améliorées

- **Applications : limite par machine.** Vous pouvez maintenant limiter le nombre d'instances d'application par machine. Cette limite s'applique à toutes les machines du site. Cette limite vient s'ajouter à la limite d'application existante pour tous les utilisateurs du groupe de mise à disposition et à la limite par utilisateur. Cette fonctionnalité est disponible uniquement via PowerShell, pas dans Studio. Pour plus de détails, consultez la section [Configurer les limites d'application](#).
- **Windows Server 2019.** Vous pouvez maintenant installer des VDA pour OS de serveur sur des ordinateurs Windows Server 2019, comme indiqué dans [Configuration système requise](#).

Septembre 2018

Fonctionnalités nouvelles et améliorées

- **Administration déléguée.** L'administration déléguée de Citrix Cloud vous permet de configurer les autorisations d'accès requises par tous vos administrateurs conformément à leur rôle dans votre organisation. Pour de plus amples informations, veuillez consulter la section [Administration déléguée](#). La surveillance prend en charge l'attribution de rôles intégrés ; ils sont actuellement disponibles dans leur intégralité. Pour plus d'informations sur les rôles intégrés disponibles pour la surveillance et comment les affecter, consultez [Rôles d'administrateur délégué](#).
- **Journalisation de la configuration.** La journalisation de la configuration permet aux administrateurs de suivre les modifications de configuration et les activités administratives. Pour plus de détails, voir [Journalisation de la configuration](#).

Plusieurs cmdlets PowerShell dans le SDK PowerShell distant qui étaient précédemment désactivées sont maintenant activées, à utiliser avec la journalisation de la configuration :

- Log:GetLowLevelOperation
- Log:GetHighLevelOperation
- Log:GetSummary
- Log:GetDataStore

- Log:ExportReport
- **Cache d'hôte local.** Le cache d'hôte local est maintenant entièrement disponible. La fonctionnalité de cache d'hôte local permet de poursuivre les opérations de négociation de connexion lorsqu'un Cloud Connector dans un emplacement de ressources ne peut pas communiquer avec Citrix Cloud. Pour plus d'informations, veuillez consulter [Cache d'hôte local](#).
- **Citrix Provisioning.** Pour provisionner les VDA, vous pouvez maintenant utiliser Citrix Provisioning ou les Machine Creation Services existants. Pour des informations Citrix Provisioning spécifiques à l'environnement cloud, voir [Citrix Provisioning géré par Citrix Cloud](#).

Corrections

Dans les versions antérieures, lors de l'utilisation du provisioning Azure à la demande, toutes les VM étaient supprimées lors de la mise hors tension. Désormais, seules les VM regroupées sont supprimées. Les VM persistantes (dédiées) ne sont pas supprimées lors de leur mise hors tension.

Août 2018

- **Nouveaux noms de produits**

Si vous êtes client ou partenaire Citrix depuis un certain temps, vous remarquerez de nouveaux noms dans nos produits et dans la documentation de ces produits. Si vous découvrez ce produit Citrix, vous pourrez parfois rencontrer des noms différents pour un produit ou un composant.

Les nouveaux noms de produits et de composants représentent mieux le portefeuille toujours croissant de Citrix et sa stratégie cloud. Les articles de cette documentation utilisent les noms suivants.

- **Citrix Virtual Apps and Desktops :** Citrix Virtual Apps and Desktops offre une solution de bureaux et d'applications virtuels, fournie sous la forme d'un service cloud et d'un produit sur site, donnant aux employés la liberté de travailler n'importe où et sur n'importe quel appareil, tout en réduisant les coûts informatiques. Mettez à disposition des applications Windows, Linux, Web et SaaS ou des bureaux virtuels complets à partir de n'importe quel cloud : public, local ou hybride. La solution Virtual Apps and Desktops s'appelait auparavant XenApp et XenDesktop.
- **Application Citrix Workspace :** l'application Citrix Workspace intègre la technologie Citrix Receiver existante ainsi que les autres technologies clientes de Citrix Workspace. Elle a été améliorée pour offrir des fonctionnalités supplémentaires afin de proposer aux utilisateurs finaux une expérience contextuelle unifiée qui leur permet d'interagir avec toutes les applications professionnelles, les fichiers et les périphériques dont ils ont besoin pour travailler efficacement. Pour plus d'informations, consultez ce billet de blog.

- **Citrix SD-WAN** : NetScaler SD-WAN, une technologie essentielle pour nos clients et partenaires qui transforment leurs réseaux de succursales et leurs réseaux WAN avec la technologie cloud, s'appelle désormais Citrix SD-WAN.
- **Citrix Secure Web Gateway** : dans le cadre de notre portefeuille Citrix Networking toujours croissant, nous sommes fiers d'offrir notre robuste service Citrix Secure Web Gateway, précédemment appelé NetScaler Secure Web Gateway.
- **Citrix Gateway** : NetScaler Unified Gateway, notre solution robuste qui permet un accès sécurisé et contextuel aux applications et aux données dont vous avez besoin pour travailler efficacement, s'appelle désormais Citrix Gateway.
- **Citrix Content Collaboration et Citrix Files pour Windows** : les fonctionnalités avancées d'accès, de collaboration, de flux de travail, de gestion des droits et d'intégration de ShareFile sont désormais disponibles dans le composant Citrix Content Collaboration de Citrix Workspace, notre solution intégrée, contextuelle et sécurisée. Citrix Files pour Windows vous permet d'accéder directement à vos fichiers Content Collaboration via un lecteur mappé, offrant ainsi une expérience identique à l'Explorateur de fichiers Windows natif.
- **Citrix Hypervisor** : la technologie XenServer pour l'infrastructure de virtualisation, basée sur l'hyperviseur XenProject, est désormais Citrix Hypervisor.

Voici un résumé rapide :

Est	Était
Citrix Virtual Apps and Desktops	XenApp et XenDesktop
Application Citrix Workspace	Intègre Citrix Receiver et d'importantes améliorations
Citrix SD-WAN	NetScaler SD-WAN
Citrix Secure Web Gateway	NetScaler Secure Web Gateway
Citrix Gateway	NetScaler Unified Gateway
Citrix Content Collaboration	ShareFile
Citrix Files pour Windows	ShareFile Desktop App, ShareFile Sync, ShareFile Drive Mapper
Citrix Hypervisor	XenServer
Citrix Provisioning	Citrix Provisioning Services

L'implémentation de cette transition dans nos produits et leur documentation est en cours.

- Le contenu intégré au produit peut encore contenir les anciens noms. Par exemple, vous pouvez voir des instances des anciens noms dans le texte de la console, les messages et

les noms de répertoire/fichier.

- Il est possible que certains éléments (tels que les commandes et les MSI) continuent à conserver leurs anciens noms pour éviter de casser les scripts clients existants.
- La documentation produit associée et les autres ressources (telles que les vidéos et les billets de blog) auxquelles la documentation de ce produit renvoie peuvent toujours contenir des noms anciens.
- Pour Citrix Hypervisor : le nouveau nom sera utilisé sur le site Web de Citrix et dans les informations produit à partir de septembre 2018. Vous verrez également le nouveau nom dans les consoles d'administration de certains produits Citrix, tels que Citrix Virtual Apps and Desktops. Le produit XenServer et la documentation technique continueront à utiliser XenServer 7.x jusqu'au début de 2019.

Nous vous remercions de votre patience pendant cette transition.

Pour plus de détails sur les nouveaux noms, voir <https://www.citrix.com/about/citrix-product-guide/>.

• **Changements de numéros de version des produits et composants**

Citrix installe et gère la plupart des composants Citrix Virtual Apps and Desktops, vous ne serez donc pas concerné par ces numéros de version. Cependant, vous pouvez voir les numéros de version lors de l'installation de Cloud Connectors, ainsi que lors de l'installation ou de la mise à niveau de VDA dans des emplacements de ressources.

Les numéros de version des produits et composants Citrix Virtual Apps and Desktops sont affichés au format suivant : **AAMM.c.m.b**

- AAMM = Année et mois de publication du produit ou du composant. Par exemple, une version sortie en septembre 2018 apparaît comme 1809.
- c = numéro de version Citrix Cloud pour le mois.
- m = version de maintenance (le cas échéant).
- b = numéro de compilation. Ce champ s'affiche uniquement sur la page À propos du composant et dans la fonctionnalité du système d'exploitation permettant de supprimer ou de modifier des programmes.

Par exemple, **Citrix Virtual Apps and Desktops 1809.1.0** indique que le composant est sorti en septembre 2018. Il est associé à Citrix Cloud version 1 ce mois-là et n'est pas une version de maintenance. Certains écrans affichent uniquement l'année et le mois de la version : par exemple, **Citrix Virtual Apps and Desktops 1809**.

Dans les versions antérieures (7.18 et versions antérieures), les numéros de version étaient affichés au format : *7.version*, où la valeur augmentait de 1 pour chaque version. Par exemple, la version VDA suivant XenApp and XenDesktop 7.17 était 7.18. Les versions antérieures (7.18 et antérieures) ne seront pas mises à jour avec le nouveau format de numérotation.

- **Fin de prise en charge des versions TLS.** Pour améliorer la sécurité de Citrix Virtual Apps and Desktops Service, Citrix bloquera toute communication via TLS (Transport Layer Security) 1.0 et 1.1 à compter du 31 décembre 2018. Pour plus de détails, voir [Fin de prise en charge des versions TLS](#).
- **Environnement de virtualisation Google Cloud Platform.** Citrix Virtual Apps and Desktops Service prend en charge la possibilité de mettre manuellement hors/sous tension les VM Virtual Apps and Desktops sur Google Cloud Platform (GCP). Pour plus d'informations, voir [Environnements de virtualisation Google Cloud Platform](#).

Juillet 2018

- **Exportation de données de filtres.** Vous pouvez désormais exporter les données de surveillance en temps réel dans l'onglet **Surveiller** > **Filtres** vers des fichiers au format CSV. La fonction d'exportation est disponible à partir des pages Filtres de Machines, Sessions, Connexions et Instances d'application. Vous pouvez sélectionner un filtre personnalisé prédéfini ou sélectionner des critères de filtre appropriés, choisir les colonnes requises dans le tableau et exporter les données. Des données pouvant atteindre 100 000 enregistrements peuvent être exportées. Les fichiers CSV exportés offrent une vue complète des données en temps réel et facilitent l'analyse des grands ensembles de données.

Juin 2018

- **Connexions à Azure Resource Manager.** Dans l'assistant de création de connexion de Studio, la sélection de l'environnement Azure sur la page **Connexion** inclut tous les clouds Azure valides pour votre abonnement Azure. La disponibilité générale pour Azure US Government Cloud et Azure Germany Cloud remplace les versions préliminaires de ces deux environnements dans les versions antérieures.

Mai 2018

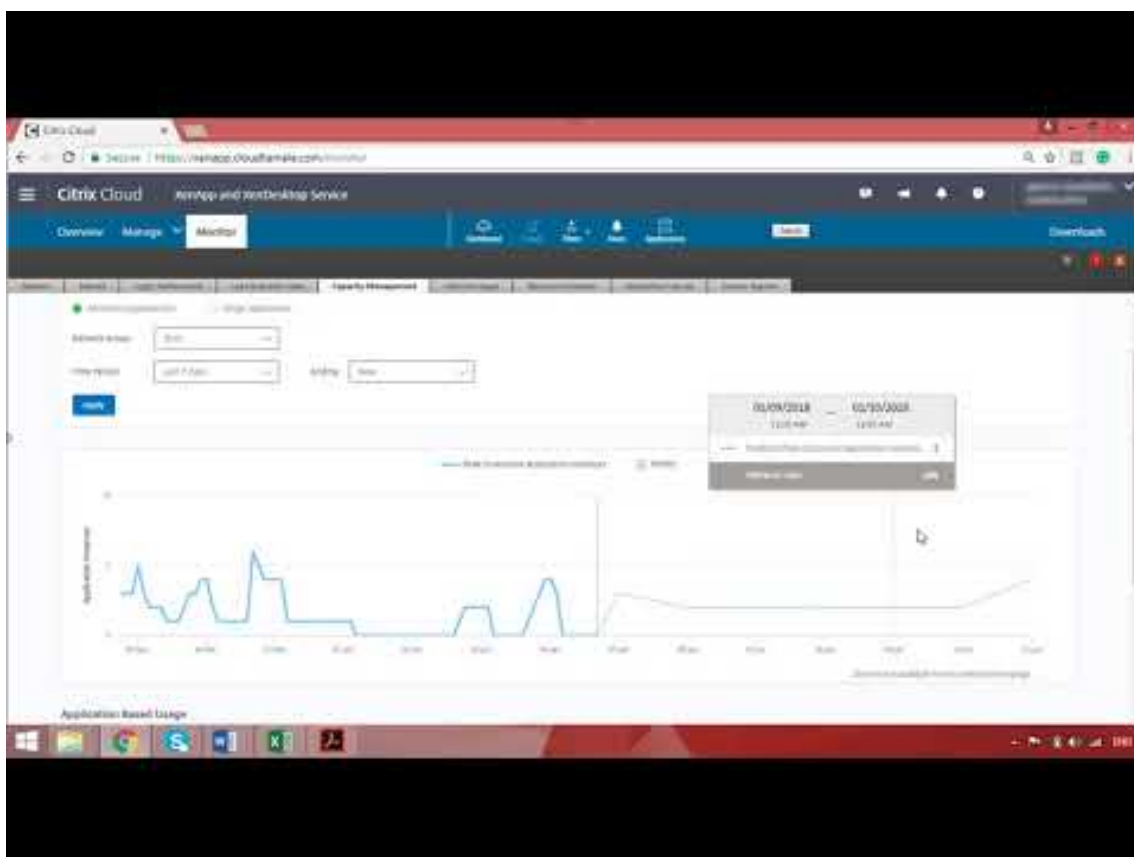
- **Déploiement rapide d'Azure.** Lorsque votre emplacement de ressources utilise des machines Azure Resource Manager pour fournir des applications et des postes de travail, vous pouvez maintenant choisir une méthode de déploiement :
 - Configuration complète : cette méthode existante utilise la console de gestion Studio, qui vous guide dans la création d'un catalogue de machines et d'un groupe de mise à disposition.
 - Déploiement rapide d'Azure : cette nouvelle option fournit une interface plus simple qui permet un déploiement plus rapide des applications et des postes de travail.

Pour plus de détails, voir [Déploiement rapide d'Azure](#).

- **Lien Citrix Health Assistant.** La page Détails de la machine d'une machine non enregistrée dans la console de surveillance contient désormais un bouton **Health Assistant**. Le lien pointe actuellement vers l'article [Dépanner les machines](#) sur docs.citrix.com et vers l'article du Centre de connaissances, [Citrix Health Assistant - Troubleshoot VDA Registration and Session Launch](#), à partir duquel vous pouvez télécharger l'outil. Citrix Health Assistant est un outil qui permet de résoudre les problèmes de configuration dans les VDA non enregistrés. L'outil automatise un certain nombre de vérifications de l'état pour identifier les causes possibles des problèmes courants d'enregistrement de VDA, de lancement de session et de configuration de la redirection de fuseau horaire.
- **Détails de la session interactive.** Dans la console de monitoring, le panneau de la vue Détails de l'utilisateur > Durée de connexion contient maintenant des informations sur l'étape Session interactive du processus de connexion. Pour permettre une résolution et un dépannage plus précis de cette phase de la connexion, Session interactive comporte désormais trois sous-phases : Pre-userinit, Userinit et Shell. Dans cette version, placer le curseur sur Session interactive permet d'afficher une info-bulle montrant les sous-phases et un lien vers la documentation. Pour une description des sous-phases et savoir comment améliorer les performances de chaque phase, voir [Diagnostiquer les problèmes de connexion utilisateur](#).

Mars 2018

- **Prédiction d'instances d'applications (fonctionnalité préliminaire).** Il s'agit de la première fonction de surveillance basée sur l'analyse prédictive. La prévision de modèles d'utilisation des ressources est importante pour les administrateurs afin d'organiser les ressources et le nombre requis de licences sur chaque ressource. La fonction de prédiction d'instances d'applications indique le nombre d'instances d'applications hébergées susceptibles d'être lancées par site ou groupe de mise à disposition au cours d'une période donnée. Des algorithmes d'apprentissage automatique basés sur des modèles de données créés avec des données historiques existantes sont utilisés pour effectuer la prédiction. Le niveau de tolérance indique la qualité de la prédiction.



Pour de plus amples informations, consultez la section [Prédiction d'instances d'applications](#) dans Director. Partagez vos commentaires sur l'utilité de cette fonctionnalité dans le [forum de discussion Citrix Cloud](#).

- **API de groupes de mise à disposition - Tech Preview**

La Tech Preview des API de groupes de mise à disposition fournit un ensemble d'API REST que vous pouvez utiliser pour automatiser la gestion des groupes de mise à disposition. L'ensemble complet des API disponibles peut être consulté et testé dans la documentation Citrix Cloud APIs sur <https://developer.cloud.com/index.html>.

- **Authentification Web Studio**

La console de gestion du service sur Citrix Cloud utilise désormais un jeton du porteur pour authentifier les clients. Le jeton du porteur est nécessaire pour authentifier l'accès à l'API REST Delivery Groups.

- **Accès aux données du Monitoring Service à l'aide de la version 4 de l'API OData (fonctionnalité préliminaire)**

Vous pouvez créer des tableaux de bord de surveillance et de reporting personnalisés en fonction des données du Monitor Service à l'aide du point de terminaison OData V.4. OData V.4 est basé sur l'API Web ASP.NET et prend en charge les requêtes d'agrégation. Utilisez votre nom

d'utilisateur et votre jeton du porteur Citrix Cloud pour accéder aux données avec le point de terminaison V4. Pour plus d'informations et d'exemples, consultez la section [Access Monitor Service data using the OData v4 endpoint in Citrix Cloud](#).

Partagez vos commentaires sur l'utilité de cette fonctionnalité dans le [forum de discussion Citrix Cloud](#).

Corrections

- Vous pouvez renommer, déplacer ou supprimer des dossiers d'applications. [#STUD-2376]

Janvier 2018

- **Vérification des licences RDS.** La création de catalogues de machines contenant des machines avec OS de serveur Windows comprend désormais une vérification automatique de licence RDS. Tous les problèmes de licence RDS détectés sont affichés, afin que vous puissiez prendre les mesures appropriées pour éviter une interruption du service. Pour de plus amples informations, consultez la section [Créer des catalogues de machines](#).
- **Accès à la console de la machine à partir de Surveiller.** Le panneau Détails de la machine de Surveiller permet désormais d'accéder aux consoles de machines hébergées sur la version 7.3 de l'hyperviseur XenServer. Vous pouvez maintenant résoudre les problèmes rencontrés dans les VDA directement à partir de Surveiller. Pour obtenir davantage d'informations, veuillez consulter la section [Accès à la console machine](#) dans Dépanner les machines.

Décembre 2017

Fonctionnalités nouvelles et améliorées

- **Citrix Workspace.** L'espace de travail Citrix est maintenant disponible pour les **nouveaux** clients de XenApp and XenDesktop Service. Pour plus d'informations, consultez la section [Configuration de l'espace de travail](#).
- **Analyses des applications.** Vous pouvez maintenant analyser et surveiller les performances des applications de manière efficace avec la nouvelle page Analyse des applications disponible dans l'onglet **Surveiller > Applications**. La page fournit une vue consolidée de l'état et de l'utilisation de toutes les applications publiées sur votre site. Il affiche des métriques telles que le nombre d'instances par application et les défaillances et erreurs associées aux applications publiées. Cette fonctionnalité requiert des VDA de version 7.15 ou ultérieure.

Pour obtenir davantage d'informations, veuillez consulter la section [Analyses des applications](#) dans Director.

Novembre 2017

Fonctionnalités nouvelles et améliorées

- **Cache d'hôte local.** La fonctionnalité de cache d'hôte local permet de poursuivre les opérations de négociation de connexion lorsqu'un Cloud Connector dans un emplacement de ressources ne peut pas communiquer avec Citrix Cloud. Pour plus d'informations, veuillez consulter [Cache d'hôte local](#).
- **Azure Managed Disks.** Azure Managed Disks sont maintenant utilisés par défaut pour les VM provisionnées avec MCS dans les environnements Azure Resource Manager. Si vous le souhaitez, vous pouvez utiliser des comptes de stockage conventionnels. Pour de plus amples informations, consultez la section [Environnements de virtualisation Microsoft Azure Resource Manager](#).
- **Administrateur du service d'assistance.** Lors de la gestion des administrateurs du service pour un compte client Citrix Cloud, vous disposez désormais d'un nouveau choix : Administrateur du service d'assistance. Un administrateur du service d'assistance peut accéder aux fonctions de surveillance du service. Pour de plus amples informations, consultez la section [Gérer](#).

Corrections

- Vous pouvez désormais utiliser l'assistant de la console de gestion du service pour créer un catalogue de machines Remote PC Access. Dans les versions antérieures, vous deviez utiliser une applet de commande PowerShell pour créer un catalogue (tel que documenté dans l'article [CTX220737](#)). Ensuite, vous deviez revenir sur la console de gestion pour créer un groupe de mise à disposition. Désormais, vous créez le catalogue et le groupe de mise à disposition de manière séquentielle dans la console de gestion.
- Les catalogues créés avec MCS peuvent utiliser des comptes d'ordinateurs Active Directory existants. [#DNA-24566]
- Lors de la surveillance d'un déploiement, le défilement dans un tableau **Tendances > Sessions** trié affiche des résultats précis. [DNA-51257]

Plus d'informations

- [Problèmes connus](#).
- Pour plus d'informations sur les logiciels tiers inclus dans le service, consultez la section [Avis de tiers](#).

Problèmes connus

March 6, 2019

Le service Citrix Virtual Apps and Desktops présente les problèmes connus suivants :

- La création d'un catalogue de machines dans Azure entraîne le retard du lancement d'une application. Machine Creation Services (MCS) prend un instantané de la machine virtuelle principale, puis crée un disque à partir de cet instantané. Dans les déploiements avec des machines virtuelles non gérées, l'instantané copie le disque dur virtuel, puis crée une machine virtuelle à partir du disque copié. Cette approche a un impact négatif sur les performances car elle introduit des niveaux élevés d'utilisation du disque et du processeur pendant une période prolongée jusqu'à ce que la configuration initiale du disque soit finalisée. Ce problème de performances entraîne une augmentation des coûts dans les environnements Azure. Par exemple, les déploiements d'une taille d'image de 80 Go utilisant un stockage Premium pour un instantané d'image préparé pourraient entraîner une augmentation des coûts d'environ 6 \$ US. Cette augmentation des coûts est causée par les caractéristiques de performance introduites par le lancement tardif d'une application. [PMCS-3934]
- Si vous utilisez Azure AD Domain Services : les noms UPN de connexion à Workspace (ou StoreFront) doivent contenir le nom de domaine qui a été spécifié lors de l'activation de Azure AD Domain Services. Les connexions ne peuvent pas utiliser les noms UPN d'un domaine personnalisé que vous créez, même si ce domaine personnalisé est désigné comme le domaine principal.
- Citrix Studio permet l'attribution de plusieurs règles d'attribution de bureau (DAR) pour différents utilisateurs ou groupes d'utilisateurs à un seul VDA du groupe de mise à disposition. StoreFront affiche le bureau attribué avec le nom d'affichage correspondant selon le DAR de l'utilisateur connecté. Toutefois, Director ne prend pas en charge les fichiers DAR et affiche le bureau attribué à l'aide du nom de groupe de mise à disposition indépendamment de l'utilisateur connecté. Par conséquent, vous ne pouvez pas mapper un bureau spécifique à une machine dans Director. [DNA-53578]

Solution : pour mapper le bureau attribué affiché dans StoreFront au nom du groupe de mise à disposition affiché dans Director, utilisez la commande PowerShell suivante :

```
1 Get-BrokerDesktopGroup' | Where-Object {
2   $_.Uid -eq (Get-BrokerAssignmentPolicyRule | Where-Object {
3     $_.PublishedName -eq "<Name on StoreFront>" }
4   ).DesktopGroupUid }
5 | Select-Object -Property Name, Uid
```

- Lors du déploiement sur Azure et la création d'une version 7.9 (ou ultérieure) d'un catalogue MCS avec le cache en écriture différée activé, une erreur se produit. En outre, vous ne pouvez rien créer qui soit lié à Personal vDisk pour Microsoft Azure. Pour contourner le problème, sélectionnez

tionnez une autre version de catalogue à déployer sur Azure ou désactivez le cache en écriture différée. Pour désactiver le cache en écriture différée lorsque vous créez un catalogue, décochez les cases **Mémoire allouée au cache** et **Taille du cache disque** sur la page **Machines**.

- Les rapports PDF exportés avec les graphiques de l'onglet **Surveiller > Tendances** générés pour le dernier mois ayant 28/30 jours, ne comportent pas l'axe X. Ce problème ne se produit pas si le mois a 31 jours ou lorsque vous exportez au format Excel. [DIR-184]

Pour les problèmes liés aux VDA actuels, consultez la section [Problèmes connus](#).

Configuration système requise

March 6, 2019

REMARQUE :

vous trouverez des informations sur les changements de nom de produit [ici](#).

Introduction

La configuration système requise des composants non couverts dans ce document (telles que Store-Front, application Citrix Workspace et Citrix Provisioning) est décrite dans leur documentation respective.

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 obtenir davantage d'informations sur la globalisation, veuillez consulter l'article [CTX119253](#).

Nous ne pouvons pas fournir de recommandations relatives au dimensionnement des VM chargées de mettre à disposition des applications et postes de travail en raison de la nature complexe et dynamique des offres de matériel. Chaque déploiement a des besoins uniques. En général, le dimensionnement d'une VM de Citrix Virtual Apps 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.

Rappel : dans un déploiement Citrix Virtual Apps and Desktops Service, vous n'avez pas besoin d'installer ni de gérer les composants principaux (Delivery Controller, la base de données de site, Studio et Director).

Cloud Connector

Pour des informations complètes, consultez la section [Installation de Cloud Connector](#).

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

Systèmes d'exploitation pris en charge :

- Windows 10
 - Pour connaître les éditions prises en charge, voir l'article [CTX224843](#).
 - Pour les problèmes connus de Citrix avec la version 1709, voir l'article [CTX229052](#).
 - La redirection de la composition du bureau et le mode graphique d'ancienne génération ne sont pas pris en charge sur Windows 10.

Exigences :

- Microsoft .NET Framework 4.7.1 est automatiquement installé si cette version ou une version ultérieure n'est pas déjà installée.
- 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 Citrix Virtual Desktops Remote PC Access sur Windows 10.

Plusieurs fonctionnalités d'accélération multimédia (telles que la redirection Windows Media HDX Mediasream) 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 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 Windows Server 2016. Consultez [Server VDI](#) pour plus d'informations.

Pour plus d'informations sur l'installation d'un VDA sur une machine Windows 7, voir [Systèmes d'exploitation antérieurs](#).

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

Systèmes d'exploitation pris en charge :

- Windows Server 2019, éditions Standard et Datacenter
- Windows Server 2016, édition Standard et Datacenter
- Windows Server 2012 R2, édition Standard et Datacenter.

Le programme d'installation déploie automatiquement les composants suivants :

- Microsoft .NET Framework 4.7.1 est automatiquement installé si cette version ou une version ultérieure n'est pas déjà installée.
- 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. Cela déclenche un redémarrage.

Plusieurs fonctionnalités d'accélération multimédia (telles que la redirection Windows Media HDX Mediasream) 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 versions de Windows Server, la fonctionnalité Media Foundation est installée via le Gestionnaire de serveur. Toutefois, N éditions n'incluent pas certaines technologies multimédia ; vous pouvez obtenir ce logiciel depuis Microsoft ou un composant tiers.

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](#).

Pour plus d'informations sur l'installation d'un VDA sur une machine Windows Server 2008 R2, voir [Systèmes d'exploitation antérieurs](#).

Hôtes et ressources de virtualisation

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. L'article [Connexions et ressources](#) répertorie les sources d'informations de l'hôte.

- **Microsoft Azure Resource Manager**
- **XenServer**
 - XenServer 7.6
 - XenServer 7.1 LTSR (CU2 uniquement)

- **VMware vSphere (vCenter + ESXi)**

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

- VMware vSphere 6.7
- VMware vSphere 6.5
- VMware vSphere 6.0
- VMware vSphere 5.5
- Boîtier VMware vCenter 5.5, 6 et 6.5

- **Microsoft 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

- **services Web Amazon (AWS)**

- Vous pouvez configurer des applications et des bureaux sur les systèmes d'exploitation Windows pris en charge.
- Le service Amazon de la base de données relationnelle (RDS) n'est pas pris en charge.

- **Nutanix Acropolis**

- Lors de l'utilisation de Citrix Provisioning : 4.5 (ou versions ultérieures prises en charge)
- Lors de l'utilisation de MCS : 4.6.1 (ou versions ultérieures prises en charge)

- **Oracle Cloud Infrastructure (OCI) Classic**

Pour plus d'informations, consultez le guide de déploiement : [Déploiement de Citrix Cloud XenApp and XenDesktop Service avec Oracle Cloud Infrastructure Classic](#).

- **Microsoft Azure Classic** (*obsolète*)

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

Pour plus d'informations sur Active Directory, consultez la section [Active Directory].(/fr-fr/citrix-virtual-apps-desktops/technical-overview/active-directory.html)

Technologies HDX

Pour accéder aux informations de prise en charge et de configuration requise pour les fonctionnalités HDX, consultez la section [HDX](#).

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.

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 3.0.1 est la version minimale prise en charge avec cette version. Pour utiliser la fonctionnalité de préférence de zone, vous devez utiliser StoreFront 3.7 et Citrix Gateway (anciennement NetScaler Gateway) 11.0-65.x au minimum

Lors de l'utilisation de Citrix Provisioning (anciennement appelé Provisioning Services) avec cette version, la version minimale de Provisioning Services prise en charge est la version 7.0.

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. Visual Studio 2015 runtime doit être installé sur la machine sur laquelle vous installez CitrixGroupPolicyManagement_x64.msi. Pour plus d'informations, veuillez consulter la documentation Microsoft.

Plusieurs cartes d'interface réseau sont prises en charge.

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 l'application Citrix Workspace 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. 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](#).

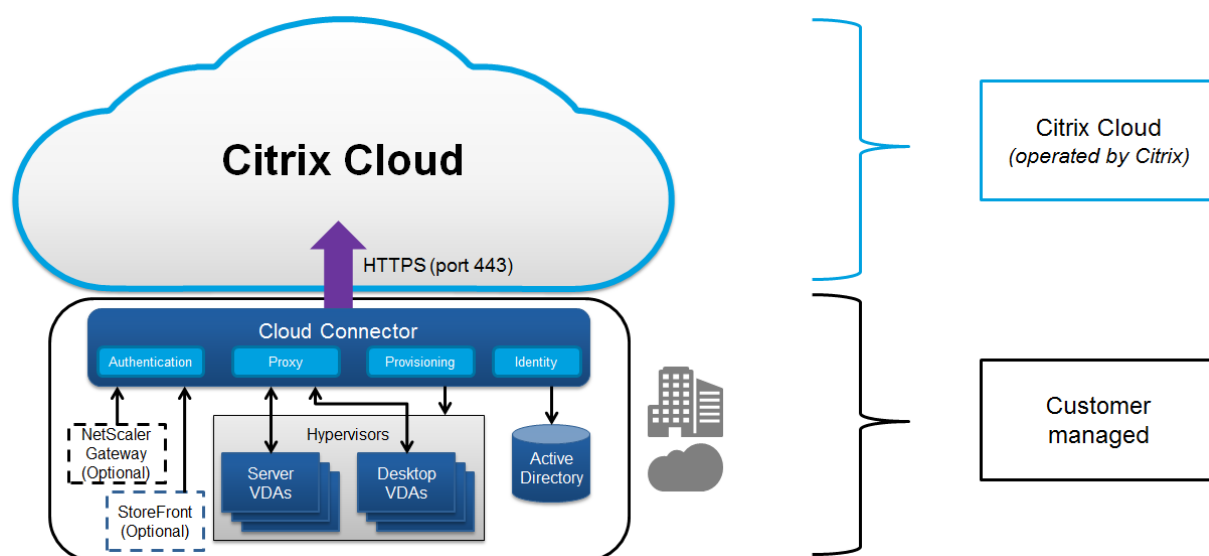
Vue d'ensemble de la sécurité technique

March 6, 2019

Vue d'ensemble de la sécurité technique

Ce document s'applique à tous les services Citrix Virtual Apps et Desktops hébergés dans Citrix Cloud, y compris Citrix Virtual Apps Essentials et Citrix Virtual Desktops Essentials.

Citrix Cloud permet de gérer le fonctionnement du plan de contrôle pour les environnements Citrix Virtual Apps et Desktops. Cela comprend les Delivery Controller, les consoles de gestion, la base de données SQL, le serveur de licences et éventuellement StoreFront et Citrix Gateway (anciennement NetScaler Gateway). Les Virtual Delivery Agents (VDA) hébergeant les bureaux et applications restent sous le contrôle du client dans le datacenter de leur choix, sur cloud ou sur site. Ces composants sont connectés au service de cloud à l'aide d'un agent appelé le Citrix Cloud Connector. Si les clients choisissent d'utiliser Citrix Workspace, ils peuvent également choisir d'utiliser Citrix Gateway Service au lieu d'exécuter Citrix Gateway dans leur datacenter. Le schéma ci-dessous illustre le service et ses limites de sécurité.



Flux de données

Étant donné que les composants hébergés par le service de cloud n'incluent pas les VDA, les données applicatives du client et les images principales requises pour le provisioning sont toujours hébergées au sein de l'installation du client. Le plan de contrôle a accès aux métadonnées, telles que les noms d'utilisateur, les noms de machines et les raccourcis d'application, ce qui limite l'accès à la propriété intellectuelle du client à partir du plan de contrôle.

Les données qui transitent entre le cloud et les locaux du client utilisent une connexion sécurisée TLS sur le port 443.

Isolation des données

Citrix Virtual Apps and Desktops Service stocke uniquement les métadonnées requises pour la communication et le contrôle des applications et bureaux du client. Les informations sensibles, y compris les images principales, les profils utilisateur et d'autres données applicatives restent dans les locaux du client ou dans leur abonnement avec un fournisseur de cloud public.

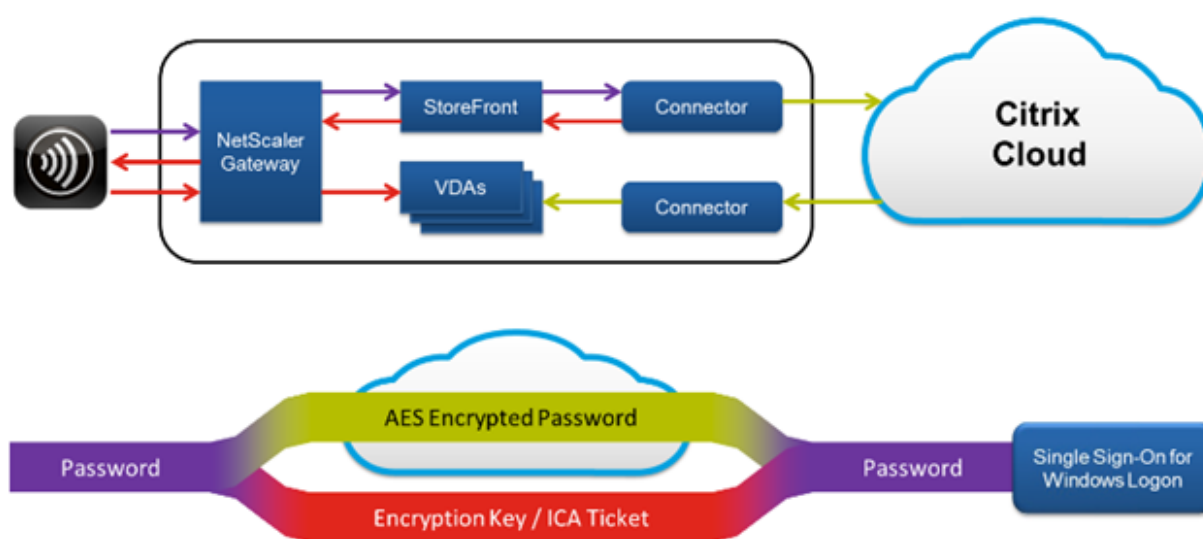
Éditions de service

Les fonctionnalités de Citrix Virtual Apps and Desktops Service varient d'une édition à l'autre. Par exemple, Citrix Virtual Apps Essentials ne prend en charge que Citrix Gateway Service et Citrix Workspace. Consultez la documentation Produit pour en savoir plus sur les fonctionnalités prises en charge.

Gestion des informations d'identification

Le service gère quatre types d'informations d'identification :

- Informations d'identification de l'utilisateur : lors de l'utilisation d'un StoreFront géré par le client, les informations d'identification utilisateur sont cryptées par le Citrix Cloud Connector à l'aide du cryptage AES-256 et d'une clé à usage unique générée aléatoirement pour chaque démarrage. La clé n'est jamais transmise au cloud et elle est uniquement renvoyée à l'application Citrix Workspace. Cette clé est ensuite transmise au VDA directement par l'application Citrix Workspace afin de décrypter le mot de passe utilisateur lors du lancement de session pour une expérience SSO. Le flux entier est affiché dans la figure ci-dessous.



- Informations d'identification d'administrateur : les administrateurs s'authentifient auprès de Citrix Cloud, qui utilise le système d'authentification de Citrix Online. Ceci génère un jeton Web signé JSON (JWT) à usage unique qui donne à l'administrateur l'accès à Citrix Virtual Apps and Desktops Service.
- Mots de passe d'hyperviseur : les hyperviseurs sur site qui requièrent un mot de passe pour l'authentification disposent d'un mot de passe généré par l'administrateur et stocké et crypté directement dans la base de données SQL dans le cloud. Les clés d'homologue sont gérées par Citrix pour s'assurer que les informations d'identification de l'hyperviseur sont uniquement disponibles pour les processus authentifiés.
- Informations d'identification Active Directory (AD) : Machine Creation Services utilise le connecteur pour créer des comptes de machines dans l'Active Directory d'un client. Étant donné que le compte de machine du connecteur possède uniquement un accès en lecture à Active Directory, l'administrateur est invité à entrer des informations d'identification pour chaque opération de création ou de suppression de machine. Ces informations d'identification sont uniquement stockées en mémoire et conservées pour un seul événement de provisioning.

Considérations de déploiement

Citrix recommande aux utilisateurs de consulter la documentation sur les meilleures pratiques pour le déploiement d'applications et de VDA Citrix Gateway dans leurs environnements. Considérations supplémentaires relatives au déploiement de StoreFront sur site et la connectivité réseau :

Exigences d'accès au réseau de Citrix Cloud Connector

Les Citrix Cloud Connector requièrent uniquement le trafic sortant vers Internet sur le port 443 et peuvent être hébergés derrière un proxy HTTP.

- Le protocole de communication utilisé dans Citrix Cloud pour HTTPS est TLS 1.0, 1.1 ou 1.2.
- Dans le réseau interne, le connecteur doit avoir accès aux composants suivants pour Citrix Virtual Apps and Desktops Service :
 - VDA (port 80, entrant et sortant) ainsi que 1494 et 2598 entrants si vous utilisez Citrix Gateway Service
 - Serveurs StoreFront (port 80 entrant)
 - Citrix Gateway, si configuré comme une STA (le port 80 entrant)
 - Contrôleurs de domaine Active Directory
 - Hyperviseurs (sortant uniquement ; veuillez consulter la documentation de l'hyperviseur pour les ports spécifiques)

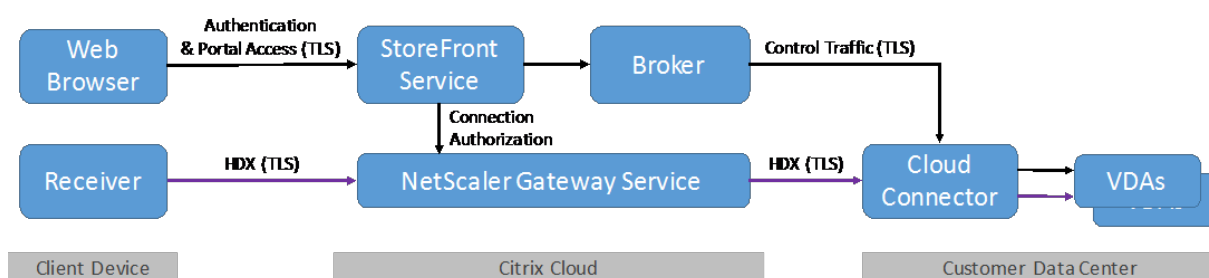
Le trafic entre les VDA et les connecteurs cloud est crypté à l'aide de la sécurité au niveau du message de Kerberos.

StoreFront géré par le client

Un StoreFront géré par le client offre davantage d'options de configuration de sécurité et une plus grande flexibilité pour l'architecture de déploiement, y compris la possibilité de gérer les informations d'identification utilisateur sur site. StoreFront peut être hébergé derrière Citrix Gateway afin de fournir un accès à distance sécurisé, appliquer une authentification multi-facteurs et ajouter d'autres fonctionnalités de sécurité.

Citrix Gateway Service et Citrix Workspace

L'utilisation de Citrix Gateway Service évite le besoin de déployer Citrix Gateway dans les datacenters des clients. Pour utiliser Citrix Gateway Service, il est obligatoire d'utiliser Storefront Service mis à disposition depuis Citrix Cloud. Le flux de données lors de l'utilisation de Citrix Gateway Service est affiché dans la figure ci-dessous.



Remarque : ce diagramme illustre les flux de données logiques. Toutes les connexions TLS entre le Cloud Connector et Citrix Cloud sont initiées du Cloud Connector vers Citrix Cloud. Aucun mappage de port de pare-feu entrant n'est requis.

Fin de prise en charge des versions TLS

Pour améliorer la sécurité de Citrix Virtual Apps and Desktops Service, Citrix bloquera toute communication via TLS (Transport Layer Security) 1.0 et 1.1, à compter du 15 mars 2019.

Impact sur l'utilisateur

Si vous utilisez une version de Citrix Receiver inférieure (antérieure) à celle répertoriée ci-dessous, tout utilisateur essayant de se connecter à Citrix Workspace ne pourra pas se connecter.

Receiver	Version
Windows	4.2.1000
Mac	12.0
Linux	13.2
Android	3.7
iOS	7.0

Que faire

Dans la mesure où cette modification perturbera vos utilisateurs, assurez-vous que tous les Citrix Receiver sont mis à niveau vers une version ultérieure. Les versions ultérieures utilisent TLS 1.2. Accédez à : <https://www.citrix.com/products/receiver/>.

Vous pouvez également mettre à niveau vers notre nouvelle application Citrix Workspace qui utilise TLS 1.2. Accédez à : <https://www.citrix.com/downloads/workspace-app/>. Vous trouverez des informations supplémentaires sur l'application Citrix Workspace sur <https://www.citrix.com/products/>

[workspace-app/](#).

Important :

Pour obtenir des instructions supplémentaires, consultez le document [CTX247067](#).

Si vous devez utiliser TLS 1.0 ou TLS 1.1

Si vous devez continuer à utiliser TLS 1.0 ou 1.1 (par exemple, si vous utilisez un client léger basé sur une version antérieure de Receiver pour Linux), installez StoreFront dans votre emplacement de ressource et pointez tous les Citrix Receiver vers StoreFront.

Plus d'informations

Consultez les ressources suivantes pour de plus amples informations sur la sécurité :

- Site de sécurité de Citrix : <https://www.citrix.com/security>
- [Guide de déploiement sécurisé pour NetScaler](#)
- [Considérations de sécurité et meilleures pratiques](#)
- [Cartes à puce](#)
- [Transport Layer Security \(TLS\)](#)

Remarque :

Ce document vise à fournir au lecteur une introduction et un aperçu des fonctionnalités de sécurité de Citrix Cloud et à définir le partage des responsabilités entre Citrix et les clients en ce qui concerne la sécurisation du déploiement de Citrix Cloud. Il n'est pas conçu pour servir de manuel de configuration et d'administration de Citrix Cloud ou de l'un de ses composants ou services.

Méthodes de mise à disposition

November 30, 2018

Une seule méthode de mise à disposition ne répondra probablement pas à tous vos besoins.

Vous pouvez envisager plusieurs méthodes de mise à disposition d'applications. Le choix de la méthode appropriée permet d'améliorer la capacité à monter en charge, la gestion et l'expérience utilisateur.

- **Application installée** : l'application fait partie de l'image de bureau de base. Le processus d'installation implique l'exécution de fichiers dll, exe et d'autres fichiers copiés sur le lecteur d'image ainsi que des modifications du registre. Pour de plus amples informations, consultez la section [Créer des catalogues de machines](#).

- **Applications livrées en streaming (Microsoft App-V) :** l'application est profilée et mise à disposition à la demande sur les bureaux du réseau. Les fichiers d'applications et les paramètres du Registre sont placés dans un conteneur sur le bureau virtuel et isolés du système d'exploitation et les uns des autres, ce qui permet de résoudre les problèmes de compatibilité. Pour plus d'informations, consultez [App-V](#).
- **Application en couche (Citrix application Layering) :** chaque couche contient une seule application, un seul agent ou un seul système d'exploitation. En intégrant une couche d'OS, une couche de plate-forme (VDA, agent Citrix Provisioning) et de multiples couches d'applications, un administrateur peut facilement créer de nouvelles images déployables. Le layering simplifie les activités de maintenance régulières, car un système d'exploitation, une application et un agent existent dans une seule couche. Lorsque vous mettez à jour la couche, toutes les images déployées contenant cette couche sont mises à jour. Consultez la section [Citrix application Layering](#).
- **Application Windows hébergée :** application installée sur un hôte Citrix Virtual Apps multi-utilisateur et déployée en tant qu'application et non en tant que bureau. Un utilisateur accède à l'application Windows hébergée en toute transparence à partir d'un bureau VDI ou d'une machine de point de terminaison, ce qui occulte le fait que l'application est exécutée à distance. Pour de plus amples informations, consultez la section [Créer des groupes de mise à disposition](#).
- **Application locale :** application déployée sur la machine de point de terminaison. L'interface applicative s'affiche dans la session de VDI hébergée de l'utilisateur, bien qu'elle soit exécutée sur le point de terminaison. Pour de plus amples informations, consultez [Local App Access et redirection d'adresse URL](#).

Pour les bureaux, vous pouvez envisager des bureaux publiés Citrix Virtual Apps ou des bureaux VDI.

Applications et bureaux publiés avec Citrix Virtual Apps

Utilisez les machines avec OS de serveur pour mettre à disposition des applications publiées et des bureaux publiés Citrix Virtual Apps.

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 des 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 datacenter.
- 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 de machines 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 session supplémentaire 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.

VM hosted Apps

Utilisez des 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. Vous voulez fournir à ces utilisateurs des applications affichées 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 datacenter, ce qui fournit une solution de mise à disposition d'applications 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 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 nécessaires au 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.

Bureaux VDI

Utilisez des machines avec OS de bureau pour mettre à disposition des bureaux VDI Citrix Virtual Desktops.

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 Citrix Virtual Apps, 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. Cela fournit aux utilisateurs un haut degré de personnalisation.

Lorsque vous créez un catalogue de machines pour les bureaux VDI, vous créez un de ces types de bureaux :

- **Bureaux aléatoires non persistants, également appelé bureaux VDI regroupés :** chaque fois qu'un utilisateur ouvre une session sur l'un de ces bureaux, cet utilisateur se connecte à un bureau sélectionné à partir d'un groupe de bureaux. Ce groupe est basé sur une image principale unique. Toutes les modifications apportées au bureau sont perdues lorsque la machine redémarre.
- **Bureau statique non persistant :** lors de la première connexion, un bureau est affecté à un utilisateur à partir d'un pool de bureaux. (Chaque machine dans le pool est basée sur une image principale unique.) Après la première utilisation, chaque fois qu'un utilisateur ouvre une session sur l'un de ces bureaux, cet utilisateur se connecte au même bureau qui lui a été affecté lors

de la première utilisation. Toutes les modifications apportées au bureau sont perdues lorsque la machine redémarre.

- **Bureau statique persistant** : à l'inverse des autres types de bureaux VDI, les utilisateurs peuvent entièrement personnaliser ces bureaux. Lors de la première connexion, un bureau est affecté à un utilisateur à partir d'un pool de bureaux. Les ouvertures de session suivantes de cet utilisateur se connectent au bureau qui a été affecté lors de la première utilisation. Les modifications apportées au bureau sont conservées lorsque la machine redémarre.

Installer et configurer

March 6, 2019

Remarque :

vous trouverez des informations sur les changements de nom de produit [ici](#).

Utilisez la séquence suivante pour configurer votre déploiement de Citrix Virtual Apps and Desktops Service. Passez en revue l'ensemble du processus avant de commencer le déploiement afin de savoir à quoi vous attendre. Des liens sont fournis vers la documentation et les vidéos du produit.

Si vous ne connaissez pas les composants et la terminologie utilisés dans un déploiement Citrix Virtual Apps and Desktops, consultez la section [Citrix Virtual Apps and Desktops Service](#).

Mise en route

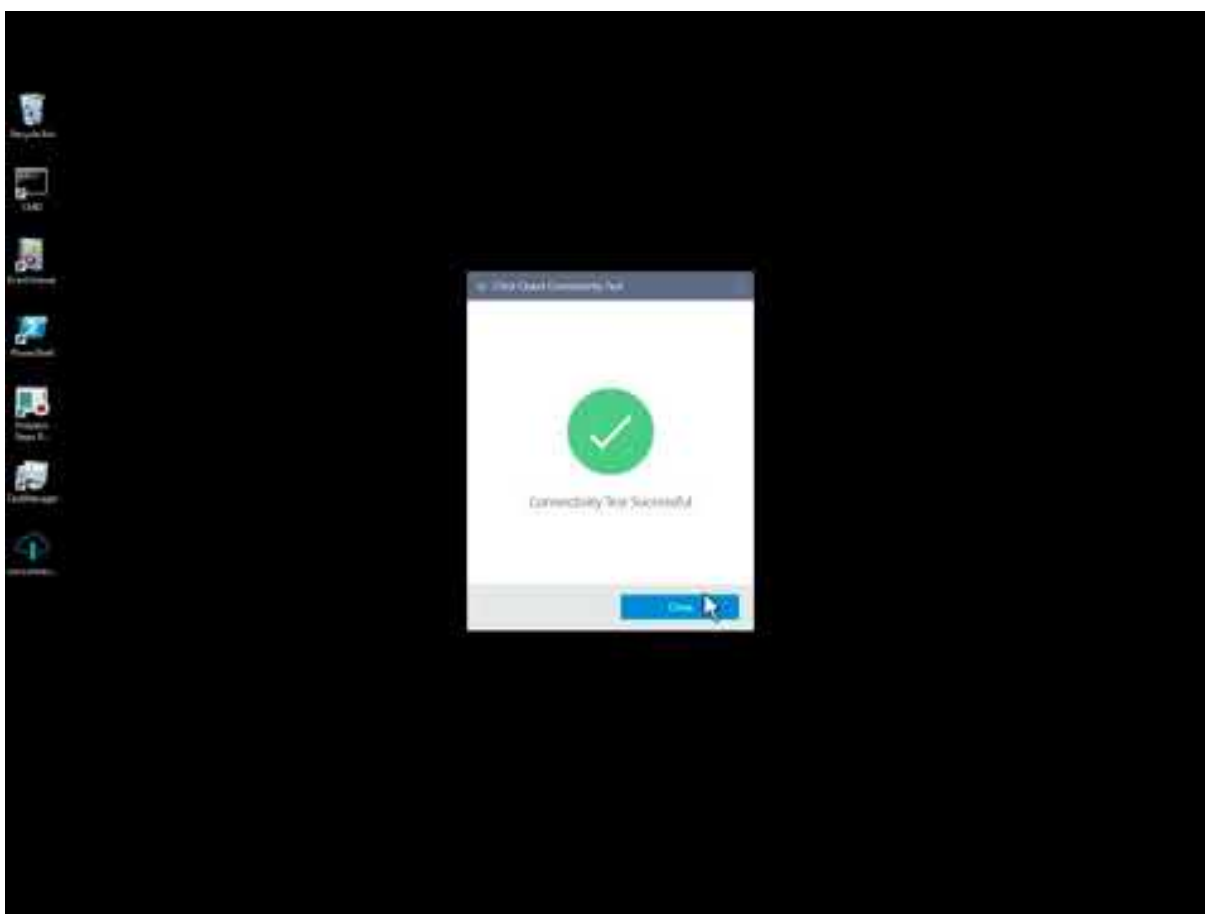
[Commencez](#) en ouvrant un compte Citrix et en demandant une version d'évaluation de Citrix Virtual Apps and Desktops Service.

Configurer un emplacement de ressources et installer des Cloud Connector

Les emplacements de ressources contiennent des serveurs d'infrastructure (tels que Active Directory et Citrix Cloud Connector) ainsi que les machines qui fournissent des applications ou des bureaux aux utilisateurs.

- Commencez la séquence d'installation en configurant votre hyperviseur hôte ou votre service cloud, et Active Directory : [Configurer des emplacements de ressources](#).
- Continuez la configuration de l'emplacement de ressources : [Installer des Cloud Connector](#).

Vidéo sur la façon d'installer des Cloud Connector.



Créer une connexion à l'emplacement de ressources

Après avoir ajouté un emplacement de ressources, utilisez la console de gestion de Studio pour [créer une connexion](#) entre le plan de contrôle du service et l'emplacement des ressources.

Si vous déployez une preuve de concept simple, cette étape n'est pas nécessaire.

Installer des VDA

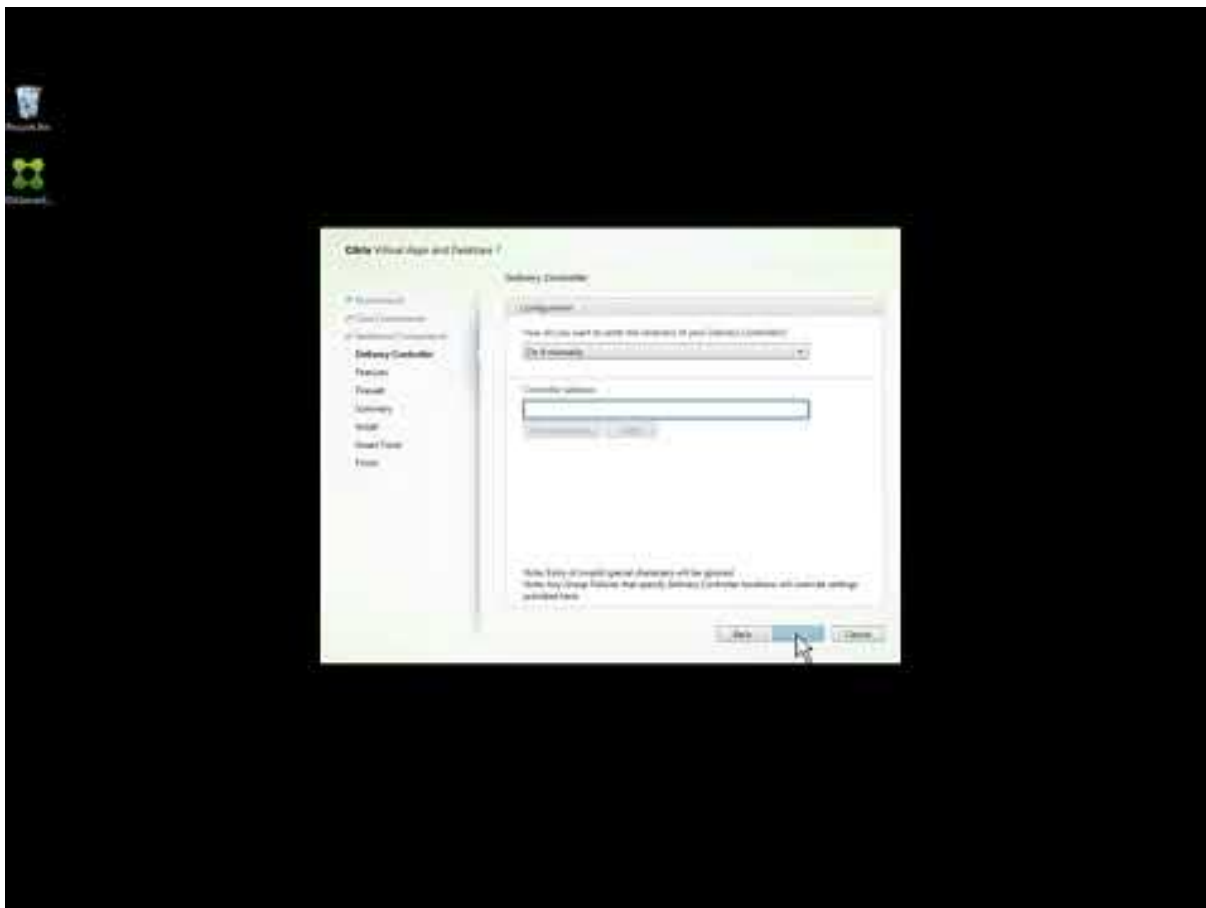
Chaque machine qui fournit des applications et des bureaux aux utilisateurs doit être équipée d'un Virtual Delivery Agent (VDA) Citrix. Si vous utilisez une image principale pour provisionner des machines virtuelles, installez un VDA sur l'image principale.

- Pour des instructions d'installation, consultez la section [Installer des VDA](#). En plus d'instructions détaillées, cet article contient également des informations techniques sur les VDA et décrit les programmes d'installation de VDA disponibles.
- Pour des instructions d'installation de VDA avec la ligne de commande, consultez la section [Installer des VDA à l'aide de la ligne de commande](#).

Pour un déploiement Remote PC Access, installez un VDA pour OS de bureau sur chaque PC de bureau physique. Vous pouvez utiliser vos méthodes ESD (distribution électronique de logiciels) existantes.

Si vous déployez une preuve de concept simple, téléchargez et installez un VDA sur une machine.

Vidéo sur la façon de télécharger et d'installer un VDA.



Pour un déploiement complet, vous pouvez utiliser les outils Citrix pour provisionner un catalogue de machines contenant plusieurs machines.

Vous créez une image principale sur votre hyperviseur ou service cloud à utiliser pour le provisioning. En plus d'installer des applications ou des bureaux sur l'image principale, vous installez un VDA. Chaque machine provisionnée à l'aide de cette image principale contient ce VDA.

La création d'une image principale est décrite dans la section [Créer des catalogues de machines](#).

Créer un catalogue de machines

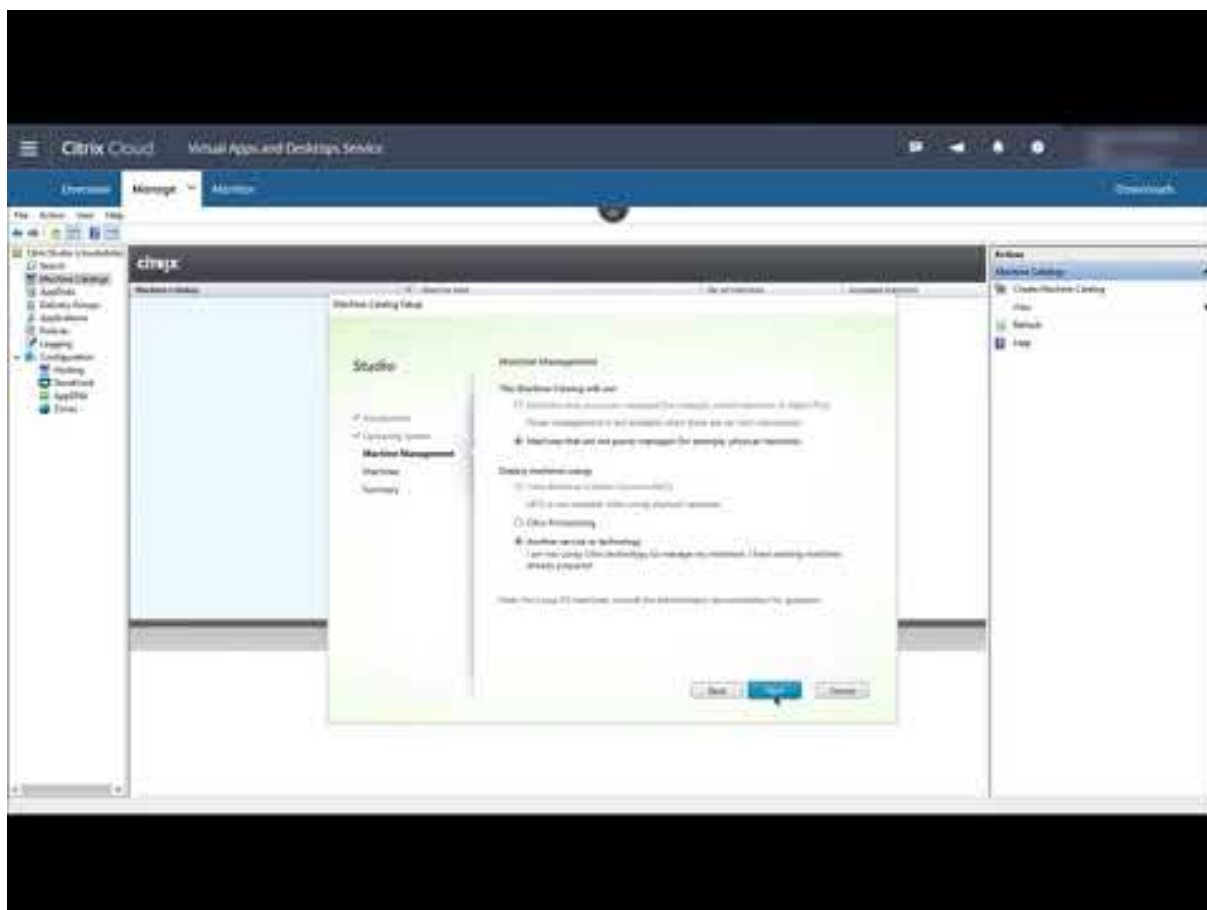
Remarque :

Si vous utilisez Azure Resource Manager pour héberger vos ressources, vous pouvez éventuelle-

ment utiliser la méthode Déploiement rapide d'Azure au lieu de la méthode Configuration complète décrite dans la vidéo ci-dessous. Pour plus de détails, voir [Déploiement rapide d'Azure](#).

Après avoir créé une connexion à votre emplacement de ressources, le workflow de Studio vous aide à [créer un catalogue de machines](#). Un catalogue contient des machines physiques ou virtuelles qui fournissent les applications ou les bureaux à vos utilisateurs.

Vidéo sur la façon de créer un catalogue de machines.



La documentation Produit décrit également comment créer et utiliser une image principale pour créer un catalogue de machines provisionnées avec un outil Citrix.

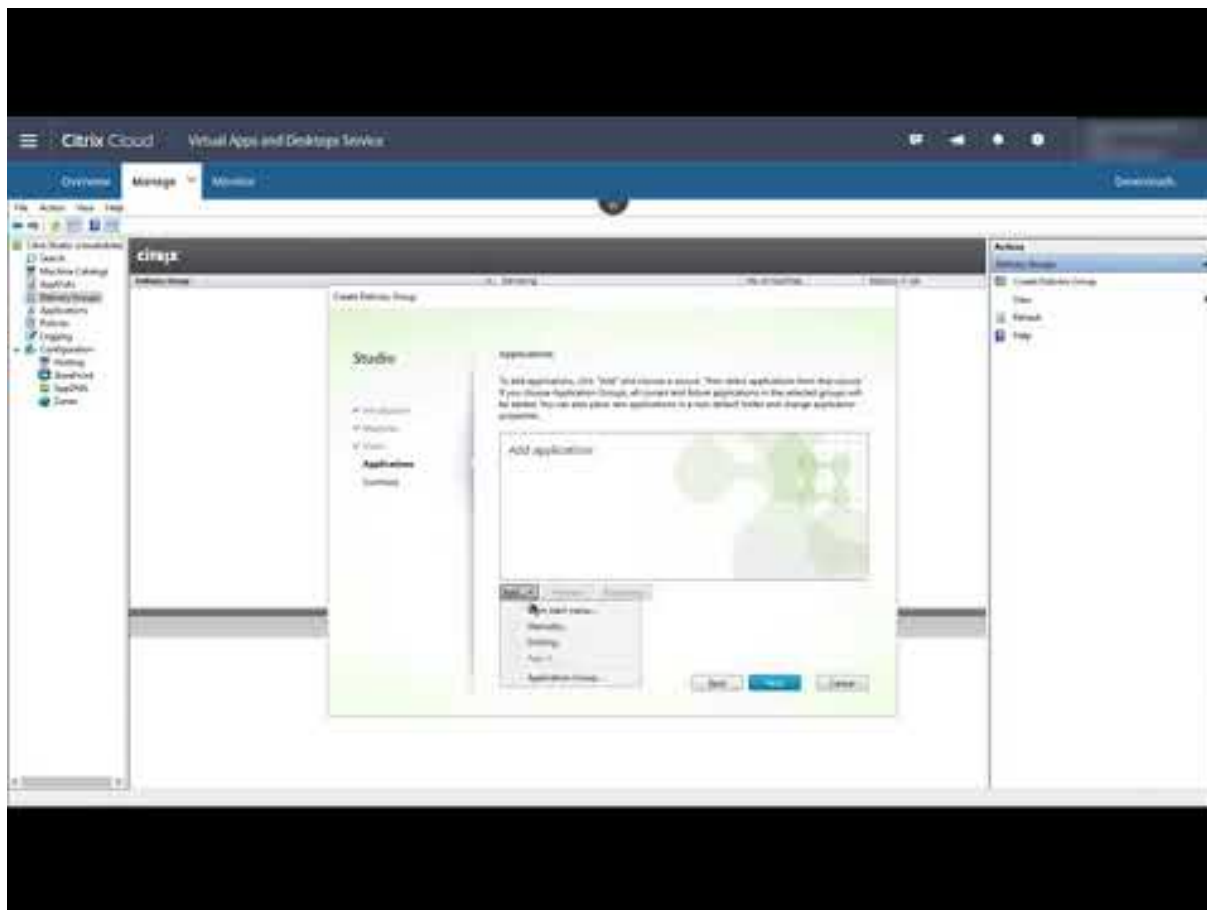
Créer un groupe de mise à disposition

Après la création du premier catalogue de machines, Studio vous guide dans le processus de [création d'un groupe de mise à disposition](#).

Un groupe de mise à disposition spécifie les machines qui peuvent être utilisées depuis un catalogue de machines sélectionné. Vous pouvez spécifier les utilisateurs qui peuvent utiliser ces machines et les applications disponibles sur ces machines.

Éventuellement, vous pouvez spécifier les utilisateurs et applications via des offres de bibliothèque Citrix Cloud, plutôt que directement dans un groupe de mise à disposition.

Vidéo sur la façon de créer un groupe de mise à disposition.



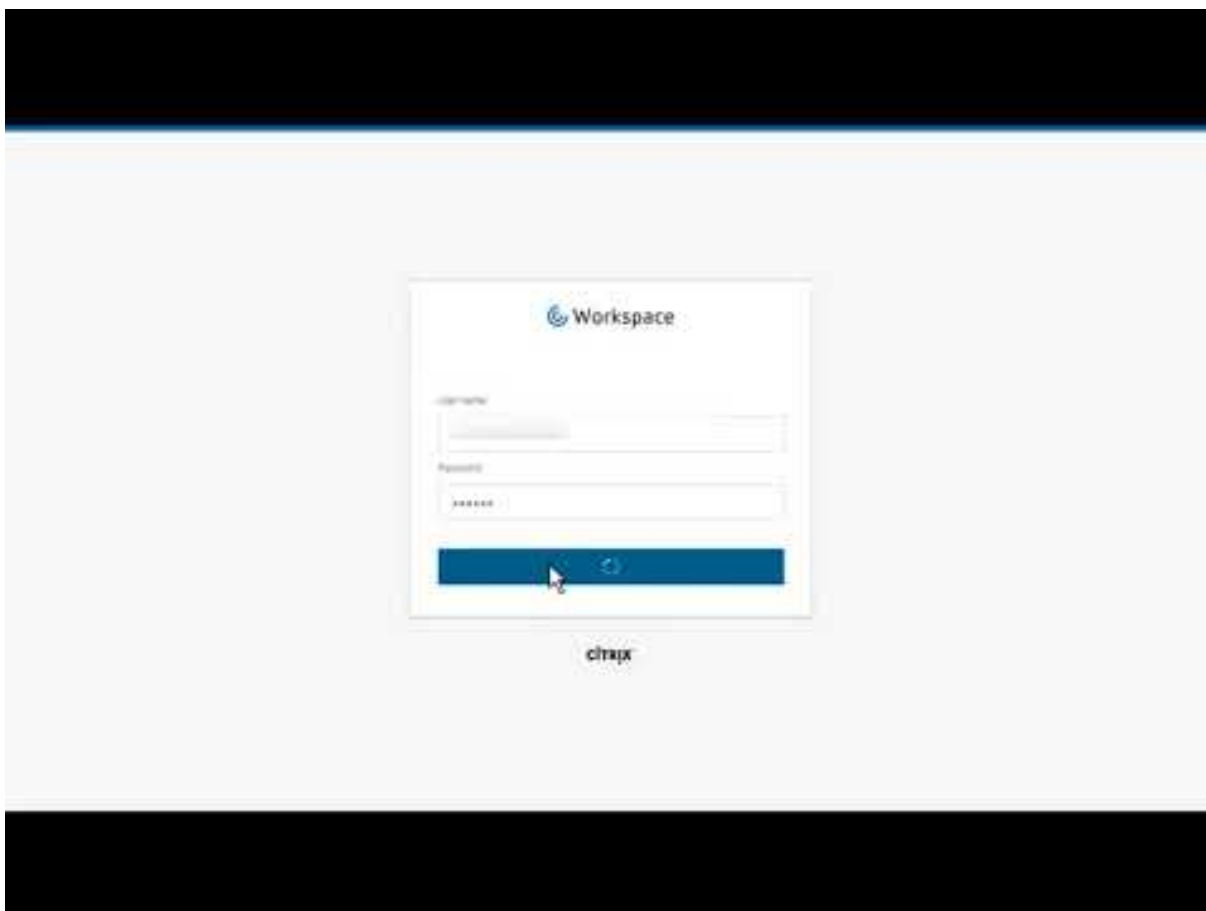
Lancer des applications et des bureaux

Après avoir terminé les étapes précédentes, la publication se produit automatiquement. Les applications et bureaux que vous avez spécifiés sont mis à la disposition des utilisateurs dans leur espace de travail. Un utilisateur accède simplement à l'URL de l'espace de travail et sélectionne une application ou un bureau, qui se lance immédiatement.

En tant qu'administrateur, vous pouvez trouver l'URL de l'espace de travail à deux endroits :

- Dans la console Citrix Cloud, sélectionnez **Configuration de l'espace de travail** et cliquez sur le menu dans l'angle supérieur gauche. Pour plus d'informations, consultez la section [Configuration de l'espace de travail](#).
- Dans la page d'accueil de Citrix Virtual Apps and Desktops Service, l'URL de l'espace de travail apparaît au bas de la page.

Vidéo courte sur le lancement d'applications et de bureaux depuis votre espace de travail.



Mise en route

October 10, 2018

Lorsque vous évaluez ou achetez le service Citrix Virtual Apps and Desktops, l'équipe Citrix Service Operations fournit une aide continue pour l'intégration. Cette équipe communique également avec vous pour s'assurer que les principaux composants du service Citrix Virtual Apps and Desktops sont exécutés et configurés correctement.

Les étapes d'intégration sont les suivantes :

1. Ouvrir un compte Citrix et demander un compte d'évaluation du service Citrix Virtual Apps and Desktops.
2. Discuter des exigences d'intégration avec Citrix.
3. Compléter les paramètres dans le portail Citrix Cloud.

Pour ouvrir un compte Citrix et demander une version d'évaluation, contactez votre représentant Citrix. Lorsque vous êtes prêt à continuer, allez à <https://onboarding.cloud.com>.

Une fois connecté, dans la vignette du service Citrix Virtual Apps and Desktops, cliquez sur **Demander évaluation**. Le texte devient ensuite **Évaluation demandée**. Vous recevrez un e-mail lorsque votre version d'évaluation est disponible.

En attendant la version d'évaluation, vous pouvez consulter les informations référencées dans *Autres ressources*. Bien que Citrix héberge et délivre votre service Citrix Virtual Apps and Desktops, vous gérez les machines qui mettent à disposition les applications et bureaux, ainsi que les applications et les utilisateurs. Vous pouvez mettre à profit cette période pour configurer l'infrastructure de vos services d'entreprise, tels que Active Directory.

Lorsque vous êtes autorisé à accéder à la version d'évaluation, le texte de la vignette du service Citrix Virtual Apps and Desktops devient **Gérer**.

Lorsque vous cliquez sur **Gérer**, un workflow de configuration 1-2-3 s'ouvre dans la console de gestion de Studio. Toutefois, avant de pouvoir continuer avec ce workflow, configurez votre emplacement de ressources (ou définissez-le) en ajoutant des Citrix Cloud Connector.

Autres ressources

- Si vous n'avez pas encore configuré votre hyperviseur ou votre service de cloud, ou Active Directory, consultez la section [Configurer un emplacement de ressources](#).
- Si votre environnement hôte et Active Directory sont déjà configurés, consultez la section [Créer une connexion](#).
- Pour passer en revue l'ensemble du processus de configuration, consultez la section [Installer et configurer](#).

Configurer des emplacements de ressources

March 6, 2019

La configuration d'un emplacement de ressource commence par les tâches suivantes :

- Configurez votre environnement hôte (hyperviseur ou service cloud).
- Configurez votre domaine Active Directory.

À propos des emplacements de ressources

Si vous n'êtes pas familier avec les emplacements de ressources, consultez ces informations.

Que contient un emplacement de ressources ?

Les emplacements de ressources contiennent les ressources requises pour mettre des applications

et bureaux à la disposition des utilisateurs. Vous gérez ces éléments depuis Citrix Cloud et la console Studio. En général, les ressources comprennent :

- Contrôleur de domaine Active Directory
- Hyperviseurs ou services de cloud, appelés *hôtes*
- Virtual Delivery Agents (VDA)
- Citrix Gateway (facultatif) : pour activer l'accès externe sécurisé aux applications et bureaux proposés aux utilisateurs, ajoutez un boîtier Citrix Gateway VPX à l'emplacement de ressources et configurez Citrix Gateway (anciennement NetScaler Gateway).
- Serveurs Citrix StoreFront (facultatif)

Pour communiquer avec Citrix Cloud, chaque emplacement de ressources doit contenir un Citrix Cloud Connector. Au moins deux Cloud Connector par emplacement de ressources sont recommandés afin d'assurer une disponibilité permanente.

Un emplacement de ressource est considéré comme une zone dans un environnement de service Citrix Virtual Apps and Desktops.

Où dois-je placer l'emplacement de ressources ?

Un emplacement de ressources peut se trouver là où vous en avez besoin : dans un cloud public, cloud privé ou un datacenter local. Vous pouvez configurer plusieurs emplacements de ressources pour répondre aux besoins spécifiques de votre entreprise. La planification de l'emplacement des ressources peut dépendre de ce qui suit :

- Proximité des utilisateurs
- Proximité des données
- Exigences en matière de montée en charge
- Attributs de sécurité

Par exemple, un emplacement de ressources situé dans le datacenter de votre siège social peut servir les utilisateurs qui doivent être proches des données. Un autre emplacement de ressources dans un cloud public peut servir les utilisateurs à travers le monde. Ou, les emplacements de ressources situés dans des succursales peuvent fournir des applications qui sont plus à même de convenir aux employés de succursale en matière de proximité. Enfin, des applications restreintes peuvent être placées dans un emplacement de ressources distinct, afin d'en réduire la visibilité à d'autres ressources et utilisateurs sans avoir à configurer d'autres emplacements de ressources.

Configuration requise de l'hôte

Le service de cloud ou l'hyperviseur dans lequel vous provisionnez des VM qui fournissent des applications ou des bureaux aux utilisateurs peut avoir une autorisation ou des conditions d'installation uniques.

- Si l'hyperviseur ou le service de cloud requiert des réseaux virtuels ou d'autres éléments, suivez les instructions dans la documentation qui l'accompagne.
- Créez le cloud privé virtuel (VPC) ou les réseaux virtuels pour les machines que vous allez ajouter à votre emplacement de ressources, si nécessaire. Par exemple, si vous utilisez AWS, définissez un VPC avec des sous-réseaux publics et privés.
- Créez des règles appropriées pour sécuriser le trafic Internet entrant et sortant, ainsi que le trafic entre les machines dans le réseau virtuel. Par exemple, si vous utilisez AWS, assurez-vous que des règles appropriées sont configurées sur le groupe de sécurité du VPC de façon à ce que les machines dans le VPC soient accessibles uniquement aux adresses IP que vous spécifiez.

Consultez l'article pour le type d'hôte que vous utilisez.

- [Environnements de virtualisation Microsoft System Center Virtual Machine Manager](#)
- [Environnements de virtualisation Microsoft Azure Classic](#)
- [Environnements de virtualisation Microsoft Azure Resource Manager](#)
- [Environnements de virtualisation Amazon Web Services \(AWS\) et Citrix XenDesktop sur AWS](#)
- [Environnement de virtualisation XenServer](#)
- [Environnements de virtualisation VMware](#)

Active Directory

Provisionnez un serveur Windows, installez les services de domaine Active Directory et promouvez-le en contrôleur de domaine. Pour plus d'informations, consultez la documentation de Microsoft Active Directory.

- Vous devez disposer d'au moins un contrôleur de domaine exécutant les services de domaine Active Directory.
- N'installez aucun composant Citrix sur un contrôleur de domaine.
- N'utilisez pas de barre oblique (/) lorsque vous spécifiez les noms d'unité d'organisation dans Studio.

Pour des détails techniques, consultez :

- La section [Configuration système requise](#) répertorie les niveaux fonctionnels d'Active Directory pris en charge.
- [Active Directory](#) contient des détails sur le support Citrix
- [Niveaux fonctionnels Active Directory pris en charge](#)

Ajouter un emplacement de ressources dans Citrix Cloud

Pour ajouter un emplacement de ressources :

1. Connectez-vous à [Citrix Cloud](#).

2. Dans le menu en haut à gauche, sélectionnez **Emplacements des ressources**.
3. Si vous n'avez pas encore installé de Citrix Cloud Connector, vous êtes invité à en télécharger un. Suivez les instructions de la section [Installer des Cloud Connector](#).
4. Après avoir installé un Cloud Connector (de préférence au moins deux), revenez dans la console Citrix Cloud, entrez un nom pour l'emplacement de ressources et cliquez sur **Enregistrer**.

Autres ressources

[Installer des Cloud Connector](#)

Pour passer en revue l'ensemble du processus de configuration, consultez la section [Installer et configurer](#).

Environnements de virtualisation Microsoft Azure Resource Manager

March 6, 2019

Suivez les instructions dans cet article si vous utilisez Microsoft Azure Resource Manager pour provisionner des machines virtuelles dans votre déploiement de Citrix Virtual Apps and Desktops Service.

Nous supposons que vous connaissez les solutions 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.

Provisioning à la demande d'Azure

Lorsque vous utilisez MCS pour créer des catalogues de machines dans Azure Resource Manager, la fonctionnalité de provisioning à la demande d'Azure :

- Réduit vos coûts de stockage
- Accélère la création de catalogues
- Accélère les opérations d'alimentation de machine virtuelle (VM)

Pour l'administrateur, le provisioning à la demande ne modifie pas les procédures de création de connexions hôtes et de catalogues de machines MCS de Studio. Les différences résident dans la méthode

et le moment auxquels les ressources sont créées et gérées dans Azure et la visibilité des VM dans le portail Azure.

Avant que le provisioning à la demande d'Azure ne soit utilisé avec Citrix Virtual Apps and Desktops, lorsque MCS créait un catalogue, les VM étaient créées dans Azure durant le processus de provisioning.

Avec le provisioning à la demande d'Azure, les VM sont créées uniquement lorsque Citrix Virtual Apps and Desktops initie une action d'alimentation, une fois que le provisioning est terminé. Une VM est visible dans le portail Azure uniquement lorsqu'elle est exécutée. (Dans Studio, les VM sont visibles si elles sont en cours d'exécution.)

Lorsque vous créez un catalogue MCS, le portail Azure affiche les groupes de ressources, le groupe de sécurité réseau, les comptes de stockage, les interfaces réseau, les images de base et les disques d'identité. Le portail Azure n'affiche pas la VM tant que Citrix Virtual Apps and Desktops n'a pas initié une action d'alimentation pour celle-ci. (Ensuite, l'état de la VM dans Studio devient Activé.)

- Pour une machine regroupée, le disque du système d'exploitation et le cache en écriture différée existent uniquement lorsque la VM existe. L'utilisation du cache peut entraîner des économies de stockage significatives si vous arrêtez régulièrement les machines (par exemple, en dehors des heures de travail).
- Pour une machine dédiée, le disque du système d'exploitation est créé la première fois que la VM est démarrée. Il reste dans le stockage jusqu'à ce que l'identité de la machine soit supprimée.

Lorsque Citrix Virtual Apps and Desktops met une VM hors tension, l'identité de cette machine est supprimée dans Azure. Elle n'apparaît plus dans le portail Azure. (Dans Studio, l'état de la VM devient Désactivé.)

Catalogues créés avant le provisioning à la demande

Si vous disposez de catalogues de machines qui ont été créés avant que Citrix Virtual Apps and Desktops ne prenne en charge le provisioning à la demande d'Azure (mi-2017), les VM dans ces catalogues sont visibles dans le portail Azure si elles sont en cours d'exécution. Vous ne pouvez pas convertir ces VM en machines à la demande.

Pour bénéficier des améliorations apportées aux performances et des avantages liés aux coûts de stockage du provisioning à la demande, créez des catalogues à l'aide de MCS.

Azure Managed Disks

Azure Managed Disks est un système de stockage sur disque élastique que vous pouvez utiliser avec les catalogues de machines créés avec MCS, comme alternative à l'utilisation de comptes de stockage conventionnels.

La fonctionnalité de disques gérés masque la complexité liée à la création et à la gestion des comptes de stockage et fournit une solution simple à haute disponibilité pour la création et gestion de disques.

Vous pouvez utiliser des disques gérés en tant qu'images principales, en plus des machines virtuelles. L'utilisation de disques gérés peut améliorer la création de catalogues de machines et la durée de mise à jour. (Pour plus d'informations, consultez la section [En savoir plus sur les disques gérés.](#))

Par défaut, un catalogue de machines utilise des disques gérés. Vous pouvez remplacer le comportement par défaut lorsque vous créez le catalogue.

Lorsque l'optimisation des E/S est configurée (qui utilise trois disques par VM), vous pouvez provisionner jusqu'à 3 333 VM par abonnement. Lorsque l'optimisation des E/S n'est pas configurée (qui utilise deux disques par VM), vous pouvez provisionner jusqu'à 5 000 disques de VM dans un abonnement. (La fonctionnalité Managed Disks vous permet de créer jusqu'à 10 000 disques de VM dans un abonnement.)

Utilisation de disques gérés

Lorsque vous créez un catalogue de machines dans Studio, la page **Image principale** de l'assistant de création de catalogue répertorie les disques gérés, ainsi que les VM et les disques durs virtuels. (Les régions Azure ne prennent pas toutes en charge la fonctionnalité Managed Disks. Les disques gérés apparaissent dans la liste pour toute région visible par la connexion hôte du catalogue.)

Le temps de création du catalogue est optimisé lorsque l'image et le catalogue se trouvent dans la même région.

La fonctionnalité Managed Disks ne prend actuellement pas en charge la copie de disques entre les régions Azure. Si vous sélectionnez une image dans une région autre que celle où MCS provisionne le catalogue, l'image est copiée sur un disque dur virtuel dans un compte de stockage conventionnel dans la région du catalogue. Elle est ensuite reconvertie en disque géré.

Dans la page **Types de stockage et de licence** de l'assistant de création de catalogue, vous pouvez cocher une case pour utiliser des comptes de stockage conventionnels au lieu de disques gérés. (Cette case à cocher est désactivée lorsque vous effectuez le provisioning dans une région Azure qui ne prend pas en charge les disques gérés.)

Créer une connexion à Azure Resource Manager

La section [Créer et gérer des connexions](#) décrit les assistants qui créent une connexion. Les informations suivantes traitent d'informations spécifiques aux connexions de Azure Resource Manager.

Notions importantes :

- Le rôle de contributeur pour l'abonnement doit avoir été accordé aux principaux de service.
- Lorsque vous créez la première connexion, Azure vous invite à leur accorder les autorisations nécessaires. Vous devrez toujours vous authentifier pour les futures connexions, mais Azure mémorise votre accord préalable et n'affiche plus l'invite.

- Les comptes utilisés pour l'authentification doivent être des co-administrateurs de l'abonnement.
- Le compte utilisé pour l'authentification doit être un membre du répertoire de l'abonnement. Il existe deux types de comptes : « Professionnel ou école » et « compte Microsoft personnel ». Consultez l'article [CTX219211](#) pour plus de détails.
- Bien que vous puissiez utiliser un compte Microsoft existant en l'ajoutant en tant que membre du répertoire de l'abonnement, cela peut entraîner des complications si un accès invité à l'une des ressources du répertoire a précédemment été accordé à l'utilisateur. Dans ce cas, le répertoire peut contenir une entrée fictive qui ne lui accorde pas les autorisations nécessaires, et une erreur est renvoyée. Il est possible de remédier au problème en supprimant les ressources du répertoire et en les rajoutant explicitement. Soyez toutefois prudent, car cela a des effets indésirables sur d'autres ressources auxquelles ce compte peut accéder.
- Il existe un problème connu dans lequel certains comptes sont détectés en tant qu'invités du répertoire alors qu'ils en sont membres. Des configurations comme celle-ci se produisent généralement avec d'anciens comptes de répertoire établis. Solution : ajoutez un nouveau compte au répertoire, qui prendra la valeur d'appartenance appropriée.
- Les groupes de ressources sont des conteneurs de ressources qui peuvent contenir des ressources provenant de régions autres que leur propre région. Cela peut porter à confusion si vous vous attendez à ce que toutes les ressources affichées dans la région d'un groupe de ressources soient disponibles.
- Assurez-vous que votre réseau et sous-réseau sont suffisamment grands pour héberger le nombre de machines dont vous avez besoin. Cela peut nécessiter une démarche prospective, mais Microsoft vous permet de spécifier les valeurs correctes, en fournissant des conseils sur la capacité de l'espace d'adressage.

Il existe deux méthodes permettant d'établir une connexion hôte avec Azure Resource Manager :

- S'authentifier auprès d'Azure Resource Manager pour créer un 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 principal de service

Avant de commencer, vérifiez les points suivants :

- 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 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 donner à Citrix Virtual Apps and Desktops les autorisations répertoriées. Citrix Virtual Apps and Desktops 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 dans les sections suivantes.

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 utilisez ce mot de passe comme secret d'application lors de la création de la connexion hôte.

Pour créer un principal de service :

1. Connectez-vous à votre abonnement Azure Resource Manager.

Login-AzureRmAccount

2. Sélectionnez l'abonnement Azure Resource Manager sur lequel vous souhaitez créer le principal de service.

Select-AzureRmSubscription -SubscriptionID \$SubscriptionId;

3. Créez l'application dans votre locataire AD.

```
1 $AzureADApplication = New-AzureRmADApplication -DisplayName
   $ApplicationName -HomePage "https://localhost/$ApplicationName"
   -IdentifierUri https://$ApplicationName -Password
   $ApplicationPassword
```

1. Créez un principal de service.

New-AzureRmADServicePrincipal -ApplicationId \$AzureADApplication.ApplicationId

2. Attribuez un rôle au principal de service.

New-AzureRmRoleAssignment -RoleDefinitionName Contributor -ServicePrincipalName \$AzureADApplication.ApplicationId -scope /subscriptions/\$SubscriptionId

3. Dans la sortie de la fenêtre de la console PowerShell, notez la valeur ApplicationId. Vous fournissez cet ID lors de la création de la connexion hôte.

Dans l'assistant 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 des caractères non ASCII ou spéciaux.)
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 sont 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**).
5. Les ressources comprennent la région et le réseau. Sur la page **Région**, sélectionnez une région.
6. 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 ou des caractères non-ASCII ou spéciaux.
 - 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.
7. 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 la section [Créer des catalogues de machines](#).

Une image principale est le modèle qui est 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, consultez l'article [Créer des catalogues de machines](#).

Dans l'assistant de création de catalogue de machines :

- 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 HUB avec succès, exécutez la commande **PowerShell** : **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/>.

Azure Managed Disks est utilisé pour les VM dans le catalogue par défaut. Si vous souhaitez plutôt utiliser des comptes de stockage standard, cochez la case en bas de la page.

- 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 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.

- (Lors de l'utilisation de MCS) Sur la page **Groupes de ressources**, choisissez si vous souhaitez créer des groupes de ressources ou utiliser des groupes existants.
 - Si vous choisissez de créer des groupes de ressources, cliquez sur **Suivant**.
 - Si vous choisissez d'utiliser des groupes de ressources existants, sélectionnez les groupes dans la liste **Groupes de ressources de provisioning disponibles**. **Rappel** : sélectionnez un nombre suffisant de groupes pour prendre en charge les machines que vous créez dans le catalogue. Studio affiche un message indiquant si vous en choisissez trop peu. Vous pouvez sélectionner un nombre supérieur au minimum requis si vous envisagez d'ajouter

d'autres VM au catalogue ultérieurement. Vous ne pouvez pas ajouter d'autres groupes de ressources à un catalogue après que le catalogue a été créé.

Pour de plus amples informations, consultez la section *Groupes de ressources Azure* plus loin dans cet article.

- 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.

Groupes de ressources Azure

Les groupes de ressources de provisioning d'Azure permettent de provisionner les VM qui fournissent des applications et bureaux aux utilisateurs. Vous pouvez ajouter des groupes de ressources Azure vides existants lorsque vous créez un catalogue de machines MCS dans Studio, ou ils peuvent être créés pour vous.

Pour plus d'informations sur les groupes de ressources Azure, consultez la section [Présentation d'Azure Resource Manager](#).

Exigences

- Chaque groupe de ressources peut contenir jusqu'à 240 VM. La région dans laquelle vous créez le catalogue doit contenir suffisamment de groupes de ressources vides disponibles. Si vous souhaitez utiliser des groupes de ressources existants lorsque vous créez un catalogue de machines, vous devez sélectionner un nombre suffisant de groupes disponibles pour prendre en charge le nombre de machines qui ont été créées dans le catalogue. Par exemple, si vous spécifiez 500 machines dans l'assistant de création de catalogues, sélectionnez au moins trois groupes de ressources de provisioning disponibles.

Vous ne pouvez pas ajouter de groupes de ressources à un catalogue de machines après que le catalogue a été créé. Par conséquent, pensez à ajouter suffisamment de groupes de ressources pour prendre en charge les machines que vous pourriez ajouter au catalogue ultérieurement.

- Créez des groupes de ressources vides dans la même région que votre connexion hôte.
- Si vous souhaitez que Citrix Virtual Apps and Desktops Service crée des groupes de ressources pour chaque catalogue MCS, le principal de service Azure associé à la connexion hôte doit être autorisé à créer et supprimer des groupes de ressources. Si vous souhaitez que Citrix Virtual Apps and Desktops Service utilise des groupes de ressources vides existants, le principal de service Azure associé à la connexion hôte doit avoir l'autorisation *Contributeur* sur ces groupes de ressources vides.

- Lorsque vous créez une connexion hôte dans Studio à l'aide de l'option **Créer nouveau**, le principal de service créé dispose d'autorisations de contribution à l'étendue de l'abonnement. Vous pouvez également utiliser l'option **Utiliser existant** pour créer la connexion et fournir les détails d'un principal de service d'étendue de l'abonnement existant. Si vous utilisez l'option **Créer nouveau** et que vous créez le principal de service dans Studio, il dispose des autorisations nécessaires pour créer et supprimer de nouveaux groupes de ressources ou provisionner dans des groupes de ressources vides existants.
- Des principaux de service à étendue limitée doivent être créés à l'aide de PowerShell. En outre, lorsque vous utilisez un principal de service à étendue limitée, vous devez utiliser PowerShell ou le portail Azure pour créer des groupes de ressources vides pour chaque catalogue sur lequel MCS provisionne des machines virtuelles. Pour des instructions, voir l'article de blog <https://www.citrix.com/blogs/2016/11/09/azure-role-based-access-control-in-xenapp-xendesktop/>.

Si vous utilisez un principal de service à étendue limitée pour la connexion hôte et que vous ne voyez pas votre groupe de ressources d'image principale sur la page **Image principale** de l'assistant de création de catalogues, cela est probablement dû au fait que le principal de service à étendue limitée que vous utilisez ne dispose pas de l'autorisation « Microsoft.Resources/subscriptions/resourceGroups/read » requise pour afficher le groupe de ressources de l'image principale. Fermez l'assistant, mettez à jour le principal de service avec les autorisations nécessaires (consultez le post de blog pour obtenir des instructions) et redémarrez l'assistant. (La mise à jour dans Azure peut prendre jusqu'à 10 minutes à s'afficher dans Studio.)

Configurer des groupes de ressources pour un catalogue de machines dans Studio

La page Groupes de ressources dans l'assistant de création de catalogues vous permet de choisir si vous souhaitez créer des groupes de ressources ou utiliser des groupes existants. Consultez la section Créer un catalogue de machines à l'aide d'une image principale Azure Resource Manager.

Qu'advient-il des groupes de ressources lorsque vous supprimez un catalogue de machines ? Si vous laissez Citrix Virtual Apps and Desktops Service créer des groupes de ressources lorsque vous créez le catalogue de machines et que vous supprimez le catalogue ultérieurement, ces groupes de ressources et les autres ressources qu'ils contiennent sont également supprimés.

Si vous utilisez des groupes de ressources existants lorsque vous créez le catalogue de machines et que vous supprimez le catalogue ultérieurement, toutes les ressources qu'ils contiennent sont supprimées, mais pas les groupes de ressources.

Considérations, limitations et résolution des problèmes

Lorsque vous utilisez des groupes de ressources existants, la liste des groupes de ressources disponibles sur la page Groupes de ressources dans l'assistant de création de catalogues ne

s'actualise pas automatiquement. Par conséquent, si cette page de l'assistant est ouverte et que vous créez ou ajoutez des autorisations à des groupes de ressources dans Azure, les modifications ne sont pas reflétées dans la liste de l'assistant. Pour voir les dernières modifications, revenez sur la page Gestion des machines de l'assistant et resélectionnez les ressources associées à la connexion hôte. Ou, fermez et redémarrez l'assistant. Les modifications apportées dans Azure peuvent prendre jusqu'à 10 minutes à s'afficher dans Studio.

Utilisez un groupe de ressources dans un seul catalogue de machines. Toutefois, l'exigence d'un seul groupe de ressources dans un catalogue de machines n'est pas appliquée. Par exemple, vous sélectionnez 10 groupes de ressources lors de la création d'un catalogue, mais ne créez qu'une seule machine dans le catalogue. Neuf des groupes de ressources sélectionnés restent vides après que le catalogue est créé. Vous pourriez vouloir les utiliser pour étendre votre capacité dans le futur, c'est pourquoi ils restent associés à ce catalogue. Vous ne pouvez pas ajouter de groupes de ressources à un catalogue après sa création, il est donc judicieux de planifier vos futurs besoins en capacité. Toutefois, si un autre catalogue est créé, ces neuf groupes de ressources apparaissent dans la liste. Citrix Virtual Apps and Desktops ne peut pas déterminer à quels catalogues de machines les groupes de ressources sont attribués. Cette tâche vous incombe.

Si votre connexion utilise un principal de service qui peut accéder à des groupes de ressources vides dans différentes régions, ils apparaissent tous dans la liste. Veillez à choisir des groupes de ressources dans la même région que celle où vous créez le catalogue de machines.

Résolution des problèmes

Les groupes de ressources n'apparaissent pas dans la liste de la page Groupes de ressources de l'assistant de création de catalogues.

Le principal de service doit disposer des autorisations appropriées appliquées aux groupes de ressources que vous voulez inclure dans la liste. Consultez la section Exigences.

Lorsque vous ajoutez des machines à un catalogue de machines créé précédemment, les machines ne sont pas toutes provisionnées.

Après la création d'un catalogue et l'ajout de machines supplémentaires au catalogue, ne dépassez pas la capacité de machines des groupes de ressources initialement sélectionnés pour le catalogue (240 par groupe). Vous ne pouvez pas ajouter de groupes de ressources après que le catalogue a été créé. Si vous essayez d'ajouter plus de machines que les groupes de ressources existants ne peuvent accueillir, le provisioning échoue.

Par exemple, vous créez un catalogue de machines avec 300 VM et 2 groupes de ressources. Les groupes de ressources peuvent accueillir jusqu'à 480 VM (240 * 2). Si vous essayez d'ajouter 200 VM au catalogue, cela dépasse la capacité des groupes de ressources. 300 VM + 200 nouvelles VM = 500, alors que les groupes de ressources peuvent en contenir uniquement 480.

Plus d'informations

- [Connexions et ressources](#)
- [Créer des catalogues de machines](#)
- [CTX219211](#) : Set up a Microsoft Azure Active Directory account
- [CTX219243](#) : Grant XenApp and XenDesktop access to your Azure subscription
- [CTX219271](#) : Deploy hybrid cloud using site-to-site VPN

Environnements de virtualisation XenServer

October 10, 2018

Créer une connexion à XenServer

Lorsque vous créez une connexion à XenServer, 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.

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.)

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 Citrix Virtual Desktops)**. 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 Citrix Virtual Apps and Desktops, 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 :
 - Sélectionnez **Partagé** en tant que type de stockage.
 - Sélectionnez la case à cocher **Utiliser IntelliCache**.

Créez un catalogue de machines à l'aide d'une connexion XenServer

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 (Passthrough ou vGPU).
3. Installez un système d'exploitation pris en charge et activez RDP.
4. Installez XenServer Tools et les pilotes NVIDIA.
5. Désactivez 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.

Plus d'informations

- [Connexions et ressources](#)
- [Créer des catalogues de machines](#)

Environnements de virtualisation Microsoft System Center Virtual Machine Manager

March 6, 2019

Suivez ce guide si vous utilisez Hyper-V avec Microsoft System Center Virtual Machine Manager (VMM) pour fournir des machines virtuelles.

La section [Configuration système requise](#) répertorie les versions de VMM prises en charge.

Vous pouvez utiliser Machine Creation Services ou Citrix Provisioning (anciennement 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)

Installer et configurer un hyperviseur

Installez Microsoft Hyper-V Server et VMM sur vos serveurs.

Vérifiez les informations de compte suivantes :

Dans Studio, le compte que vous spécifiez lors de la création d'une connexion doit être 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 la connexion.

Votre compte d'utilisateur doit également être membre du groupe de sécurité Administrateurs local sur chaque serveur Hyper-V pour prendre en charge la gestion du cycle de vie des VM (telle que la création, la mise à jour et la suppression de VM).

Installer la console VMM

Installez une console System Center Virtual Machine Manager sur chaque serveur contenant un Citrix Cloud Connector.

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.

Créer une VM principale

- Installez un VDA sur la VM principale et sélectionnez l'option d'optimisation du bureau. Cela améliore les performances.
- Réalisez un instantané de la VM principale à utiliser comme sauvegarde.
- Créez des bureaux virtuels.

Créer une connexion

Si vous utilisez MCS pour provisionner des VM, procédez comme suit dans l'assistant de création de connexion de Studio :

- Entrez l'adresse en tant que nom de domaine complet du serveur hôte.
- Entrez les informations d'identification du compte d'administrateur créé préalablement. Ce compte doit être autorisé à créer des VM.
- Dans la boîte de dialogue Détails d'hôte, sélectionnez le cluster ou l'hôte autonome à utiliser pour créer vos 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, les informations d'identification doivent satisfaire aux exigences suivantes pour s'assurer que les appels provenant de Citrix Hypervisor Communications Library (HCL) se connectent 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.

Lors de l'utilisation de VMM 2012 SP1 avec Hyper-V sur Windows Server 2012 : lorsque vous utilisez SMB comme méthode de stockage, activez Authentication Credential Security Support Provider (CredSSP) depuis le Cloud Connector sur différentes machines Hyper-V individuelles. Pour obtenir davantage d'informations, veuillez consulter l'article [CTX137465](#).

À l'aide d'une session à distance PowerShell V3 standard, le HCL dans le Cloud Connector 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 qui proviennent du HCL. Les scripts sont alors envoyés 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 :

```
$ims = Get-WmiObject -class $class -namespace "root\virtualization\v2";  
$result = $ims.ConvertVirtualHardDisk($diskName, $vhdstext)  
$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 = $ims.CreateVirtualHardDisk($vhdstext);  
$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 Cloud Connector, 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.

Plus d'informations

- [Connexions et ressources](#)
- [Créer des catalogues de machines](#)

Environnements de virtualisation VMware

October 10, 2018

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 Machine Creation Services (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 Citrix Virtual Apps ou Citrix Virtual Desktops 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 Citrix Virtual Apps and Desktops 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
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 (Citrix Provisioning)

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
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

Kit de développement	Interface utilisateur
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
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

Kit de développement	Interface utilisateur
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

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 Cloud Connector.

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.
2. Obtenez le certificat vCenter à l'aide de l'une des trois méthodes suivantes :

Depuis le serveur vCenter :

- a) Copiez le fichier rui.crt depuis le serveur vCenter vers un emplacement accessible sur vos Cloud Connector.
- b) Sur le Cloud Connector, 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.

- a) Ouvrez votre navigateur Web et créez une connexion Web sécurisée vers le serveur vCenter (par exemple <https://server1.domain1.com>).
- b) Acceptez les avertissements relatifs à la sécurité.
- c) Cliquez sur la barre d'adresse sur laquelle l'erreur de certificat est affichée.
- d) Affichez le certificat puis cliquez sur l'onglet Détails.

- e) Sélectionnez **Copier dans un fichier puis effectuez l'exportation au format .CER**, en fournissant un nom lorsque vous êtes invité à le faire.
- f) Enregistrez le certificat exporté.
- g) Naviguez vers l'emplacement du certificat exporté et ouvrez le fichier .CER.

Importez directement depuis Internet Explorer exécuté en tant qu'administrateur :

- a) Ouvrez votre navigateur Web et créez une connexion Web sécurisée vers le serveur vCenter (par exemple <https://server1.domain1.com>).
 - b) Acceptez les avertissements relatifs à la sécurité.
 - c) Cliquez sur la barre d'adresse sur laquelle l'erreur de certificat est affichée.
 - d) Affichez le certificat.
3. Importez le certificat dans le magasin de certificats sur chacun de vos Cloud Connector.
- a) Cliquez sur **Installer le certificat**, sélectionnez **Machine locale**, puis cliquez sur **Suivant**.
 - b) Sélectionnez **Placer tous les certificats dans le magasin suivant**, puis cliquez sur **Parcourir**. 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.

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 gérés par Citrix dans le 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 Citrix Virtual Apps ou Citrix Virtual Desktops, même s’il ne l’est pas par les Controller.

Lors de la création d’une connexion hôte vSphere, 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.

Plus d’informations

- [Connexions et ressources](#)
- [Créer des catalogues de machines](#)

Environnements de virtualisation Amazon Web Services

March 6, 2019

Cet article vous guide au travers de la configuration de votre compte Amazon Web Services (AWS) en tant qu’emplacement de ressources que vous pouvez utiliser avec le service Citrix Virtual Apps and Desktops. L’emplacement de ressources inclut un jeu de composants standard, idéal pour les déploiements de preuve de concept ou d’autres déploiements qui ne requièrent pas de ressources réparties sur plusieurs zones de disponibilité. Après avoir terminé ces tâches, vous pouvez installer des VDA, provisionner des machines, créer des catalogues de machines et créer des groupes de mise à disposition.

Remarque : plutôt que d’effectuer les tâches de configuration décrites dans cet article, consultez le guide [Get Started with AWS guide](#). Ce guide vous explique comment :

- Créer un compte AWS et créer des clés d’accès appropriées.
- Vous abonner à Citrix Gateway VPX dans Amazon Marketplace.
- Utiliser Smart Tools pour configurer et déployer des machines dans le nouvel emplacement de ressources.

Une fois les tâches décrites dans cet article terminées, votre emplacement de ressources comprendra les composants suivants :

- Un cloud privé virtuel (VPC) avec des sous-réseaux publics et privés à l'intérieur d'une seule zone de disponibilité.
- Une instance qui s'exécute en tant que contrôleur de domaine Active Directory et serveur DNS, située dans le sous-réseau privé du VPC.
- Deux instances appartenant au domaine sur lesquelles le Citrix Cloud Connector est installé, situées dans le sous-réseau privé du VPC.
- Une instance qui agit en tant qu'hôte Bastion, située dans le sous-réseau public de votre VPC. Cette instance est utilisée pour initier des connexions RDP aux instances dans le sous-réseau privé à des fins d'administration. Après avoir terminé la configuration de votre emplacement de ressources, vous pouvez arrêter cette instance de façon à ce qu'elle ne soit plus accessible. Lorsque vous avez besoin de gérer d'autres instances dans le sous-réseau privé, telles que des instances de VDA, vous pouvez redémarrer l'instance de l'hôte Bastion.

Vue d'ensemble des tâches

Définir un cloud privé virtuel (VPC) avec des sous-réseaux publics et privés. Lorsque vous avez terminé cette tâche, AWS déploie une instance NAT avec une adresse IP Elastic dans le sous-réseau public, ce qui permet aux instances du sous-réseau privé d'accéder à Internet. Les instances du sous-réseau public sont accessibles au trafic public entrant ce qui n'est pas le cas des instances du sous-réseau privé.

Configurer des groupes de sécurité. Les groupes de sécurité agissent en tant que pare-feu virtuels qui contrôlent le trafic pour les instances dans votre VPC. Vous devez ajouter des règles à vos groupes de sécurité permettant aux instances de votre sous-réseau public de communiquer avec les instances de votre sous-réseau privé. Vous associez également ces groupes de sécurité avec chaque instance dans votre VPC.

Créer une série d'options DHCP. Avec un VPC Amazon, les services DHCP et DNS sont fournis par défaut, ce qui affecte la manière dont vous configurez le DNS sur votre contrôleur de domaine Active Directory. Le DHCP d'Amazon ne peut pas être désactivé et le DNS d'Amazon peut être utilisé uniquement pour la résolution de DNS public, et non pour la résolution de nom Active Directory. Pour spécifier le domaine et nommer les serveurs qui doivent être transmis aux instances via DHCP, vous créez une nouvelle série d'options DHCP. Cette série attribue le suffixe de domaine Active Directory et spécifie le serveur DNS pour toutes les instances dans votre VPC. Pour vous assurer que les enregistrements hôte (A) et recherche inversée (PTR) sont enregistrés automatiquement lorsque des instances rejoignent le domaine, vous configurez les propriétés de la carte réseau pour chaque instance que vous ajoutez au sous-réseau privé.

Ajouter un hôte Bastion, un contrôleur de domaine et des Citrix Cloud Connector au VPC. Au travers de l'hôte Bastion, vous pouvez vous connecter à des instances du sous-réseau privé pour configurer le domaine, joindre des instances au domaine et installer le Citrix Cloud Connector.

Tâche 1 : Configurer le VPC

1. À partir de la console de gestion AWS, cliquez sur **VPC**.
2. Dans le tableau de bord VPC, cliquez sur **Start VPC Wizard**.
3. Sélectionnez **VPC with Public and Private Subnets** et cliquez sur **Select**.
4. Entrez un nom de VPC et modifiez les plages IP CIDRE block et Public and Private subnet IP, si nécessaire.
5. Si une passerelle NAT est sélectionnée, cliquez sur **Use a NAT Instance instead**.
6. Pour l'instance NAT, spécifiez le type d'instance et la paire de clés que vous voulez utiliser. La paire de clés vous permet de vous connecter en toute sécurité à l'instance ultérieurement.
7. Dans Enable DNS hostnames, laissez l'option **Yes** sélectionnée.
8. Cliquez sur **Create VPC**. AWS crée les sous-réseaux publics et privés, une passerelle Internet, des tables de routage et un groupe de sécurité par défaut. Une instance NAT est également créée ; une adresse IP Elastic lui est attribuée.

Tâche 2 : Configurer des groupes de sécurité

Cette tâche crée et configure les groupes de sécurité suivants pour votre VPC :

- Un groupe de sécurité pour l'instance NAT.
- Un groupe de sécurité public, avec lequel les instances de votre sous-réseau public seront associées.
- Un groupe de sécurité privé, avec lequel les instances de votre sous-réseau privé seront associées.

Pour créer les groupes de sécurité

1. Dans le tableau de bord VPC, cliquez sur **Security Groups**.
2. Créez un groupe de sécurité pour l'instance NAT : cliquez sur **Create Security Group** et entrez une balise et une description pour le groupe. Dans le menu VPC, sélectionnez le VPC que vous avez créé précédemment. Cliquez sur **Yes, Create**.
3. Répétez l'étape 2 pour créer un groupe de sécurité public et un groupe de sécurité privé.

Configurer le groupe de sécurité NAT

1. Depuis la liste de groupes de sécurité, sélectionnez le groupe de sécurité NAT.
2. Cliquez sur l'onglet **Inbound Rules** et cliquez sur **Edit** pour créer les règles suivantes :

Type	Source
ALL Traffic	Sélectionnez le groupe de sécurité privé.

Type	Source
22 (SSH)	0.0.0.0/0

3. Lorsque vous avez terminé, cliquez sur **Enregistrer**.

Configurer le groupe de sécurité public

1. Depuis la liste de groupes de sécurité, sélectionnez le groupe de sécurité public.
2. Cliquez sur l'onglet **Inbound Rules** et cliquez sur Edit pour créer les règles suivantes :

Type	Source
ALL Traffic	Sélectionnez le groupe de sécurité privé.
ALL Traffic	Sélectionnez le groupe de sécurité public.
ICMP	0.0.0.0/0
22 (SSH)	0.0.0.0/0
80 (HTTP)	0.0.0.0/0
443 (HTTPS)	0.0.0.0/0
1494 (ICA/HDX)	0.0.0.0/0
2598 (Session Reliability)	0.0.0.0/0
3389 (RDP)	0.0.0.0/0

3. Lorsque vous avez terminé, cliquez sur **Enregistrer**.
4. Cliquez sur l'onglet **Outbound Rules** et cliquez sur **Edit** pour créer les règles suivantes :

Type	Destination
ALL Traffic	Sélectionnez le groupe de sécurité privé.
ALL Traffic	0.0.0.0/0
ICMP	0.0.0.0/0

5. Lorsque vous avez terminé, cliquez sur **Enregistrer**.

Configurer le groupe de sécurité privé

1. Depuis la liste de groupes de sécurité, sélectionnez le groupe de sécurité privé.
2. Cliquez sur l'onglet **Inbound Rules** et cliquez sur **Edit** pour créer les règles suivantes :

Type	Source
ALL Traffic	Sélectionnez le groupe de sécurité NAT.
ALL Traffic	Sélectionnez le groupe de sécurité privé.
ALL Traffic	Sélectionnez le groupe de sécurité public.
ICMP	Sélectionnez le groupe de sécurité public.
TCP 53 (DNS)	Sélectionnez le groupe de sécurité public.
UDP 53 (DNS)	Sélectionnez le groupe de sécurité public.
80 (HTTP)	Sélectionnez le groupe de sécurité public.
TCP 135	Sélectionnez le groupe de sécurité public.
TCP 389	Sélectionnez le groupe de sécurité public.
UDP 389	Sélectionnez le groupe de sécurité public.
443 (HTTPS)	Sélectionnez le groupe de sécurité public.
TCP 1494 (ICA/HDX)	Sélectionnez le groupe de sécurité public.
TCP 2598 (Session Reliability)	Sélectionnez le groupe de sécurité public.
3389 (RDP)	Sélectionnez le groupe de sécurité public.
TCP 49152-65535	Sélectionnez le groupe de sécurité public.

3. Lorsque vous avez terminé, cliquez sur **Enregistrer**.
4. Cliquez sur l'onglet **Outbound Rules** et cliquez sur **Edit** pour créer les règles suivantes :

Type	Destination
ALL Traffic	Sélectionnez le groupe de sécurité privé.
ALL Traffic	0.0.0.0/0
ICMP	0.0.0.0/0
UDP 53 (DNS)	0.0.0.0/0

5. Lorsque vous avez terminé, cliquez sur **Enregistrer**.

Tâche 3 : Associer l'instance NAT au groupe de sécurité NAT

1. À partir de la console de gestion AWS, cliquez sur **EC2**.
2. Dans le tableau de bord EC2, cliquez sur **Instances**.
3. Sélectionnez l'instance NAT, puis cliquez sur **Actions > Networking > Change Security Groups**.
4. Décochez la case du groupe de sécurité par défaut.
5. Sélectionnez le groupe de sécurité NAT que vous avez créé précédemment et cliquez sur **Assign Security Groups**.

Tâche 4 : Lancer des instances

Les étapes suivantes créent quatre instances EC2 et décryptent le mot de passe administrateur par défaut généré par Amazon.

1. À partir de la console de gestion AWS, cliquez sur **EC2**.
2. Dans le tableau de bord EC2, cliquez sur **Launch Instance**.
3. Sélectionnez une image de machine Windows Server et un type d'instance.
4. Sur la page Configure Instance Details, entrez un nom pour l'instance et sélectionnez le VPC configuré précédemment.
5. Dans **Subnet**, effectuez les sélections suivantes pour chaque instance :
 - Bastion host : sélectionnez le sous-réseau public.
 - Domain controller and Connectors : sélectionnez le sous-réseau privé.
6. Dans **Auto-assign Public IP address**, effectuez les sélections suivantes pour chaque instance :
 - Bastion host : sélectionnez **Enable**.
 - Domain controller and Connectors : sélectionnez **Use default setting** ou **Disable**.
7. Dans **Network Interfaces**, entrez une adresse IP principale au sein de la plage d'adresses IP de votre sous-réseau privé pour le contrôleur de domaine et les instances de Cloud Connector.
8. Sur la page Add Storage, modifiez la taille du disque, si nécessaire.
9. Sur la page Tag Instance, entrez un nom convivial pour chaque instance.
10. Sur la page Configure Security Groups, sélectionnez **Select an existing security group** puis effectuez les sélections suivantes pour chaque instance :
 - Bastion host : sélectionnez le groupe de sécurité public.
 - Domain controller and Cloud Connectors : sélectionnez le groupe de sécurité privé.

11. Vérifiez vos sélections et cliquez sur **Launch**.
12. Créez une nouvelle paire de clés ou sélectionnez-en une existante. Si vous créez une nouvelle paire de clés, téléchargez votre fichier de clé privée (.pem) et conservez-le dans un endroit sûr. Vous devrez fournir votre clé privée pour obtenir le mot de passe administrateur par défaut de l'instance.
13. Cliquez sur **Launch Instances**. Cliquez sur **View Instances** pour afficher une liste de vos instances. Attendez que l'instance nouvellement lancée ait passé toutes les vérifications avant d'y accéder.
14. Obtenez le mot de passe administrateur par défaut pour chaque instance :
 - a) Dans la liste des instances, sélectionnez l'instance et cliquez sur **Connect**.
 - b) Cliquez sur **Get Password** et fournissez votre fichier de clé privée (.pem) lorsque vous y êtes invité.
 - c) Cliquez sur **Decrypt Password**. AWS affiche le mot de passe par défaut.
15. Répétez les étapes 2-14 jusqu'à ce que vous ayez créé quatre instances : une instance d'hôte Bastion dans votre sous-réseau public et trois instances dans votre sous-réseau privé à utiliser en tant que contrôleur de domaine et deux Cloud Connector.

Tâche 5 : Créer une série d'options DHCP

1. Dans le tableau de bord VPC, cliquez sur **DHCP Options Sets**.
2. Entrez les informations suivantes :
 - Name tag : entrez un nom convivial pour la série.
 - Domain name : entrez le nom de domaine complet que vous allez utiliser lors de la configuration de l'instance du contrôleur de domaine.
 - Domain name servers : entrez l'adresse IP privée que vous avez attribuée à l'instance du contrôleur de domaine et la chaîne **AmazonProvidedDNS**, en les séparant par des virgules.
 - NTP servers : laissez ce champ vide.
 - NetBIOS name servers : entrez l'adresse IP privée de l'instance du contrôleur de domaine.
 - NetBIOS node type : entrez **2**.
3. Cliquez sur **Yes, Create**.
4. Associez la nouvelle série à votre VPC :
 - a) Dans le tableau de bord VPC, cliquez sur **Your VPCs** et sélectionnez le VPC configuré précédemment.
 - b) Cliquez sur **Actions > Edit DHCP Options Set**.

- c) Lorsque vous y êtes invité, sélectionnez la nouvelle série que vous avez créée et cliquez sur **Save**.

Tâche 6 : Configurer les instances

1. À l'aide d'un client RDP, connectez-vous à l'adresse IP publique de l'instance de l'hôte Bastion. Lorsque vous y êtes invité, entrez les informations d'identification du compte d'administrateur.
2. À partir de l'instance de hôte Bastion, lancez la connexion au Bureau à distance et connectez-vous à l'adresse IP privée de l'instance que vous souhaitez configurer. Lorsque vous y êtes invité, entrez les informations d'identification d'administrateur de l'instance.
3. Pour toutes les instances du sous-réseau privé, configurez les paramètres DNS :
 - a) Cliquez sur **Démarrer > Panneau de configuration > Réseau et Internet > Centre Réseau et partage > Modifier les paramètres de la carte**. Cliquez deux fois sur la connexion réseau affichée.
 - b) Cliquez sur **Propriétés**, sélectionnez **Protocole Internet version 4 (TCP/IPv4)**, puis cliquez sur **Propriétés**.
 - c) Cliquez sur **Avancé**, puis sur l'onglet **DNS**. Assurez-vous que les paramètres suivants sont activés et cliquez sur OK :
 - Enregistrer les adresses de cette connexion dans DNS
 - Utilisez le suffixe DNS de cette connexion dans l'enregistrement DNS
4. Pour configurer le contrôleur de domaine :
 - a) À l'aide du Gestionnaire de serveur, ajoutez le rôle Services de domaine Active Directory avec toutes les fonctionnalités par défaut.
 - b) Promouvez l'instance en contrôleur de domaine. Lors de la promotion, activez le DNS et utilisez le nom de domaine que vous avez spécifié lors de la création de la nouvelle série d'options DHCP. Redémarrez l'instance lorsque vous y êtes invité.
5. Pour configurer le premier Cloud Connector :
 - a) Joignez l'instance au domaine et redémarrez lorsque vous y êtes invité. À partir de l'instance de hôte Bastion, reconnectez-vous à l'instance à l'aide de RDP.
 - b) Connectez-vous à Citrix Cloud. Sélectionnez **Emplacements des ressources** à partir du menu en haut à gauche.
 - c) Téléchargez le Cloud Connector.
 - d) Lorsque vous y êtes invité, exécutez le fichier cwconnector.exe et entrez vos informations d'identification Citrix Cloud. Suivez les instructions de l'assistant.
 - e) Lorsque vous avez terminé, cliquez sur **Actualiser** pour afficher la page Emplacements des ressources. Une fois le Cloud Connector enregistré, l'instance s'affiche sur la page.

6. Répétez l'étape 5 pour configurer le deuxième Cloud Connector.

Créer une connexion

Lorsque vous créez une connexion à l'aide de Studio :

- Vous devez fournir les valeurs de la clé API et de 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, la gestion de Citrix Virtual Apps and Desktops 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.

Plus d'informations

- [Connexions et ressources](#)
- [Créer des catalogues de machines](#)

Environnements de virtualisation Nutanix

November 30, 2018

Suivez ces instructions lors de l'utilisation de Nutanix Acropolis pour fournir des machines virtuelles dans votre déploiement Citrix Virtual Apps ou Citrix Virtual Desktops. Le processus d'installation comprend les tâches suivantes :

- Installer et enregistrer le plug-in Nutanix dans votre environnement Citrix Virtual Apps ou Citrix Virtual Desktops.
- 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 Acropolis MCS, disponible sur le [portail d'assistance Nutanix](#).

Installer et enregistrer le plug-in Nutanix

Réalisez la procédure suivante pour installer et enregistrer le plug-in Nutanix sur les Cloud Connector. Vous pourrez ensuite utiliser les fonctions Gérer dans Citrix Cloud 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 Cloud Connector.
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 été enregistré :

Add-PSSnapin Citrix*

Get-HypervisorPlugin

Créer une connexion à Nutanix

Dans l'assistant 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 la section [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. Avant de créer le catalogue, créez des images et des instantanés dans Nutanix. Consultez la documentation Nutanix pour plus d'informations.

Dans l'assistant de création de catalogues :

- Les pages **Système d'exploitation** et **Gestion des machines** ne contiennent aucune information spécifique à Nutanix.

- 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 Citrix Virtual Apps and Desktops. 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.

Plus d'informations

- [Connexions et ressources](#)
- [Créer des catalogues de machines](#)

Environnements de virtualisation Google Cloud Platform

October 10, 2018

Le service Citrix Virtual Apps and Desktops prend en charge la possibilité de mettre manuellement hors/sous tension les VM Citrix Virtual Apps and Desktops sur Google Cloud Platform (GCP). Avec cette fonctionnalité, vous pouvez :

- Importer des VM GCP Windows Server créées manuellement dans un catalogue de machines Citrix Virtual Apps and Desktops.
- Supprimer des VM GCP Windows Server créées manuellement d'un catalogue Citrix Virtual Apps and Desktops.
- Tirer parti de toutes les fonctionnalités de gestion de l'alimentation Citrix Virtual Apps and Desktops existantes pour gérer de manière optimale les VM GCP Windows Server, en définissant par exemple un calendrier de redémarrage.

Cette fonctionnalité ne nécessite aucune modification du workflow de provisioning Citrix Virtual Apps and Desktops existant, ni la suppression de toute fonctionnalité existante.

Vous ne pouvez gérer que les VM persistantes créées précédemment sur Google Cloud Platform. Citrix vous recommande de provisionner manuellement les VM avant de créer une connexion dans Studio.

Exigences

- Compte Citrix Cloud. La fonctionnalité décrite dans cet article est uniquement disponible dans Citrix Cloud.
- Abonnement au service Citrix Virtual Apps and Desktops. Pour plus de détails, voir [Commencer](#).
- Un projet GCP. Le projet stocke toutes les ressources de calcul associées au catalogue de machines. Il peut s'agir d'un projet existant ou un nouveau.
- Compte de service GCP. Ce compte s'authentifie auprès de Google Cloud pour permettre l'accès au projet. Voir *Configurer le compte Google Cloud*.
- Deux API activées dans votre projet Google Cloud. Pour plus de détails, voir *Activer les API Google Cloud*.

Après avoir rempli les conditions requises, vous pouvez *créer une connexion à GCP* et ensuite *créer un catalogue contenant des VM GCP*.

Configurer le compte de service Google Cloud

Un compte Google vous permet de créer et de gérer des ressources au sein de projets GCP. Un compte de service Google Cloud est requis pour activer la fonctionnalité de gestion de l'alimentation décrite dans cet article.

Conseil : le compte Google Cloud s'authentifie auprès de Citrix Cloud à l'aide d'une [clé privée](#) générée par Google Cloud. Chaque compte (personnel ou de service) contient différents rôles définissant la gestion du projet. La fonctionnalité décrite dans cet article nécessite le rôle **Cloud Resource Manager**

Browser et les autorisations **Compute** suivantes :

- compute.instances.get
- compute.instances.list
- compute.instances.reset
- compute.instances.start
- compute.instances.stop
- compute.regions.list
- compute.zoneOperations.get
- compute.zoneOperations.list
- compute.zones.list

Ces autorisations sont accordées en créant un rôle personnalisé. Pour plus de commodité, le rôle Compute **Instance Admin (v1)** peut être utilisé à la place du rôle personnalisé, mais il fournit un accès plus étendu que ce qui est strictement nécessaire.

Pour plus de détails, voir la [page contenant des informations sur les rôles GCP](#) .

Lors de la création d'un compte de service, il est possible de créer une clé privée pour le compte. Utilisez cette clé privée lors de la création d'une connexion dans Studio. L'accès à la clé privée se

présente sous la forme d'un fichier d'informations d'identification que vous téléchargez lors de sa création. Lors de la création d'un fichier d'informations d'identification, assurez-vous que le type de fichier de clé est défini sur JSON, le type de fichier attendu par Studio.

Conseil : créez de nouvelles clés de service à l'aide de la page du compte de service sur la console GCP. Citrix recommande de changer de clés régulièrement pour des raisons de sécurité. Pour fournir de nouvelles clés sont fournies à l'application Citrix Virtual Apps and Desktops, modifiez une connexion GCP existante.

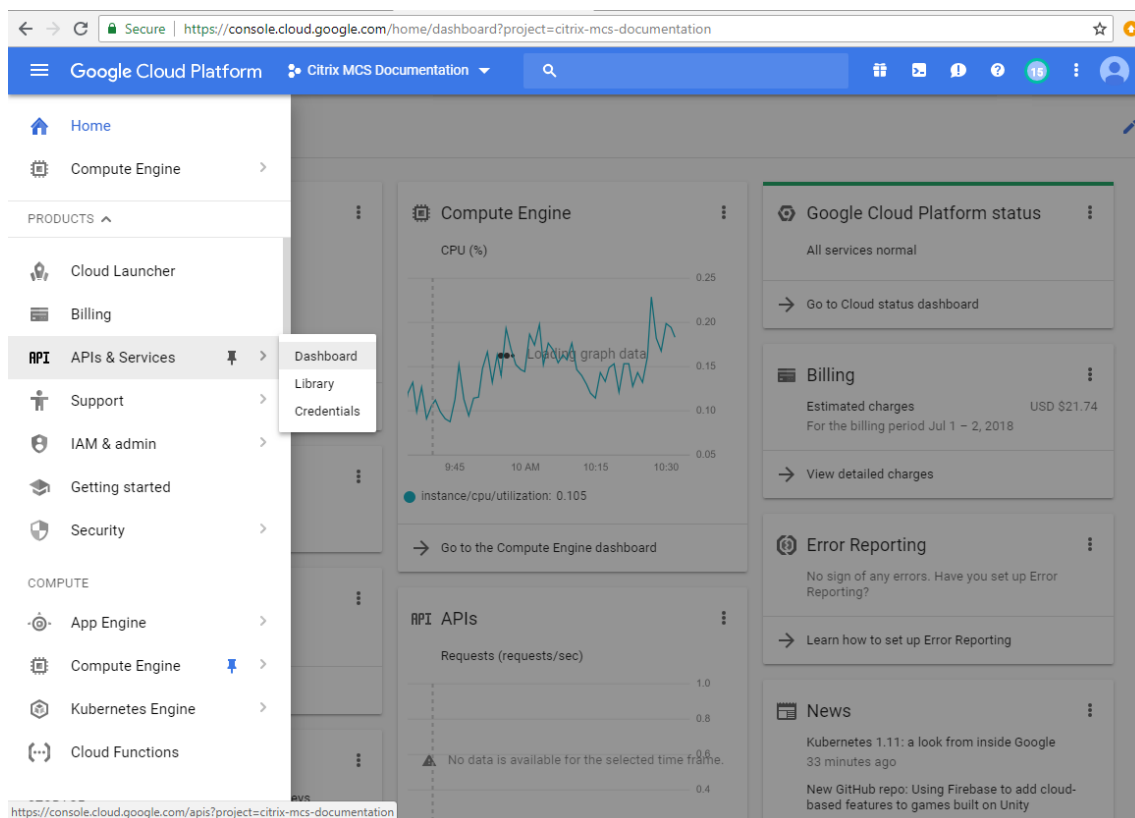
Activer les API Google Cloud

Pour utiliser la fonctionnalité Google Cloud avec Citrix Studio, vous devez activer deux API dans votre projet Google Cloud :

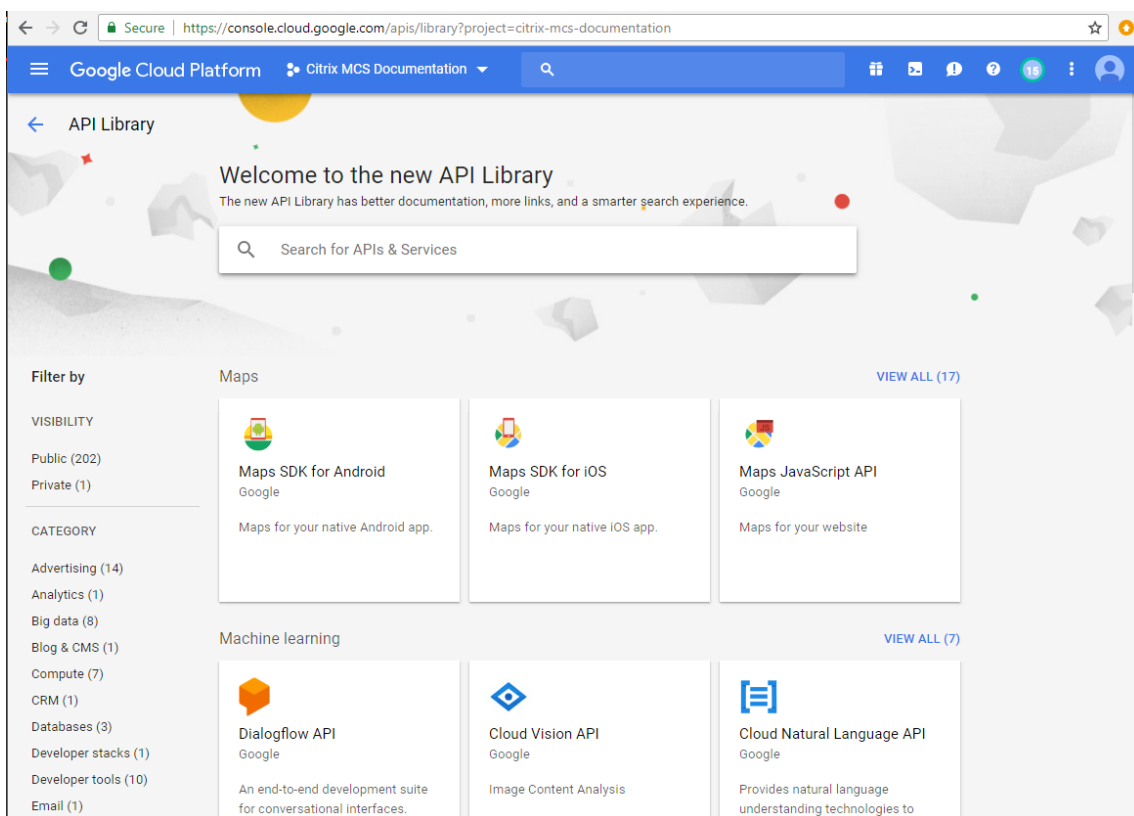
- API Computer Engine
- API Cloud Resource Manager

Depuis l'écran principal de Google Cloud Platform :

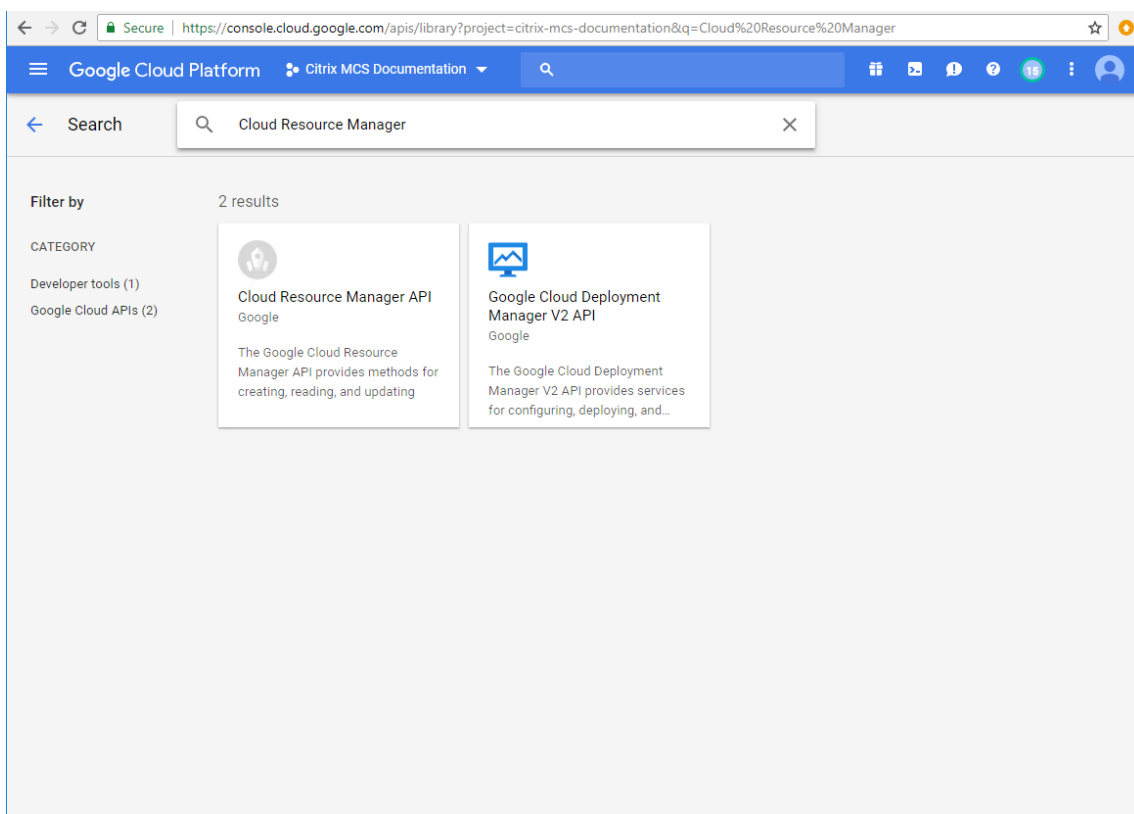
1. Dans le menu supérieur gauche, sélectionnez API et services > Tableau de bord.



2. Dans l'écran Tableau de bord, assurez-vous que l'état de l'API Compute Engine est activé.
3. Dans le volet de gauche, sélectionnez API et services > Bibliothèque.



4. Dans le champ de recherche, tapez Cloud Resource Manager.
5. Dans les résultats de la recherche, cliquez sur Cloud Resource Manager API.



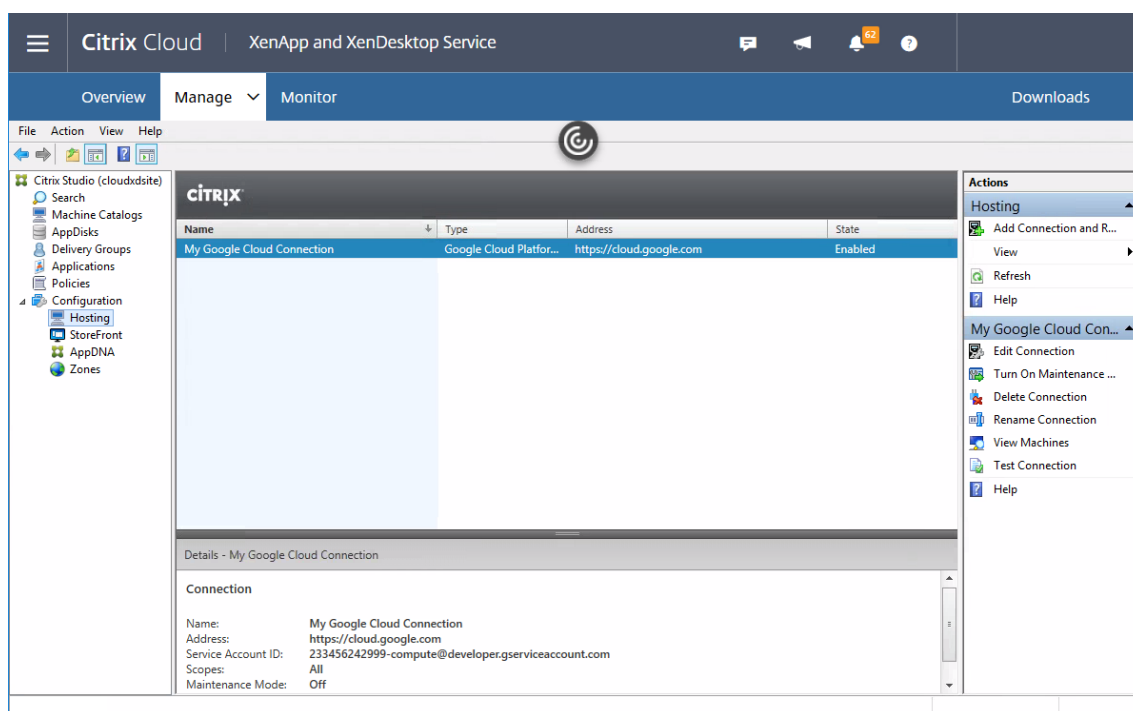
Dans l'écran de l'API Cloud Resource Manager, cliquez sur **Activer**. L'état de l'API est affiché.

Créer une connexion

Dans Studio, suivez les instructions sous [Créer une connexion et des ressources](#). Les informations suivantes sont uniques aux connexions Google Cloud Platform.

The screenshot shows the 'Add Connection and Resources' window in Citrix Studio. On the left, there is a sidebar with 'Studio' and 'Connection Summary'. The main area is titled 'Connection' and has two radio buttons: 'Use an existing Connection' (with a dropdown menu showing 'Azure Connection') and 'Create a new Connection' (which is selected). Under 'Create a new Connection', there are four fields: 'Connection type' (dropdown menu showing 'Google Cloud Platform'), 'Service account key' (button labeled 'Import key'), 'Service account ID' (text box containing '233456242999-compute@developer.gserviceaccount.c'), and 'Connection name' (text box with placeholder 'Connection Name'). At the bottom right, there are three buttons: 'Back', 'Next', and 'Cancel'.

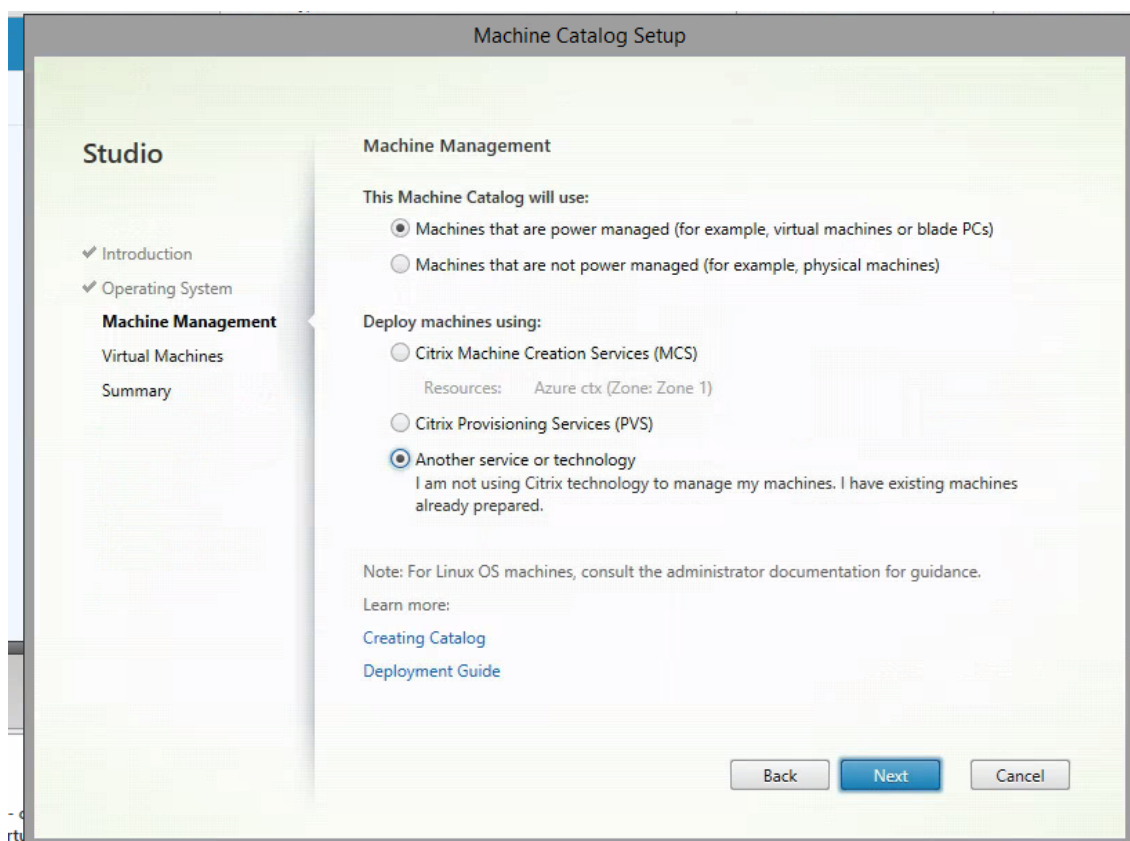
1. Sur la page Connexion :
 - Sélectionnez **Créer une nouvelle connexion**.
 - Sélectionnez **Google Cloud Platform** comme **Type de connexion**.
 - Cliquez sur **Importer clé** pour charger le fichier d'informations d'identification Google. Ce fichier contient les informations d'identification du compte de service appliqué. Le champ ID du compte de service est automatiquement renseigné avec les informations de la clé importée.
 - Entrez un nom pour la connexion et cliquez sur **Suivant**.
2. Sur la page **Résumé**, vérifiez les informations et cliquez sur **Terminer**.
Studio répertorie la connexion que vous avez créée.



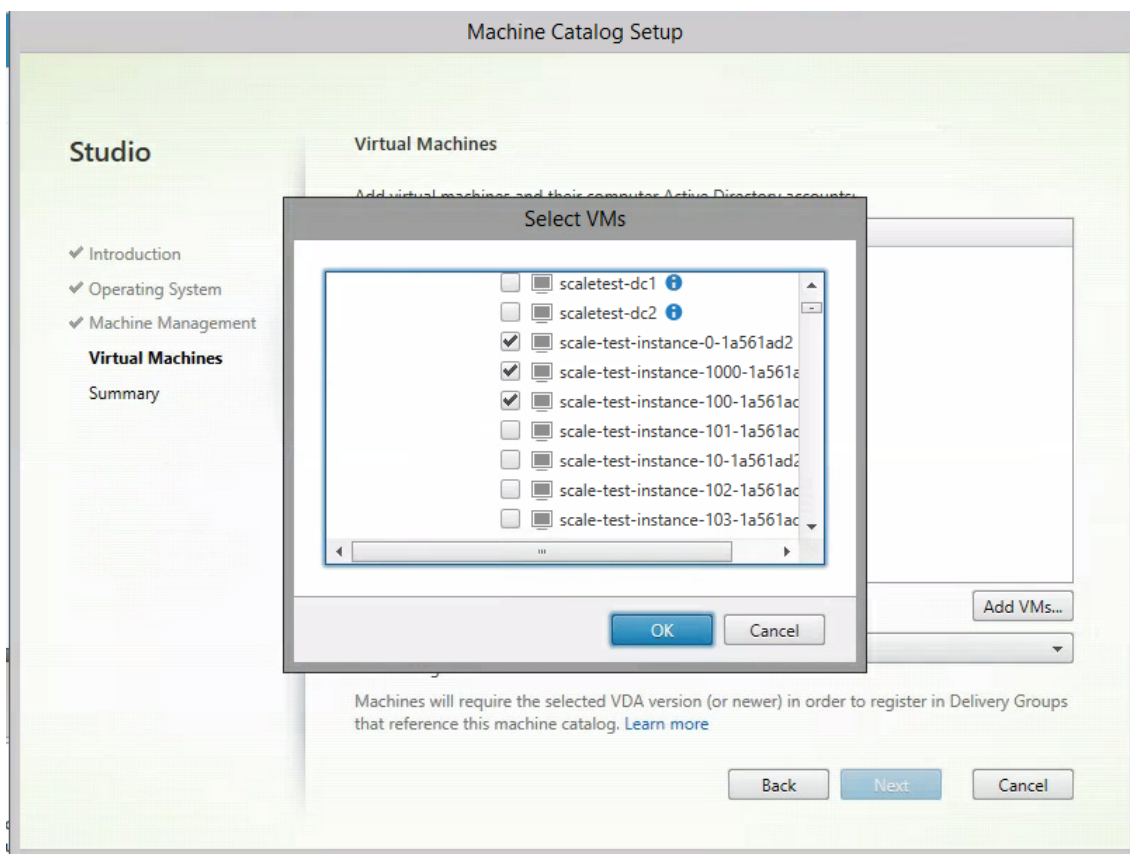
Créer un catalogue de machines

Dans Citrix Studio, suivez les instructions de la section [Créer des catalogues de machines](#). Les informations suivantes sont uniques aux catalogues de Google Cloud Platform.

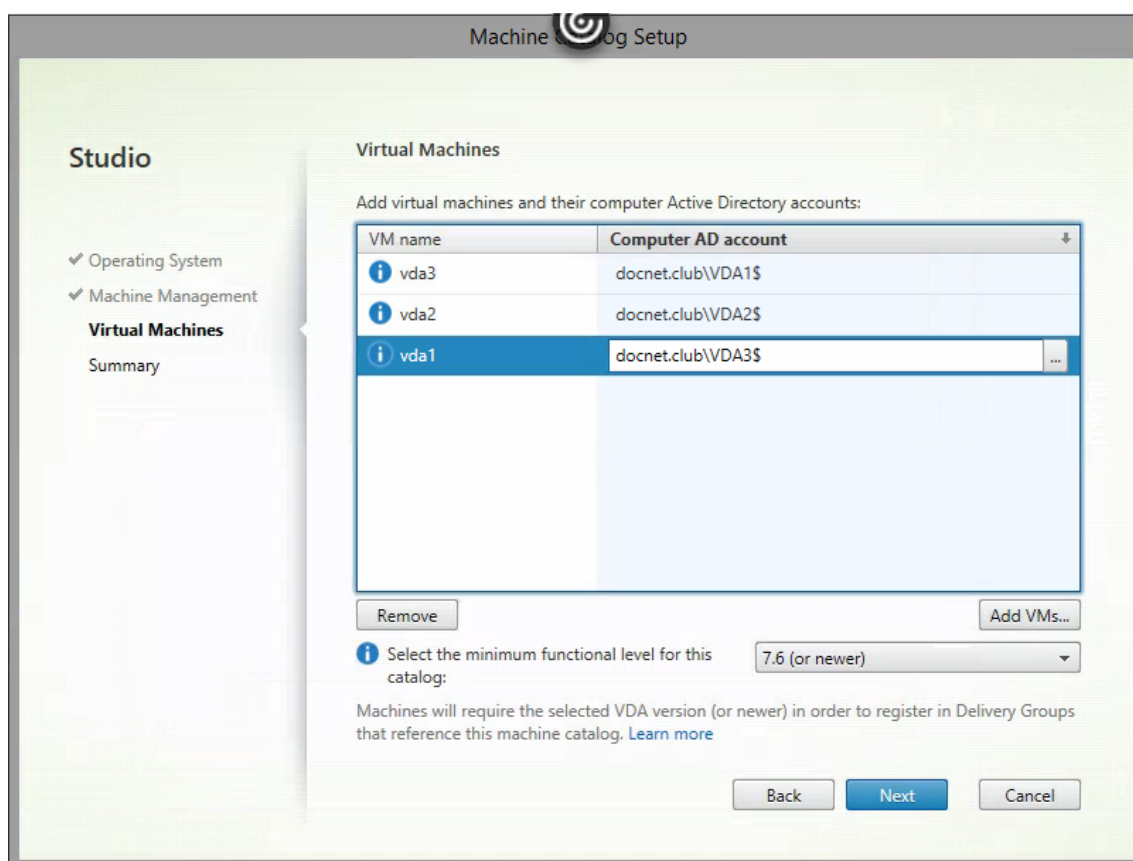
1. Sur la page **Système d'exploitation**, sélectionnez **OS de serveur**.
2. Sur la page **Gestion des machines**, sélectionnez les deux boutons radio suivants :
 - **des machines dont l'alimentation est gérée...**
 - **Autre service ou technologie.**



3. Sur la page **Machines virtuelles**, sélectionnez **Ajouter des VM**. Accédez à la zone Google Cloud contenant les machines. Sélectionnez les machines, puis cliquez sur **OK**.



4. Fournissez les comptes d'ordinateur Active Directory existants pour les machines sélectionnées, puis cliquez sur **OK**.



5. Sur la page **Résumé**, confirmez les informations que vous avez fournies, spécifiez un nom pour la connexion, puis cliquez sur **Terminer**.

Dépanner la connexion

Une fois l'assistant de création de connexion terminé, si l'état de la connexion est « Non disponible », il est possible que les éléments de Google Cloud Platform n'existent pas sur le Citrix Cloud Connector :

- Vérifiez que vos Cloud Connector sont en cours d'exécution.
- Vérifiez que vos Cloud Connector ont été mis à jour vers la dernière version.
- Si les Cloud Connector ne répondent pas à Citrix Cloud, assurez-vous que le serveur du contrôleur de domaine Active Directory est en cours d'exécution.

Installer des Cloud Connector

December 11, 2018

Citrix Cloud Connector comble le fossé entre les services gérés par Citrix et les composants gérés par

le client. Le Cloud Connector est un groupe de services de Citrix Cloud qui permet aux VDA, StoreFront gérés par le client et Delivery Controller basés sur le cloud de communiquer entre eux. Vous pouvez installer des Cloud Connector de manière interactive ou à partir de la ligne de commande.

Rappel : après avoir terminé l'installation du premier Cloud Connector, répétez les étapes pour le deuxième Cloud Connector dans l'emplacement de ressources. Vous devez disposer d'un minimum de deux Cloud Connector dans chaque emplacement de ressources.

Après l'installation, assurez-vous que les serveurs contenant des Cloud Connector sont sous tension en permanence pour garantir un bon fonctionnement. Ne déplacez pas une machine contenant un Cloud Connector sur un autre domaine.

Considérations sur le dimensionnement et la scalabilité

Lorsque vous évaluez le dimensionnement et la scalabilité de Citrix Virtual Apps and Desktops Service, tenez compte de tous les composants. Effectuez des recherches et des tests sur la configuration des Cloud Connector et du StoreFront géré par le client de manière à déterminer celle qui répond le mieux à vos besoins spécifiques. Le sous-dimensionnement des machines peut avoir un impact négatif sur les performances du système.

Les articles suivants contiennent des informations sur le test du dimensionnement et de la scalabilité. Ils fournissent des détails sur les capacités maximales testées, ainsi que des recommandations sur les meilleures pratiques en matière de configuration de la machine Cloud Connector.

- [Considérations sur le dimensionnement et la scalabilité des Cloud Connector](#)
- [Considérations sur le dimensionnement et la scalabilité du cache d'hôte local](#)

Préparer des machines

Provisionnez deux ordinateurs Windows Server 2012 R2 ou Windows Server 2016.

Chaque machine hébergeant le Cloud Connector doit satisfaire aux exigences suivantes :

- Microsoft .NET Framework 4.5.1 ou version supérieure installé.
- Être associée à un domaine Active Directory contenant les ressources et les utilisateurs que vous utiliserez pour créer des offres et les mettre à la disposition de vos utilisateurs.
- Être connectée à un réseau qui peut contacter les ressources que vous utiliserez dans votre emplacement de ressources. Pour de plus amples informations, consultez la section [Configuration du pare-feu et du proxy d'un Cloud Connector](#).
- Être connectée à Internet. Pour de plus amples informations, consultez la section [Exigences en terme de connexion Internet](#).
- L'horloge du serveur doit être définie sur l'heure UTC correcte.
- Le port TCP sortant 443 est ouvert pour la communication avec Citrix Cloud.

Pour d'autres considérations et détails importants, consultez la section [Installation de Cloud Connector](#).

Important :

- Pour d'autres considérations et détails importants, consultez la section [Installation de Cloud Connector](#).
- Pour des conseils sur le dimensionnement, consultez la section [Dimensionnement de Cloud Connector](#).

Lorsque vous utilisez Microsoft System Center Virtual Machine Manager pour provisionner des machines qui fournissent des applications et des bureaux (l'hôte), installez une console VMM sur chaque serveur contenant un Citrix Cloud Connector. Si vous omettez cette installation, un message d'erreur s'affiche : « La version 2012 ou ultérieure de la console SCVMM n'est pas installée sur les Delivery Controller suivants... »

Installer un Cloud Connector de manière interactive

À partir du serveur sur lequel vous allez installer le Cloud Connector, connectez-vous à Citrix Cloud. À partir du menu dans le coin supérieur gauche, sélectionnez **Emplacements des ressources**.

← Resource Locations

Cliquez sur **Télécharger** et suivez l'assistant.

- Vous êtes invité à entrer des informations d'identification d'administrateur de Citrix Cloud. (Il

s'agit des informations d'identification que vous avez utilisées pour vous connecter à Citrix Cloud.)

- Si vous êtes un administrateur pour plus d'un client, choisissez le client pour lequel vous installez le Cloud Connector.
- Si le client a plus d'un emplacement de ressources, choisissez celui sur lequel vous voulez installer le Cloud Connector.

Le programme d'installation exécute des tests de connectivité sur Citrix Cloud au début et à la fin de l'installation.

Après avoir terminé l'installation du premier Cloud Connector, répétez les étapes pour le deuxième Cloud Connector dans l'emplacement de ressources. Chaque emplacement de ressources doit disposer d'un minimum de deux Cloud Connector.

Citrix vous recommande de télécharger un nouveau Cloud Connector à partir du centre de contrôle de Citrix Cloud pour chaque installation. Ne réutilisez pas un téléchargement pour installer un autre Cloud Connector.

Installer un Cloud Connector à partir de la ligne de commande

Exécutez la commande suivante :

```
Exécutez CWCCConnector.exe /q /Customer:<client> /ClientId:<id-client> /ClientSecret:<secret-client>  
/ResourceLocationId:<id-emplacement-ressources> /AcceptTermsOfService:true
```

Pour afficher une liste des paramètres pris en charge, entrez : **CWCCConnector /?**

Paramètre	Description
q	Lance une installation silencieuse. Si ce paramètre est omis, une installation interactive est lancée.
Client	Obligatoire. ID client. Situé sur la page Accès aux API, dans Gestion des identités et des accès.
ClientId	Obligatoire. ID de client sécurisé qu'un administrateur peut créer. Situé sur la page Accès aux API.
ClientSecret	Obligatoire. Clé secrète du client sécurisé disponible en téléchargement après création d'un client sécurisé. Située sur la page Accès aux API.

Paramètre	Description
ResourceLocationId	Facultatif. Situé sur la page Emplacements des ressources, à l'aide du bouton ID.
AcceptTermsOfService	Obligatoire.

Résultats de l'installation

Codes de sortie :

- 1603: An unexpected error occurred. (Une erreur inattendue s'est produite)
- 2: A prerequisite check failed. (Échec de vérification des conditions préalables)
- 0: The installation completed successfully. (L'installation s'est terminée avec succès)

Les journaux d'installation sont stockés dans :

- %LOCALAPPDATA%\Temp\CitrixLogs\CloudServicesSetup
- %ProgramData%\Citrix\WorkspaceCloud\IntallLogs

Si une installation échoue, exécutez **Start /Wait CWCCconnector.exe /parameter:value** pour examiner les codes d'erreur. Une fois l'installation terminée, exécutez **echo %ErrorLevel%**.

Plus d'informations

- [Citrix Cloud Connector](#)
- [Détails techniques sur Citrix Cloud Connector](#)
- [Installation de Cloud Connector](#)
- [Configuration du pare-feu et du proxy d'un Cloud Connector](#)
- [Considérations sur le dimensionnement et la scalabilité des Cloud Connector](#)
- [Considérations sur le dimensionnement et la scalabilité du cache d'hôte local](#)

Autres ressources

[Créer une connexion](#)

Pour passer en revue l'ensemble du processus de configuration, consultez la section [Installer et configurer](#).

Créer et gérer des connexions

March 6, 2019

Introduction

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.

Vous devez être un administrateur complet pour effectuer les tâches de connexion et de gestion des ressources.

Où trouver des informations sur les types de connexion

La section [Configuration système requise](#) répertorie les versions d'hyperviseurs et de services de cloud prises en charge. Pour de plus amples informations, consultez la documentation du fournisseur, ainsi que les articles suivants.

- [Environnements de virtualisation Microsoft System Center Virtual Machine Manager](#)
- [Environnements de virtualisation Microsoft Azure Resource Manager](#)
- [Environnements de virtualisation Amazon Web Services \(AWS\) et Citrix XenDesktop sur AWS](#)
- [Environnements de virtualisation XenServer](#)
- [Environnements de virtualisation VMware](#)
- [Environnements de virtualisation Nutanix](#)

Stockage hôte

Un produit de stockage est pris en charge s'il peut être géré par un hyperviseur pris en charge. Le support Citrix aidera les fournisseurs de produits de stockage à résoudre les problèmes, et à documenter ces problèmes dans le centre de connaissances, si nécessaire.

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 Content Collaboration (anciennement 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.

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.

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

IMPORTANT :

Les ressources hôte (stockage et réseau) dans votre emplacement de ressources doivent être disponibles avant de créer une connexion.

1. Connectez-vous à Citrix Cloud.
2. Dans le menu en haut à gauche, sélectionnez **Mes services > Virtual Apps and Desktops**.
3. Cliquez sur **Manage**. Studio s'ouvre. Si aucune connexion n'a encore été créée, vous êtes invité à en créer une.
4. Sélectionnez **Configuration > Hébergement** dans le volet de navigation.
5. Sélectionnez **Ajouter une connexion et des ressources** dans le volet Actions.
6. L'assistant vous guide à travers les pages suivantes. Le contenu de la page dépend du type de connexion sélectionné. Après avoir complété chaque page, cliquez sur **Suivant** jusqu'à la page **Résumé**.

Étape 1 – Connexion

The screenshot shows the 'Add Connection and Resources' dialog box in Citrix Studio. The 'Connection' tab is selected in the left-hand 'Studio' pane. The main area is titled 'Connection' and contains the following elements:

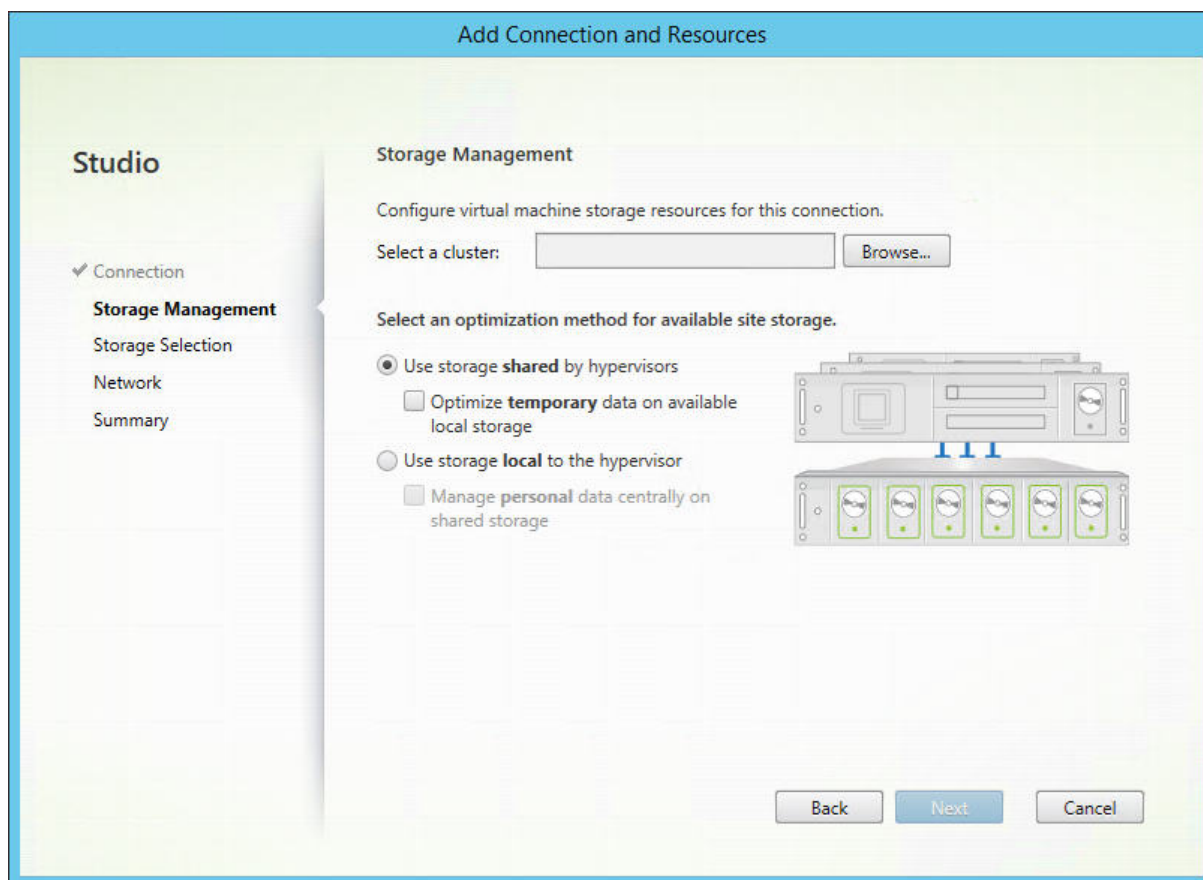
- Two radio buttons: 'Use an existing Connection' (unselected) and 'Create a new Connection' (selected).
- A dropdown menu showing 'vmwvc5u2' under the 'Use an existing Connection' option.
- Under 'Create a new Connection':
 - 'Connection type': A dropdown menu showing 'Citrix XenServer®'.
 - 'Connection address': A text box with the example 'http://xenserver.example.com'.
 - 'User name': A text box with the example 'root'.
 - 'Password': An empty text box.
 - 'Connection name': A text box with the example 'MyConnection'.
- 'Create virtual machines using': Two radio buttons: 'Studio tools (Machine Creation Services)' (selected) and 'Other tools' (unselected).
- At the bottom right, three buttons: 'Back', 'Next', and 'Cancel'.

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 utiliserez pour créer des machines virtuelles : outils Studio et autres.

Les informations sur la page **Connexion** diffèrent en fonction de l'hôte (type de connexion) que vous utilisez. Par exemple, lorsque vous utilisez Azure Resource Manager, vous pouvez utiliser un principal de service existant ou en créer un nouveau. Pour de plus amples informations, consultez la page d'environnement de virtualisation répertoriée ci-dessus qui correspond à votre type de connexion.

Étape 2 – 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 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. Voir [Environnements de virtualisation XenServer](#).

Étape 3 – Sélection du stockage

Add Connection and Resources

Studio

- ✓ Connection
- ✓ Storage Management
- Storage Selection**
- Network
- Summary

Storage Selection

When using local storage, you must select the type of data to store on each local storage device; machine operating system data, temporary data, and if not storing personal user data remotely, personal user data. At least one device must be selected for each data type.

Select data storage locations:

Show storage devices as groups Show all storage devices

Name	OS	Temporary
datastore1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
localdisk1	<input type="checkbox"/>	<input type="checkbox"/>
localdisk2	<input type="checkbox"/>	<input type="checkbox"/>
localdisk3	<input type="checkbox"/>	<input type="checkbox"/>

Select shared storage to store personal user data on personal vDisks:

1 storage device selected

Select...

Back Next Cancel

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**.

Étape 4 – Région

L'assistant de connexion de certains types de connexions (telles que Azure Resource Manager) contient une page de **région**. La région sélectionnée contrôle où les VM seront déployées. Dans l'idéal, choisissez une région proche de l'endroit où les utilisateurs accéderont à leurs applications.

Étape 5 – 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.

Certains types de connexions (telles que Azure Resource Manager) dressent également la liste des sous-réseaux que les machines virtuelles utiliseront. Sélectionnez un ou plusieurs sous-réseaux.

Étape 6 – 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.

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 qui accèdent à cette ressource doivent utiliser une image principale appropriée spécifique au GPU. Créez une nouvelle connexion.

1. Dans Studio, sélectionnez **Configuration > Hébergement** dans le volet de navigation.
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** :

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.

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. Dans Studio, sélectionnez **Configuration > Hébergement** dans le volet de navigation.
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. Dans Studio, sélectionnez **Configuration > Hébergement** dans le volet de navigation.
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. Dans Studio, sélectionnez **Configuration > Hébergement** dans le volet de navigation.
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. Dans Studio, sélectionnez **Configuration > Hébergement** dans le volet de navigation.
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. Dans Studio, sélectionnez **Configuration > Hébergement** dans le volet de navigation.
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. Dans Studio, sélectionnez **Configuration > Hébergement** dans le volet de navigation.
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. Dans Studio, sélectionnez **Configuration > Hébergement** dans le volet de navigation.
2. Sélectionnez la ressource puis sélectionnez l'entrée appropriée dans le volet Actions : **Supprimer les ressources**, **Renommer les ressources** ou **Tester les ressources**.

Horloges de connexion

Vous pouvez utiliser des paramètres de stratégie Citrix pour 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.

Autres ressources

Si vous êtes dans le processus de déploiement initial, [créez un catalogue de machines](#).

Installer des VDA

March 6, 2019

Cet article commence par une description des VDA et des programmes d'installation de VDA disponibles. Le reste de l'article décrit les étapes de l'assistant d'installation de VDA. Des lignes de commande équivalentes sont fournies. Consultez la section [Installer des VDA à l'aide de la ligne de commande](#) pour plus de détails.

À propos des VDA

L'article [Service Citrix Virtual Apps and Desktops](#) décrit ce que sont les VDA et à quoi ils servent. Vous trouverez ci-après plus d'informations utiles.

- **Collection d'analyses** : 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. Pour de plus amples informations sur ces programmes, consultez les informations relatives aux VDA dans [Citrix Insight Services](#).
- **Application Citrix Workspace** : l'application Citrix Workspace pour Windows n'est pas installée par défaut lorsque vous installez un VDA. Vous ou vos utilisateurs pouvez télécharger et installer (et mettre à niveau) les versions ultérieures de l'application Citrix Workspace pour Windows et d'autres applications Citrix Workspace à partir du site Web de Citrix. Vous pouvez aussi mettre à disposition ces applications Citrix Workspace à partir du Workspace ou d'un serveur StoreFront.
- **Service de spouleur d'impression** : le service de 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 ; assurez-vous donc que ce service est activé avant d'installer un VDA.
- **Microsoft Media Foundation** : la plupart des éditions Windows prises en charge sont fournies avec Media Foundation. Si la machine sur laquelle vous installez un VDA n'est pas dotée de Microsoft 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 l'option `/no_mediafoundation_ack` pour confirmer la limitation. 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
- **Groupes d'utilisateurs locaux** : 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.
- **Exigences en matière d'adresse Cloud Connector** : le VDA doit avoir au moins une adresse de Cloud Connector valide (dans le même emplacement de ressources) avec laquelle communiquer. Sinon, les sessions ne peuvent pas être établies. Vous spécifiez les adresses de Cloud

Connector lorsque vous installez le VDA. Pour plus d'informations sur les autres méthodes permettant de spécifier des adresses de Cloud Connector auprès desquelles les VDA peuvent s'enregistrer, consultez la section [Enregistrement de VDA](#).

- **Considérations sur le système d'exploitation :**

- Consultez [Configuration système requise](#) pour connaître les plates-formes, systèmes d'exploitation et versions pris en charge.
- Assurez-vous que chaque système d'exploitation dispose des dernières mises à jour.
- Assurez-vous que les horloges système des VDA 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](#).
- Si vous tentez d'installer (ou de mettre à niveau) un VDA Windows sur un système d'exploitation non pris en charge par cette version de VDA, un message décrit vos options. Par exemple, si vous tentez d'installer le dernier VDA sur une machine Windows 7, un message vous guide vers l'article [CTX139030](#). Pour de plus amples informations, consultez la section [Systèmes d'exploitation antérieurs](#).

Outils de prise en charge VDA

Chaque programme d'installation VDA inclut un MSI de prise en charge qui contient des outils Citrix pour vérifier les performances du VDA, telles que son intégrité globale et la qualité des connexions. Activez ou désactivez l'installation de ce fichier MSI sur la page **Composants supplémentaires** de l'interface graphique du programme d'installation VDA. À partir de la ligne de commande, vous pouvez désactiver l'installation avec l'option /exclude "Citrix Supportability Tools".

Par défaut, le MSI de prise en charge est installé dans c:\Program Files (x86)\Citrix\Supportability Tools. Vous pouvez modifier cet emplacement sur la page **Composants** de l'interface graphique du programme d'installation VDA ou avec l'option de ligne de commande /installdir. Notez que la modification de l'emplacement modifie l'emplacement pour tous les composants VDA installés, pas seulement pour les outils de prise en charge.

Outils actuels dans le MSI de prise en charge :

- Assistant d'intégrité Citrix : pour plus de détails, consultez [CTX207624](#).
- Utilitaire de nettoyage de VDA : pour plus de détails, voir l'article [CTX209255](#).

Si vous n'installez pas les outils lorsque vous installez le VDA, l'article CTX contient un lien vers le pack de téléchargement actuel.

Redémarrages durant 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, l'installation du VDA continue. (Si vous installez à partir de la ligne de commande, vous pouvez empêcher cela avec l'option /noresume.)

REMARQUE :

Un redémarrage se produit lors de la mise à niveau d'un VDA vers la version 7.17 ou une version ultérieure prise en charge. Cela ne peut pas être évité.

Programmes d'installation de VDA

Les programmes d'installation de VDA peuvent être téléchargés directement depuis la console Citrix Cloud.

Par défaut, les fichiers contenus dans les programmes d'installation auto-extractibles sont extraits dans le dossier Temp. 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.

VDAWorkstationSetup.exe

Installe un VDA pour OS de bureau.

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. Ce programme d'installation déploie uniquement les services fondamentaux nécessaires aux connexions VDA. Par conséquent, il ne prend en charge qu'un sous-ensemble des options qui sont valides avec le programme 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 Surveillance.
- Machine Identity Service.
- Personal vDisk ou AppDisks.
- Application Citrix Workspace pour Windows.
- Outils de prise en charge Citrix.
- Citrix Files pour Windows.

Ce programme d'installation n'installe pas et ne contient pas l'application Citrix Workspace pour Windows.

L'utilisation de VDAWorkstationCoreSetup.exe équivaut à utiliser le programme d'installation VDAWorkstationSetup pour installer un VDA avec OS de bureau et :

- Dans l'interface graphique : sélection de l'option **Remote PC Access** sur la page **Environnement**.
- Dans l'interface de ligne de commande : spécification de l'option /remotepc.
- 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 WMI Plugin" "Citrix Supportability Tools" "Citrix Files for Windows".

Si vous avez installé un VDA avec le programme d'installation VDAWorkstationCoreSetup.exe et que vous avez mis à niveau ce VDA à l'aide du programme d'installation VDAWorkstationSetup.exe à une date ultérieure, vous avez la possibilité d'installer les composants/fonctionnalités omis.

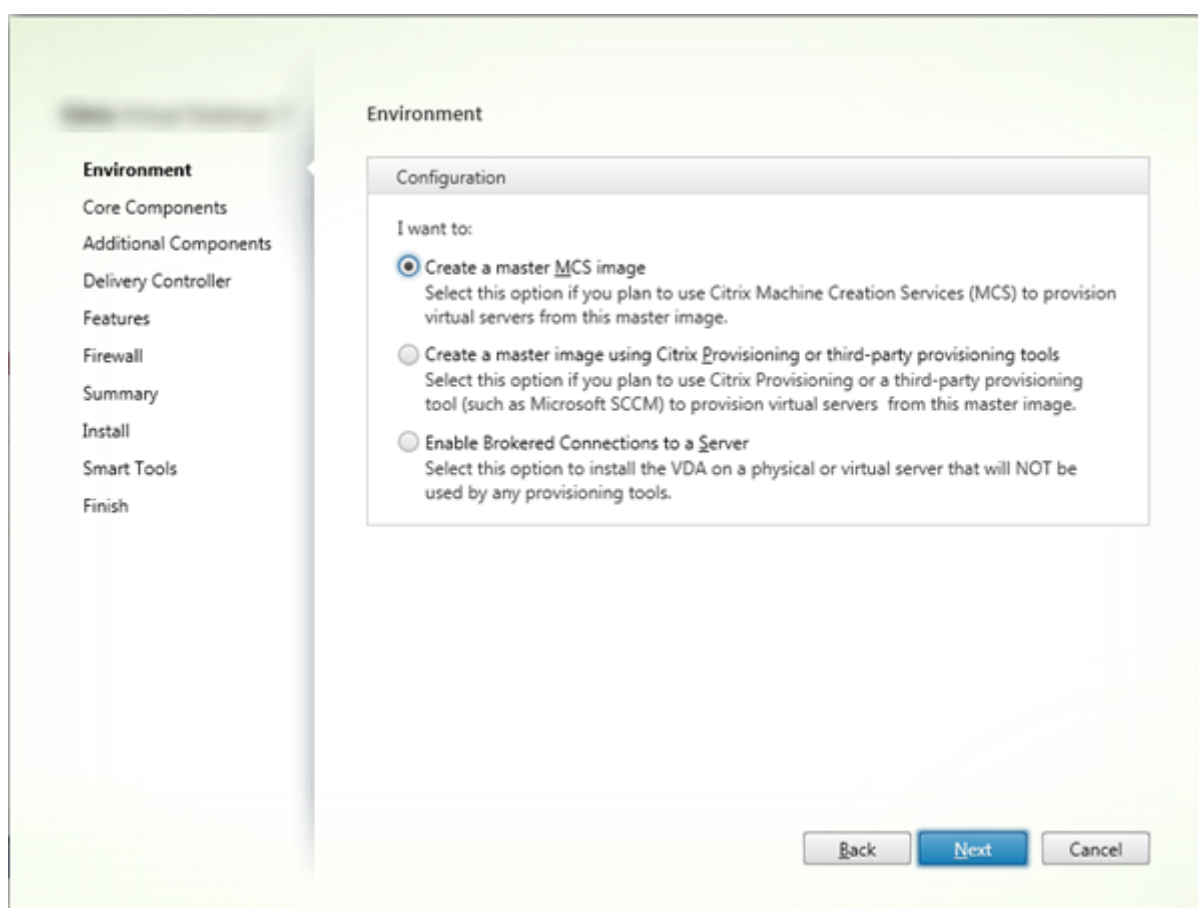
Installer un VDA

Étape 1 – Télécharger le logiciel du produit et démarrer l'assistant

1. Sur la machine sur laquelle vous installez le VDA, connectez-vous à [Citrix Cloud](#).
2. Dans le menu en haut à gauche, sélectionnez **Mes services > Virtual Apps and Desktops**.
3. Sur le côté droit, cliquez sur **Téléchargements** et sélectionnez **Télécharger VDA**. Vous serez redirigé vers la page de téléchargement du VDA. Recherchez le programme d'installation du VDA que vous souhaitez et cliquez sur **Télécharger fichier**.
4. Une fois le téléchargement terminé, cliquez avec le bouton droit sur le fichier et sélectionnez **Exécuter en tant qu'administrateur**. L'assistant d'installation démarre.

Subsidiairement aux étapes 1 à 3, vous pouvez télécharger le VDA directement à partir de la [page de téléchargement de Citrix](#).

Étape 2 – Spécifier comment le VDA sera utilisé



Sur la page **Environnement**, indiquez comment vous prévoyez d'utiliser le VDA, en indiquant si vous utiliserez ou non cette machine en tant qu'image principale pour provisionner des machines sup-

plémentaires. L'option que vous choisissez affecte les outils de provisionnement Citrix installés automatiquement (le cas échéant) et les valeurs par défaut de la page Composants supplémentaires du programme d'installation de VDA. Plusieurs MSI (Provisioning et autres) sont installés automatiquement lorsque vous installez un VDA. La seule façon d'empêcher leur installation est d'utiliser l'option `/exclude` dans une installation par ligne de commande.

Sélectionnez l'une des options suivantes :

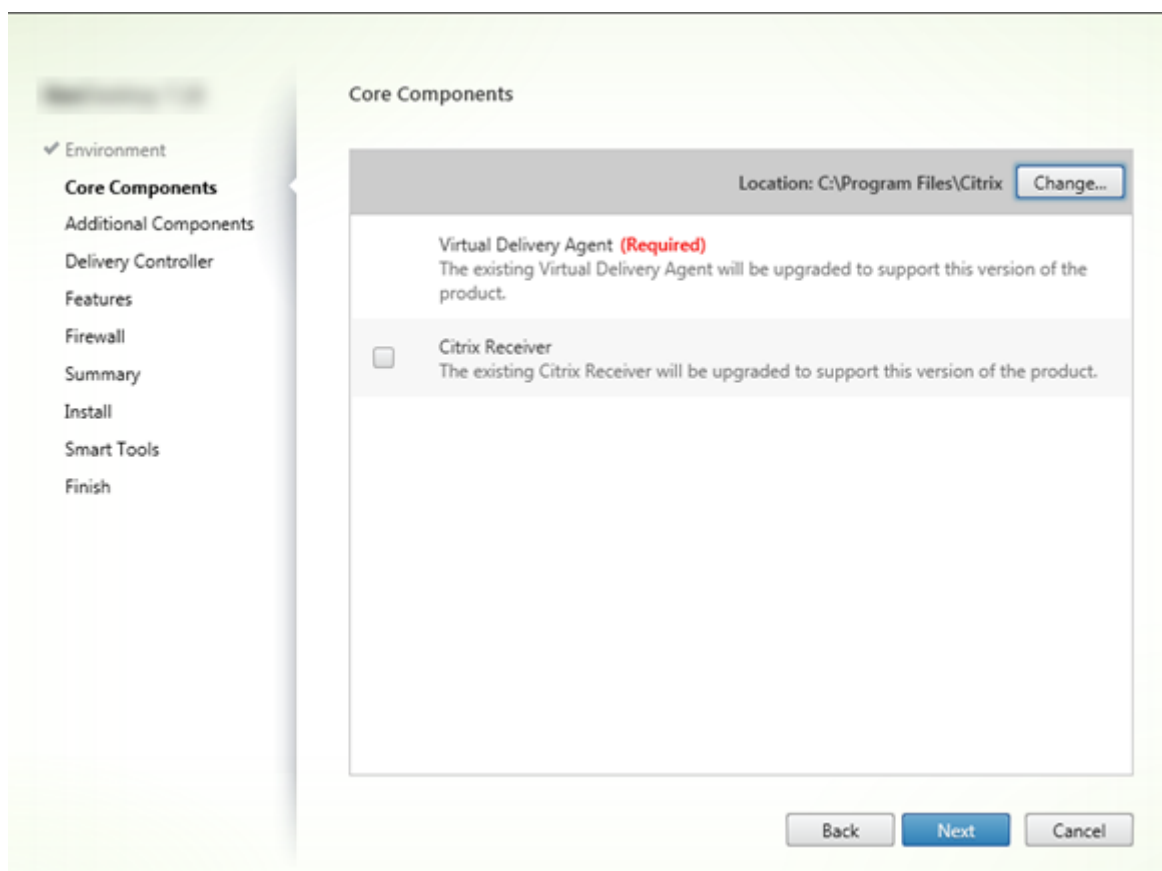
- **Créer une image MCS principale** : sélectionnez cette option pour installer un VDA sur une image principale de VM, si vous prévoyez d'utiliser Machine Creation Services pour provisionner les machines virtuelles. Option par défaut. (option de ligne de commande : `/mastermcsimage` ou `/masterimage`)
- **Créer une image principale à l'aide de Citrix _Provisioning ou d'outils de provisioning tiers** : sélectionnez cette option pour installer un VDA sur une image principale de VM, si vous envisagez d'utiliser Citrix Provisioning ou des outils tiers (tels que Microsoft System Center Configuration Manager) pour mettre à disposition des VM. Option de ligne de commande : `/masterpvsimage`
- (Apparaît uniquement sur les machines avec OS de serveur) **Activer connexions réparties à un serveur** : sélectionnez cette option pour installer un VDA sur une machine physique ou virtuelle qui ne sera pas utilisée comme image principale pour provisionner d'autres machines. Option de ligne de commande : `/remotepc`
- (Apparaît uniquement sur les machines avec OS de bureau) **Activer Remote PC Access** : sélectionnez cette option pour installer un VDA sur une machine physique à utiliser avec Remote PC Access. Option de ligne de commande : `/remotepc`

Cliquez sur **Next**.

Cette page ne s'affiche pas :

- si vous mettez à niveau un VDA
- si vous utilisez le programme d'installation `VDAWorkstationCoreSetup.exe`

Étape 3 – Sélectionner les composants à installer et l'emplacement d'installation

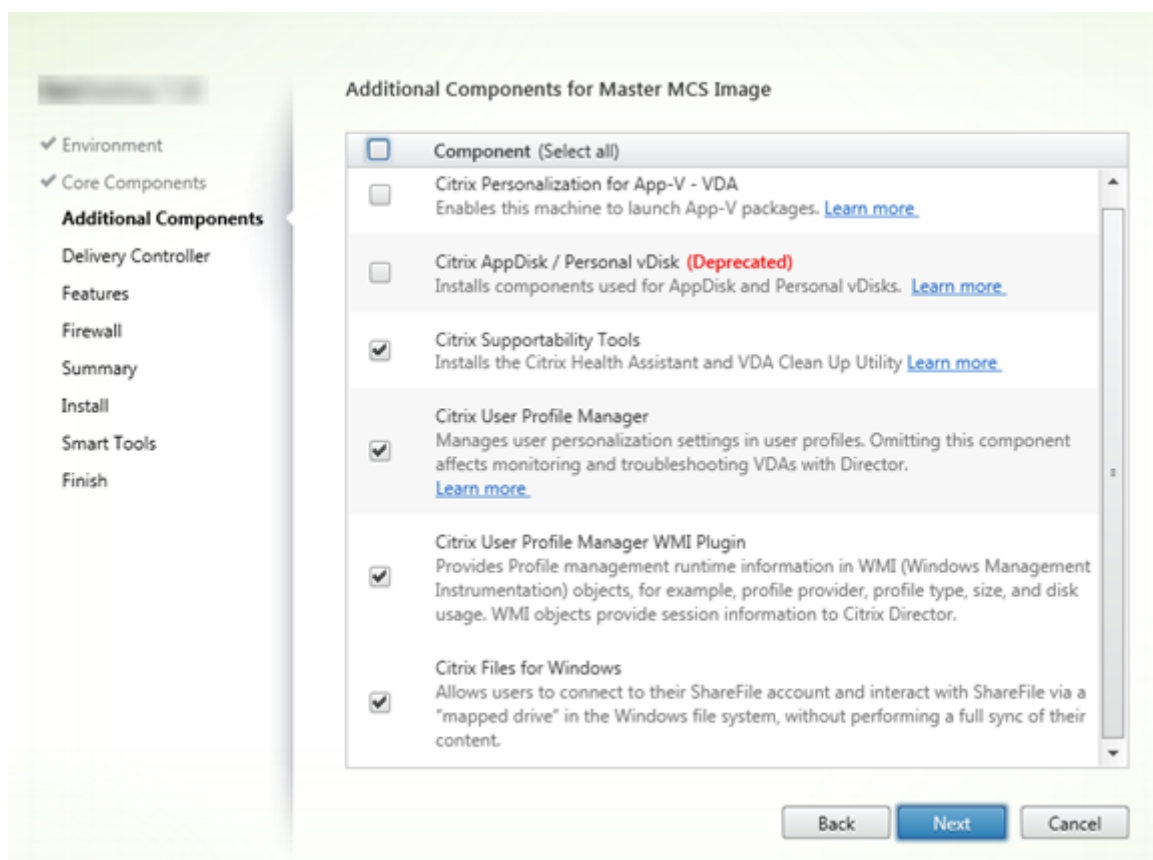


Sur la page **Composants principaux** :

- **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. Option de ligne de commande : /installdir
- **Composants** : par défaut, l'application Citrix Workspace pour Windows n'est pas installée avec le VDA. Si vous utilisez le programme d'installation VDAWorkstationCoreSetup.exe, l'application Citrix Workspace pour Windows n'est jamais installée, donc cette case à cocher n'est pas affichée. Option de ligne de commande : /components vda, plugin pour installer le VDA et l'application Citrix Workspace pour Windows.

Cliquez sur **Next**.

Étape 4 – 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. Dans une installation par ligne de commande, vous pouvez utiliser l'option `/exclude` ou `/includeadditional` pour omettre ou inclure expressément un ou plusieurs composants disponibles.

Le tableau suivant indique le paramètre par défaut des éléments sur cette page. Le paramètre par défaut dépend de l'option que vous avez sélectionnée sur la page **Environnement**.

Page Composants supplémentaires	Page Environnement : « Image principale avec MCS » ou « Image principale avec Citrix Provisioning ... » sélectionné	Page Environnement : « Activer connexions réparties à un serveur » (pour OS de serveur) ou « Remote PC Access » (pour OS de bureau) sélectionné
Citrix Personalization pour AppV	Non sélectionné	Non sélectionné
Citrix AppDisk/Personal vDisk	Non sélectionné	Non affiché car non valide pour ce cas d'utilisation.

Page Composants supplémentaires	Page Environnement : « Image principale avec MCS » ou « Image principale avec Citrix Provisioning ... » sélectionné	Page Environnement : « Activer connexions réparties à un serveur » (pour OS de serveur) ou « Remote PC Access » (pour OS de bureau) sélectionné
Outils de prise en charge Citrix	Sélectionné	Non sélectionné
Citrix User Profile Manager	Sélectionné	Non sélectionné
Citrix User Profile Manager WMI Plugin	Sélectionné	Non sélectionné
Citrix Files pour Windows	Non sélectionné	Non sélectionné

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.)

La liste des composants peut inclure :

- **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 : /includeadditional "Citrix Personalization for App-V – VDA" pour permettre l'installation du composant, /exclude "Citrix Personalization for App-V – VDA" pour empêcher l'installation du composant

- **Citrix AppDisk/Personal vDisk** : ces technologies sont [obsolètes](#). 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.

Option de ligne de commande : /includeadditional "Personal vDisk" pour permettre l'installation du composant, /exclude "Personal vDisk" pour empêcher l'installation des composants AppDisk et Personal vDisk

- **Outils de prise en charge Citrix** : installe le fichier MSI contenant les outils de prise en charge Citrix, tels que l'Assistant d'intégrité Citrix.

Option de ligne de commande : `/includeadditional "Citrix Supportability Tools"` pour permettre l'installation du composant, `/exclude "Citrix Supportability Tools"` pour empêcher l'installation du composant

- **Citrix User Profile Manager** : 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 de l'installation affecte la surveillance et la résolution des problèmes des VDA dans Citrix Cloud. Sur les pages Détails de l'utilisateur et Point de terminaison de l'onglet Surveiller, 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 : `/includeadditional "Citrix User Profile Manager"` pour permettre l'installation du composant, `/exclude "Citrix User Profile Manager"` pour empêcher l'installation du composant

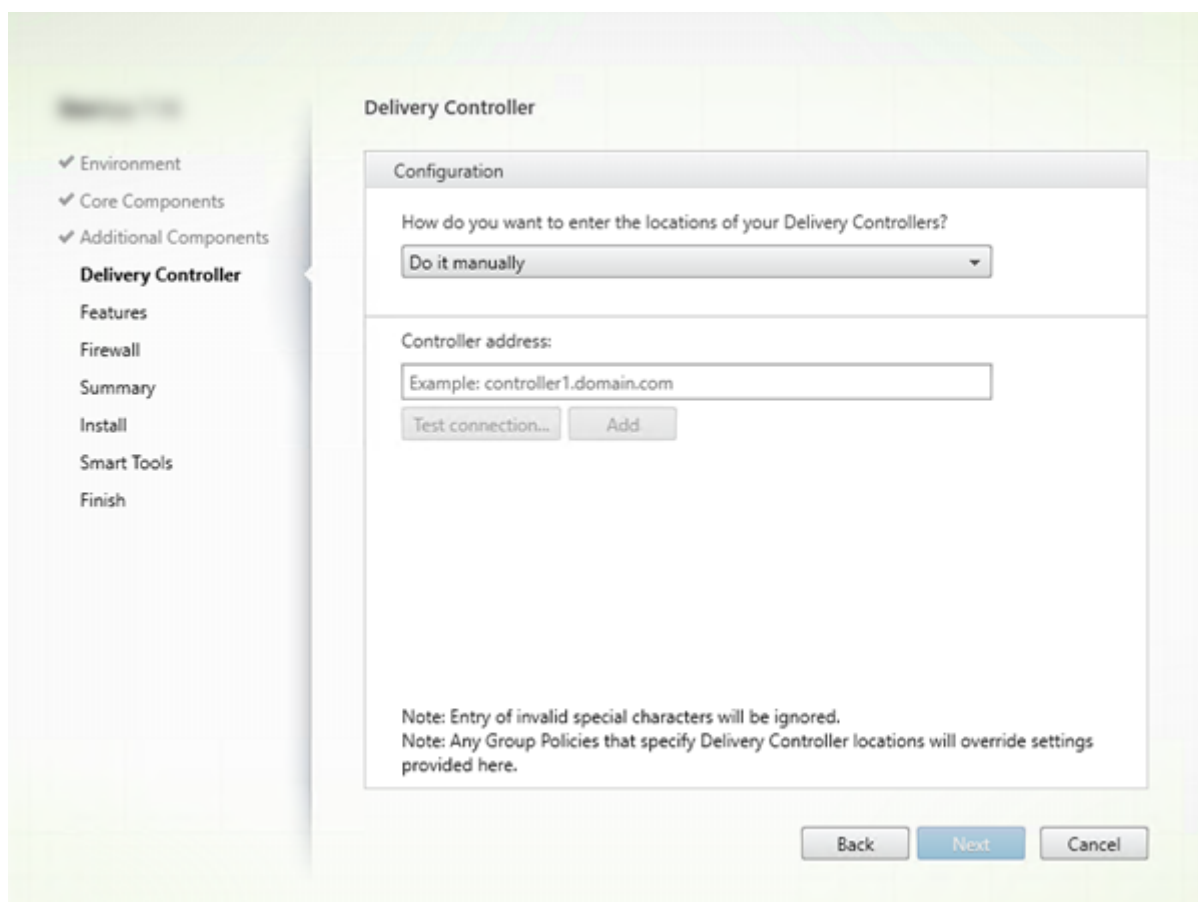
- **Citrix User Profile Manager WMI Plugin** : ce plug-in fournit des informations d'exécution sur Profile Management dans les objets WMI (Infrastructure de gestion Windows), par exemple le fournisseur de profils, le type de profil, la taille et l'utilisation du disque. Les objets WMI fournissent des informations sur les sessions à Director.

Option de ligne de commande : `/includeadditional "Citrix User Profile Manager WMI Plugin"` pour permettre l'installation du composant, `/exclude "Citrix User Profile Manager WMI Plugin"` pour empêcher l'installation du composant

- **Citrix Files pour Windows** : ce composant permet aux utilisateurs de se connecter à leur compte Citrix Files. Ils peuvent ensuite interagir avec Citrix Files via un lecteur mappé dans le système de fichiers Windows (sans nécessiter une synchronisation complète de leur contenu).

Options de ligne de commande : `/includeadditional "Citrix Files for Windows"` pour permettre l'installation du composant, `/exclude "Citrix Files for Windows"` pour empêcher l'installation du composant

Étape 5 – Adresses de Cloud Connector



Sur la page **Delivery Controller**, sélectionnez **Effectuer manuellement**. Entrez le nom DNS d'un Cloud Connector installé, puis cliquez sur **Ajouter**. Si vous avez installé des Cloud Connector supplémentaires dans l'emplacement de ressources, ajoutez leurs noms DNS.

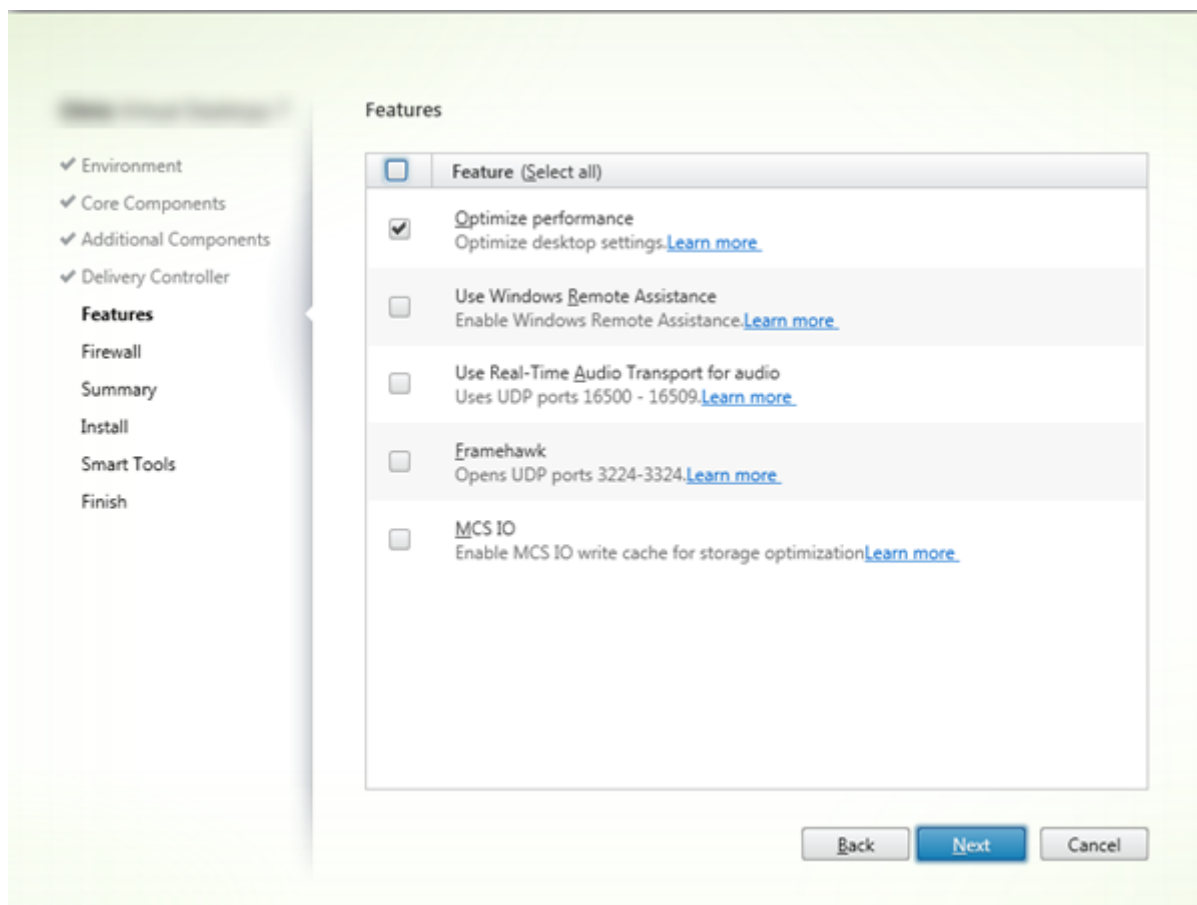
Cliquez sur **Next**.

Notions importantes :

- L'adresse peut contenir uniquement des caractères alphanumériques.
- L'enregistrement du VDA requiert que les ports de pare-feu utilisés pour communiquer avec le Cloud Connector soient ouverts. Ce paramètre est activé par défaut sur la page **Pare-feu** de l'assistant.

Options de ligne de commande : /controllers

Étape 6 – Activer ou désactiver des fonctionnalités



Sur la page **Fonctionnalités**, utilisez les cases à cocher pour activer ou désactiver les fonctionnalités que vous souhaitez utiliser.

- **Optimisation des 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.

- **Use Windows Remote Assistance** : lorsque cette option est activée, l'Assistance à distance Windows est utilisée avec la fonctionnalité d'observation utilisateur du composant Director dans

Citrix Cloud. 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 application Citrix Workspace ou Citrix Gateway) et externes (Citrix Gateway vers application Citrix Workspace). Si Citrix 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** : ces technologies sont [obsolètes](#). 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.

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.

- **E/S de MCS** : valide uniquement lors de l'utilisation de MCS pour provisionner des machines virtuelles. Lorsque cette option est sélectionnée, le pilote de mise en cache en écriture MCSIO est installé. Pour plus d'informations, consultez les sections [Stockage partagé par les hyper-viseurs](#) et [Configurer un cache pour les données temporaires](#).

Option de ligne de commande : `/install_mcsio_driver`

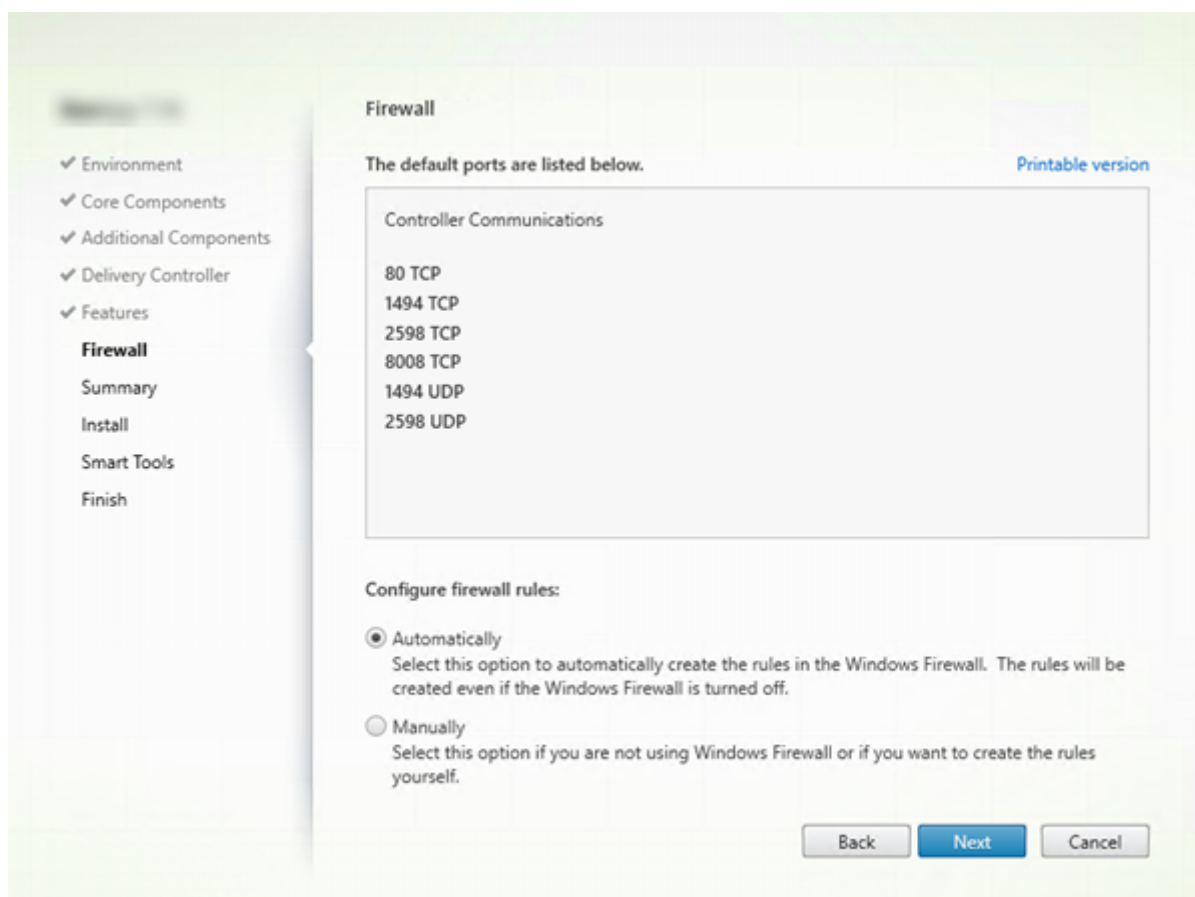
Important :

Cette fonctionnalité n'est pas activée par défaut (le pilote n'est donc pas installé). Vous devez installer ce pilote pour utiliser la fonctionnalité de mise en cache des données tem-

poraires MCS.

Cliquez sur **Next**.

Étape 7 – Ports du pare-feu

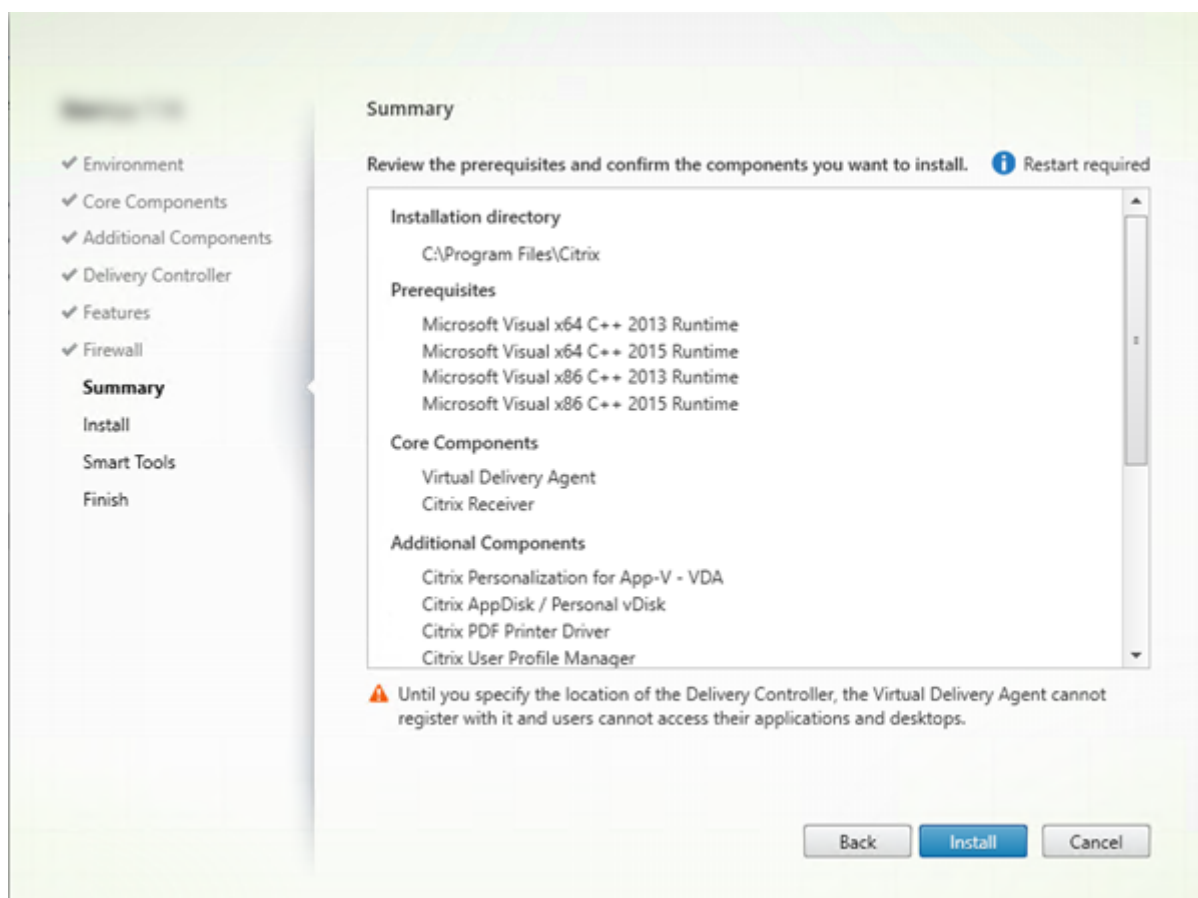


La page **Pare-feu** indique les ports que le VDA et les Cloud Connector utilisent pour communiquer entre eux. Par défaut, ces ports sont ouverts automatiquement si le service Pare-feu Windows est en cours d'exécution, même si le pare-feu n'est pas activé. Ce paramètre par défaut convient à la plupart 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 8 – Vérifier les composants requis et confirmer l'installation

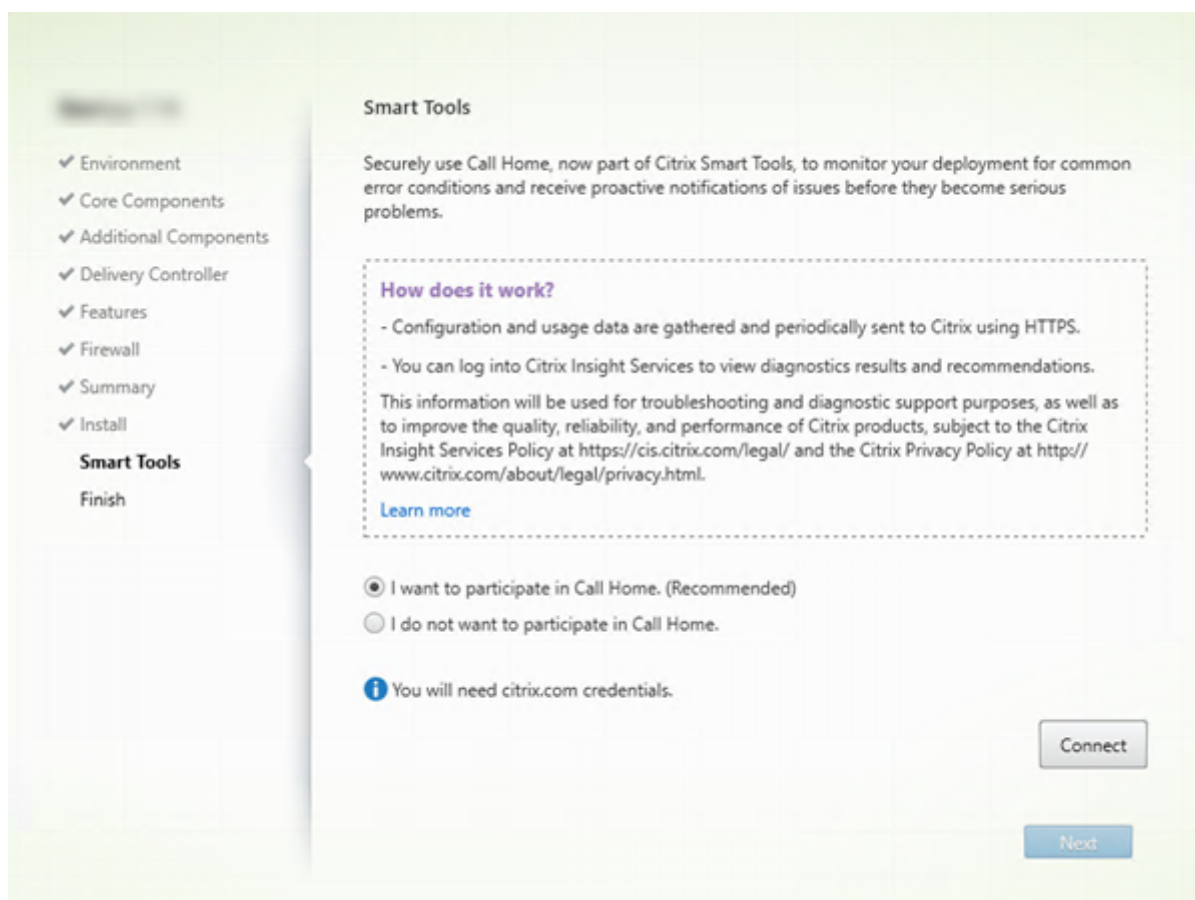


La page **Résumé** répertorie les éléments qui seront installés. Utilisez le bouton Précédent pour revenir sur les pages précédentes de l'assistant et modifier les réglages.

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](#).

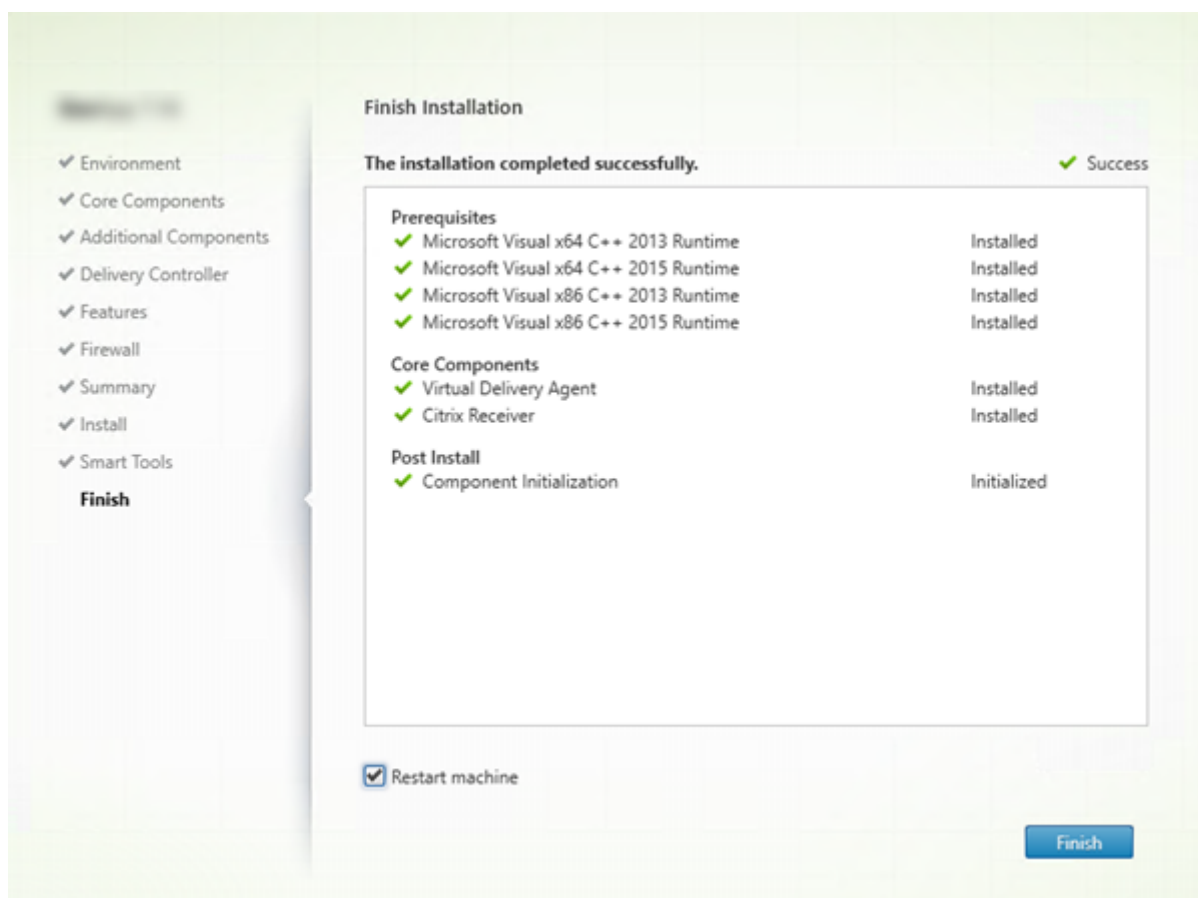
Étape 9 – Participer au programme Call Home



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 10 – 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).

(Si vous installez un VDA sur des machines individuelles (plutôt qu'une image principale), répétez les étapes ci-dessus pour installer un VDA sur d'autres machines, si nécessaire.)

Dépannage

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.

Personnaliser un VDA

Pour personnaliser ultérieurement (modifier les informations) 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 :
 - Adresses de Cloud Connector
 - 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

Autres ressources

[Créer des catalogues de machines](#)

Pour passer en revue l'ensemble du processus de configuration, consultez la section [Installer et configurer](#).

Installer des VDA à l'aide de la ligne de commande

March 6, 2019

Cet article explique comment installer et personnaliser des VDA sur des machines avec systèmes d'exploitation Windows.

Important :

Cet article explique comment émettre des commandes d'installation de VDA. Avant de commencer l'installation, consultez la section [Installer des VDA](#) pour en savoir plus sur l'installation, les programmes d'installation et les informations que vous spécifiez pendant l'installation.

Citrix fournit des exemples de scripts pour installer, supprimer ou mettre à niveau des VDA. Pour de plus amples informations, consultez [Installer les VDA à l'aide de scripts](#).

Installer un VDA

Pour installer un VDA (et voir le progrès d'exécution des commandes et les valeurs de retour), vous devez disposer de privilèges d'administrateur élevés ou utiliser **Exécuter en tant qu'administrateur**.

1. Sur la machine sur laquelle vous installez le VDA, connectez-vous à [Citrix Cloud](#).

2. Dans le menu en haut à gauche, sélectionnez **Mes services > Virtual Apps and Desktops**.
3. Sur le côté supérieur droit, cliquez sur **Téléchargements** et sélectionnez **Télécharger VDA** depuis le menu déroulant. Vous serez redirigé vers la [page de téléchargement du VDA](#). Recherchez le programme d'installation du VDA que vous souhaitez et cliquez sur **Télécharger fichier**.
4. Une fois le téléchargement terminé, exécutez le programme d'installation. Utilisez les options décrites dans cet article.
 - Pour le composant Server OS Virtual Delivery Agent, exécutez `VDAServerSetup.exe`
 - Pour le composant Desktop OS Virtual Delivery Agent, exécutez `VDAWorkstationSetup.exe`
 - Pour le composant Desktop OS Core Services Virtual Delivery Agent, exécutez `VDAWorkstationCoreSetup.exe`

Pour extraire les fichiers avant de les installer, 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 `VDAWorkstationCoreSetup.exe` à partir du répertoire contenant le contenu extrait (dans l'exemple ci-dessus, `CitrixVDAInstallMedia`). Utilisez les options valides répertoriées dans cet article.

Options de ligne de commande pour installer un VDA

Les options suivantes sont valides avec une ou plusieurs des commandes : `VDAServerSetup.exe`, `VDAWorkstationSetup.exe` et `VDAWorkstationCoreSetup.exe`.

- **`/baseimage`**

Cette technologie est [obsolète](#). 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.

Cette option n'est pas valide lors de l'utilisation du programme d'installation `VDAWorkstationCoreSetup.exe`.

- **`/components component[,component]`**

Liste séparée par des virgules des composants à installer ou supprimer. Les valeurs autorisées sont :

- **VDA** : Virtual Delivery Agent
- **PLUGINS** : Application Citrix Workspace pour Windows

Pour installer le VDA et l'application Citrix Workspace, spécifiez `/components vda,plugins`.

Cette option n'est pas valide lors de l'utilisation du programme d'installation VDAWorkstationCoreSetup.exe. Ce programme d'installation ne peut pas installer l'application Citrix Workspace.

- **/controllers** “*controller [controller]..*”

Noms de domaines complets (FQDN) séparés par des espaces et entourés de guillemets droits des Citrix Cloud Connector avec lesquels le VDA peut communiquer. 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_ports**

Ouvre les ports du pare-feu Windows requis par le Cloud Connector 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](#).

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](#).

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 les fonctions de surveillance du composant Director de Citrix Cloud. 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 et 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 le composant Machine Identity Service. Les valeurs autorisées sont :

- AppDisk VDA Plug-in
- 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
- Outils de prise en charge Citrix
- Agent Smart Tools
- Citrix Files pour Windows

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 le composant Director de Citrix Cloud. 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.

Si vous envisagez d'utiliser MCS pour provisionner des machines virtuelles, n'excluez pas Machine Identity Service.

Si vous spécifiez à la fois /exclude et /includeadditional avec le même nom de composant supplémentaire, le composant n'est pas installé.

Cette option n'est pas valide lors de l'utilisation du programme d'installation VDAWorkstation-CoreSetup.exe. Ce programme d'installation exclut automatiquement un grand nombre de ces éléments.

- **/h or /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.

- **/includeadditional** "*component*"[, "*component*"] ...

Inclut l'installation d'un ou de plusieurs composants facultatifs séparés par des virgules et entourés de guillemets droits. Cette option peut être utile lorsque vous créez un déploiement Remote PC Access et souhaitez installer des composants supplémentaires qui ne sont pas inclus par défaut. Les valeurs autorisées sont :

- Personal vDisk
- Citrix User Profile Manager
- Citrix User Profile Manager WMI Plugin
- Client d'impression universelle Citrix
- Citrix Telemetry Service
- Citrix Personalization pour AppV : VDA
- Outils de prise en charge Citrix
- Agent Smart Tools
- Citrix Files pour Windows

Si vous spécifiez à la fois `/exclude` et `/includeadditional` avec le même nom de composant supplémentaire, ce composant n'est pas installé.

- **/installdir** *directory*

Répertoire vide existant où les composants seront installés. Valeur par défaut : `c:\Program Files\Citrix`.

- **/install_mcsio_driver**

Active le cache en écriture des E/S de MCS pour optimiser le stockage.

- **/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 est équivalente à `/mastermcsimage`.

Cette option n'est pas valide lors de l'utilisation du programme d'installation VDAWorkstation-CoreSetup.exe.

- **/mastermcsimage**

Indique que cette machine sera utilisée comme image principale avec Machine Creation Services pour provisionner les machines virtuelles.

- **/masterpvsimage**

Indique que cette machine sera utilisée comme image principale avec Citrix Provisioning ou un outil de provisioning tiers (tel que Microsoft System Center Configuration Manager) pour provisionner les machines virtuelles.

- **/no_mediafoundation_ack**

Reconnait 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.

- **/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 (OS de bureau) ou les connexions négociées (OS de serveur). Exclut l'installation des composants suivants :

- Citrix Personalization pour AppV
- Citrix User Profile Manager
- Citrix User Profile Manager WMI Plugin
- Machine Identity Service
- Personal vDisk
- Outils de prise en charge Citrix
- Citrix Files pour Windows

Cette option n'est pas valide lors de l'utilisation du programme d'installation `VDAWorkstation-CoreSetup.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 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** *directory*

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

La commande suivante installe un VDA sur un OS de serveur. Le VDA sera utilisé comme image principale.

```
VDAServerSetup.exe /quiet /controllers "Contr-East.domain.com"/enable_hdx_ports /masterimage
```

La commande suivante installe un VDA Core Services sur un OS de bureau à utiliser dans un déploiement VDI ou Remote PC Access. L'application Citrix Workspace et les autres services non fondamentaux ne sont pas installés. L'adresse d'un Cloud Connector est spécifiée, et les ports du Service de pare-feu Windows seront automatiquement ouverts. L'administrateur doit gérer les redémarrages.

```
VDAServerSetup.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. Exécutez `XenDesktopVDASetup.exe`, en utilisant une ou plusieurs des options suivantes.

- `/reconfigure` (option requise lors de la personnalisation d'un VDA)
- `/h` ou `/help`
- `/quiet`
- `/noreboot`
- `/controllers`
- `/portnumber port`
- `/enable_hdx_ports`

Autres ressources

[Créer des catalogues de machines](#)

Pour passer en revue l'ensemble du processus de configuration, consultez la section [Installer et configurer](#).

Créer des catalogues de machines

March 6, 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.

Remarque :

Si vous utilisez Azure Resource Manager pour héberger vos ressources, vous pouvez éventuellement utiliser la méthode Déploiement rapide d'Azure au lieu de Studio comme décrit dans les sections suivantes. Pour plus de détails, voir [Déploiement rapide d'Azure](#).

Studio vous guide dans le processus de création du premier catalogue de machines. 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 Citrix Provisioning. Ou vous pouvez utiliser vos propres outils pour fournir des machines.

- Si vous utilisez Citrix Provisioning pour créer des machines, consultez la documentation [Citrix Provisioning](#) 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 la console de gestion 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 pour créer le premier catalogue, vous spécifiez une connexion hôte que vous avez créée précédemment. 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.

Vérification des licences RDS

La création d'un catalogue de machines contenant des machines avec OS de serveur Windows comprend une vérification automatique des licences RDS. Studio recherche dans le catalogue une machine sous tension et enregistrée sur laquelle effectuer la vérification.

- Si une machine sous tension et enregistrée ne peut pas être trouvée, un avertissement s'affiche, indiquant que la vérification des licences RDS ne peut pas être exécutée.
- Si une machine est trouvée, et qu'une erreur est détectée, Studio affiche un message d'avertissement pour le catalogue de machines contenant le problème détecté. Pour supprimer un avertissement de licence RDS d'un catalogue (afin qu'il n'apparaisse plus dans Studio), sélectionnez le catalogue. Cliquez sur **Supprimer l'avertissement de licence RDS** dans le volet **Actions**. Lorsque vous y êtes invité, confirmez l'action.

Enregistrement de VDA

Un VDA doit être enregistré auprès d'un Cloud Connector 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 plusieurs raisons pour lesquelles un VDA peut ne pas être enregistré, un grand nombre d'entre elles pouvant être résolues. 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.

Dans l'assistant de création de catalogue, 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 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

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 Citrix Provisioning, vous pouvez utiliser une image principale ou un ordinateur physique comme machine cible principale. Citrix Provisioning utilise une terminologie différente de MCS pour faire référence aux images ; consultez la documentation Citrix Provisioning pour plus de détails (</fr-fr/provisioning.html>).
- 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.

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 Citrix Provisioning 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 Citrix Provisioning, 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 Citrix Provisioning.
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.

Commencer à créer le catalogue

Avant de créer un catalogue :

- Consultez cette section pour en savoir plus sur les choix à effectuer et les informations que vous devez fournir.
- Assurez-vous d'avoir créé une connexion à l'hyperviseur, au service de cloud et aux autres ressources qui hébergent vos machines.
- Si vous avez créé une image principale pour provisionner des machines, assurez-vous d'avoir installé un VDA sur cette image.

Pour lancer l'assistant de création de catalogues :

1. Connectez-vous à [Citrix Cloud](#). Dans le menu en haut à gauche, sélectionnez **Mes services > Virtual Apps and Desktops**.
2. Cliquez sur **Manage**.
3. S'il s'agit du premier catalogue que vous créez, Studio vous indique quelle option choisir (telle que « Configurer les machines et créer des catalogues de machines pour exécuter les applications et les bureaux »). L'assistant de création de catalogues s'ouvre et vous guide au travers des éléments décrits ci-dessous.

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 vous guide au travers des pages décrites ci-dessous. Les pages qui s'affichent peuvent être différentes selon les sélections que vous effectuez et la connexion (à un hôte) que vous utilisez. Pour des conseils spécifiques, consultez l'article correspondant à votre type d'hôte.

- [Environnements de virtualisation Microsoft System Center Virtual Machine Manager](#)
- [Environnements de virtualisation Microsoft Azure Classic](#)
- [Environnements de virtualisation Microsoft Azure Resource Manager](#)
- [Environnements de virtualisation Amazon Web Services \(AWS\) et Citrix XenDesktop sur AWS](#)
- [Environnements de virtualisation XenServer](#)
- [Environnements de virtualisation VMware](#)

Étape 1 – 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.

- **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.

Étape 2 – Gestion de machine

Cette page ne s'affiche pas lorsque vous créez un catalogue 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** : vous permet de gérer des machines cibles en tant que collection de machines. Une image vDisk Citrix Provisioning 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.

Étape 3 – 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 Citrix Provisioning 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.

Étape 4 – 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.

Rappel :

- Lorsque vous utilisez MCS ou Citrix Provisioning, 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.

Ne modifiez pas la sélection de version de VDA minimale par défaut.

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.

Étape 5 – Plate-forme cloud et environnements de service

Lorsque vous utilisez un service ou une plate-forme cloud pour héberger des machines virtuelles, l'assistant de création de catalogue peut contenir des pages supplémentaires spécifiques à cet hôte. Par exemple, lorsque vous utilisez une image principale Azure Resource Manager, l'assistant de création de catalogue contient une page **Types de stockage et de licence**.

Conseil :

Pour de plus amples informations, consultez la section [Environnements de virtualisation Microsoft Azure Resource Manager](#).

Étape 6 – Collection de machines

Cette page s'affiche uniquement lorsque vous utilisez Citrix Provisioning 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 Citrix Provisioning.

Étape 7 – 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 VM.
 - **Important :** chaque machine virtuelle créée dispose 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 utilise plusieurs zones, vous pouvez sélectionner une zone (emplacement de ressources) 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.

- **Lors de l'utilisation de Citrix Provisioning 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 Citrix Provisioning ou d'autres outils (mais pas MCS) :**

Une icône et une info-bulle pour chaque machine ajoutée (ou importée, ou provenant d'une collection de machines Citrix Provisioning) vous aident à identifier les machines qu'il peut ne pas être possible d'ajouter au catalogue, ou d'enregistrer auprès d'un Cloud Connector.

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.

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. Cette fonctionnalité est appelée [MCSIO](#).

Important :

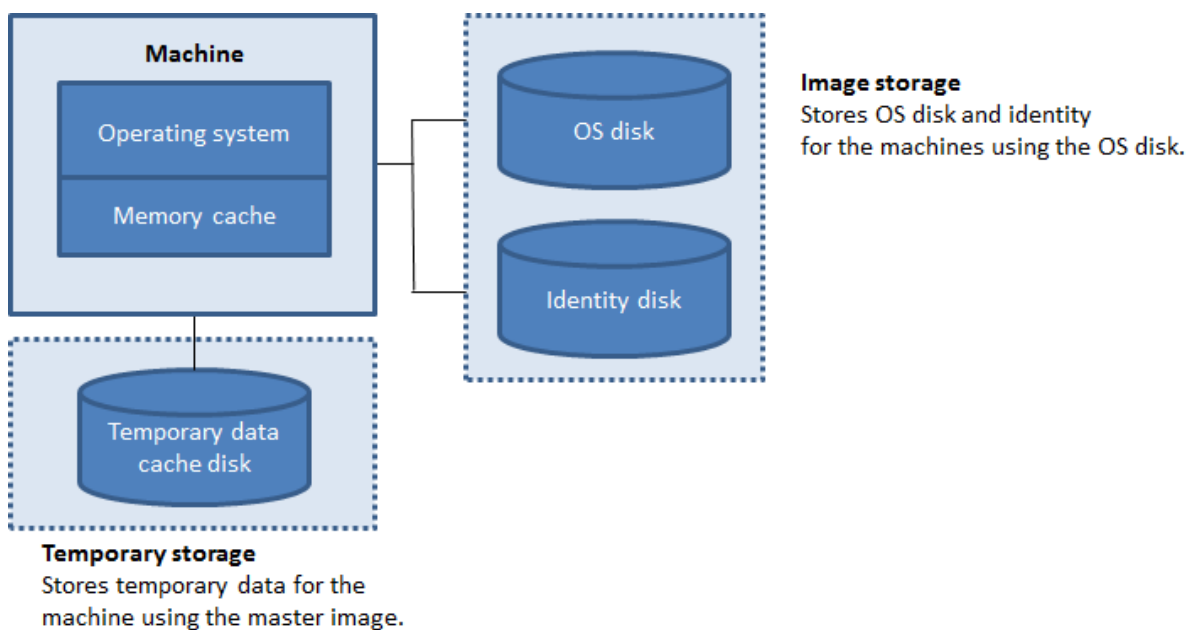
cette fonctionnalité nécessite un pilote MCSIO actuel. L'installation de ce pilote est une option lorsque vous installez ou mettez à niveau un VDA. Par défaut, ce pilote n'est pas installé.

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)**. Par défaut, ces cases à cocher sont désactivées. Lorsque vous activez une ou plusieurs cases, 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 décochez ces deux cases, les données temporaires ne seront 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.

Vous ne pouvez pas modifier les valeurs de cache dans un catalogue de machines après sa création.

Étape 8 – 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.

Étape 9 – 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.

Étape 10 – 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 des comptes ou utiliser des comptes existants, ainsi que l'emplacement de ces comptes.

- Si vous créez des 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 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.

- 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]  
nomcompteordinateurAD.domaine
```

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 Citrix Provisioning, les comptes d'ordinateur pour les machines cibles sont gérés différemment ; consultez la documentation Citrix Provisioning.

Étape 11 – Résumé, nom et description

Sur la page **Résumé**, vérifiez les paramètres que vous avez spécifiés. Entrez un nom et une description pour le catalogue. Ces informations s'affichent dans Studio.

Lorsque vous avez terminé, cliquez sur **Terminer** pour démarrer la création du catalogue.

Plus d'informations

- [Gestion des images Citrix Virtual Apps and Desktops](#)
- [Connexions et ressources](#)
- [Gérer des catalogues de machines](#)

Autres ressources

S'il s'agit du premier catalogue créé, Studio vous explique comment [créer un groupe de mise à disposition](#).

Pour passer en revue l'ensemble du processus de configuration, consultez la section [Installer et configurer](#).

Déploiement rapide d'Azure

February 15, 2019

Dans le service Citrix Virtual Apps and Desktops, si votre emplacement de ressources utilise des machines Azure Resource Manager pour fournir des applications et des postes de travail publiés, vous pouvez choisir une méthode de déploiement :

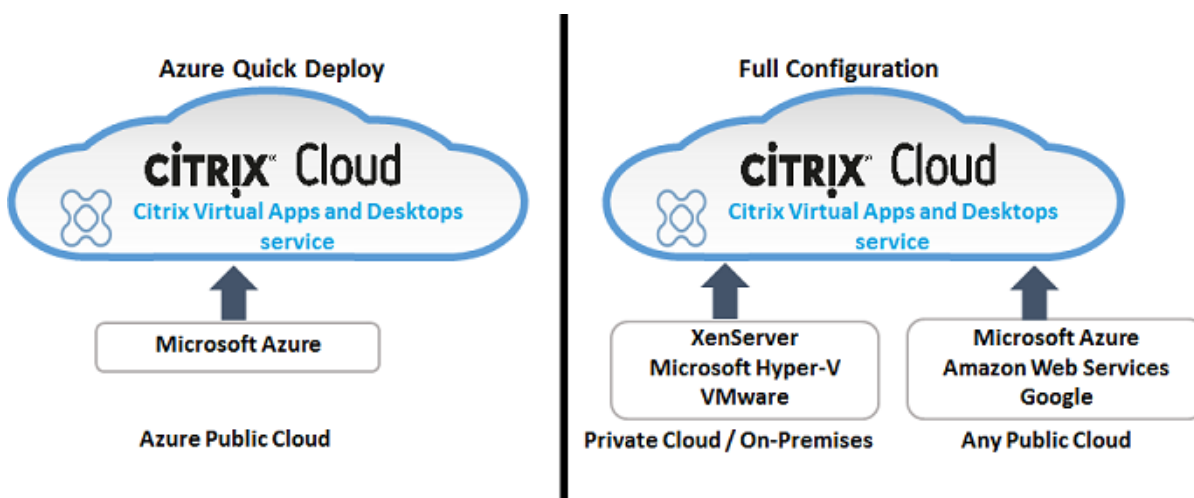
- **Configuration complète** : cette option utilise la console de gestion Studio, qui vous guide dans la création d'un catalogue de machines et d'un groupe de mise à disposition. Cette méthode de déploiement offre des fonctionnalités de configuration avancées. Cette méthode peut être utilisée pour n'importe quel type d'hôte pris en charge.
- **Déploiement rapide d'Azure** : l'option Déploiement rapide d'Azure fournit une interface plus simple qui permet un déploiement plus rapide des applications et des postes de travail. Cette méthode de déploiement offre une configuration de base, sans fonctionnalités avancées. Cette méthode est valide uniquement lorsque vous utilisez Azure Resource Manager en tant qu'hôte.

Le Déploiement rapide d'Azure offre un moyen rapide de configurer un environnement de preuve de concept ou de démarrer avec le service Citrix Virtual Apps and Desktops lors de l'utilisation d'Azure Resource Manager.

Si vous maîtrisez l'utilisation de Studio pour déployer des catalogues (sur une installation locale du service Citrix Virtual Apps and Desktops, ou la Configuration complète du service Citrix Virtual Apps and Desktops), il existe certaines différences.

- Le Déploiement rapide d'Azure utilise une terminologie différente : vous créez un catalogue. En Configuration complète (Studio), vous créez un catalogue de machines.
- Le Déploiement rapide d'Azure crée automatiquement des VM de serveur et installe deux Cloud Connector dans votre emplacement de ressources. En Configuration complète, il s'agit d'étapes distinctes que vous devez effectuer avant de créer un catalogue.
- Le Déploiement rapide d'Azure n'utilise pas de groupes de mise à disposition. Dans le Déploiement rapide d'Azure, vous configurez tous les éléments de déploiement du catalogue : le catalogue, les machines, les applications, les postes de travail et les abonnés. (Un groupe de mise à disposition est automatiquement créé pour chaque catalogue Déploiement rapide d'Azure (en utilisant le même nom que le catalogue), mais cette action se produit en arrière-plan. Aucune intervention de l'administrateur du client n'est requise.)
- Le style et la présentation de l'interface du Déploiement rapide d'Azure sont différents. Elle propose plus de conseils à l'écran.

Le graphique et le tableau suivants comparent les méthodes de déploiement.



	Fonctionnalité	Déploiement rapide d'Azure	Configuration complète
Déployer	Déployer sur Azure	Oui	Oui
	Déployer sur Amazon Web Services et Google Cloud	Non	Oui
	Déployer sur des hyperviseurs installés localement	Non	Oui

	Fonctionnalité	Déploiement rapide d'Azure	Configuration complète
Mettre à disposition	Mettre à disposition des applications Windows	Oui	Oui
	Mettre à disposition des postes de travail Windows partagés (serveur)	Oui	Oui
	Mettre à disposition des applications/postes de travail Linux	Non	Oui
	Mettre à disposition des bureaux Windows avec OS client	Non	Oui
Expérience utilisateur	Remote PC Access	Non	Oui
	Expérience utilisateur simplifiée	Oui	Non

Si vous maîtrisez le service Citrix Virtual Apps Essentials, l'interface de Déploiement rapide d'Azure est très similaire. Elle est facile à utiliser, surtout si vous ne connaissez pas Studio.

Les méthodes de déploiement ne sont pas mutuellement exclusives. Vous pouvez utiliser une méthode pour créer des ressources, puis utiliser l'autre méthode pour créer des ressources supplémentaires. Cependant, l'endroit où vous modifiez un catalogue peut avoir des effets ; Voir Modification des catalogues Déploiement rapide d'Azure.

Affichage des catalogues

Les catalogues créés avec Déploiement rapide d'Azure sont visibles à la fois dans Déploiement rapide d'Azure et dans Studio.

Les catalogues de machines créés à l'origine dans Studio ne sont pas visibles dans l'affichage de Déploiement rapide d'Azure.

Limitations

- Déploiement rapide d'Azure est disponible uniquement lorsque vous utilisez Azure Resource Manager en tant qu'hôte. Il n'est pas disponible avec d'autres types d'hôtes.
- La fonction Déploiement rapide d'Azure est disponible uniquement dans le service Citrix Virtual Apps and Desktops et le service Citrix Virtual Apps. Elle n'est pas offerte dans le service Citrix Virtual Desktops.
- Déploiement rapide d'Azure fournit des machines Windows Server. Vous ne pouvez pas l'utiliser pour déployer des machines d'OS de bureau.
- Vous devez être un administrateur complet pour avoir accès aux deux options de déploiement. Si vous n'êtes pas un administrateur complet, l'option Déploiement rapide d'Azure n'apparaîtra pas et la Configuration complète sera automatiquement utilisée.
- Reportez-vous à la remarque importante dans la modification des catalogues Déploiement rapide d'Azure.

Considération Citrix Gateway

Si vous utilisez votre propre Citrix Gateway, il doit avoir accès au VNET spécifié dans l'assistant de création de catalogues. Un VPN peut fournir cet accès.

Alternativement, le Citrix Gateway Service fonctionne automatiquement avec les catalogues Déploiement rapide d'Azure.

Modification des catalogues Déploiement rapide d'Azure

Après avoir déployé un catalogue à l'aide de Déploiement rapide d'Azure, il apparaît dans la catégorie Catalogues Déploiement rapide de l'écran Gérer > Catalogues. Vous pouvez utiliser le menu des points de suspension sur la ligne d'un catalogue pour sélectionner les actions suivantes :

- Ajouter ou supprimer des applications
- Ajouter ou supprimer des abonnés
- Changer la capacité
- Sélectionner une image principale différente
- Supprimer le catalogue

IMPORTANT :

Vous pouvez également utiliser Studio pour modifier un catalogue déployé avec Déploiement rapide d'Azure. Toutefois, si vous utilisez Studio pour modifier ce catalogue ou son groupe de mise à disposition correspondant, vous ne pourrez plus modifier ce catalogue à partir de l'interface de Déploiement rapide d'Azure (Gérer > Catalogues). Le catalogue sera toujours

répertorié dans **Gérer > Catalogues**, mais il ne pourra plus être géré ou supprimé à partir de cet emplacement.

Utiliser Déploiement rapide d'Azure

La séquence de Déploiement rapide d'Azure est essentiellement la même que l'interface de déploiement du service Citrix Virtual Apps Essentials.

La plupart des conseils sont disponibles dans l'article [service Citrix Virtual Apps Essentials](#). (Dans cet article, ne tenez pas compte des informations sur la façon d'acheter et d'annuler le service.)

1. Commencez dans la section [Créer un catalogue](#), en remplaçant la procédure suivante pour l'étape 2.

Cliquez sur **Catalogues** (si ce n'est pas déjà sélectionné). Sélectionnez **Gérer > Déploiement rapide Azure**. Cliquez sur **Créer un catalogue**.
2. Suivez les procédures pour créer un catalogue.
3. Suivez les procédures de publication d'applications et d'attribution d'abonnés à un catalogue.

Lorsque vous avez terminé ces étapes, partagez l'URL de l'espace de travail avec vos abonnés. Pour de plus amples informations, consultez la section [Lancer des applications et des bureaux](#).

Créer des groupes de mise à disposition

March 6, 2019

Introduction

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 peut également indiquer les utilisateurs autorisés à utiliser ces machines ainsi que les applications et bureaux auxquels les utilisateurs peuvent accéder.

La création d'un groupe de mise à disposition est la prochaine étape de configuration de votre déploiement après 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.

Avant de créer un groupe de mise à disposition :

- Consultez cette section pour en savoir plus sur les choix à effectuer et les informations que vous devez fournir.
- Assurez-vous d'avoir créé une connexion à l'hyperviseur, au service de cloud et aux autres ressources qui hébergent vos machines.
- Assurez-vous d'avoir créé un catalogue de machines contenant des machines physiques ou virtuelles qui mettront à disposition des applications et bureaux.

Pour lancer l'assistant de création de groupe de mise à disposition :

1. Connectez-vous à [Citrix Cloud](#). Dans le menu en haut à gauche, sélectionnez **Mes services > Virtual Apps and Desktops**.
2. Cliquez sur **Gérer**.
3. S'il s'agit du premier groupe de mise à disposition que vous créez, la console vous indique quelle option choisir (telle que « Configurez des groupes de mise à disposition à afficher en tant que services »). L'assistant de création de groupe de mise à disposition s'ouvre et vous guide au travers des éléments décrits ci-dessous.
4. 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 de Studio. Sélectionnez ensuite **Créer un groupe de mise à disposition** dans le volet Actions.

L'assistant vous guide au travers des pages décrites ci-dessous. Les pages de l'assistant qui s'affichent peuvent être différentes selon les sélections que vous effectuez.

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 sélectionné.
- Un catalogue 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 tous les VDA vers la dernière version, et de mettre à niveau les catalogues de machines et les groupes de mise à disposition le cas échéant. 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. Par exemple, si l'une des machines que vous sélectionnez dispose d'un VDA version 7.1 et que d'autres machines ont une version plus récente, toutes les machines du groupe peuvent uniquement utiliser les fonctionnalités prises en charge dans le VDA 7.1. Cela signifie que certaines fonctionnalités qui nécessitent des versions de VDA plus récentes risquent de ne pas être disponibles dans ce groupe de mise à disposition.

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**. Vous ne pouvez pas activer les deux.

Si vous avez sélectionné des machines à partir d'un catalogue d'OS de serveur ou d'OS de bureau aléatoire (regroupé), le type de mise à disposition par défaut est applications et bureaux. Vous pouvez mettre à disposition des applications, des bureaux, ou les deux.

Étape 3 – AppDisks

Ignorez cette page. Cliquez sur **Suivant**.

Étape 4 – Utilisateurs

REMARQUE :

Au lieu de spécifier des applications dans l'assistant de groupe de mise à disposition (comme décrit dans cette section), vous pouvez les configurer via la bibliothèque Citrix Cloud.

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 déploiement, qui n'est pas configurée dans cette console. Par défaut, la règle de stratégie d'admissibilité d'application inclut tout le monde. Consultez les applets de commande `BrokerAppEntitlementPolicyRule` du SDK PowerShell pour plus de détails.
- Les groupes de mise à disposition.
- Les applications.

La liste des utilisateurs qui peuvent accéder à une application est formée par l'intersection des listes utilisateur ci-dessus.

Utilisateurs authentifiés et non authentifiés

Il existe deux types d'utilisateurs : authentifiés 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.

- **Authentifiés** : 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 l'application Citrix Workspace. (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 authentifiés (anonymes)** : 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 l'application Citrix Workspace. 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 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

Activer l'accès pour	Ajouter/affecter des utilisateurs et des groupes d'utilisateurs ?	Activer la case à cocher « Autoriser les utilisateurs non authentifiés » ?
À la fois les utilisateurs authentifiés et non authentifiés	Oui	Oui

Étape 5 – Applications

REMARQUE :

Au lieu de spécifier des applications dans l'assistant de groupe de mise à disposition (comme décrit dans cette section), vous pouvez les configurer via la bibliothèque Citrix Cloud.

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 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 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). Sinon, des noms en double s'afficheront dans l'application Citrix Workspace.

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**.

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 déploiement. Ou une application peut ne pas être compatible avec les types de session pris en charge sur des machines du catalogue de machines sélectionné.

Étape 6 – Bureaux (ou règles d'attribution de bureau)

REMARQUE :

Au lieu de spécifier des bureaux dans l'assistant de groupe de mise à disposition (comme décrit dans cette section), vous pouvez les configurer via les bibliothèques Citrix Cloud.

Le titre de cette page dépend du catalogue de machines que vous avez choisi précédemment dans l'assistant :

- Si vous avez choisi un catalogue contenant des machines regroupées, cette page est appelée **Bureaux**.
- Si vous avez choisi un catalogue 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 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 l'application Citrix Workspace.
- Si la fonctionnalité de balises est prise en charge : 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

- 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 l'application Workspace 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.

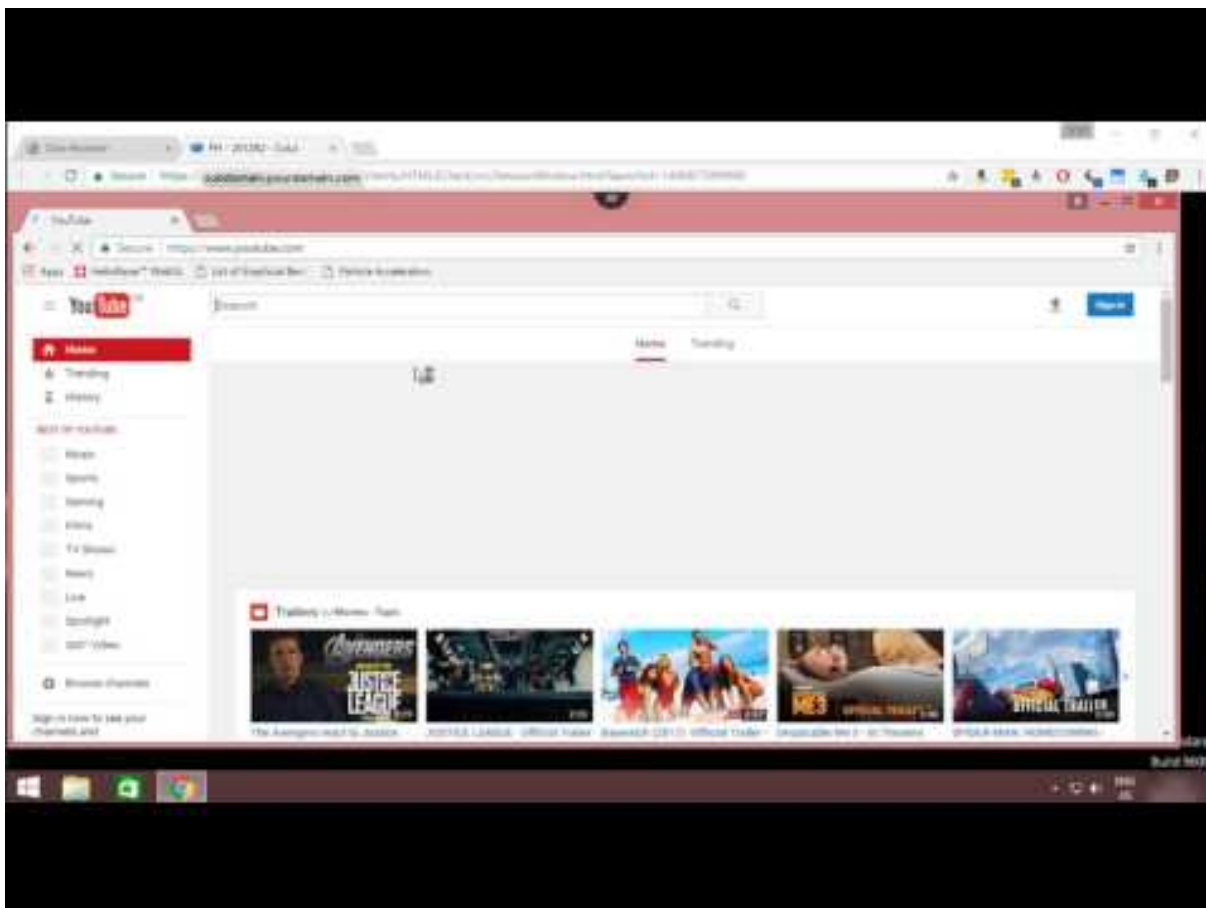
Si vous ne spécifiez pas d'utilisateurs ou d'applications dans l'assistant

Au lieu de spécifier des utilisateurs et des applications dans un groupe de mise à disposition, vous pouvez les spécifier dans la console Citrix Cloud.

1. Dans la console Citrix Cloud, sélectionnez **Bibliothèque**.
2. Recherchez la carte contenant les ressources (applications ou bureaux) que vous souhaitez. Placez le curseur sur les points de suspension dans le coin supérieur droit et sélectionnez **Gérer les abonnés**.
3. Dans la boîte de dialogue **Gérer les abonnés**, sous **Ajouter des abonnés** dans la liste déroulante de gauche, sélectionnez les abonnés (utilisateurs). Si vous avez plusieurs abonnés, vous devrez peut-être taper un ou plusieurs caractères du groupe de domaine contenant ces utilisateurs dans le champ de recherche approprié. Les correspondances apparaissent dans le tableau en-dessous des deux champs. Sélectionnez la correspondance appropriée. (S'il n'existe qu'une seule correspondance, elle est automatiquement sélectionnée). Lorsque le champ d'état indique **Prêt**, cliquez sur le **X** dans le coin supérieur droit pour fermer la boîte de dialogue.

4. Actualisez la page **Ressources**. Le coin inférieur gauche de la carte des ressources contient une valeur indiquant les utilisateurs de domaine qui ont été sélectionnés.

Voici une vidéo de ce processus.



Plus d'informations

- [Gérer les groupes de mise à disposition](#)
- [Applications](#)

Créer des groupes d'applications

March 6, 2019

Remarque :

La fonction Restriction de balise n'est actuellement pas disponible.

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.
- (Fonction actuellement non disponible.) 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 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 con-

dition 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

Remarque :

La fonction Restriction de balise n'est actuellement pas disponible.

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. Conditions requises :

1. Mise à niveau des VDA sur les machines utilisées dans le groupe de mise à disposition
2. Mise à niveau des catalogues de machines contenant ces machines
3. Mise à niveau du 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. Consultez [Administration déléguée](#) pour plus de détails.

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 souhaitez 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 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.

Étape 1 – Groupes de mise à disposition

La page **Groupes de mise à disposition** répertorie tous les groupes de mise à disposition, avec le nombre de machines que chaque groupe contient.

- 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 ne fournissent que des postes de travail, si les deux conditions suivantes sont remplies :

- Le groupe de mise à disposition contient des machines partagées et a été créé avec une version XenDesktop antérieure à 7.9.x.
- Vous avez 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.

(Fonction actuellement non disponible.) Pour ajouter une restriction de balise, sélectionnez **Restreindre les lancements aux machines dotées de balises**, puis sélectionnez la balise dans la liste déroulante.

Étape 2 – 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.

Pour plus d'informations sur l'emplacement des listes d'utilisateurs dans un déploiement, voir [Où les listes d'utilisateurs sont spécifiées](#).

Étape 3 – 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, des noms en double s'afficheront dans l'application Citrix Workspace.
- 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 nou-

velle 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 sélectionné l'une des options suivantes :

- Groupes d'applications qui n'ont pas de groupes de mise à disposition associés.
 - Groupes d'applications avec des groupes de mise à disposition associés qui ne contiennent pas de machines.
 - Groupe de mise à disposition ne contenant pas de machines.
- **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).

Étape 4 – Étendues

Cette page s'affiche uniquement si vous avez déjà créé une étendue. personnalisée Par défaut, l'étendue **Tous** est sélectionnée. Pour plus d'informations, veuillez consulter la section [Administration déléguée](#).

Étape 5 – Synthèse

Entrez un nom pour le groupe d'applications. Vous pouvez également entrer une description (facultatif).

Consultez les informations récapitulatives, puis cliquez sur **Terminer**.

Supprimer des composants

October 10, 2018

Pour supprimer des composants que vous avez installés (tels que des VDA), Citrix vous recommande d'utiliser la fonctionnalité Windows de suppression/modification de programmes. Vous pouvez également supprimer des composants à l'aide de la ligne de commande ou d'un script.

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 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 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 un VDA à l'aide de la ligne de commande

Exécutez la commande utilisée pour installer le VDA : `VDAServerSetup.exe`, `VDAWorkstationSetup.exe` ou `VDAWorkstationCoreSetup.exe`. Consultez la section [Installer à l'aide de la ligne de commande](#) pour une description de la syntaxe.

- Pour supprimer uniquement le VDA ou le application Citrix Workspace, utilisez les options `/remove` et `/components`.
- Pour supprimer le VDA et application Citrix Workspace, utilisez l'option `/removeall`.

Par exemple, la commande suivante supprime le VDA et l'application Citrix Workspace d'une machine d'OS de serveur.

```
VDA ServerSetup.exe /removeall
```

Par exemple, la commande suivante supprime le VDA mais pas l'application Citrix Workspace pour Windows (si elle est installée) d'une machine d'OS de bureau.

```
VDA WorkstationSetup.exe /remove /component vda
```

Vous pouvez également supprimer un VDA à l'aide d'un script fourni par Citrix. Consultez la section [Supprimer des VDA à l'aide du script](#).

Mise à niveau

October 10, 2018

REMARQUE :

vous trouverez des informations sur les changements de nom de produit [ici](#).

Citrix conserve tous les composants du service Citrix Virtual Apps et Desktops dans votre déploiement à l'exception des VDA.

Pour mettre à niveau un VDA, il vous suffit de télécharger le programme d'installation (comme vous l'avez fait pour l'installer) et de l'exécuter sur la machine ou l'image. Vous pouvez utiliser l'interface graphique du programme d'installation ou l'interface de ligne de commande.

Si vous avez installé le VDA à l'aide du programme d'installation `VDAWorkstationCoreSetup.exe`, cette configuration sera conservée si vous le mettez à niveau avec la dernière version du même programme d'installation. Si vous exécutez le programme d'installation `VDAWorkstationSetup.exe` sur cette machine, vous pouvez activer les fonctionnalités qui ne sont pas prises en charge dans le programme d'installation `VDAWorkstationCoreSetup.exe`. (N'oubliez pas que certaines de ces fonctionnalités peuvent être activées par défaut dans le programme d'installation `VDAWorkstationSetup.exe`.) Vous aurez également la possibilité d'installer application Citrix Workspace.

Un redémarrage se produit lors de la mise à niveau d'un VDA vers la version 7.17 ou une version ultérieure prise en charge. Cela ne peut pas être évité. La mise à niveau reprend automatiquement après le redémarrage (sauf si vous spécifiez `/noresume` sur la ligne de commande).

Une fois les VDA mis à niveau, mettez à jour les images principales et les catalogues qui utilisent ce VDA.

Systèmes d'exploitation antérieurs

Pour les machines dont les systèmes d'exploitation ne sont plus pris en charge et ne permettent pas d'installer le dernier VDA (tels que Windows 7 et Windows Server 2008 R2), vous disposez de plusieurs options.

- Créez une nouvelle image de la machine sur une version prise en charge de Windows, puis installez le nouveau VDA.
- Si réimager la machine n'est pas une option mais que vous voulez mettre à niveau le système d'exploitation, désinstallez le VDA avant la mise à niveau du système d'exploitation. Sinon, le VDA sera dans un état non pris en charge. Installez ensuite le nouveau VDA.
- Si vous voulez continuer à utiliser des machines avec un système d'exploitation qui n'est plus pris en charge pour le VDA 7.16 ou version ultérieure, XenApp et XenDesktop 7.15 LTSR est la dernière version de VDA prise en charge pour Windows 7 et Windows Server 2008 R2.
 - Si la version 7.15 LTSR est installée sur la machine (et vous tentez d'installer une version plus récente), un message vous informe que vous utilisez la dernière version prise en charge.
 - Si une version antérieure à LTSR 7.15 est installée sur la machine, un message vous renvoie à l'article [CTX139030](#) pour plus d'informations. Vous pouvez télécharger la version VDA 7.15 LTSR à partir du site Web de Citrix.

Plus d'informations

- [Installer des VDA](#)
- [Installer des VDA à l'aide de la ligne de commande](#)
- [Gérer des catalogues de machines](#)

Imprimer

October 10, 2018

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.

Pour obtenir des informations complètes sur l'impression dans un environnement Citrix Virtual Apps and Desktops, commencez par lire l'article [Imprimer](#). Vous pourrez ensuite passer à :

- [Exemples de configuration d'impression](#)
- [Recommandations](#)
- [Stratégies et préférences d'impression](#)
- [Provisionner des imprimantes](#)
- [Gérer l'environnement d'impression](#)

Installer le serveur d'impression universel sur vos serveurs d'impression

1. Assurez-vous que Microsoft Visual C ++ Runtime 2013 32 bits et 64 bits est installé sur chaque serveur d'impression.
2. Accédez à la [page de téléchargement](#) du serveur d'impression universel Citrix et cliquez sur **Télécharger le fichier**.
3. Exécutez l'une des commandes suivantes sur chaque serveur d'impression :
 - Pour un système d'exploitation 32 bits : **UpsServer_x86.msi**.
 - Pour un système d'exploitation 64 bits : **UpsServer_x64.msi**.

Après avoir installé le serveur d'impression universel, configurez ce dernier à l'aide des instructions de la section [Provisionner les imprimantes](#).

Technologies HDX

October 10, 2018

Citrix HDX offre une large gamme de technologies conçues pour apporter une expérience utilisateur haute définition sur l'appareil, le réseau et le datacenter. Pour de plus amples informations, consultez les articles dans les catégories suivantes :

- [HDX](#)
- [Appareils](#)
- [Graphiques](#)
- [Multimédia](#)
- [Redirection de contenu](#)

Stratégies

October 10, 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, et si vous n'attribuez pas spécifiquement les stratégies, les paramètres sont appliqués à toutes les connexions.

Pour plus d'informations sur les stratégies Citrix, commencez par lire l'article [Stratégies](#). Vous pourrez ensuite passer à :

- [Utilisation des stratégies](#)
- [Modèles de stratégie](#)
- [Créer des stratégies](#)
- [Comparer, donner un ordre de priorité, modéliser et résoudre les problèmes des stratégies](#)
- [Paramètres de stratégie par défaut](#)
- [Référence des paramètres de stratégie](#)

Gérer

October 11, 2018

Citrix gère les déploiements du service Citrix Virtual Apps and Desktops en installant et en gérant les fonctionnalités et composants principaux dans Citrix Cloud. Vous vous chargez des machines (VDA) dans les emplacements de ressources qui mettent à disposition des applications et des postes de travail. Vous gérez également les connexions à ces emplacements de ressources, ainsi qu'aux applications, postes de travail et utilisateurs.

- **Gérer des catalogues de machines** et **Gérer des groupes de mise à disposition** : gérez les catalogues de machines et les groupes de mise à disposition que vous avez créés lors de la mise en route.
- **Applications** : permet de gérer les applications dans les groupes de mise à disposition.
- **Adresses IP virtuelles 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.*).

- **Enregistrement de VDA** : avant qu'un VDA ne puisse mettre à disposition des applications et des postes de travail, il doit s'enregistrer (établir la communication) auprès d'un Cloud Connector. Vous pouvez spécifier les adresses de Cloud Connector à l'aide de plusieurs méthodes, qui sont décrites dans cet article. Les VDA doivent disposer d'informations récentes lorsque vous ajoutez des Cloud Connector.
- **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.
- **Utilisation de la recherche** : pour afficher des informations sur les machines, sessions, catalogues de machines, applications ou groupes de mise à disposition dans Studio, utilisez la fonctionnalité de recherche flexible.
- **Prise en charge IPv4/IPv6** : Citrix Virtual Apps and Desktops 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.
- **Profile Management** : Citrix Profile Management peut être installé lorsque vous installez un VDA. Si vous utilisez cette solution de gestion des profils utilisateur, consultez la documentation l'accompagnant.
- **Citrix Insight Services** : Citrix Insight Services (CIS) est une plate-forme Citrix depuis laquelle vous pouvez générer des informations d'instrumentation, de télémétrie et d'autres données stratégiques. Des informations analytiques et de diagnostic sont collectées lorsque vous installez un VDA.
- **Cache d'hôte local** : la fonctionnalité de cache d'hôte local permet de poursuivre les opérations de négociation de connexion lorsqu'un Cloud Connector dans un emplacement de ressources ne peut pas communiquer avec Citrix Cloud.
- **Administration déléguée** : l'administration déléguée de Citrix Cloud vous permet de configurer les autorisations d'accès requises par tous vos administrateurs conformément à leur rôle dans votre organisation.
- **Journalisation de la configuration** : la journalisation de la configuration permet aux administrateurs de suivre les modifications de configuration et les activités administratives.

Zones

October 10, 2018

Introduction

Les déploiements du service Citrix Virtual Apps and Desktops répartis sur différents emplacements géographiques et connectés à un réseau étendu peuvent rencontrer des problèmes de latence réseau et de fiabilité. L'utilisation 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. Dans un environnement de service Citrix Virtual Apps and Desktops, chaque emplacement de ressource est considéré comme une zone.

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, ce qui améliore les performances. Les zones 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.

Le nombre de Cloud Connector configurés sur le site peut affecter les performances de certaines opérations. Pour éviter ce problème, nous vous recommandons de limiter le nombre de zones à un maximum de 10.

Dans cet article, le terme « local » fait référence à la zone dont il est question. Par exemple, « Un VDA s'enregistre auprès d'un Cloud Connector local » signifie qu'un VDA s'enregistre auprès d'un Cloud Connector dans la zone dans laquelle le VDA est situé.

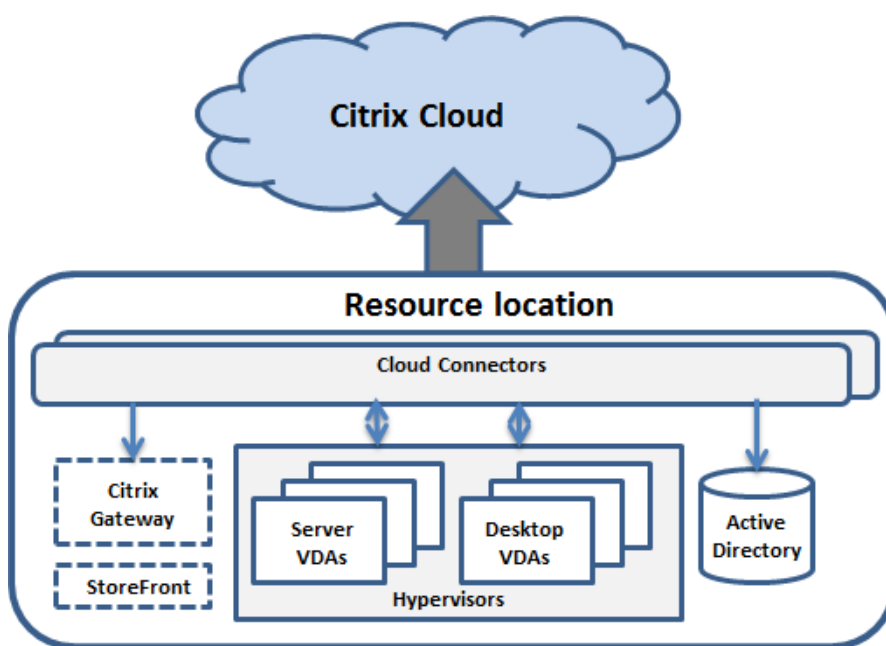
Différences par rapport aux zones des environnements Citrix Virtual Apps et Desktops locaux

Les zones d'un environnement de service Citrix Virtual Apps et Desktops sont similaires, mais pas identiques à celles d'un déploiement local de Citrix Virtual Apps and Desktops.

- Dans le service Citrix Virtual Apps and Desktops, les zones sont créées automatiquement lorsque vous créez un emplacement de ressources et y ajoutez un Cloud Connector. Contrairement à un déploiement local, un environnement de service ne classe pas les zones en tant que zones primaires ou satellites.
- Dans XenApp version 6.5 et versions antérieures, les zones incluaient des collecteurs de données. Le service Citrix Virtual Apps and Desktops n'utilise pas de collecteurs de données pour les zones. En outre, les zones de basculement et les zones préférées fonctionnent différemment.

Que contient une zone ?

Une zone équivaut à un emplacement de ressources. Lorsque vous créez un emplacement de ressources et installez un Cloud Connector, une zone est automatiquement créée pour vous. Chaque zone peut contenir différents types de ressources, en fonction de vos besoins et de votre environnement.



Au moins un Cloud Connector doit être installé sur chaque zone, de préférence deux ou plus, afin d'assurer la redondance.

Vous pouvez placer des catalogues de machines, hyperviseurs, connexions hôtes, utilisateurs et applications dans une zone. Une zone peut également contenir des serveurs Citrix Gateway et StoreFront. Pour utiliser la fonctionnalité de cache d'hôte local, une zone doit disposer d'un serveur StoreFront.

Les zones fonctionnent avec la fonctionnalité d'espace de travail Citrix Cloud et le Citrix Gateway Service.

Le placement d'éléments dans une zone affecte la façon dont le service interagit avec ces derniers et avec d'autres objets qui leur sont liés.

- Lorsqu'une connexion d'hyperviseur est placée dans une zone, il est supposé que tous les hyperviseurs gérés via cette connexion résident également dans cette zone.
- Lorsqu'un catalogue de machines est placé dans une zone, il est supposé que tous les VDA de ce catalogue se trouvent dans la zone.
- Des instances de Citrix Gateway peuvent être ajoutées aux zones. Lorsque vous créez un emplacement de ressources, vous avez la possibilité d'ajouter un Citrix Gateway. Lorsqu'une passerelle Citrix Gateway est associée à une zone, elle est utilisée de préférence lorsque des connexions à des VDA dans cette zone sont utilisées.
- Dans l'idéal, Citrix Gateway situé dans une zone est utilisé pour les connexions utilisateur entrant dans cette zone depuis d'autres zones ou des emplacements externes. Vous pouvez également l'utiliser pour les connexions au sein de la zone.
- Après avoir créé des emplacements de ressources supplémentaires et y avoir installé des Cloud Connector (ce qui crée automatiquement des zones supplémentaires), vous pouvez déplacer des ressources entre les zones. La contrepartie de cette flexibilité est le risque de séparer des

éléments qui fonctionnent mieux quand ils sont proches les uns des autres. Par exemple, le déplacement d'un catalogue vers une zone différente de 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.

Si la connexion entre une zone et Citrix Cloud échoue, la fonctionnalité Cache d'hôte local active un Cloud Connector dans la zone afin de continuer à établir des connexions avec les VDA de cette zone. (Un StoreFront doit être installé sur la zone) Ce scénario peut par exemple être efficace dans un bureau où les utilisateurs utilisent un site StoreFront local pour accéder à leurs ressources locales, même si la liaison WAN connectant leur bureau au réseau d'entreprise échoue. Pour plus d'informations, veuillez consulter la section [Cache d'hôte local](#).

Où les VDA sont-ils enregistrés ?

Les VDA doivent être à la version minimale 7.7 pour utiliser ces fonctionnalités d'enregistrement de zone :

- Un VDA situé dans une zone s'enregistre auprès d'un Cloud Connector local.
 - Tant que ce Cloud Connector peut communiquer avec Citrix Cloud, les opérations normales se poursuivent.
 - Si ce Cloud Connector est opérationnel, mais qu'il ne peut pas communiquer avec Citrix Cloud (et que la zone est dotée d'un StoreFront local), il entre en mode panne Cache d'hôte local.
 - Si un Cloud Connector échoue, les VDA dans cette zone tentent de s'enregistrer auprès d'autres Cloud Connector locaux. Un VDA dans une zone ne tente jamais de s'enregistrer auprès d'un Cloud Connector dans une autre zone.
- Si vous ajoutez ou supprimez un Cloud Connector d'une zone (à l'aide de la console de gestion Citrix Cloud), et que la mise à jour automatique est activée, les VDA dans cette zone reçoivent des listes mises à jour des Cloud Connector qui sont disponibles ; cela leur permet de savoir auprès de quels Cloud Connector ils peuvent s'enregistrer et accepter des connexions.
- Si vous déplacez un catalogue de machines vers une autre zone (à l'aide de Studio), les VDA de ce catalogue s'enregistrent auprès des Cloud Connector situés dans la zone dans laquelle vous avez déplacé le catalogue. Lorsque vous déplacez un catalogue, assurez-vous de déplacer également toute connexion hôte associée à la même zone.
- Lors d'une panne (lorsque les Cloud Connector d'une zone ne peuvent pas communiquer avec Citrix Cloud), seules les ressources associées aux machines enregistrées dans cette zone sont disponibles.

Préférence de zone

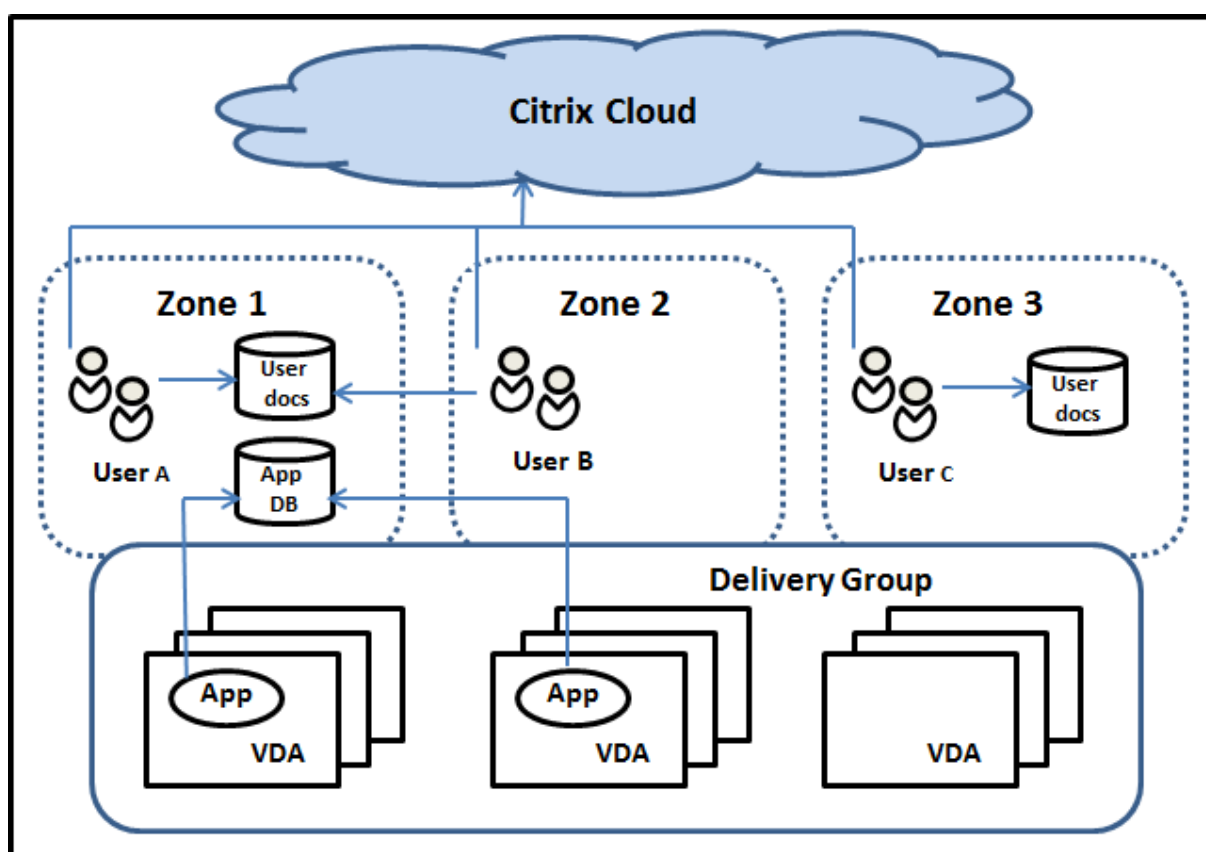
Dans un site multi-zone, la fonctionnalité de préférence de zone permet à l'administrateur de mieux contrôler les VDA utilisés pour lancer une application ou un bureau.

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 l'application Citrix Workspace est exécutée). Il s'agit de l'emplacement de l'utilisateur. L'emplacement de l'utilisateur requiert StoreFront 3.7 et Citrix Gateway (anciennement NetScaler Gateway) 11.0-65.x au minimum.

Le graphique suivant illustre un exemple de configuration multi-zone.



Dans cet exemple, les VDA sont répartis entre trois zones, mais ils sont tous dans le même groupe de mise à disposition. Par conséquent, le broker du service Citrix Virtual Apps and Desktops peut

choisir le VDA à utiliser pour une demande de lancement d'un utilisateur. Cet exemple montre que les utilisateurs peuvent exécuter leurs points de terminaison d'application Citrix Workspace à différents emplacements. L'utilisateur A utilise un périphérique avec l'application Citrix Workspace dans la zone 1. L'utilisateur B utilise un périphérique dans la zone 2. De même, les documents d'un utilisateur peuvent être stockés dans différents endroits. Les utilisateurs A et B utilisent un partage situé dans la zone 1 ; L'utilisateur C utilise un partage dans la zone 3. De plus, l'une des applications publiées utilise une base de données qui se trouve dans la zone 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 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. 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. 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 application Citrix Workspace (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 est (ou n'est pas) utilisée.

- **Utilisation obligatoire de la zone d'accueil utilisateur :** dans un groupe de mise à disposition, vous pouvez spécifier « Lancer la session dans la zone d'accueil de l'utilisateur (si l'utilisateur

dispose d'une zone d'accueil), sans basculement vers une autre zone si aucune ressource n'est disponible 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 « Lancer l'application uniquement dans cette zone, sans basculement vers une autre zone si aucune ressource n'est disponible 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 « Ne considérer aucune des zones utilisateur lors du lancement de cette application. » Par exemple, utilisez l'emplacement de l'utilisateur comme préférence de zone si vous voulez que les utilisateurs exécutent une application spécifique sur un VDA proche de leur machine, 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 non préférée.
3. Démarrer une nouvelle session dans la zone préférée.
4. Se reconnecter à une session connectée existante dans une zone non préférée.
5. Démarrer une nouvelle session dans une zone non 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, application Citrix Workspace sur la machine de point de terminaison doit être détecté par le boîtier Citrix Gateway par le biais duquel la machine est connectée. Citrix doit être configuré pour associer des plages d'adresses IP à des zones particulières. L'identité de zone détectée doit être transmise via StoreFront au service Citrix Virtual Apps and Desktops.

Bien que rédigé pour l'utilisation sur site des zones, le post de blog [Zone Preference Internals](#) contient des détails techniques pertinents.

Autorisations pour gérer les zones

Un administrateur complet peut effectuer toutes les tâches de gestion de zone prises en charge. 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.

Si vous utilisez Citrix Provisioning : étant donné que la console Citrix Provisioning ne peut pas identifier les zones, Citrix vous recommande d'utiliser Studio pour créer les catalogues de machines que vous souhaitez placer dans des zones spécifiques. Utilisez l'assistant Studio pour créer le catalogue, et spécifiez la zone. Puis, utilisez la console Citrix Provisioning pour provisionner des machines dans ce catalogue

Création de zone

Lorsque vous créez un emplacement de ressources dans Citrix Cloud et que vous y ajoutez un Cloud Connector, le service Citrix Virtual Apps and Desktops crée et nomme automatiquement une zone. Vous pouvez éventuellement ajouter une description plus tard.

Une fois que vous avez créé plus d'un emplacement de ressources (et que des zones sont créées automatiquement), vous pouvez déplacer des ressources d'une zone à une autre.

Les zones et emplacements de ressources sont synchronisés périodiquement, généralement et environ toutes les cinq minutes. Par conséquent, si vous modifiez le nom d'un emplacement de ressources dans Citrix Cloud, cette modification est propagée à la zone associée dans les cinq minutes.

Ajouter ou modifier la description d'une zone

Bien que vous ne puissiez pas modifier le nom d'une zone, vous pouvez ajouter une description ou la modifier dans Studio.

1. Cliquez sur **Configuration > Zones** dans le volet de navigation.
2. Sélectionnez une zone dans le volet central, puis cliquez sur **Modifier la zone** dans le volet Actions.
3. Ajoutez une description ou modifiez la description de la zone.
4. Cliquez sur **OK** ou **Appliquer**.

Déplacer des ressources d'une zone à une autre

1. Cliquez sur **Configuration > Zones** dans le volet de navigation de 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 cliquez sur **Déplacer des éléments** dans le panneau Actions et spécifiez la zone vers laquelle les déplacer. (Bien que vous puissiez sélectionner des Cloud Connector, vous ne pouvez pas les déplacer vers une autre zone.)

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.

Suppression de zone

Vous ne pouvez pas supprimer une zone. Toutefois, vous pouvez supprimer un emplacement de ressources (après suppression de ses Cloud Connector). La suppression de l'emplacement de

ressources supprime automatiquement la zone.

- Si la zone ne contient pas d'éléments (tels que des catalogues, connexions, applications ou utilisateurs), elle est supprimée lors de la prochaine synchronisation entre les zones et les emplacements de ressources, qui se produit toutes les cinq minutes.
- Si la zone contient des éléments, elle est automatiquement supprimée après suppression de tous les éléments.

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. Cliquez sur **Configuration > Zones** dans le volet de navigation de Studio.
2. Sélectionnez une zone dans le volet central, puis cliquez sur **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. Cliquez sur **Configuration > Zones** dans le volet de navigation de Studio.
2. Sélectionnez une zone dans le volet central, puis 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. Cette action

supprime uniquement les utilisateurs de la zone. Ces utilisateurs restent dans les groupes de mise à disposition 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.

- Lors de la [création d'un groupe de mise à disposition](#) ou de l'[ajout d'applications à des groupes existants](#), cliquez sur **Propriétés** sur la page **Applications** de l'assistant.
- Pour modifier les propriétés d'une application lorsque l'application est ajoutée, cliquez sur **Applications** dans le volet de navigation de Studio. Sélectionnez une application, puis cliquez sur **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.
 - 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 n'est utilisée pour déterminer l'emplacement du lancement de cette application.

Autres actions impliquant la spécification de zones

Si vous disposez de plusieurs zones, vous pouvez spécifier une zone lorsque vous ajoutez une connexion hôte ou que vous créez un catalogue. Les zones sont répertoriées par ordre alphabétique dans les listes de sélection. Par défaut, le premier nom par ordre alphabétique est sélectionné.

Cache d'hôte local

March 6, 2019

La fonctionnalité de cache d'hôte local (LHC) permet de poursuivre les opérations de négociation de connexion dans un déploiement du service Citrix Virtual Apps and Desktops lorsqu'un Cloud Connector ne peut pas communiquer avec Citrix Cloud. Le cache d'hôte local est activé lorsque la connexion réseau est perdue pendant 20 secondes.

Grâce au cache d'hôte local, les utilisateurs qui sont connectés lorsqu'une panne se produit peuvent continuer à travailler sans interruption. Les délais des nouvelles connexions et des reconnexions sont réduits.

Important :

Chaque zone satellite (emplacement de ressources) doit avoir un StoreFront installé et configuré localement. Le cache de l'hôte local fonctionne uniquement dans les emplacements de ressources contenant un StoreFront local.

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 :

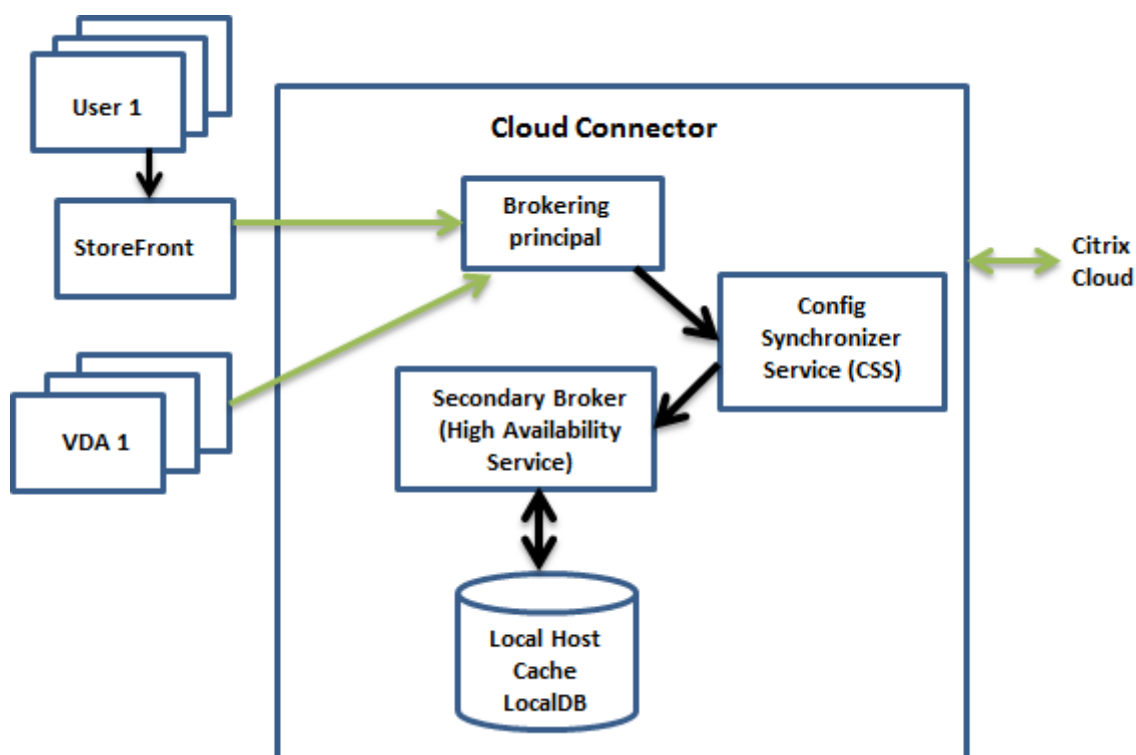
- Identités des utilisateurs et des groupes auxquels sont spécifiquement attribués des droits sur les ressources publiées à partir du site.
- Identités des utilisateurs qui utilisent actuellement ou ont récemment utilisé des ressources publiées à partir du site.
- Identités des machines VDA (y compris les machines Remote PC Access) configurées sur le site.
- Identités (noms et adresses IP) des machines de l'application Citrix Workspace 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 l'application Citrix Workspace.
- Identités des machines d'infrastructure (telles que les serveurs Citrix Gateway et StoreFront) impliquées dans le site.
- Dates/heures et types d'activités récentes des utilisateurs.

Fonctionnement

En mode de fonctionnement normal :

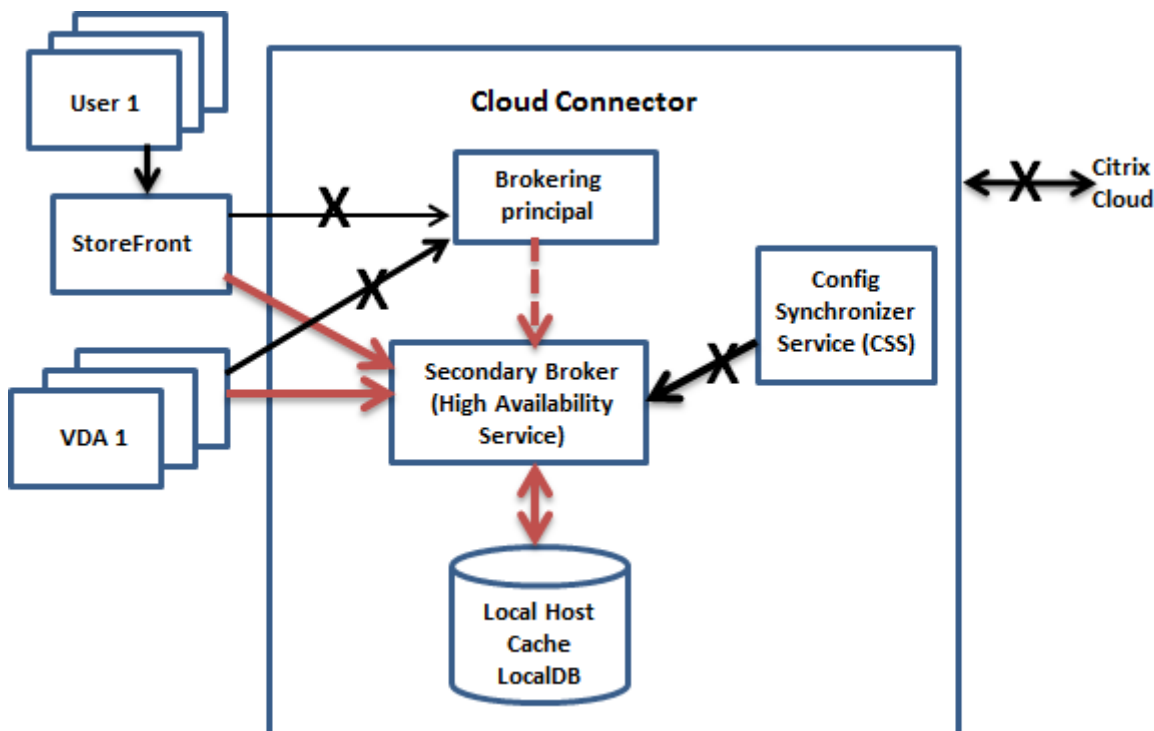


- Le broker principal (Citrix Remote Broker Provider Service) sur un Cloud Connector accepte des requêtes de connexion provenant de StoreFront, et communique avec Citrix Cloud pour connecter les utilisateurs aux VDA qui sont enregistrés auprès du Cloud Connector.
- Citrix Config Synchronizer Service (CSS) interroge le broker dans Citrix Cloud environ toutes les deux minutes pour savoir si des modifications ont été apportées à la configuration. Ces modifications peuvent avoir été initiées par un administrateur (telles que la modification d'une propriété de groupe de mise à disposition) ou être des actions du système (telles que les attributions de machine).
- Si la configuration a été modifiée depuis la dernière vérification, le service CSS synchronise les informations (copie) sur un broker secondaire (Citrix High Availability Service, HA broker dans l'illustration ci-dessus) sur le Cloud Connector. Toutes les données de configuration 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 Cloud Connector. Le service CSS s'assure que les informations de la base de données LocalDB du broker secondaire correspondent aux informations de la base de données du site dans Citrix Cloud. La base de données LocalDB est recréée chaque fois que la synchronisation se produit.

La base de données LocalDB est installée automatiquement lorsque vous installez un Cloud Connector. Cette base de données ne peut pas être partagée sur des Cloud Connector. Vous n'avez pas besoin de sauvegarder cette base de données ; elle est recréée chaque fois qu'une modification de la configuration est détectée.

- Si aucune modification n'a été apportée depuis la dernière vérification, les données de configuration ne sont pas copiées.

Durant une panne :



Lorsqu'une panne commence :

- Le broker secondaire démarre l'écoute et traite les demandes de connexion.
- Lorsque la panne commence, le broker secondaire ne dispose pas des données d'enregistrement de VDA, mais dès qu'un VDA communique avec lui, un processus d'enregistrement est déclenché. Au cours de ce processus, le broker secondaire obtient également des informations de session sur ce VDA.
- Bien que le broker secondaire gère les connexions, le broker principal continue à surveiller la connexion à Citrix Cloud. 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 d'enregistrement est déclenché. Le broker secondaire supprime les enregistrements de VDA restants de la panne précédente. Le service CSS reprend la synchronisation des informations lorsqu'il détecte des modifications de la configuration dans Citrix Cloud.

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 consigne les synchronisations et les pannes.

Aucun délai n'est imposé pour le fonctionnement en mode panne.

Vous pouvez également déclencher intentionnellement une panne. Voir [Forcer une panne pour savoir quand cela peut être nécessaire et comment procéder](#).

Emplacements de ressources (zones satellite) avec plusieurs Cloud Connector

Parmi ses différentes tâches, le service CSS fournit régulièrement au broker secondaire des informations sur tous les Cloud Connector dans l'emplacement de ressources. 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 s'enregistrent auprès du broker secondaire qui vient d'être sélectionné.

Durant une panne, si un Cloud Connector est redémarré :

- Si ce Cloud Connector n'est pas le broker principal sélectionné, le redémarrage n'a aucun impact.
- Si ce Cloud Connector est le broker principal sélectionné, un autre Cloud Connector est sélectionné, et par conséquent les VDA s'enregistrent. Une fois que le Cloud Connector redémarré est sous tension, il reprend automatiquement la négociation des connexions, et les VDA s'enregistrent à nouveau. Dans ce scénario, les performances peuvent être affectées lors des enregistrements.

Le journal d'événements contient des informations sur les sélections.

Considérations relatives à la conception et configuration requise

Aucun délai n'est imposé pour le fonctionnement en mode panne. Toutefois, si la défaillance est due à la perte locale de la connectivité à Citrix Cloud à partir de leur emplacement de ressources, les clients doivent restaurer la connectivité à partir de leur emplacement de ressources affecté le plus rapidement possible.

Fonctionnalités indisponibles durant une panne et autres différences

- Vous ne pouvez pas utiliser Studio ou exécuter des applets de commande PowerShell.
- Les données de surveillance ne sont pas envoyées à Citrix Cloud pendant une panne. Par conséquent, les fonctions de **surveillance** (Director) n'affichent pas l'activité lors d'une défaillance.
- 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 des bureaux uniquement à partir de VDA enregistrés dans la zone contenant le High Availability Service actuellement actif/sélectionné. Les lancements entre zones (depuis un High Availability Service dans une zone vers un VDA situé dans une autre zone) ne sont pas pris en charge durant une panne.

Le cache d'hôte local fonctionne uniquement avec un StoreFront déployé par le client. Il ne fonctionne pas avec Workspace.

Le cache d'hôte local est pris en charge pour les applications et les bureaux hébergés sur le serveur, et les bureaux statiques (attribués).

Par défaut, les VDA de bureau avec alimentation gérée dans des groupes de mise à disposition regroupés (créés par MCS ou Citrix Provisioning) dont la propriété `ShutdownDesktopsAfterUse` est activée sont placés en mode de maintenance lorsqu'une défaillance 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. Contactez l'assistance pour l'activer au niveau du site (cette commande ne peut pas être exécutée à l'aide du SDK Remote PowerShell).

```
Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true
```

Pour chaque groupe de mise à disposition affecté, exécutez l'applet de commande PowerShell suivante.

```
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.

Considérations sur la taille de la 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 Cloud Connector, il se peut donc que vous deviez augmenter la quantité totale de capacité RAM.

Considérations sur la configuration des sockets et des cœurs d'UC

La configuration d'UC d'un Cloud Connector, notamment le nombre de cœurs disponibles pour SQL Server Express LocalDB, affecte directement les performances du 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.

Considérations sur le 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 lorsqu'une modification de la configuration est détectée. 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.

Considérations sur les performances

Durant une panne, un seul broker gère toutes les connexions. Dans les emplacements de ressources qui équilibrent la charge entre plusieurs Cloud Connector (dans des conditions de fonctionnement normales), 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 sont plus nombreuses. Chaque broker dans l'emplacement de ressources doit être en mesure de gérer la charge supplémentaire imposée par la base de données LocalDB et tous les VDA affectés, car le broker sélectionné lors d'une panne peut changer.

Limites de VDI :

- Dans un déploiement avec un seul emplacement de ressources, jusqu'à 10 000 VDA peuvent être gérés efficacement au cours d'une panne.
- Dans un déploiement VDI avec plus d'un emplacement de ressources, jusqu'à 10 000 VDA dans chaque emplacement de ressources peuvent être gérés au cours d'une panne, avec un maximum de 40 000 VDA dans le déploiement. Par exemple, chacun des déploiements suivants peut être géré de manière efficace durant une panne :
 - Un déploiement avec quatre emplacements de ressources secondaires contenant chacun 10 000 VDA.
 - Un déploiement avec sept zones secondaires, une contenant 10 000 VDA et six contenant 5 000 VDA chacune.

Durant une panne, la gestion de la charge peut être affectée. Les calculateurs de charge (et plus particulièrement les règles du nombre de sessions) peuvent être dépassés.

Pendant que tous les VDA s'enregistrent 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 de l'enregistrement) est inévitable. Lorsqu'une panne démarre, les sessions connectées 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 des VDA doivent s'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.

Le temps nécessaire à la synchronisation entre les brokers augmente avec le nombre d'objets (VDA, applications, groupes) Par exemple, la synchronisation de 5 000 VDA peut prendre plus de dix minutes.

Exigences de StoreFront

Important :

Chaque zone satellite (emplacement de ressources) doit avoir un StoreFront installé et configuré localement. Le cache de l'hôte local fonctionne uniquement dans les emplacements de ressources contenant un StoreFront local.

Différences par rapport aux versions XenApp 6.x

Bien que cette implémentation du cache d'hôte local porte le même nom que la fonctionnalité de cache d'hôte local dans XenApp 6.x 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.

Gérer le cache d'hôte local

Le cache d'hôte local est toujours activé dans un déploiement du service Citrix Virtual Apps and Desktops. Vous n'avez rien d'autre à faire pour le configurer ou le gérer.

Comme indiqué précédemment, la base de données LocalDB est installée automatiquement lorsque vous installez un Cloud Connector dans un emplacement de ressources. N'essayez pas de la désactiver ou de la supprimer. (Citrix met à jour le Cloud Connector régulièrement. Si vous désactivez ou supprimez le logiciel LocalDB manuellement, la prochaine mise à jour du Cloud Connector le remplace.)

Vérifier que le cache d'hôte local fonctionne

Pour vérifier que le cache d'hôte local est configuré et fonctionne correctement :

- Vérifiez que l'emplacement de ressources contient un StoreFront local qui pointe vers les Cloud Connector dans cet emplacement de ressources.
- Assurez-vous que les importations de synchronisation se déroulent correctement. Vérifiez les journaux d'événements.

- Assurez-vous que SQL Server LocalDB a été créé sur chaque Cloud Connector. Cela confirme que le High Availability Service peut prendre le relais, si nécessaire.
 - Sur le serveur Cloud Connector, accédez à c:\Windows\ServiceProfiles\NetworkService\
 - Vérifiez que HaDatabaseName.mdf et HaDatabaseName_logldf sont créés
- Forcez une interruption sur tous les Cloud Connector dans l'emplacement de ressources. Après avoir vérifié que le cache d'hôte local fonctionne, n'oubliez pas de remettre tous les Cloud Connector en mode normal. Cela peut prendre environ 15 minutes pour éviter les pics d'enregistrement de VDA.

Consultez également [Scalability considerations for using Local Host Cache with Cloud Connectors](#).

Journaux d'événements

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 : Citrix Config Sync Service a reçu une configuration mise à jour. Cet événement se produit chaque fois que le High Availability Service reçoit une configuration mise à jour de Citrix Cloud. Il indique le début du processus de synchronisation. Un événement 504 ou 505 suit toujours cet événement.
- 504 : Citrix Config Sync Service a importé une configuration mise à jour. L'importation de la configuration s'est terminée avec succès.
- 505 : Échec d'une importation par Citrix Config Sync Service. L'importation de la configuration n'a pas réussi. Si une configuration précédente réussie est disponible, elle sera utilisée en cas de panne. Cependant, elle sera obsolète à partir de la configuration actuelle. Si aucune configuration précédente n'est disponible, le service ne peut pas participer à l'intermédiation de session pendant une panne. Dans ce cas, consultez la section Dépannage et contactez le support Citrix.
- 507 : Citrix Config Sync Service a abandonné une importation car le système est en mode d'arrêt et le cache d'hôte local est utilisé pour la négociation de connexions. Le service a reçu une nouvelle configuration, mais l'importation a été abandonnée en raison d'une panne. Il s'agit du comportement attendu.

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.

Forcer une interruption

Vous pouvez souhaiter délibérément forcer une interruption.

- 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 (et les fréquents enregistrements de VDA qui en résultent).
- Pour tester un plan de récupération d'urgence.
- Pour vous assurer que le cache d'hôte local fonctionne correctement.

Pour forcer une interruption, modifiez le registre de chaque serveur Cloud Connector. Dans HKLM\Software\Citrix\DesktopServer\LHC, définissez `OutageModeForced` sur 1. Ce réglage demande au broker d'entrer en mode d'interruption, quel que soit l'état de la connexion à Citrix Cloud. Si vous définissez la valeur sur 0, le broker sort du mode d'interruption.

Dépannage

Plusieurs outils de dépannage sont disponibles lorsque l'importation d'une 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, peuvent identifier le problème.

Rapport : si l'importation d'une synchronisation échoue, vous pouvez générer un rapport. Ce rapport s'arrête à l'objet qui a causé l'erreur. 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 la commande :

```
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\CitrixBrokerConfigSyncReport.html

Une fois le rapport généré, entrez la commande suivante pour désactiver la fonctionnalité de rapport :

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -Value 0
```


Considérations sur le dimensionnement et la scalabilité du cache d'hôte local

March 6, 2019

Généralités

La fonctionnalité Cache d'hôte local de Citrix Virtual Apps and Desktops Service permet d'établir des connexions dans un site afin de continuer en cas de panne. Une panne se produit si la liaison WAN entre le site et la console de gestion échoue dans un environnement Citrix Cloud. En décembre 2017, nous avons testé la configuration de machines Citrix Cloud Connector à l'aide de la fonctionnalité de cache d'hôte local du service Citrix Virtual Apps and Desktops. Les résultats des tests fournis dans ce document détaillent les maximums testés en décembre 2017. Les recommandations en matière de meilleures pratiques sont basées sur les maximums testés.

Ce document suppose que le lecteur peut configurer un environnement Citrix Cloud selon les normes recommandées, avec au moins trois connecteurs Cloud Connector.

Il est important de noter que le cache d'hôte local prend en charge uniquement un StoreFront local dans chaque emplacement ou zone de ressources. De plus, le cache d'hôte local prend en charge les applications et les bureaux hébergés sur le serveur, et les bureaux attribués. Le cache d'hôte local ne prend pas en charge les bureaux regroupés.

Lorsque le mode de panne est actif, si le connecteur sélectionné négociant les sessions a une panne, le deuxième connecteur devient le service à haute disponibilité sélectionné. Après la sélection, le deuxième connecteur prend le relais pour négocier les sessions. La fonction de cache d'hôte local utilise un seul socket pour les processeurs multicœurs pour la configuration des VM de connecteur. Dans ce scénario, nous recommandons une configuration à 4 cœurs et à 1 socket.

Synthèse

Tous les résultats de ce récapitulatif sont basés sur les conclusions des environnements de test que nous avons configurés comme indiqué dans les sections suivantes. Des configurations de système différentes peuvent donner des résultats différents.

Principales recommandations basées sur les résultats des tests

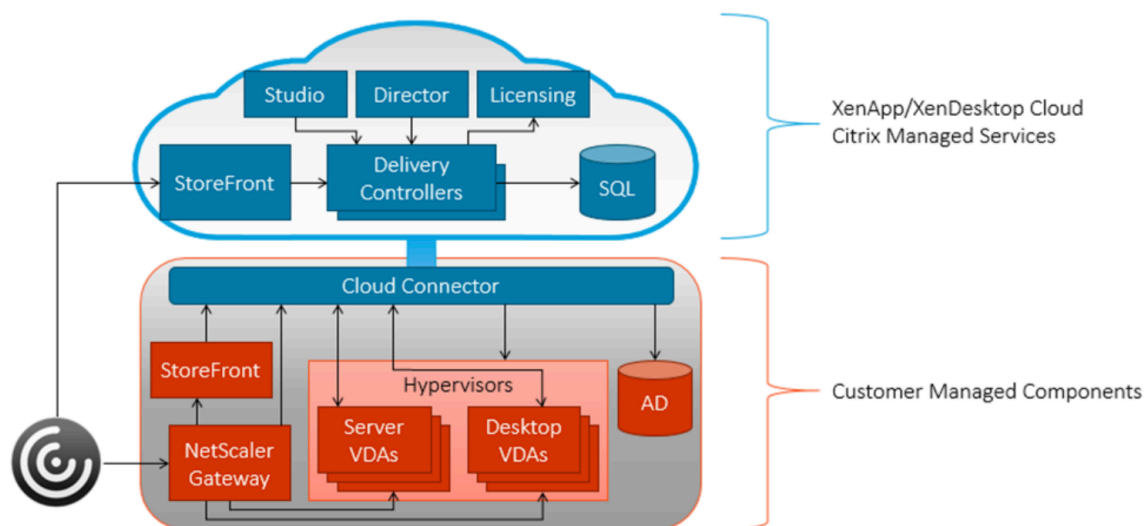
- Pour les sites à haute disponibilité n'hébergeant pas plus de 5 000 postes de travail ou 500 VDA de serveur, nous vous recommandons de configurer 3 VM dédiées au Cloud Connector. Chaque VM Cloud Connector nécessite 4 vCPU avec 4 Go de RAM. Cette configuration est une configuration à haute disponibilité N+1. Les Cloud Connector sont déployés dans des groupes à haute

disponibilité. La charge des Cloud Connector n'est pas répartie. Étant donné que chaque processeur peut traiter un nombre limité de connexions, le processeur est le facteur limitatif le plus important lié au nombre de postes de travail ou de VDA de serveur pris en charge.

- Bien que ce document se concentre sur des environnements de test comportant deux Cloud Connector, un ensemble N+1 de trois Cloud Connector est recommandé.
- Nous avons effectué des tests de lancement de session pour comparer le mode de panne actif/inactif du cache d'hôte local après la synchronisation et l'importation d'une nouvelle configuration. Les tests de lancement ont couvert des scénarios portant sur le lancement de 5 000, 20 000 et 1 000 sessions avec un certain nombre de postes de travail disponibles.
 - 5 000 sessions lancées avec 5 000 VDA de poste de travail
 - * Les tests ont utilisé 2 VM Cloud Connector, chacune disposant de 4 vCPU et de 4 Go de RAM. Selon la recommandation d'une configuration N+1, les environnements de production doivent inclure 3 VM Cloud Connector répondant à ces spécifications.
 - * Le pic du service de cache d'hôte local a consommé 91 % des ressources du processeur, avec une moyenne de 563 Mo de mémoire disponible.
 - * Il a fallu environ 10 minutes à partir du moment où le High Availability Service a détecté une panne pour que tous les VDA se réenregistrent auprès du High Availability Service, qui est désormais le broker. Nous avons mesuré à partir du moment où le High Availability Service est entré en mode de panne jusqu'à ce qu'il soit à nouveau prêt à établir des sessions.
 - 20 000 sessions lancées avec 500 VDA serveur
 - * Les tests ont utilisé 2 VM Cloud Connector, chacune disposant de 4 vCPU et de 4 Go de RAM. Selon la recommandation d'une configuration N+1, les environnements de production doivent inclure 3 VM Cloud Connector répondant à ces spécifications.
 - * Le pic du service de cache d'hôte local a consommé 90 % des ressources du processeur, avec une moyenne de 471 Mo de mémoire disponible.
 - * Il a fallu environ 8 minutes à partir du moment où le High Availability Service a détecté une panne pour que tous les VDA se réenregistrent auprès du High Availability Service. Nous avons mesuré à partir du moment où le High Availability Service est entré en mode de panne jusqu'à ce qu'il soit à nouveau prêt à établir des sessions.
 - 1 000 sessions lancées avec 1 000 VDA de poste de travail
 - * Les tests ont utilisé 2 VM Cloud Connector, chacune disposant de 2 vCPU et de 4 Go de RAM. Selon la recommandation d'une configuration N+1, les environnements de production doivent inclure 3 VM Cloud Connector répondant à ces spécifications.
 - * Le pic du service de cache d'hôte local a consommé 95 % des ressources du processeur, avec une moyenne de 589 Mo de mémoire disponible.
 - * Il a fallu environ 7 minutes à partir du moment où le High Availability Service a détecté une panne pour que tous les VDA se réenregistrent auprès du High Availability Service, qui est désormais le broker. Nous avons mesuré à partir du moment où le

High Availability Service est entré en mode de panne jusqu'à ce qu'il soit à nouveau prêt à établir des sessions.

Environment Overview



Citrix Cloud gère les services Cloud Connector et le client gère les machines.

Méthodologie des tests

Nous avons effectué des tests en ajoutant de la charge et en mesurant les performances des composants de l'environnement :

- UC
- memory
- Charge de la base de données
- Citrix Remote Broker Provider Service
- Citrix High Availability Service

Nous avons collecté des données de performances, de durée de connexion ou les deux. Dans certains cas, des outils de simulation propriétaires Citrix ont été utilisés pour simuler des VDA et des sessions. Ces outils de simulation sont conçus pour utiliser les composants Citrix de la même manière que des sessions et des VDA traditionnels, sans avoir à héberger de sessions et VDA réels.

Le cache d'hôte local prend en charge un High Availability Service par zone et non par site. Par exemple, si vous disposez de cinq zones, un connecteur est choisi comme broker dans chaque zone. Le Citrix Config Synchronizer Service est chargé de l'importation de la base de données du site gérée par Citrix. Chaque synchronisation de la configuration crée une base de données. Des configurations initiales sont donc nécessaires, telles que la compilation des procédures stockées lors de la première utilisation de la base de données. Nous avons exécuté tous les tests après synchronisation de la configuration.

Tests de lancement de session

Sur des serveurs StoreFront gérés par le client, nous avons démarré 5 000 et 20 000 tests de session. Les outils de monitoring collectent les durées de connexion, d'énumération des ressources et de récupération des fichiers ICA de StoreFront.

Citrix utilise des outils de simulation pour faciliter le test d'un grand nombre d'utilisateurs. Les outils de simulation, qui sont la propriété de Citrix, nous permettent d'effectuer des tests avec moins de matériel que nécessaire pour exécuter des tests utilisant des sessions réelles à ces niveaux (5 000 et 20 000 sessions). Ces sessions simulées suivent le même processus, à savoir connexion à StoreFront, énumération des ressources et récupération des fichiers ICA, mais elles ne démarrent pas de bureaux actifs. Au lieu de cela, l'outil de simulation indique à la pile ICA que la session a démarrée et que toutes les communications entre l'agent Broker et le Broker Service sont cohérentes avec celles d'une session réelle. Les mesures de performance sont collectées à partir des Citrix Cloud Connector. Pour déterminer la réponse de l'environnement aux lancements de session, 25 sessions simultanées ont été lancées pendant toute la durée du test. Les mesures montrent donc les résultats d'un système soumis à une charge tout au long du test.

Résultats des tests

Lancement de session

Les tableaux suivants comparent les tests de lancement de session entre le mode de panne actif et inactif du cache d'hôte local après la synchronisation et l'importation d'une nouvelle configuration. Chaque tableau montre les résultats du nombre de sessions lancées dans le test.

5 000 sessions VDA de poste de travail

	Mode de panne du cache d'hôte local inactif (opérations normales)/Délai moyen	Mode de panne du cache d'hôte local actif/Délai moyen
Authentification	193 ms	95 ms
Énumération	697 ms	75 ms
Temps total d'ouverture de session	890 ms	170 ms
Récupération du fichier ICA	4 191 ms	156 ms

20 000 sessions VDA de serveur

	Mode de panne du cache d'hôte local inactif (opérations normales)/Délai moyen	Mode de panne du cache d'hôte local actif/Délai moyen
Authentification	135 ms	112 ms
Énumération	317 ms	91 ms
Temps total d'ouverture de session	452 ms	203 ms
Récupération du fichier ICA	762 ms	174 ms

- Test portant sur le lancement de 5 000 sessions VDA de poste de travail
 - Il y avait une latence d'environ 30 ms entre les Citrix Cloud Connector et Citrix Delivery Controller lorsque le mode de panne du cache d'hôte local était inactif.
 - Il existe une différence de 720 ms dans le processus de connexion lorsque le mode de panne du cache d'hôte local est actif par rapport au mode inactif, alors que StoreFront est en condition de charge.
 - La plus grande différence de temps réside dans la récupération du fichier ICA, qui est de 4 secondes. Cela est dû en grande partie au fait que le connecteur effectue le brokering, alors que normalement le trafic StoreFront traverse les connecteurs jusqu'au Citrix Delivery Controller dans Azure et inversement.
- Test de lancement de 20 000 sessions VDA de serveur
 - Il existe une différence de 249 ms dans le processus de connexion lorsque le mode de panne du cache d'hôte local est actif par rapport au mode inactif, alors que StoreFront est en condition de charge.
 - La différence dans la récupération du fichier ICA est d'environ 1 seconde.
- Par rapport au lancement de 5 000 sessions VDA de poste de travail, le test de lancement de 20 000 sessions ne contient que 500 VDA de serveur, ce qui entraîne moins d'appels du Citrix Delivery Controller aux VDA, et réduit les temps de réponse.

Comparaison de l'utilisation moyenne du processeur

Test de lancement de session		% d'UC moyenne	% de pic d'UC
5 000 sessions VDA de poste de travail	Connector 1	8.3	38.2
	Connector 2	8.4	33.3

Test de lancement de session		% d'UC moyenne	% de pic d'UC
5 000 sessions VDA de poste de travail - Mode de panne du cache d'hôte local actif	Connector 1 (High Availability Service sélectionné)	42	91
	Connector 2	0.8	5
20 000 sessions VDA de serveur	Connector 1	.	62
	Connector 2	.	55
20 000 sessions VDA de server - Mode de panne du cache d'hôte local actif	Connector 1 (High Availability Service sélectionné)	57	90
	Connector 2	0.8	6.6

- Le tableau compare l'utilisation processeur de Citrix Cloud Connector avec le mode de panne du cache d'hôte local actif et inactif durant les tests portant sur le lancement de 5 000 sessions VDA de poste de travail et 20 000 sessions VDA de serveur.
- Tous les Cloud Connector sont équipés de 4 vCPU et de 4 Go de RAM
- Les machines High Availability Service sélectionnées ont culminé à respectivement 91 % et 90 % d'utilisation globale du processeur. Il convient de noter que, même si le High Availability Service non sélectionné n'est pas très utilisé, il peut devenir actif en cas de panne du High Availability Service sélectionné. Il est donc essentiel que les connecteurs aient des spécifications de connecteur identiques.

Utilisation de la mémoire disponible

Test de lancement de session		Mémoire moyenne disponible (plage de travail en Mo)	Mémoire maximale disponible (plage de travail en Mo)
5 000 sessions VDA de poste de travail	Connector 1	636	657
	Connector 2	786	801

Test de lancement de session		Mémoire moyenne disponible (plage de travail en Mo)	Mémoire maximale disponible (plage de travail en Mo)
5 000 sessions VDA de poste de travail - Mode de panne du cache d'hôte local actif	Connector 1 (High Availability Service sélectionné)	563	618
	Connector 2	912	918
20 000 sessions VDA de serveur	Connector 1	1 030	1 195
	Connector 2	1 178	1 329
20 000 sessions VDA de serveur - Mode de panne du cache d'hôte local actif	Connector 1 (High Availability Service sélectionné)	471	687
	Connector 2	1 210	1 227

- Le tableau compare l'utilisation de mémoire disponible avec le mode de panne du cache d'hôte local actif et inactif durant les tests portant sur le lancement de 5 000 sessions VDA de poste de travail et 20 000 sessions VDA de serveur.
- Le nombre de sessions diminue la quantité de mémoire disponible.
- L'utilisation de la mémoire augmente de 54,35 % (559 Mo) avec 20 000 sessions VDA de serveur lorsque le mode de panne du cache d'hôte local est actif, principalement en raison de la consommation de mémoire du serveur SQL.

Utilisation du processeur Cloud Connector par composant

Test de lancement de session	Composant	% d'UC moyenne	% de pic d'UC
5 000 sessions VDA de poste de travail	Connector 1 LSASS	2.4	10.7
	Connector 1 XaXdCloudProxy	3.5	18.5
	Connector 2 LSASS	2.5	12.9

Test de lancement de session	Composant	% d'UC moyenne	% de pic d'UC
	Connector 2 XaXdCloudProxy	3.5	21.2
5 000 sessions VDA de poste de travail - Mode de panne du cache d'hôte local actif	Connector 1 (High Availability Service sélectionné) LSASS	12.9	29.5
	Connector 1 (High Availability Service sélectionné) High-AvailabilityService	14.7	49.7
20 000 sessions VDA de serveur	Connector 1 LSASS	7	12.2
	Connector 1 XaXdCloudProxy	8.7	15.5
	Connector 2 LSASS	7	12.5
	Connector 2 XaXdCloudProxy	9	15.7
20 000 sessions - Mode de panne du cache d'hôte local actif	Connector 1 (High Availability Service sélectionné) LSASS	4.3	17.2
	Connector 1 (High Availability Service sélectionné) High-AvailabilityService	4.5	18.2

- Le tableau ci-dessus présente les processus qui consomment le plus de ressources processeur lorsque le mode de panne du cache d'hôte local est actif, par rapport au mode de panne du cache d'hôte local inactif durant les tests portant sur le lancement de 5 000 sessions VDA de poste de travail et 20 000 sessions VDA de serveur.
- Le Citrix Remote Broker Provider Service (XaXdCloudProxy) est le principal consommateur de processeur lorsque le mode de panne du cache d'hôte local est inactif.
- Le service LSASS (service de sous-système de l'autorité de sécurité locale) utilise le processeur

lors des ouvertures de session. Toutes les authentifications provenant de services gérés par Citrix doivent traverser les Citrix Cloud Connector pour communiquer avec l'Active Directory géré par le client.

- Le Citrix High Availability Service est utilisé pour négocier les sessions, ce qui entraîne une utilisation accrue du processeur lorsque le mode de panne du cache d'hôte local est actif. En outre, l'utilisation du processeur a atteint 49,7 % lors du lancement de 5 000 sessions VDA de poste de travail, contre 18,25 % seulement lors du lancement de 20 000 sessions VDA de serveur (500 VDA). La différence est due au nombre de VDA.
- Le Connector 2 ne présentait aucun résultat significatif, car il ne s'agissait pas du High Availability Service sélectionné.

Durée de réenregistrement des VDA lors du passage au cache d'hôte local

Lors d'une panne d'un Delivery Controller, les 5 000 VDA de poste de travail doivent se réenregistrer auprès du broker de cache d'hôte local sélectionné. Cette durée de réenregistrement était d'environ 10 minutes. La durée de réenregistrement de 500 VDA de serveur était d'environ 8 minutes.

Nombre de VDA	Durée de réenregistrement
5 000 VDA de poste de travail	~10 minutes
500 VDA de serveur	~8 minutes

Durée des pannes

Panne	Nombre de VDA	Heure
Entrer en mode panne		10 minutes
Durée de ré-enregistrement au High Availability Service sélectionné	500	~8 minutes
	5000	~10 minutes
Quitter le mode panne		10 minutes
Durée de ré-enregistrement à Citrix Delivery Controller	500	~5.5 minutes
	5000	~1.5 minutes

- Il faut un total de 20 minutes pour entrer (10 minutes) et quitter le mode panne (10 minutes).

Ceci est dû au nombre de contrôles d'intégrité de Citrix Delivery Controller requis. Le temps requis pour réenregistrer les VDA s'ajoute à la durée totale de la panne.

- Si le réseau connaît des interruptions répétées, forcer une panne jusqu'à la résolution des problèmes réseau empêche le basculement en continu entre les modes de fonctionnement normal et de panne.

Métriques de base de données et du High Availability Service avec cache d'hôte local

	Transactions moyennes/s de base de données sur High Availability Service	Pics de transactions/s de base de données sur High Availability Service
Test de lancement de session		
5 000 sessions VDA de poste de travail	436	1 344
20 000 sessions VDA de serveur	590	2 061

Le tableau précédent indique le nombre de transactions de base de données par seconde sur le High Availability Service sélectionné.

Comparaison de l'utilisation du processeur StoreFront

Test de lancement de session	% d'UC moyenne	% de pic d'UC
5 000 sessions VDA de poste de travail	4.5	32.4
5 000 sessions VDA de serveur - Mode de panne du cache d'hôte local	13.8	32.6
20 000 sessions VDA de serveur	11.4	22.1
20 000 sessions VDA de serveur - Mode de panne du cache d'hôte local	18.6	33.2

- Le tableau précédent compare l'utilisation du processeur StoreFront lorsque le mode de panne du cache d'hôte local est actif, par rapport au mode inactif durant les tests portant sur le lancement de 5 000 sessions VDA de poste de travail et 20 000 sessions VDA de serveur.

- La machine StoreFront présente les spécifications suivantes : Windows 2012 R2, 8 vCPU (2 sockets, 4 cœurs chacun), 8 Go de RAM
- Lorsque le mode de panne du cache d'hôte local est actif, l'utilisation moyenne du processeur augmente d'environ 9 % dans les tests portant sur le lancement de 5 000 sessions VDA de poste de travail et d'environ 7 % sur le lancement de 20 000 sessions VDA de serveur. L'augmentation est principalement due au fait que le serveur IIS traite plus de demandes lorsque le mode de panne du cache de l'hôte local est actif. L'utilisation du processeur est plus élevée car StoreFront traite les lancements de session plus rapidement que lorsque le mode de panne est inactif.

Comparaison de l'utilisation de la mémoire disponible dans StoreFront

Test de lancement de session	Mémoire moyenne disponible (plage de travail en Mo)	Mémoire maximale disponible (plage de travail en Mo)
5 000 sessions VDA de poste de travail	5 731	6 821
5 000 sessions VDA de poste de travail - Mode de panne du cache d'hôte local	5 345	5 420
20 000 sessions VDA de serveur	4 671	4 924
20 000 sessions VDA de serveur - Mode de panne du cache d'hôte local	4 730	5 027

- Le tableau précédent compare l'utilisation de la mémoire disponible dans StoreFront lorsque le mode de panne du cache d'hôte local est actif, par rapport au mode inactif durant les tests portant sur le lancement de 5 000 sessions VDA de poste de travail et 20 000 sessions VDA de serveur.
- Lorsque le mode Cache d'hôte local est actif, l'utilisation de la mémoire augmente de 6,73 % au cours du test de lancement de 5 000 sessions VDA de poste de travail.

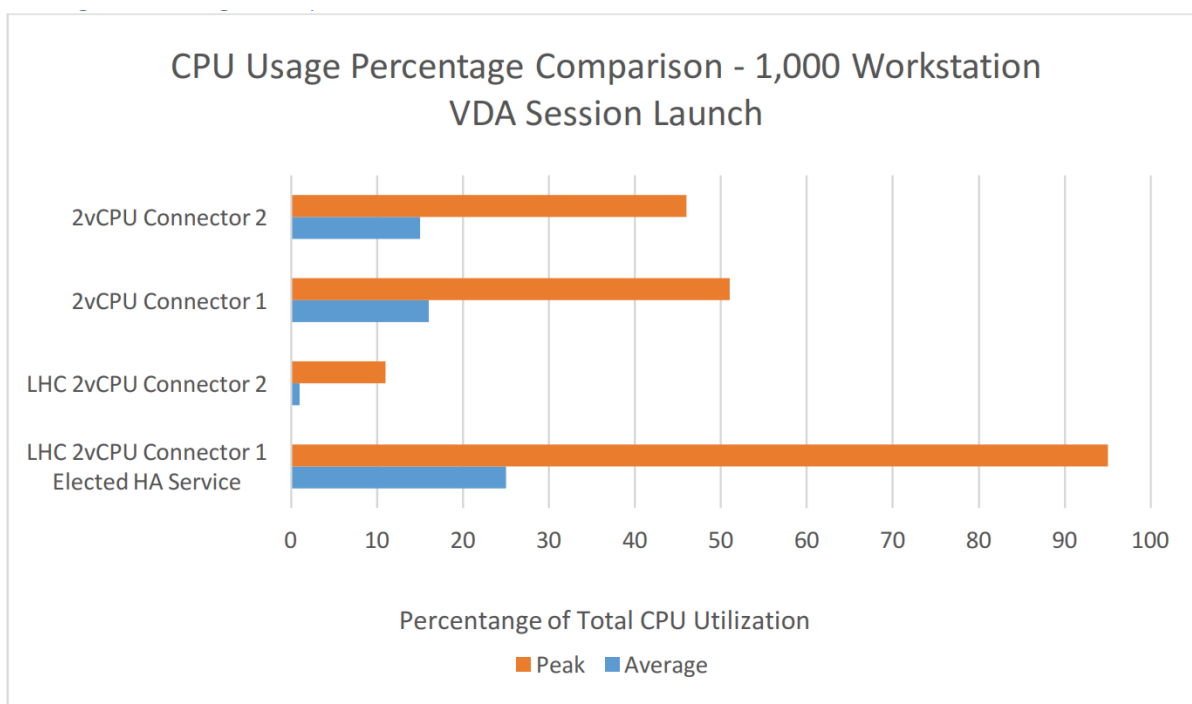
Le tableau ci-dessous compare le mode de panne actif/inactif après l'importation d'une nouvelle synchronisation de configuration, le lancement de 1 000 sessions sur 1 000 VDA de poste de travail avec cache d'hôte local et l'utilisation de Citrix Cloud Connector configurés avec 2 VM vCPU.

Comparaison du lancement de sessions

	Mode de panne du cache de l'hôte local inactif (opérations normales)	Mode de panne du cache d'hôte local actif
Authentification	359 ms	89 ms
Énumération	436 ms	180 ms
Temps total d'ouverture de session	795 ms	269 ms
Récupération du fichier ICA	804 ms	549 ms

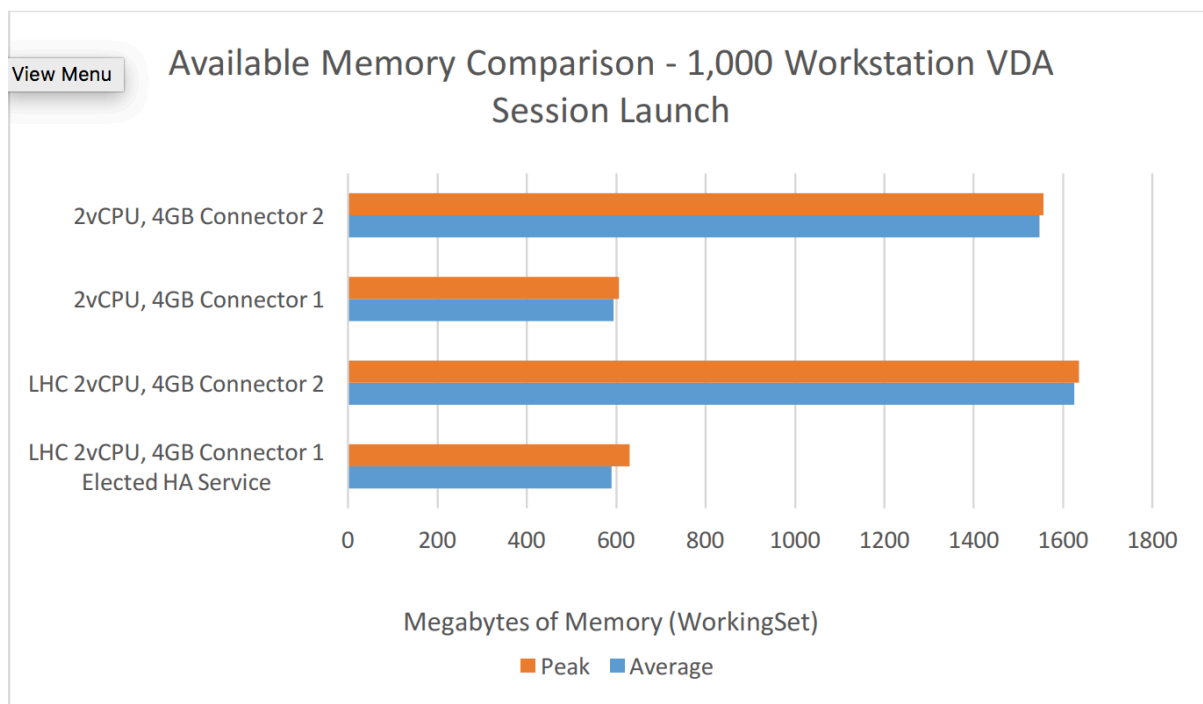
- Lorsque StoreFront est soumis à des charges, il existe une différence de 526 ms dans le processus de connexion lorsque le mode de panne du cache d'hôte local est actif par rapport au mode inactif.
- Il existe une différence de 255 ms dans la récupération du fichier ICA lorsque le mode de panne du cache de l'hôte local est actif par rapport au mode inactif. La différence augmente avec le nombre de sessions.

Comparaison de l'utilisation moyenne du processeur



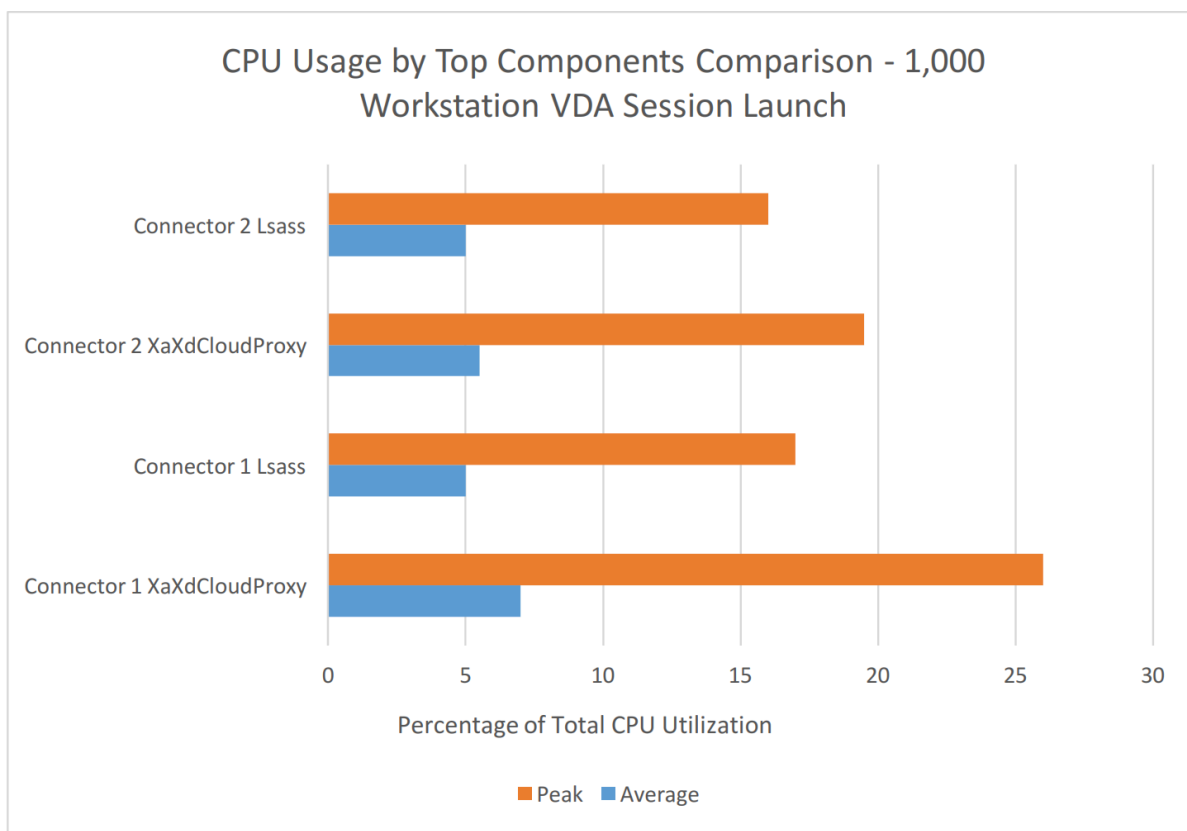
Le High Availability Service sélectionné a atteint un maximum de 95 % d'utilisation globale du processeur, ce qui indique que 1 000 VDA de poste de travail constituent une configuration optimale pour une VM connector à 2vCPU.

Comparaison de l'utilisation moyenne de mémoire

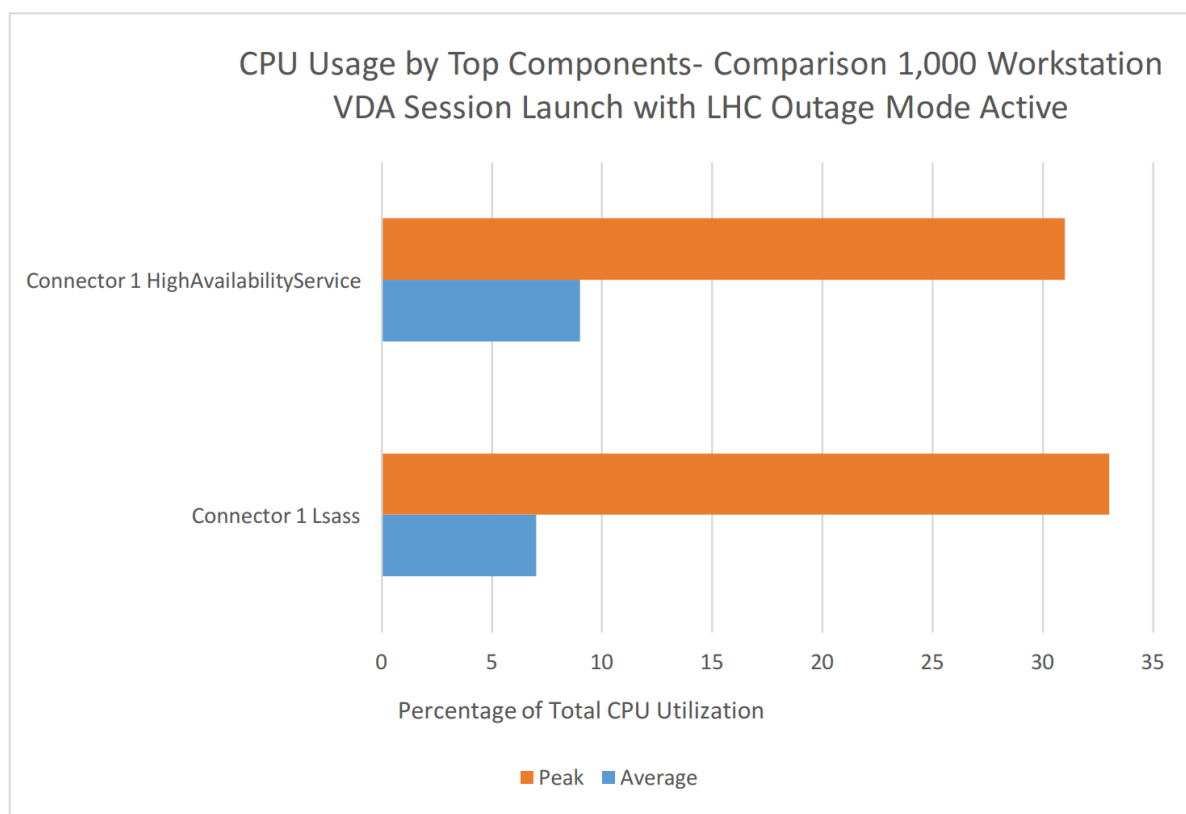


Le graphique précédent présente une comparaison de l'utilisation de la mémoire disponible de Citrix Cloud Connector lorsque le mode de panne du cache d'hôte local est actif par rapport au mode inactif lors du lancement de 1 000 sessions VDA de poste de travail. Il n'y a pas de différence significative dans l'utilisation de la mémoire en fonction du mode de panne du cache d'hôte local.

Comparaison d'utilisation du processeur par composant Cloud Connector



Le graphique précédent affiche les processus qui consomment le plus de ressources processeur lorsque le mode de panne du cache d'hôte local est inactif.

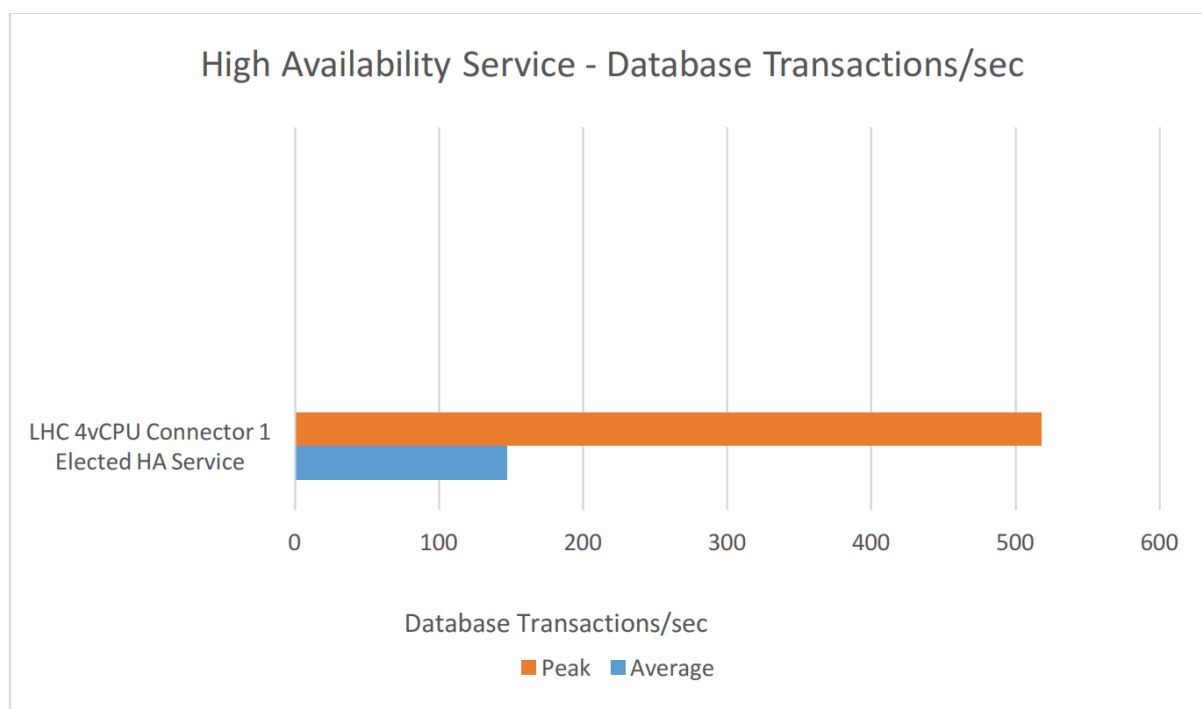


- Le graphique précédent affiche les processus qui consomment le plus de ressources processeur lorsque le mode de panne du cache d'hôte local est actif.
- Le Connector 2 ne présentait aucun résultat significatif.

Durée de réenregistrement des VDA lors du basculement vers le cache d'hôte local

Lors d'une panne d'un Delivery Controller, les 1 000 VDA de poste de travail doivent se réenregistrer auprès du broker de cache d'hôte local sélectionné. La durée de réenregistrement était d'environ 7 minutes.

Métriques de base de données et du High Availability Service avec cache d'hôte local



Le graphique précédent affiche le nombre de transactions de base de données par seconde sur le High Availability Service sélectionné.

Impact de l'augmentation du nombre de zones sur les durées d'importation de base de données

Une zone supplémentaire (avec une paire de ses propres connecteurs) a été ajoutée au site de test pour en comprendre l'impact. La première zone comprend 5 500 objets uniques (2 catalogues). La zone secondaire est un miroir de la première zone et possède ses propres objets uniques, totalisant 11 000 objets. Il est important de noter que le cache d'hôte local est recommandé uniquement pour les zones ne contenant pas plus de 10 000 objets. Avant l'ajout de la zone secondaire, la durée d'importation de la base de données sur les connecteurs était d'environ 4 minutes, 20 secondes. Après avoir ajouté la zone secondaire et l'avoir renseignée avec 11 000 objets, la durée d'importation a augmenté d'environ 30 secondes à environ 4 minutes et 50 secondes. L'ajout de davantage de catalogues a un impact marginal sur les durées d'importation. Les principaux facteurs contribuant à la dégradation des performances et à l'augmentation des durées d'importation sont basés sur le nombre de machines attribuées, d'utilisateurs et de PC distants. De plus, 5 500 objets ont été répartis entre 2 zones et la durée d'importation est restée la même

Nombre de zones	Nombre total d'objets	Durée d'importation
1	5 500	4 minutes 20 secondes
2.	11 000	4 minutes 50 secondes

Nombre de zones	Nombre total d'objets	Durée d'importation
2.	5 500	4 minutes 20 secondes

Guide de dimensionnement des connecteurs

Pour des performances optimales, les configurations suivantes sont recommandées pour Citrix Cloud Connector lorsque le mode Cache d'hôte local est activé.

Recommandation 1 : pour prendre en charge 1 000 VDA de poste de travail utilisant le mode cache d'hôte local avec Citrix Cloud Connector

- 2 VM Windows 2012 R2, chacune dotée de 2 vCPU (1 socket, 2 cœurs), 4 Go de RAM
- Ce dimensionnement recommandé est basé sur une utilisation maximale du processeur de 95 % et une moyenne d'utilisation de la mémoire disponible de 589 Mo de Citrix Cloud Connector lorsque le mode de cache d'hôte local est actif.

Recommandation 2 : pour prendre en charge 5 000 VDA de poste de travail OU 500 VDA de serveur utilisant le mode cache d'hôte local avec Citrix Cloud Connector

- 2 VM Windows 2012 R2, chacune dotée de 4 vCPU (1 socket, 4 cœurs), 4 Go de RAM
- Ce dimensionnement recommandé est basé sur
 - 5 000 sessions VDA de poste de travail lancées avec le mode cache d'hôte local actif
 - * 91 % d'utilisation maximale du processeur
 - * 563 Mo de mémoire disponible moyenne
 - 20 000 sessions VDA de serveur lancées avec le mode cache d'hôte local actif
 - * 90 % d'utilisation maximale du processeur
 - * 471 Mo de mémoire disponible moyenne

Pour plus d'informations, consultez le papier blanc du service Citrix Cloud Virtual Apps and Desktops répertoriant les considérations sur le dimensionnement et la scalabilité.

Environnement de test

L'environnement de test a utilisé des outils de test propriétaires développés en interne et des VM configurées selon les spécifications détaillées dans les sections suivantes.

Outils utilisés

Nous avons utilisé un outil de test interne pour collecter les données de performance et les mesures depuis les machines testées et pour initier les lancements de sessions. L'outil de test interne orchestre le lancement des sessions utilisateur dans l'environnement Citrix Virtual Apps and Desktops. L'outil

de test fournit également un emplacement central à partir duquel nous recueillons des données de temps de réponse et des mesures de performance. En substance, l'outil de test administre les tests et collecte les résultats.

Configuration du test – Citrix Virtual Apps and Desktops Service

Vous trouverez ci-dessous une liste des spécifications de machine et de système d'exploitation utilisées lors des tests de Citrix Virtual Apps and Desktops Service.

- **Cloud Connector :**
 - 2 VM Windows 2012 R2, chacune dotée de 4 vCPU (1 socket, 4 cœurs), 4 Go de RAM
 - 2 VM Windows 2012 R2, chacune dotée de 2 vCPU (1 socket, 2 cœurs), 4 Go de RAM
- **StoreFront (géré par le client) :** Windows 2012 R2, 8 vCPU (2 sockets, 4 cœurs chacun), 8 Go de RAM
- **Hyperviseur :** Citrix XenServer 7.0 + mises à jour, 5x HP Blade BL 460C Gen 9, 2x processeurs Intel E5-2620, 256 Go de RAM
- **Stockage d'hyperviseur :** partage NFS 2 To sur NetApp 3250
- **VDA :** Windows 2012 R2

Collecte des données

Nous recueillons les mesures suivantes pour chaque test : augmentation moyenne de l'utilisation globale du processeur, de la mémoire et des composants (processus du cloud).

- Durée de ré-enregistrement des VDA lors du basculement vers le High Availability Service avec cache d'hôte local sélectionné
- Métriques de base de données et du High Availability Service lorsque le mode de panne du cache d'hôte local est actif
- Comparaison des lancements de session, durée moyennes pour
 - Authentification
 - Énumération
 - Récupération du fichier ICA
- Impact de l'augmentation du nombre de zones sur les durées de synchronisation de la base de données
 - Temps requis pour la synchronisation après un changement de configuration

Administration déléguée

October 11, 2018

Généralités

L'administration déléguée de Citrix Cloud vous permet de configurer les autorisations d'accès requises par tous vos administrateurs conformément à leur rôle dans votre organisation.

Par défaut, les administrateurs ont un accès complet. Cela permet d'accéder à toutes les fonctions d'administration et de gestion client disponibles dans Citrix Cloud, ainsi qu'à tous les services souscrits. Pour personnaliser l'accès d'un administrateur :

- Configurez un accès personnalisé pour les autorisations de gestion générale d'un administrateur dans Citrix Cloud.
- Configurez un accès personnalisé pour les services souscrits. Dans le service Citrix Virtual Apps and Desktops, vous pouvez configurer un accès personnalisé lorsque vous invitez un nouvel administrateur. Vous pouvez modifier l'accès d'un administrateur ultérieurement.

Des détails sur l'affichage de la liste des administrateurs et la définition des autorisations d'accès sont disponibles dans [Ajouter des administrateurs à un compte Citrix Cloud](#).

Cet article explique comment configurer un accès personnalisé au service Citrix Virtual Apps and Desktops.

Administrateurs, rôles et étendues

L'administration déléguée utilise trois concepts pour l'accès personnalisé : les administrateurs, les rôles et les étendues.

- **Administrateurs** : un administrateur représente une personne identifiée par sa connexion Citrix Cloud, qui est généralement une adresse électronique. Chaque administrateur est associé à une ou plusieurs paires rôle/étendue.
- **Rôles** : un rôle représente une fonction de tâche à laquelle des permissions sont associées. Ces autorisations permettent certaines tâches uniques au service. Par exemple, le rôle Administrateur du groupe de mise à disposition est autorisé à créer un groupe de mise à disposition et à supprimer un bureau d'un groupe de mise à disposition, et dispose d'autres autorisations associées. Un administrateur peut avoir plusieurs rôles. Un administrateur peut être Administrateur du groupe de mise à disposition et Administrateur du catalogue de machines.

Le service offre plusieurs rôles intégrés avec accès personnalisé. (Vous ne pouvez pas créer d'autres rôles avec accès personnalisés.) Vous ne pouvez pas modifier les autorisations de ces rôles intégrés avec accès personnalisé, ni supprimer ces rôles. Vous pouvez modifier les rôles attribués à un administrateur.

Un rôle est toujours associé à une étendue.

- **Étendues** : une étendue représente une collection d'objets. Les étendues permettent de regrouper des objets de manière pertinente pour votre organisation. Les objets peuvent être dans plusieurs étendues.

Il existe une étendue intégrée appelée « Tous » qui contient tous les objets. Les administrateurs Citrix Cloud et Service d'assistance sont toujours associés à l'étendue Tous. Cette étendue ne peut pas être modifiée pour ces administrateurs.

Lorsque vous invitez (ajoutez) un administrateur pour ce service, un rôle est toujours associé à une étendue (par défaut, l'étendue Tous).

Les étendues sont créées et supprimées depuis la console Studio. Les paires rôle/étendue sont affectées dans la console Citrix Cloud.

Une étendue n'est pas affichée pour les administrateurs avec accès complet. Par définition, ces administrateurs ont accès à tous les objets de services d'abonnements et Citrix Cloud gérés par le client.

Étendues et rôles intégrés avec accès personnalisé

Le service a les rôles intégrés à accès personnalisé suivants.

- **Administrateur Cloud** : peut effectuer toutes les tâches pouvant être lancées à partir du service.

Peut voir les onglets **Gérer** et **Surveiller** dans la console. Ce rôle est toujours combiné à l'étendue Tous, vous ne pouvez pas modifier l'étendue.

Le nom de ce rôle peut porter à confusion. Un administrateur cloud avec accès personnalisé ne peut pas effectuer de tâches de niveau Citrix Cloud (les tâches Citrix Cloud nécessitent un accès complet).

- **Administrateur en lecture seule** : peut afficher tous les objets dans les étendues spécifiées (en plus des informations générales), mais ne peut rien modifier. Par exemple, un administrateur en lecture seule avec l'étendue = Londres peut voir tous les objets globaux 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).

Peut voir l'onglet **Gérer** dans la console, ne peut pas voir l'onglet **Surveiller**. Vous pouvez changer l'étendue.

- **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.

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.

Peut voir l'onglet **Surveiller** dans la console, ne peut pas voir l'onglet **Gérer**. Ce rôle est toujours combiné à l'étendue Tous, vous ne pouvez pas modifier l'étendue.

- **Administrateur du catalogue de machines** : peut créer et gérer des catalogues de machines et y provisionner les machines. Peut gérer les images de base et installer le logiciel, mais ne peut pas assigner les applications ou bureaux aux utilisateurs.

Peut voir l'onglet **Gérer** dans la console, ne peut pas voir l'onglet **Surveiller**. Vous pouvez changer l'étendue.

- **Administrateur du groupe de mise à disposition** : peut mettre à disposition des applications, des bureaux et des machines. Peut également gérer les sessions associées. Il peut gérer les configurations d'applications et de bureaux, telles que les stratégies et les paramètres de gestion de l'alimentation.

Peut voir l'onglet **Gérer** dans la console, ne peut pas voir l'onglet **Surveiller**. Vous pouvez changer l'étendue.

- **Administrateur hôte** : peut gérer les connexions hôtes et leurs paramètres de ressources associés. Impossible de mettre à disposition des machines, applications ou bureaux aux utilisateurs.

Peut voir l'onglet **Gérer** dans la console, ne peut pas voir l'onglet **Surveiller**. Vous pouvez changer l'étendue.

Le tableau suivant récapitule les onglets de la console visibles pour chaque rôle avec accès personnalisé du service et indique si le rôle peut être utilisé avec des étendues personnalisées.

Rôle administrateur à accès personnalisé	Peut voir l'onglet Gérer dans la console ?	Peut voir l'onglet Surveiller dans la console ?	Le rôle peut-il être utilisé avec des étendues personnalisées ?
Administrateur Cloud	Oui	Oui	Non
Administrateur en lecture seule	Oui	Non	Oui
Administrateur du service d'assistance	Non	Oui	Non
Administrateur du catalogue de machines	Oui	Non	Oui

Rôle administrateur à accès personnalisé	Peut voir l'onglet Gérer dans la console ?	Peut voir l'onglet Surveiller dans la console ?	Le rôle peut-il être utilisé avec des étendues personnalisées ?
Administrateur de groupe de mise à disposition	Oui	Non	Oui
Administrateur d'hôte	Oui	Non	Oui

Pour afficher les autorisations associées à un rôle :

1. Connectez-vous à [Citrix Cloud](#) si vous ne l'avez pas déjà fait. Sélectionnez **Mes services > Virtual Apps and Desktops** dans le menu en haut à gauche. Sélectionnez l'onglet **Gérer**.
2. Cliquez sur **Configuration > Administrateurs** dans le volet de navigation de Studio, puis cliquez sur l'onglet **Rôles**.
3. Sélectionnez un rôle dans le volet central supérieur. L'onglet **Définition du rôle** dans le volet inférieur répertorie les catégories et les autorisations. Sélectionnez une catégorie pour voir les autorisations spécifiques. L'onglet **Administrateurs** répertorie les administrateurs auxquels le rôle sélectionné au-dessus a été attribué.

Problème connu : une entrée Administrateur complet dans Studio n'affiche pas le jeu d'autorisations correct pour un administrateur de service à accès complet.

Nombre d'administrateurs dont vous avez besoin

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 à accès personnalisé. Dans ce cas, chaque administrateur dispose d'un accès complet, qui a toujours l'étendue Tous.
- 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 ont un accès complet 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 un certain département. Dans ce cas, créez de nouvelles étendues, ainsi que des administrateurs avec le rôle à accès personnalisé et les étendues appropriés.

Résumé de la gestion des administrateurs

La configuration d'administrateurs supplémentaires pour le service suit cette séquence :

1. Si vous souhaitez que le nouvel administrateur ait une étendue autre que Tous (et qu'une autre étendue est autorisée pour le rôle prévu mais qu'elle n'a pas encore été créée), créez des étendues dans Studio.
2. Depuis Citrix Cloud, invitez un administrateur. Si vous souhaitez que le nouvel administrateur dispose d'un accès autre que l'accès complet par défaut, spécifiez une paire rôle/étendue personnalisée.

Plus tard, si vous voulez changer l'accès d'un administrateur, voir Configurer un accès personnalisé.

Inviter un administrateur

L'ajout d'administrateurs suit les instructions détaillées dans [Ajouter des administrateurs à un compte Citrix Cloud](#). Un sous-ensemble de ces informations est repris ici.

1. Après vous être connecté à [Citrix Cloud](#), sélectionnez **Gestion des identités et des accès** à partir du menu supérieur gauche.
2. Sur la page **Gestion des identités et des accès**, cliquez sur **Administrateurs**. L'écran présente les administrateurs actuels du compte.
3. Cliquez sur **Ajouter admin. de**, puis sélectionnez votre méthode d'authentification. Entrez l'adresse e-mail de la personne. Vous pouvez également sélectionner une paire rôle/étendue.

Si vous ne sélectionnez pas de paire rôle/étendue personnalisée, le nouvel administrateur se voit attribuer un accès complet par défaut. Cet accès comprend l'accès à toutes les fonctions d'administrateur client de Citrix Cloud et de tous les services souscrits.

Si vous souhaitez que cet administrateur ait un accès plus limité, sélectionnez l'une des paires rôle/étendue à accès personnalisé. De cette manière, les nouveaux administrateurs ont les autorisations voulues lorsqu'ils se connectent pour la première fois à Citrix Cloud.

4. Cliquez sur **Inviter**. Citrix Cloud envoie une invitation à l'adresse e-mail que vous avez spécifiée et ajoute l'administrateur à la liste.

Lorsqu'un administrateur reçoit l'e-mail, il clique sur le lien **Joindre** pour accepter l'invitation.

Créer des étendues

Par défaut, tous les rôles ont l'étendue Tous pour leurs objets pertinents. Par exemple, un administrateur de groupe de mise à disposition peut gérer tous les groupes de mise à disposition. Pour certains rôles d'administrateur, vous pouvez créer une étendue permettant à ce rôle d'administrateur

d'accéder à un sous-ensemble d'objets pertinents. Par exemple, vous pouvez souhaiter donner à un administrateur de catalogue de machines un accès aux catalogues contenant un certain type de machines uniquement, plutôt qu'à tous les catalogues.

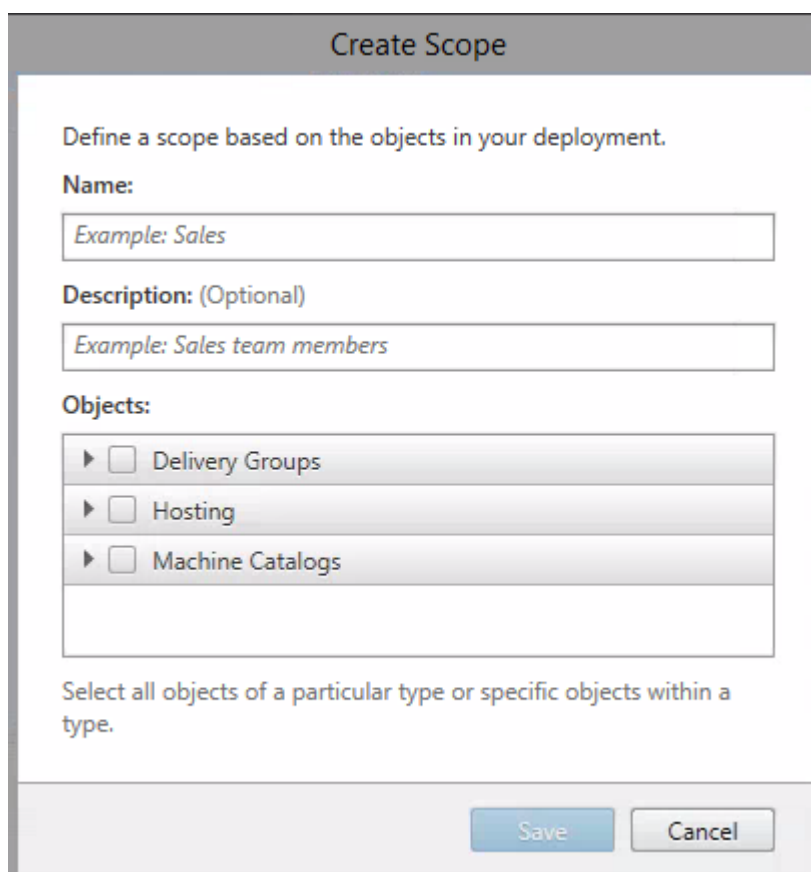
- Les administrateurs avec accès complet ou les administrateurs cloud avec accès personnalisé peuvent créer des étendues pour les rôles Administrateur en lecture seule, Administrateur du catalogue de machines, Administrateur du groupe de mise à disposition et Administrateur hôte.
- Des étendues ne peuvent pas être créées pour les administrateurs avec accès complet, ni pour les administrateurs cloud ou les administrateurs du centre d'assistance, car ces administrateurs ont toujours l'étendue Tous.

Règles de création et de gestion des étendues :

- Les noms d'étendue peuvent contenir jusqu'à 64 caractères Unicode. Les étendues 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 ou droite, barre verticale, crochet gauche ou droit, parenthèse gauche ou droite, guillemets et apostrophe.
- Les descriptions d'étendues peuvent contenir jusqu'à 256 caractères unicode.
- Lorsque vous copiez ou modifiez une étendue, n'oubliez pas que la suppression des objets dans l'étendue peut rendre ces objets inaccessibles à un 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 créer une étendue :

1. Connectez-vous à [Citrix Cloud](#) si vous ne l'avez pas déjà fait. Sélectionnez **Mes services > Virtual Apps and Desktops** dans le menu en haut à gauche. Sélectionnez l'onglet **Gérer**.
2. Cliquez sur **Configuration > Administrateurs** dans le volet de navigation de Studio, puis cliquez sur l'onglet **Étendues**.
3. Cliquez sur **Créer une étendue** dans le volet Actions. Entrez un nom et une description. Les objets sont répertoriés par type, tels que Groupe de mise à disposition et Catalogue de machines.
 - Pour inclure tous les objets d'un type particulier (par exemple, tous les groupes de mise à disposition), sélectionnez la case du type d'objet.
 - Pour inclure des objets individuels d'un type donné, développez le type, puis sélectionnez les cases des objets individuels (par exemple, des groupes de mise à disposition spécifiques).
4. Une fois terminé, cliquez sur **Enregistrer**.



Create Scope

Define a scope based on the objects in your deployment.

Name:

Example: Sales

Description: (Optional)

Example: Sales team members

Objects:

- Delivery Groups
- Hosting
- Machine Catalogs

Select all objects of a particular type or specific objects within a type.

Save Cancel

Une fois que vous avez créé une étendue dans Studio, elle apparaît dans la liste **Accès personnalisé** dans la console Citrix Cloud, associée au rôle approprié. Vous pouvez ensuite l'attribuer à un administrateur.

Par exemple, supposons que vous créez une étendue nommée CAO dans Studio, puis que vous sélectionnez les catalogues de machines contenant des machines adaptées aux applications de CAO. Lorsque vous revenez à la console Citrix Cloud, la liste des paires rôle/étendue à accès personnalisé au niveau du service contient désormais de nouvelles entrées (indiquées ci-dessous en gras) :

- Administrateur Cloud, Tous
- Administrateur du groupe de mise à disposition, Tous
- **Administrateur du groupe de mise à disposition, CAO**
- Administrateur du service d'assistance, Tous
- Administrateur hôte, Tous
- **Administrateur hôte, CAO**
- Administrateur du catalogue de machines, Tous
- **Administrateur du catalogue de machines, CAO**
- Lecture seule, Tous
- **Lecture seule, CAO**

L'administrateur Cloud et l'administrateur du centre d'assistance ont toujours l'étendue Tous, donc

l'étendue CAO ne s'applique pas à eux.

Gérer les étendues

Après avoir créé une étendue, vous pouvez la copier, la modifier ou la supprimer de Studio.

Cliquez sur **Configuration > Administrateurs** dans le volet de navigation de Studio, puis cliquez sur l'onglet **Étendues**.

- **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.
- **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.
- **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. Vous ne pouvez pas supprimer une étendue si elle est affectée à un rôle. Si vous tentez de le faire, un message d'erreur indique que vous ne disposez pas de l'autorisation. En fait, l'erreur se produit parce que la paire rôle/étendue qui utilise cette étendue est attribuée à un administrateur. Vous devez d'abord supprimer l'attribution de cette paire rôle/étendue pour tous les administrateurs qui l'utilisent. Ensuite, vous pouvez supprimer l'étendue dans Studio.

Configurer un accès personnalisé pour un administrateur

Par défaut, lorsque vous invitez des administrateurs, ils disposent d'un accès complet.

Rappel : l'accès complet permet à l'administrateur de gérer tous les services souscrits, ainsi que les opérations Citrix Cloud de l'administrateur client (telles que l'invitation d'administrateurs supplémentaires). Un déploiement Citrix Cloud nécessite au moins un administrateur avec un accès complet.

Pour configurer un accès personnalisé pour un administrateur :

1. Connectez-vous à [Citrix Cloud](#) si vous ne l'avez pas déjà fait. Sélectionnez **Gestion des identités et des accès > Administrateurs** dans le menu en haut à gauche.
2. Recherchez l'administrateur que vous souhaitez gérer, cliquez sur le menu d'ellipse et sélectionnez **Modifier l'accès**.
3. Sélectionnez **Accès personnalisé**. Pour configurer un accès personnalisé spécifique à un service, sous **Virtual Apps and Desktops**, cochez ou décochez les cases en regard d'une ou de plusieurs paires de rôles et d'étendues dans la liste d'accès personnalisé.

Si vous n'avez créé aucune étendue dans Studio ni affecté aucune à aucun rôle, tous les rôles de la liste Accès personnalisé ont l'étendue Tous. Par exemple, l'entrée rôle/étendue **Administrateur du groupe de mise à disposition, Tous** indique que le rôle a l'étendue Tous.

Si vous avez créé une étendue dans Studio, elle apparaît dans la liste d'accès personnalisé du service et peut être sélectionnée. Par exemple, si vous avez créé une étendue nommée Catalog1, la liste d'accès personnalisé comprend une entrée **Administrateur du catalogue de machines, Catalog1**, en plus de l'entrée par défaut **Administrateur du catalogue de machines, Tous**.

4. Si l'administrateur que vous modifiez dispose déjà d'un accès personnalisé et que vous souhaitez lui accorder un accès complet, sélectionnez **Accès complet**.
5. Lorsque vous avez terminé, cliquez sur **Enregistrer**.

La capture d'écran suivante montre les rôles d'administrateur intégrés avec accès complet et accès personnalisé.

⚠ Custom Access requires at least one role to be selected.

Full access
Full access allows administrators management control of Citrix Cloud and its services, as we

Custom access
ⓘ Switching to custom access will remove management access to certain services.
Custom access allows you to determine exactly which part of Citrix Cloud your administrato

[Select all](#)

General Management

Domains

Library

Notifications

Resource Location

Virtual Apps and Desktops

Cloud Administrator, All

Delivery Group Administrator, All

Help Desk Administrator, All - Access to 'Monitor' tab only

Host Administrator, All

Machine Catalog Administrator, All

Read Only Administrator, All

Différences par rapport à Citrix Virtual Apps and Desktops sur site

Si vous connaissez l'administration déléguée dans la version Citrix Virtual Apps and Desktops sur site, la version du service présente plusieurs différences.

Dans Citrix Cloud :

- Les administrateurs sont identifiés par leur connexion Citrix Cloud, plutôt que par leur compte Active Directory. Vous pouvez créer des paires rôle/étendue pour des individus Active Directory, mais pas pour des groupes.
- Les administrateurs sont créés, configurés et supprimés dans la console Citrix Cloud, plutôt que dans Studio.
- Les paires rôle/étendue sont attribuées aux administrateurs dans la console Citrix Cloud, plutôt que dans Studio.
- Les rôles personnalisés ne sont pas disponibles. (Ne confondez pas « accès personnalisé » avec la possibilité de créer des rôles personnalisés dans la version sur site.)
- Les rapports ne sont pas disponibles. Vous pouvez afficher des informations sur l'administrateur, le rôle et l'étendue dans Studio.
- L'accès personnalisé Administrateur Cloud est similaire à un administrateur complet dans la version locale. Les deux disposent d'autorisations complètes de gestion et de surveillance pour la version Citrix Virtual Apps and Desktops utilisée. Cependant, dans le service, il n'y a pas de rôle d'administrateur complet nommé. N'associez pas « accès complet » dans Citrix Cloud à « administrateur complet » dans Citrix Virtual Apps and Desktops sur site. L'accès complet dans Citrix Cloud s'étend aux domaines, à la bibliothèque, aux notifications et aux emplacements de ressources de la plate-forme, ainsi qu'à tous les services auxquels vous êtes abonné.

Différences par rapport aux versions de service antérieures

Avant la publication de la fonctionnalité d'accès personnalisé étendue dans le service (septembre 2018), il y avait deux rôles d'administrateur avec accès personnalisé : Administrateur complet et Administrateur du centre d'assistance. Lorsque l'administration déléguée est activée dans votre déploiement (ce qui correspond à un paramètre au niveau de la plate-forme), ces rôles sont automatiquement mappés.

- Un administrateur qui était auparavant configuré en tant que *Virtual Apps and Desktops* (ou *XenApp and XenDesktop*) : *Administrateur complet* avec accès personnalisé est maintenant un **Administrateur Cloud** avec accès personnalisé.
- Un administrateur qui était auparavant configuré en tant que *Virtual Apps and Desktops* (ou *XenApp and XenDesktop*) : *Administrateur du centre d'assistance* avec accès personnalisé est maintenant un **Administrateur du centre d'assistance** avec accès personnalisé.

Journalisation de la configuration

November 30, 2018

La journalisation de la configuration consigne les modifications apportées à la configuration du déploiement Citrix Virtual Apps and Desktops et aux activités administratives dans une base de données de journalisation de Citrix Cloud. 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.

Dans Studio, vous pouvez afficher le contenu du journal de configuration, filtré par plages de dates ou par recherche en texte intégral. Vous pouvez également générer un rapport CSV à l'aide de PowerShell. Vous ne pouvez ni modifier ni supprimer le contenu du journal.

Les journaux de configuration sont localisés lorsqu'ils sont créés. Par exemple, un journal créé en anglais est lu en anglais, quels que soient les paramètres régionaux du lecteur.

Autorisations requises (voir [Administration déléguée](#)) :

- Les administrateurs complets dans Citrix Cloud, ainsi que les administrateurs Cloud et les administrateurs en lecture seule du service Citrix Virtual Apps and Desktops peuvent afficher les journaux de configuration dans Studio.
- Les administrateurs complets et les administrateurs Cloud peuvent également télécharger un rapport CSV d'activités de journalisation à l'aide de PowerShell.

Qu'est-ce qui est journalisé

Les modifications de configuration et les activités administratives initiées depuis Studio (Gérer), Director (Surveiller) et des scripts PowerShell sont journalisées. Toutefois, vous ne pouvez pas voir les entrées de journal pour les opérations internes de la plateforme Citrix Cloud, telles que la configuration et la gestion de la base de données.

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 l'alimentation d'une machine virtuelle ou d'un bureau utilisateur
- Fonctions de gestion ou de surveillance envoyant un message à un utilisateur

Les opérations suivantes ne sont pas enregistrées. (Beaucoup ne sont pas disponibles pour les administrateurs clients.)

- 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 ou à partir de sources autres que Studio (Gérer), Director (Surveiller) ou PowerShell.

Afficher le contenu du journal de configuration

1. Connectez-vous à [Citrix Cloud](#). Sélectionnez **Virtual Apps and Desktops** dans le menu en haut à gauche.
2. Sélectionnez l'onglet **Gérer**.
3. Sélectionnez **Journalisation** dans le volet de navigation Studio.

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. Vous pouvez :

- Trier l'affichage par en-tête de colonne.
- Filtrer l'affichage en spécifiant un intervalle de jours ou en entrant du texte dans la zone Rechercher. Pour revenir à l'affichage standard après la recherche, désactivez le texte dans la zone Rechercher.

Caractéristiques d'affichage :

- Les opérations de haut niveau créées lors de la gestion et de la surveillance sont répertoriées dans le volet central supérieur de Studio. Une opération de haut niveau se traduit par un ou plusieurs appels de service et de SDK PowerShell, qui sont des opérations de bas niveau. Lorsque vous sélectionnez une opération de haut niveau dans le panneau central supérieur, le panneau inférieur affiche les opérations de bas niveau.
- Si vous créez une opération de bas niveau dans PowerShell sans spécifier une opération de haut niveau parente, la journalisation de la configuration crée une opération de haut niveau de substitution.
- 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 les journaux des cinq derniers jours sont demandés et qu'un journal avec une heure de début dans les cinq derniers jours n'a pas de date de fin, il est inclus.

- Rappel : vous ne pouvez pas voir les entrées de journal pour les opérations internes de la plateforme Citrix Cloud, telles que la configuration et la gestion de la base de données.

Générer des rapports

Pour générer un rapport contenant des données de journal de configuration, utilisez les applets de commande PowerShell pour le service ConfigLogging dans le SDK Remote PowerShell Citrix Virtual Apps and Desktops. Par exemple, vous pouvez récupérer une liste filtrée d'opérations de niveau supérieur ou inférieur. Pour plus de détails, voir [SDK et API](#) et [SDK Citrix Virtual Apps and Desktops](#).

Différences par rapport à Citrix Virtual Apps and Desktops sur site

Si vous avez déjà utilisé la journalisation de la configuration dans Virtual Apps and Desktops sur site, la version Citrix Cloud présente plusieurs différences.

Dans Citrix Cloud :

- La journalisation de la configuration est toujours activée. Vous ne pouvez pas la désactiver. La journalisation obligatoire n'est pas disponible.
- Vous ne pouvez pas modifier l'emplacement de la base de données de journalisation de la configuration, car celle-ci est gérée sur la plate-forme Citrix Cloud et est accessible par les administrateurs du client.
- Les affichages du journal de configuration n'incluent pas les opérations et les activités effectuées sur la plate-forme Citrix Cloud.
- Vous pouvez créer un rapport CSV des opérations consignées uniquement à l'aide des applets de commande PowerShell. Dans le produit sur site, les rapports CSV ou HTML peuvent être générés à partir de Studio ou de PowerShell.
- Vous ne pouvez pas supprimer le contenu du journal de configuration.

Analyse

March 6, 2019

Director

Les administrateurs et le personnel du support technique peuvent surveiller Citrix Virtual Apps and Desktops, qui propose un outil Web en temps réel que vous pouvez utiliser pour surveiller, dépanner et effectuer des tâches de support pour les abonnés.

- 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.

Connectez-vous à [Citrix Cloud](#). Dans le menu en haut à gauche, sélectionnez **Mes services > Virtual Apps and Desktops**. Cliquez sur **Surveiller**.

Voir [Director](#) pour de plus amples informations.

Journaux d'événements

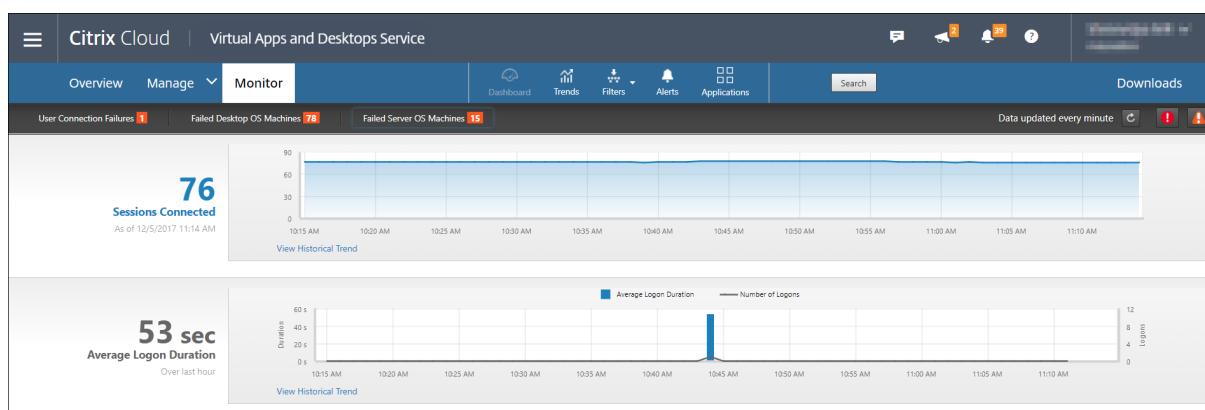
Les services dans Citrix Virtual Apps and Desktops consignent les événements qui se produisent. Les journaux d'événements peuvent être utilisés pour les opérations de surveillance et de dépannage.

Pour de plus amples informations, consultez [Journaux d'événements](#). Les articles sur chaque fonctionnalité peuvent également contenir des informations sur les événements.

Director

March 6, 2019

Director est une console de surveillance et de résolution des problèmes pour Citrix Virtual Apps and Desktops Service. Avec des permissions d'administrateur complet, lorsque vous ouvrez **Director**, le tableau de bord fournit un emplacement centralisé permettant de surveiller l'intégrité et l'utilisation historiques et en temps réel d'un site. La fonctionnalité Director est disponible sur l'onglet **Surveiller** de la console Citrix Virtual Apps and Desktops Service.



Pour plus d'informations sur l'utilisation de Director, veuillez consulter la section [Director](#).

Rôles d'administrateur délégué

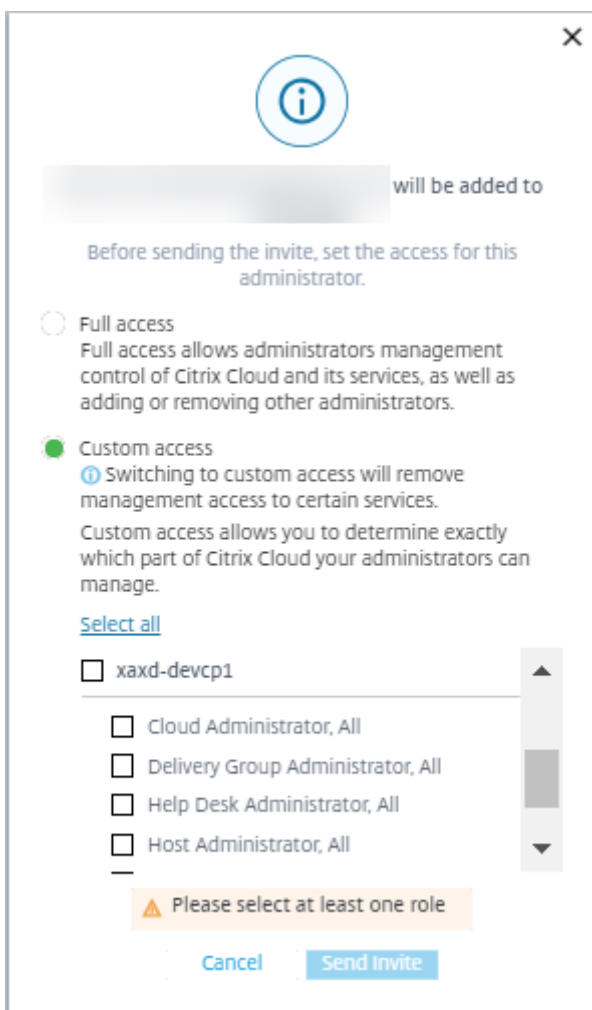
La surveillance prend désormais en charge les rôles d'administrateur délégué qui vous permettent d'attribuer des rôles intégrés aux administrateurs. Le rôle détermine les autorisations disponibles et donc la manière dont un administrateur utilise la surveillance. Vous pouvez attribuer une étendue complète ou une étendue personnalisée au rôle. L'étendue définit les objets pour lesquels le rôle est applicable.

Les rôles intégrés disponibles et leurs autorisations associées sont les suivants :

Rôle Administrateur	Autorisations dans la surveillance
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 voir tous les objets. 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.

Rôle Administrateur	Autorisations dans la surveillance
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	Peut accéder à la page Détails de machine (recherche machine).
Administrateur d'hôte	Aucun accès. Cet administrateur ne peut afficher aucune donnée de surveillance.

Pour attribuer un rôle intégré à un utilisateur, à partir du menu Citrix Cloud, accédez à **Gestion des identités et des accès** → **Administrateurs**. Lorsque vous ajoutez ou modifiez l'accès d'un administrateur à partir de cette section, vous pouvez sélectionner Accès personnalisé et l'un des rôles intégrés répertoriés.



Les rôles intégrés sont répertoriés avec une étendue personnalisée prédéfinie (Définissez une étendue personnalisée dans **Gérer** → **Citrix Studio** → **Configuration** → **Administrateurs** → **Étendues**).



-
- Cloud Administrator, All
 - Delivery Group Administrator, All
 - Delivery Group Administrator, rds1DGAndCatalog
 - Delivery Group Administrator, vdaDGOnly
 - Full Monitor Administrator, All - Access to 'Monitor' tab only
 - Full Monitor Administrator, rds1DGAndCatalog - Access to 'Monitor' tab only
 - Full Monitor Administrator, vdaDGOnly - Access to 'Monitor' tab only
 - Help Desk Administrator, All - Access to 'Monitor' tab only
 - Help Desk Administrator, rds1DGAndCatalog - Access to 'Monitor' tab only
 - Help Desk Administrator, vdaDGOnly - Access to 'Monitor' tab only
 - Host Administrator, All
 - Host Administrator, rds1DGAndCatalog
 - Host Administrator, vdaDGOnly
 - Machine Catalog Administrator, All

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'indice de calculateur de charge, qui indique la dis-

tribution des compteurs de performances et les info-bulles du nombre de sessions si vous survolez le lien avec la souris.

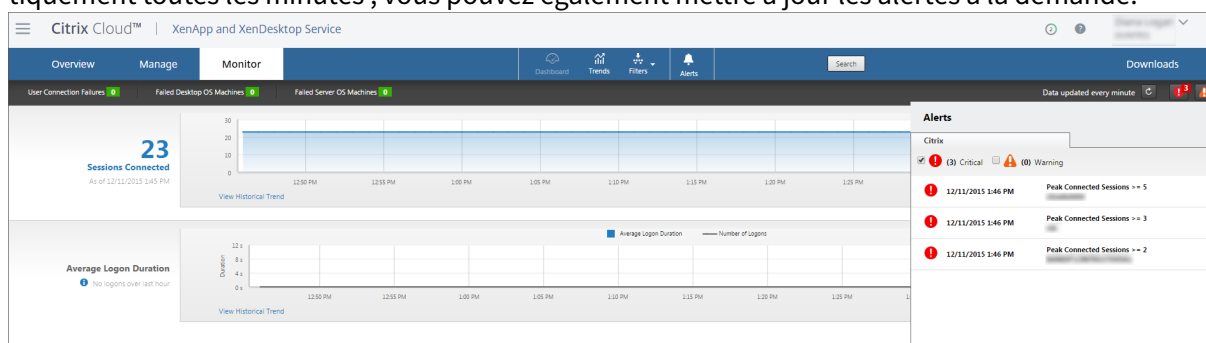
- **Sessions.** Vous pouvez également afficher le nombre de sessions depuis la vue Sessions. Utilisez les mesures de délai d'inactivité pour identifier les sessions qui restent inactives au-delà d'une période de temps donnée.
 - **Connexions.** Filtrez les connexions par différentes périodes de temps, 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 version 7.13 ou supérieure.
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.
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.
 6. Choisissez les colonnes requises dans le tableau filtré, puis cliquez sur **Exporter** pour exporter les données au format CSV. Jusqu'à 100 000 enregistrements peuvent être exportés.
 7. 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.
 8. 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](#).
 9. Dans la vue **Instances d'application**, trie 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.
 10. Dans la vue **Machines**, cliquez deux fois 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 et permet de contrôler l'alimentation.
 - Le panneau **Utilisation de machine** affiche des graphiques d'UC, de mémoire, de surveillance du disque et de surveillance du GPU. La surveillance des disques et du GPU requiert des VDA 7.14 ou de version ultérieure.
 - Cliquez sur **Afficher utilisation historique** pour afficher les tendances d'utilisation des

ressources pour la machine. Les graphiques de surveillance du disque, le nombre moyen d'E/S par seconde en temps réel et la latence de disque aident à résoudre les problèmes liés au disque sur le VDA sélectionné. Les graphiques de surveillance du GPU NVIDIA incluent le pourcentage d'utilisation du GPU NVIDIA, de la mémoire du GPU et de l'encodeur et du décodeur des VDA avec OS de serveur et de bureau. Pour les VDA qui accèdent à plusieurs GPU, la moyenne des mesures de GPU collectées à partir des GPU individuels est affichée. Les GPU sont surveillés sur les VDA exécutant Windows 64 bits, avec GPU NVIDIA Tesla M60 et un pilote d'affichage version 369.17 ou version ultérieure.

Pour obtenir davantage d'informations, veuillez consulter la section [Dépanner les machines](#).

Alertes et notifications

Les alertes sont affichées sur l'onglet Surveiller sur le tableau de bord et dans d'autres vues de haut niveau avec des symboles d'avertissement et d'alerte critique. 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** en bas de la barre latérale ou en sélectionnant **Alertes** en haut de la page Surveiller.

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 à partir de l'onglet Surveiller et qui proviennent de composants Citrix. Vous pouvez configurer les alertes Citrix à partir de l'onglet Surveiller 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.

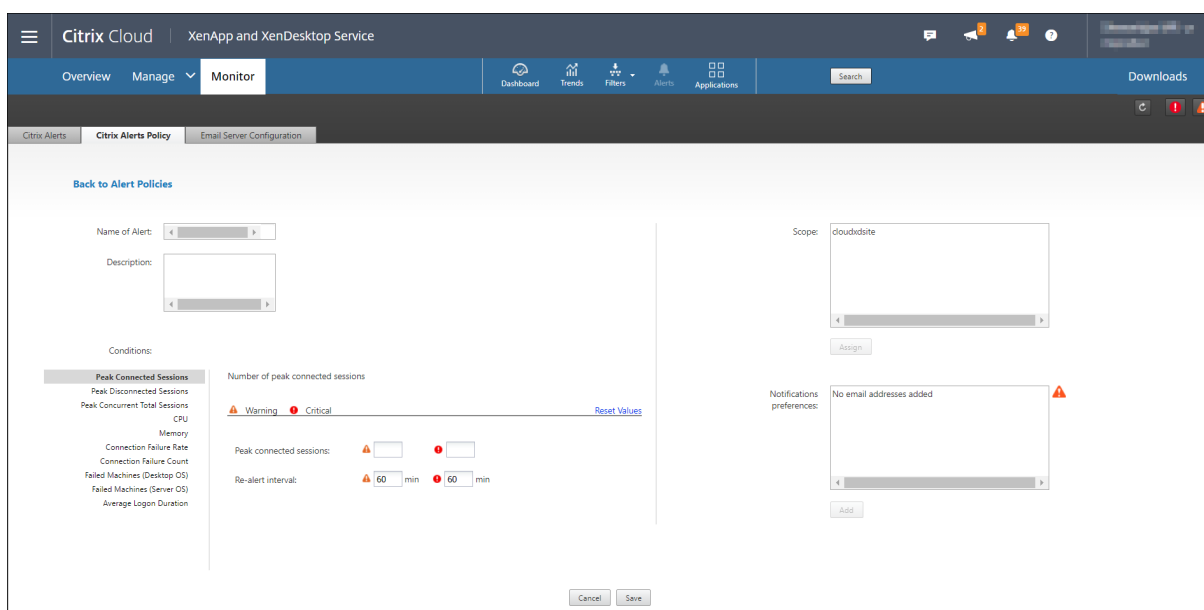
Créer des stratégies d'alerte

Pour créer une 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 **Créer**.
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**.

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).



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 l'onglet Surveiller 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 l'onglet Surveiller 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 l'onglet Surveiller 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. 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 .

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. 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 Tendence des défaillances dans l'onglet Surveiller 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 Tendence des défaillances dans l'onglet Surveiller 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 les rapports HDX Insight de Citrix ADM pour déterminer la cause. Si Citrix ADC n'est pas disponible, vérifier le RTT ICA et la latence dans la vue Détails utilisateur de l'onglet Surveiller et déterminer s'il s'agit d'un problème de réseau ou d'un problème Virtual Apps and Desktops. Pour de plus amples informations, veuillez consulter la documentation de Citrix ADM .
RTT ICA (nbre de sessions)	Nombre de sessions qui dépassent la durée seuil de la boucle ICA. Vérifier dans les rapports HDX Insight de Citrix ADM le nombre de sessions avec un RTT ICA élevé. Pour de plus amples informations, veuillez consulter la documentation de Citrix ADM . Si Citrix ADC 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 les rapports HDX Insight de Citrix ADM le nombre de sessions avec un RTT ICA élevé. Pour de plus amples informations, veuillez consulter la documentation de Citrix ADM . Si Citrix ADC 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 l'onglet Surveiller. 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 l'onglet Surveiller. 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 l'onglet Surveiller 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 l'onglet Surveiller 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.

Surveiller les tendances historiques

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 et l'utilisation des ressources 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.

Remarque

- Citrix Virtual Apps and Desktops Service conserve les données historiques pendant 90 jours uniquement. Par conséquent, les tendances et les rapports d'une année dans l'onglet Surveiller montrent les derniers 90 jours de données.
- 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 ou une période plus courte. Lorsque la période de temps est définie sur Année dernière, les informations de tendance sont disponibles sous forme de graphiques, mais pas de tableaux.

Action	Description
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 les connexions, 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.

Action	Description
Afficher les tendances des échecs de machine	Depuis Échecs > 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. L'administrateur peut choisir les colonnes à afficher et trier le rapport en fonction de n'importe quelle colonne. Pour de plus amples informations, consultez la section Diagnostiquer les problèmes de connexion utilisateur .

Action	Description
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. Cochez la case Prédire pour voir le graphique des données estimées. Pour de plus amples informations, consultez la section Prédiction d'instances d'applications .

Action	Description
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 vous sélectionnez Machine, 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.

Action	Description
Afficher l'utilisation des ressources	<p>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. Les tendances d'utilisation de mémoire et d'UC requièrent des VDA de version 7.11 ou ultérieure. Les tendances de latence de disque et d'E/S par seconde requièrent des VDA de version 7.14 ou ultérieure. 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. 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. Par défaut, la stratégie est définie sur « Interdite ». Toutes les données d'utilisation des ressources sont collectées par défaut. Cela peut être désactivé à l'aide du paramètre de stratégie Activer le suivi des ressources. Le tableau sous les graphiques affiche les données d'utilisation des ressources par machine. Remarque : Nbre moyen d'E/S par seconde indique les moyennes quotidiennes. E/S par seconde max. est calculé</p>

Action	Description
Afficher les échecs applicatifs	<p>L'onglet Échecs applicatifs affiche les échecs historiques associés aux applications publiées.</p> <p>Remarque : cette fonctionnalité requiert des VDA de version 7.15 ou ultérieure. 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 dans Résolution des problèmes d'applications. 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.</p>

Action	Description
Créer des rapports personnalisés	<p>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. À partir de la liste des requêtes de rapport personnalisé enregistrées précédemment, vous pouvez exporter le rapport au format CSV, copier et partager la requête OData correspondante, ou 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.</p> <p>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.</p> <p>Remarque : les noms de colonne dans les rapports Aperçu et Exporter générés à l'aide de requêtes OData ne sont pas localisés, mais s'affichent en anglais.</p>

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 sont disponibles pour sélection dans les filtres de tendances de l'onglet Surveiller jusqu'à ce que les données y étant associées 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

Grâce à la fonction d'exportation, vous pouvez exporter les informations 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.

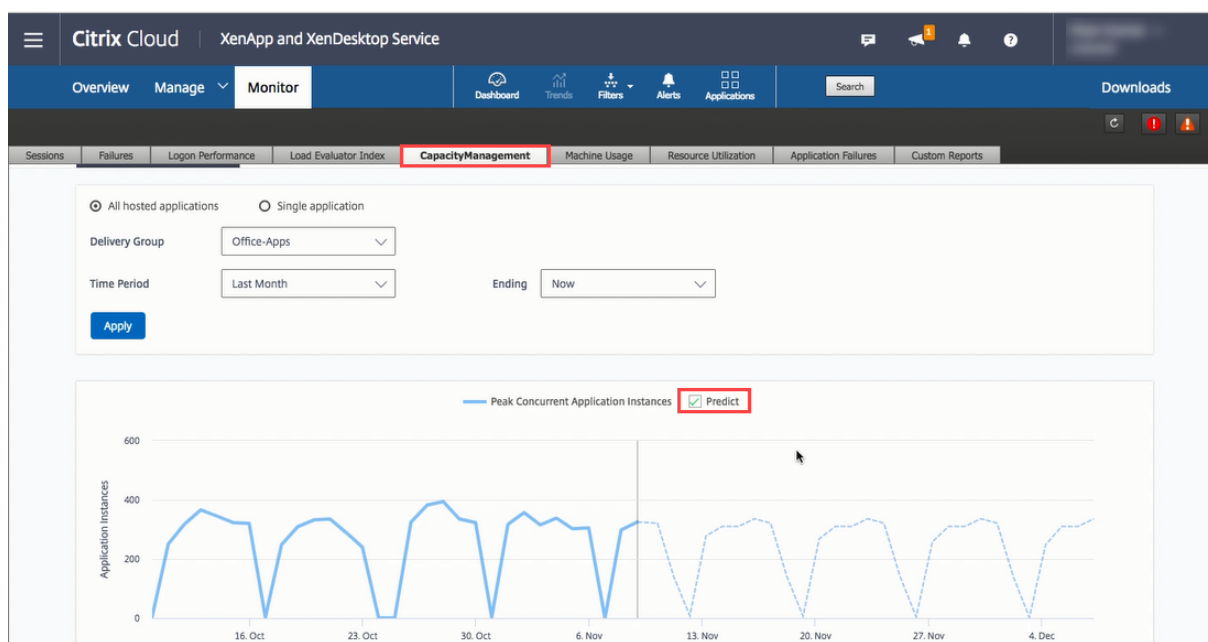
Le nombre d'opérations d'exportation simultanées et le volume de données qui peuvent être exportées sont définis sur les limites par défaut, au-delà desquelles les données tabulaires sont tronquées.

Prédiction d'instances d'applications

L'analyse prédictive vous permet de prédire l'utilisation future des ressources. Cette fonctionnalité est particulièrement utile pour les administrateurs pour organiser les ressources et les licences requises sur chaque ressource.

La fonction de prédiction d'instances d'applications indique le nombre d'instances d'applications hébergées susceptibles d'être lancées par site ou groupe de mise à disposition au cours d'une période donnée.

La prédiction d'instances d'applications est disponible dans l'onglet **Tendances > Gestion de la capacité** qui affiche l'utilisation de l'application hébergée pour la période de temps choisie. Le graphique historique contient les valeurs d'instances d'applications simultanées maximales pour la période choisie.



Pour obtenir le graphique des prédictions, cochez la case Prédire. Un graphique de prédictions en pointillé est affiché en tant qu'extension du graphique historique. Les valeurs d'instances d'applications simultanées maximales prédites sont représentées avec la chronologie étendue dans le futur pour la période de temps choisie.

Vous pouvez prédire les instances d'applications pour des périodes de 7 jours, un mois ou une année. Les dates de fin personnalisées ne sont pas prises en charge.

Des algorithmes d'apprentissage automatique basés sur des modèles de données créés avec des données historiques existantes sont utilisés pour effectuer la prédiction. L'exactitude des prédictions dépend par conséquent de la qualité des données existantes.

La précision de la prédiction est indiquée par le niveau de tolérance affiché sous forme d'une info-bulle sur le graphique de prédiction. Il indique le degré de variation possible des valeurs réelles avec les valeurs prédites.

Le niveau de tolérance peut être élevé si les données disponibles

- ne suivent pas un modèle régulier,
- sont absentes pour certaines périodes ou
- sont insuffisantes

La prédiction pour une année capture les tendances mensuelles et trimestrielles couplées avec la tendance générale pour l'année. De même, la prédiction mensuelle capture les tendances quotidiennes et hebdomadaires ainsi que les tendances hebdomadaires telles que la réduction de l'activité pendant les week-ends.

Des données historiques suffisantes doivent être disponibles pour la prédiction, comme suit :

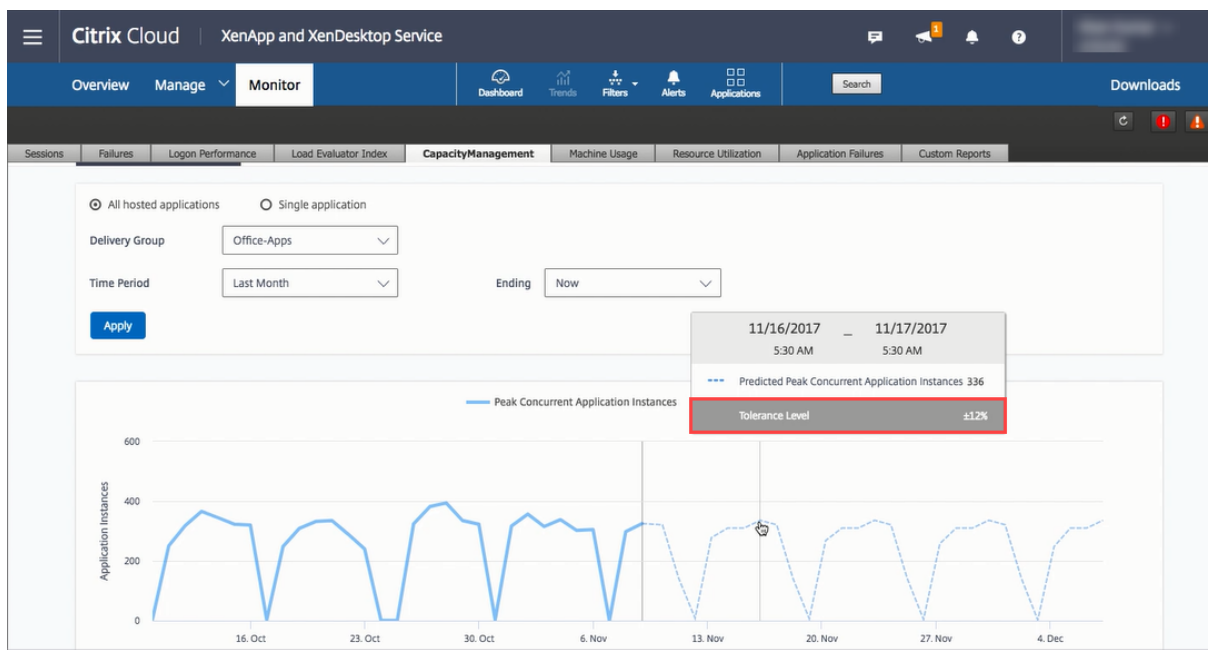
- 14 jours de données pour une prédiction sur 7 jours,

Citrix Virtual Apps and Desktops Service

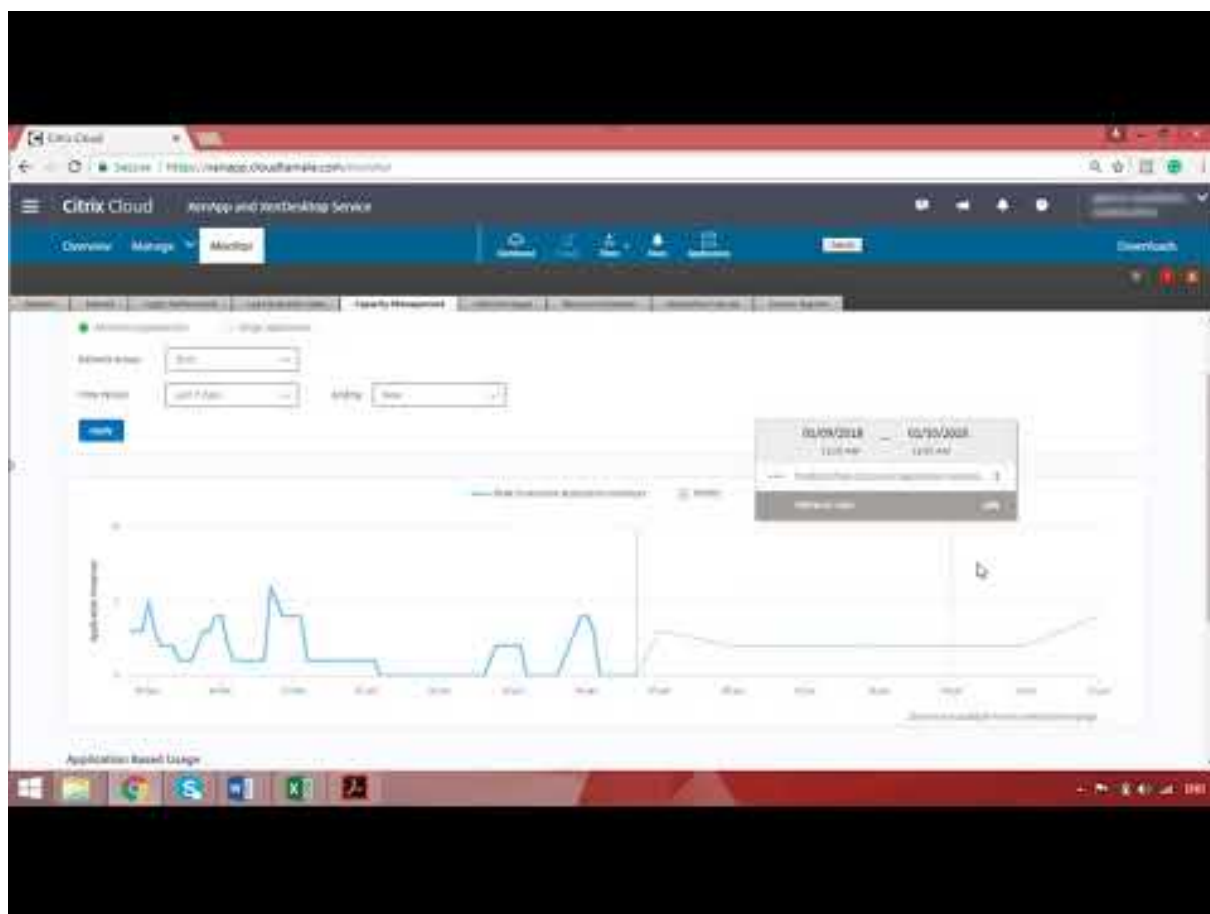
- 35 jours de données pour une prédiction sur un mois, et
- 84 jours de données pour une prédiction sur un an.

Remarque

Vous pouvez uniquement exporter le graphique historique, mais pas le graphique de prédiction.



Pour une brève démonstration de la fonctionnalité de prédiction d'instances d'applications, regardez



la vidéo.

Analyse des applications

L'onglet **Applications** affiche des analyses basées sur les applications dans une vue consolidée unique pour faciliter l'analyse et la gestion efficaces des performances des applications. Vous pouvez obtenir des informations précieuses sur l'intégrité et l'utilisation de toutes les applications publiées sur le site. Cette fonctionnalité requiert des VDA de version 7.15 ou ultérieure.

Application	Instances ↓	Application Faults (Last hour)	Application Errors (Last hour)
US LT5R7511 Outlook 2016	5	3	0
US LT5R7511 Skype for Business 2016	4	1	0
US LT5R7511 Slack	3	5	0
US LT5R7511 Internet Explorer	1	4	1
US LT5R7511 Citrix XenCenter	1	3	5
US 715LTSR1017 PowerPoint 2016	1	0	0
US LT5R7511 Mozilla Firefox	1	0	0
US LT5R7424 Skype for Business 2016	0	0	0
US LT5R7321 Word 2016	0	0	0
US 715LTSR1017 Acrobat Reader DC	0	0	0
US 715LTSR1015 Citrix XenCenter	0	0	0
US LT5R7415 Paint	0	0	0
US GA10 Slack	0	0	0
US LT5R7511 Notepad++	0	0	0

La colonne **Instances** affiche l'utilisation des applications. Elle indique le nombre d'instances d'application en cours d'exécution (instances connectées et déconnectées). Pour résoudre des problèmes, cliquez sur le champ **Instances** pour afficher la page de filtres **Instances d'application**. Dans cette page, vous pouvez sélectionner les instances d'application à fermer ou à déconnecter.

Contrôlez l'intégrité des applications publiées dans votre site avec les colonnes **Défaillances applicatives** et **Erreurs applicatives**. Ces colonnes affichent le nombre cumulé de défaillances et d'erreurs survenues lors du lancement de l'application correspondante au cours de la dernière heure. Cliquez sur le champ **Défaillances applicatives** ou **Erreurs applicatives** pour afficher les détails de l'échec sur la page **Tendances > Défaillances applicatives** correspondant à l'application sélectionnée.

Les paramètres de stratégie d'échec de l'application régissent la disponibilité et l'affichage des défaillances et des erreurs. Pour de plus amples informations sur les stratégies et comment les modifier, consultez la section [Stratégies pour la détection des défaillances applicatives](#) dans Paramètres de stratégie Surveillance.

Analyse d'application

L'analyse d'application automatise les vérifications d'intégrité des applications Citrix Virtual Apps publiées sur un site. Les résultats de l'analyse d'application sont disponibles dans l'onglet **Surveiller** de Citrix Virtual Apps and Desktops Service.

Assurez-vous que les machines de point de terminaison exécutant des agents Probe Agent sont des ordinateurs Windows dotés de Citrix Receiver pour Windows version 4.8 ou ultérieure ou de l'application Citrix Workspace pour Windows (anciennement Citrix Receiver pour Windows) version 1808 ou ultérieure. L'application Workspace pour plate-forme Windows universelle (UWP) n'est pas prise en charge.

Les comptes/autorisations d'utilisateur requis pour exécuter l'analyse d'application sont les suivants :

- Un utilisateur unique de Workspace pour effectuer une analyse sur chaque machine de point de terminaison. L'utilisateur de Workspace n'est pas tenu d'être administrateur ; les analyses peuvent s'exécuter dans un contexte non administrateur.
- Comptes d'utilisateur avec des autorisations d'administrateur Windows pour installer et configurer l'agent Citrix Probe Agent sur les machines de point de terminaison
- Un compte d'utilisateur administrateur complet avec les autorisations suivantes. La réutilisation de comptes d'utilisateur existants pour l'analyse des applications risque de déconnecter les sessions actives des utilisateurs.
 - Autorisations du groupe de mise à disposition :
 - * Lecture seule
 - Autorisations de Director :
 - * Créer/modifier/supprimer la configuration du serveur de messagerie d'alertes
 - * Créer/modifier/supprimer des configurations d'analyse
 - * Afficher la page Configurations
 - * Afficher la page des tendances

Configurer l'analyse d'application

Configurez l'exécution de vos analyses d'application pendant les heures creuses sur plusieurs zones géographiques. Les résultats d'analyse complets peuvent aider à résoudre les problèmes liés aux applications, à la machine d'hébergement ou à la connexion avant que les utilisateurs ne les rencontrent.

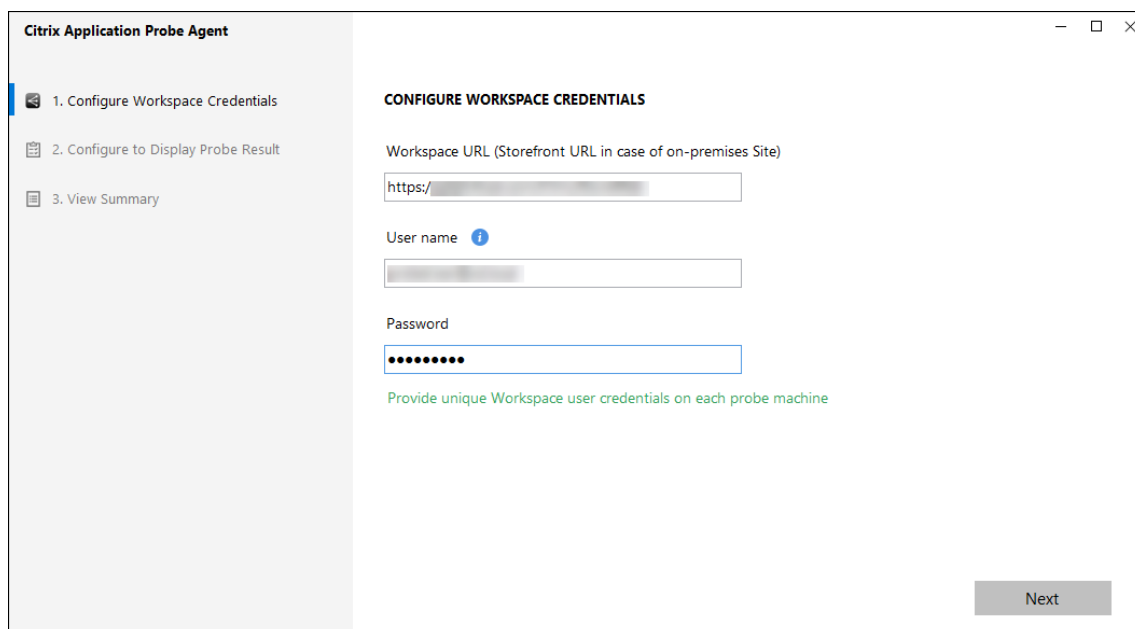
Étape 1 : Installation et configuration de Citrix Probe Agent

Citrix Probe Agent est un exécutable Windows qui simule le lancement de l'application par l'utilisateur via Citrix Workspace. Il teste les lancements d'applications configurés dans l'onglet Surveiller et communique les résultats dans l'onglet Surveiller.

1. Identifiez les machines de point de terminaison à partir desquelles vous souhaitez exécuter l'analyse d'application.
2. Les utilisateurs avec des autorisations d'administrateur peuvent installer et configurer l'agent Citrix Probe Agent sur la machine de point de terminaison Téléchargez l'exécutable Citrix Probe Agent disponible sur <https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/components/app-probe-agent.html>
3. Démarrez l'agent et configurez vos informations d'identification Citrix Workspace. Configurez un utilisateur unique de Workspace sur chaque machine de point de terminaison. Les informations d'identification sont cryptées et stockées de manière sécurisée.

Remarque :

Pour accéder au site à analyser à partir de l'extérieur du réseau, tapez l'URL d'ouverture de session de Citrix Gateway dans le champ **URL de Workspace**. Citrix Gateway achemine automatiquement la demande vers l'URL du site Workspace correspondante.



4. Dans l'onglet **Configurer pour afficher les résultats de l'analyse**, entrez les informations d'identification pour accéder à Citrix Virtual Apps and Desktops Service.

Remarque :

Vous pouvez trouver le nom du client, l'ID du client et la clé secrète à partir de la page Accès aux API dans la console Citrix Cloud.

```
1 ![Probe agent](/en-us/citrix-virtual-apps-desktops-service/media/director-probe-agent-monitor.png)
```

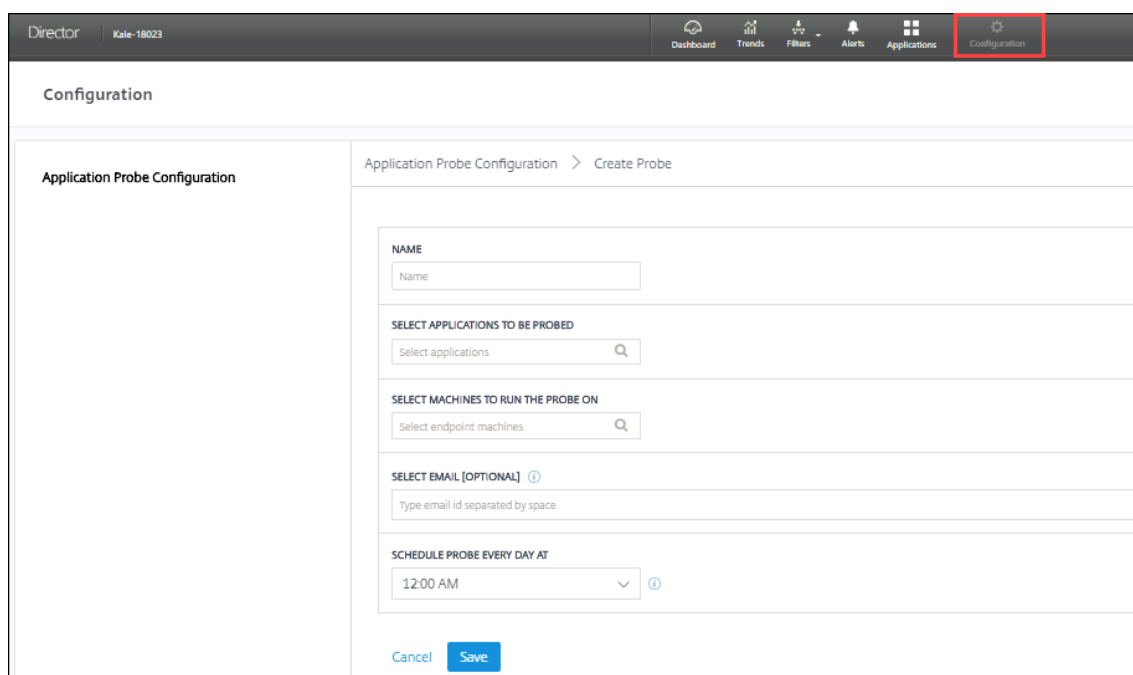
Étape 2 : Configuration de l'analyse d'application dans l'onglet Surveiller

1. Dans Citrix Virtual Apps and Desktops Service, accédez à **Configuration > Configuration de l'analyse d'application**.
2. Créez une analyse et choisissez :
 - les applications à analyser,
 - les machines de point de terminaison sur lesquelles l'analyse doit s'exécuter,
 - les adresses e-mail auxquelles les résultats de l'analyse de défaillance sont envoyés (configurez votre serveur de messagerie dans **Alertes -> Configuration du serveur de mes-**

sagerie), et

- l'heure de la journée à laquelle l'analyse doit s'exécuter (selon le fuseau horaire local de la machine de point de terminaison).

Après la configuration dans l'onglet **Surveiller**, un délai de 10 minutes est nécessaire avant que l'agent soit prêt à commencer à tester. Ensuite, il lance les analyses configurées commençant l'heure suivante.



The screenshot shows the Citrix Director interface. The top navigation bar includes 'Director', 'Kale-18023', and several icons: Dashboard, Trends, Filters, Alerts, Applications, and Configuration (highlighted with a red box). The main content area is titled 'Configuration' and contains a section for 'Application Probe Configuration'. On the right side, there is a 'Create Probe' form with the following fields:

- NAME:** A text input field labeled 'Name'.
- SELECT APPLICATIONS TO BE PROBED:** A search input field labeled 'Select applications' with a magnifying glass icon.
- SELECT MACHINES TO RUN THE PROBE ON:** A search input field labeled 'Select endpoint machines' with a magnifying glass icon.
- SELECT EMAIL [OPTIONAL]:** A text input field labeled 'Type email id separated by space' with an information icon.
- SCHEDULE PROBE EVERY DAY AT:** A dropdown menu showing '12:00 AM' with a magnifying glass icon.

At the bottom of the form are 'Cancel' and 'Save' buttons.

Étape 3 : Exécution de l'analyse

L'agent exécute l'analyse d'application en fonction de la configuration de l'analyse qu'il récupère toutes les heures de l'onglet Surveiller. Il lance des applications sélectionnées en série à l'aide de Workspace. L'agent communique les résultats à l'onglet Surveiller via la base de données de l'onglet Surveiller. Les échecs sont signalés en cinq étapes spécifiques :

- **Accessibilité de Workspace :** l'URL Workspace configurée n'est pas accessible.
- **Authentification de Workspace :** les informations d'identification Workspace configurées ne sont pas valides.
- **Énumération Workspace :** la liste des applications Workspace ne contient pas l'application à tester.
- **Téléchargement ICA :** le fichier ICA n'est pas disponible.
- **Lancement d'applications :** l'application n'a pas pu être lancée.

Étape 4 : Affichage des résultats de l'analyse

Vous pouvez afficher les résultats les plus récents de l'analyse dans la page **Applications** de Citrix Virtual Apps and Desktops Service.

Application	Probe Result	Instances	Application Faults	Application Errors
Calculator	7 out of 7 probe	1	0	0
Notepad	7 out of 7 probe	1	0	0
MapInfo	7 out of 7 probe	1	0	0
Command Prompt	7 out of 7 probe	1	0	0
Stateless Power	1 Probe Success	1	0	0
Character Map	1 Probe Success	1	0	0
Notepad	1 Probe Success	1	0	0
File Cleanup	N/A	1	0	0
Windows Memory Diagnostic	N/A	1	0	0
System Configuration	N/A	1	0	0
System Information	N/A	1	0	0
Power	N/A	1	0	0

Pour une résolution plus poussée, cliquez sur le lien du résultat de l'analyse pour voir plus de détails dans la page **Tendances > Résultats de l'analyse d'application**.

APPLICATION NAME	LAUNCH TIME	ENDPOINT NAME	PROBE RESULT
Calculator	05/22/2018 12:07 PM		ICA File didn't download
Character Map	05/22/2018 12:44 PM		No problems found
Citrix Receiver	05/22/2018 12:33 PM		No problems found
Command Prompt	05/22/2018 12:09 PM		No problems found
Defragment and Optimize Drives	05/22/2018 12:40 PM		No problems found
Disk Cleanup	05/22/2018 12:37 PM		No problems found
ICM Indicator	05/22/2018 12:32 PM		Application Launch Failure
MapInfo	05/22/2018 12:18 PM		No problems found

Les résultats des analyses consolidés sont disponibles pour les dernières 24 heures ou les 7 derniers jours sur cette page. Vous pouvez voir l'étape à laquelle l'analyse a échoué. Vous pouvez filtrer le tableau pour une application, une étape d'échec d'analyse ou une machine de point de terminaison spécifique.

Citrix Gateway

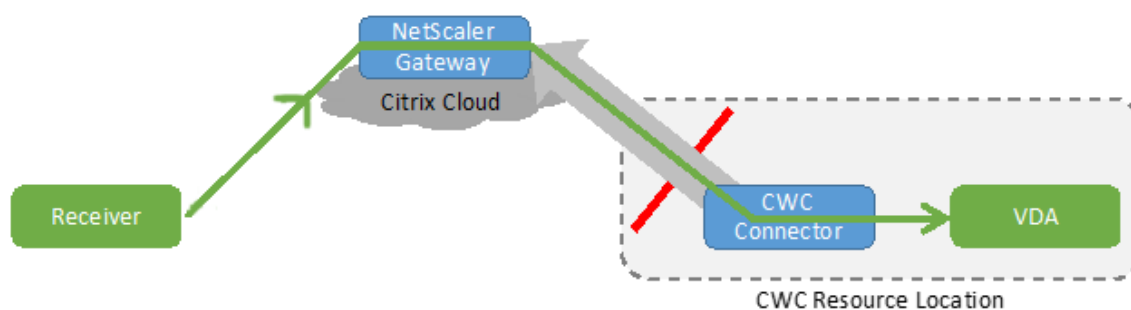
March 6, 2019

Citrix Gateway Service

Citrix Gateway offre aux utilisateurs un accès VPN sécurisé aux applications Citrix Virtual Apps and Desktops sur un large éventail d'appareils, y compris des ordinateurs portables, des postes de travail, des clients légers, des tablettes et des smartphones.

Citrix Gateway Service permet d'accéder à distance et de manière sécurisée aux applications Citrix Virtual Apps and Desktops, sans avoir à déployer Citrix Gateway dans la DMZ ou à reconfigurer votre pare-feu. Les opérations d'infrastructure liées à l'utilisation de Citrix Gateway sont transférées sur le cloud et hébergées par Citrix.

Vous activez Citrix Gateway Service dans Citrix Cloud. Après l'activation du service, les utilisateurs peuvent accéder à leurs VDA en dehors de leur réseau, comme illustré dans le diagramme suivant.



Activer ou désactiver le service Citrix Gateway

1. Connectez-vous à [Citrix Cloud](#).
2. Dans le menu en haut à gauche, sélectionnez **Configuration de l'espace de travail**. L'onglet **Intégrations de services** indique si chaque service est activé ou non.
3. Utilisez le menu des points de suspension sur la ligne contenant le nom du service pour sélectionner **Activer** ou **Désactiver**.

Problèmes connus

- Le service Citrix Gateway est activé pour une utilisation avec le trafic HDX uniquement dans le cadre du service Virtual Apps and Desktops. Les autres fonctionnalités de Citrix Gateway ne sont pas activées.
- Le Citrix Cloud Connector qui se trouve dans votre emplacement de ressources Citrix Cloud communique avec les services de cloud gérés par Citrix qui communiquent via Internet. Ce canal de communication ne prend pas en charge l'authentification sur proxys sortants pour l'accès à Internet.
- Tout le trafic réseau est protégé par SSL, mais pour fournir la fonctionnalité Citrix Gateway, le trafic HDX est présent dans la mémoire sous forme non cryptée.

- SmartAccess ne fonctionne pas pour les sessions connectées via le service Citrix Gateway.

Plus d'informations

[Documentation produit Citrix Gateway](#)

Citrix VPX

- [Déployer une instance Citrix ADC VPX sur AWS](#) : ce document fournit des informations et des instructions pertinentes pour le déploiement d'une instance Citrix ADC VPX sur AWS.
- [Déployer une instance Citrix ADC VPX sur Microsoft Azure](#) : ce document fournit des informations et des instructions pertinentes pour le déploiement d'une instance Citrix ADC VPX sur Azure.
- [Installer une instance Citrix ADC VPX sur Citrix Hypervisor \(XenServer\)](#) : ce document fournit des informations et des instructions pertinentes pour l'installation et la configuration d'une instance Citrix ADC VPX sur Citrix Hypervisor (XenServer).

Pour plus d'informations sur les déploiements de Citrix VPX sur d'autres hyperviseurs, consultez la section [Déploiement de Citrix VPX](#).

Kits de développement (SDK) et API

March 6, 2019

Kit de développement logiciel distant SDK Citrix Virtual Apps and Desktops Remote PowerShell

Le SDK Remote PowerShell (PS) automatise les tâches complexes et répétitives. Il fournit le mécanisme qui permet de configurer et gérer l'environnement Citrix Virtual Apps and Desktops (anciennement XenApp and XenDesktop) sans avoir à utiliser l'interface utilisateur de Studio.

Les composants logiciels enfichables pris en charge sont répertoriés dans la section Limites. Cette section répertorie également les applets de commande qui sont désactivées.

Différences entre ce SDK et le SDK Citrix Virtual Apps and Desktops Delivery Controller

Dans un déploiement Citrix Virtual Apps and Desktops entièrement installé et géré par les administrateurs du client, ces administrateurs exécutent des scripts et applets de commande dans un site contenant des VDA et des Delivery Controller au sein d'une structure de domaine commune. Par comparaison, Citrix Virtual Apps and Desktops Service répartit les VDA et les Controller dans un emplacement

de ressources et le plan de contrôle, respectivement. Cette répartition signifie que le SDK Citrix Virtual Apps and Desktops PS d'origine ne fonctionnera pas dans un environnement Citrix Virtual Apps and Desktops Service, car il ne peut pas traverser la limite sécurisée entre l'emplacement de ressources et le plan de contrôle.

La solution est le kit de développement logiciel distant PowerShell SDK Citrix Virtual Apps and Desktops. Lorsqu'il est exécuté dans l'emplacement de ressources, le SDK Remote PS accède au plan de contrôle comme s'il était local, et fournit les mêmes fonctionnalités qu'un site Citrix Virtual Apps and Desktops. Seule une faible couche de communication non visible existe, optimisée pour fonctionner soit dans un seul site local, soit dans l'environnement de cloud. Les applets de commande sont identiques et la plupart des scripts existants fonctionnent de la même façon.

L'applet de commande `Get-XdAuthentication` fournit l'autorisation permettant de traverser la limite sécurisée entre l'emplacement de ressources et le plan de contrôle. Par défaut, `Get-XdAuthentication` invite les utilisateurs à entrer des informations d'identification CAS, ce qui doit être effectué une seule fois par session PowerShell. L'utilisateur peut également définir un profil d'authentification à l'aide d'un client sécurisé d'accès aux API, créé dans la console Citrix Cloud. Dans les deux cas, les informations de sécurité sont conservées afin de pouvoir être utilisées dans les appels ultérieurs du SDK PS. Si cette applet de commande n'est pas explicitement exécutée, elle est appelée par la première applet de commande du SDK PS.

Installer et utiliser le SDK Remote PowerShell

Exigences :

- Assurez-vous que PowerShell 3.0 ou version ultérieure est disponible sur la machine.
- Si le SDK Citrix Virtual Apps and Desktops Delivery Controller est installé sur la machine, supprimez ce SDK (à partir de Programmes et fonctionnalités de Windows) avant d'installer le SDK Remote PowerShell.

Pour installer et utiliser le SDK Remote PowerShell :

1. Téléchargez le programme d'installation : <https://download.apps.cloud.com/CitrixPoshSdk.exe>. Le package contient les implémentations x86 et x64.
2. Dans le dossier téléchargé, recherchez et exécutez le programme d'installation.
3. Suivez les dialogues pour procéder à l'installation.

Des journaux d'installation sont créés dans %TEMP%\CitrixLogs\CitrixPoshSdk. Ils peuvent aider à résoudre les problèmes d'installation.

Exécutez le SDK Citrix Virtual Apps and Desktops Remote PS sur un ordinateur joint au domaine dans cet emplacement de ressources :

- Ouvrez une invite de commandes PowerShell. Vous n'avez pas besoin de l'exécuter en tant qu'administrateur

- Ajoutez les composants logiciels enfichables Citrix : `asnp citrix.*`.
- Vous pouvez vous authentifier explicitement à l'aide de l'applet de commande `Get-XdAuthentication`. Ou, exécutez votre première commande du SDK Citrix Virtual Apps and Desktops PS, qui vous invitera à utiliser la même authentification que `Get-XdAuthentication`.
- Pour contourner l'invite d'authentification, vous pouvez utiliser l'applet de commande `Set-XdCredentials` pour créer un profil d'authentification par défaut, à l'aide d'un client sécurisé créé dans la console Citrix Cloud.
- Continuez à exécuter les applets de commande du SDK PS ou les scripts d'automatisation du SDK PS. Voici un exemple ci-dessous.

Citrix recommande de ne pas exécuter les applets de commande de ce SDK sur les Cloud Connector. Le fonctionnement du SDK n'implique pas les Cloud Connector.

Désinstallation :

À partir de la fonctionnalité Windows de suppression ou modification des programmes, sélectionnez **Citrix Virtual Apps and Desktops Remote PowerShell SDK**. Cliquez avec le bouton droit et sélectionnez **Désinstaller**. Suivez les dialogues.

Exemples d'activités

Les activités courantes incluent la configuration de catalogues de machines, d'applications et d'utilisateurs. Un exemple de script est illustré ci-dessous.

```
1     $users = "xd.local\Domain Users"
2
3     $TSVDACatalogName = "TSVDA"
4
5     $TSVDADGName = "TSVDA"
6
7     $TSVDAMachineName = "xd\ds-tsvda2"
8
9     #Create TSVDA Catalog
10
11    $brokerUsers = New-BrokerUser -Name $users
12
13    $catalog = New-BrokerCatalog -Name $TSVDACatalogName -
        AllocationType "Random" -Description $TSVDACatalogName -
        PersistUserChanges "OnLocal" -ProvisioningType "Manual" -
        SessionSupport "MultiSession" -MachinesArePhysical $true
14
15    #Add TSVDA Machine to Catalog
16
```

```
17     $BrokeredMachine = New-BrokerMachine -MachineName $TSVDAMachineName
        -CatalogUid $catalog.uid
18
19     #Create new desktops & applications delivery group
20
21     $dg = New-BrokerDesktopGroup -Name $TSVDADGName -PublishedName
        $TSVDADGName -DesktopKind "Shared" -SessionSupport "MultiSession"
        -DeliveryType DesktopsAndApps -Description $TSVDADGName
22
23     #Create notepad application
24
25     New-BrokerApplication -ApplicationType HostedOnDesktop -Name "
        Notepad" -CommandLineExecutable "notepad.exe" -DesktopGroup $dg
26
27     #Assign users to desktops and applications
28
29     New-BrokerEntitlementPolicyRule -Name $TSVDADGName -DesktopGroupUid
        $dg.Uid -IncludedUsers $brokerUsers -description $TSVDADGName
30
31     New-BrokerAccessPolicyRule -Name $TSVDADGName -
        IncludedUserFilterEnabled $true -IncludedUsers $brokerUsers -
        DesktopGroupUid $dg.Uid -AllowedProtocols @("HDX","RDP")
32
33     New-BrokerAppEntitlementPolicyRule -Name $TSVDADGName -
        DesktopGroupUid $dg.Uid -IncludedUsers $brokerUsers -description
        $TSVDADGName
34
35     #Add machine to delivery group
36
37     Add-BrokerMachine -MachineName $TSVDAMachineName -DesktopGroup $dg
```

Limitations

Les composants logiciels enchifables PowerShell Citrix Virtual Apps and Desktops suivants sont pris en charge dans cette version:

- Broker
- Identité Active Directory (AD)
- Création d'une machine
- Configuration
- Journalisation de la configuration
- Hôte
- Administration déléguée

- Analytics

Pour plus d'informations sur les applets de commande dans ces composants logiciels enfichables, consultez la section [Citrix Virtual Apps and Desktops SDK](#).

Une fois authentifié, l'accès distant reste valide dans la session PowerShell en cours pendant 24 heures. Passé ce délai, vous devez entrer vos informations d'identification.

Le SDK Remote PS doit être exécuté sur un ordinateur dans l'emplacement de ressources.

Les applets de commande suivantes sont désactivées dans les opérations à distance pour maintenir l'intégrité et la sécurité du plan de contrôle du cloud.

Citrix.ADIIdentity.Admin.V2:

- Copy-AcctIdentityPool
- Get-AcctDBConnection
- Get-AcctDBSchema
- Get-AcctDBVersionChangeScript
- Get-AcctInstalledDBVersion
- Remove-AcctServiceMetadata
- Reset-AcctServiceGroupMembership
- Set-AcctDBConnection
- Set-AcctServiceMetadata
- Test-AcctDBConnection

Citrix.Analytics.Admin.V1:

- Get-AnalyticsDBConnection
- Get-AnalyticsDBSchema
- Get-AnalyticsDBVersionChangeScript
- Get-AnalyticsInstalledDBVersion
- Import-AnalyticsDataDefinition
- Remove-AnalyticsServiceMetadata
- Reset-AnalyticsServiceGroupMembership
- Set-AnalyticsDBConnection
- Set-AnalyticsServiceMetadata
- Set-AnalyticsSite
- Set-AnalyticsDBConnection

Citrix.DelegatedAdmin.Admin.V1:

- Add-AdminPermission
- Add-AdminRight
- Get-AdminAdministrator
- Get-AdminDBConnection

- Get-AdminDBSchema
- Get-AdminDBVersionChangeScript
- Get-AdminInstalledDBVersion
- Import-AdminRoleConfiguration
- New-AdminAdministrator
- New-AdminRole
- New-AdminScope
- Remove-AdminAdministrator
- Remove-AdminAdministratorMetadata
- Remove-AdminPermission
- Remove-AdminRight
- Remove-AdminRole
- Remove-AdminRoleMetadata
- Remove-AdminScope
- Remove-AdminScopeMetadata
- Remove-AdminServiceMetadata
- Reset-AdminServiceGroupMembership
- Set-AdminAdministrator
- Set-AdminAdministratorMetadata
- Set-AdminDBConnection
- Set-AdminRole
- Set-AdminRoleMetadata
- Set-AdminScope
- Set-AdminScopeMetadata
- Set-AdminServiceMetadata
- Test-AdminDBConnection

Citrix.Broker.Admin.V2:

- Get-BrokerDBConnection
- Get-BrokerDBSchema
- Get-BrokerDBVersionChangeScript
- Get-BrokerInstalledDBVersion
- Get-BrokerLease
- New-BrokerMachineConfiguration
- Remove-BrokerControllerMetadata
- Remove-BrokerLease
- Remove-BrokerLeaseMetadata
- Remove-BrokerMachineConfigurationMetadata
- Remove-BrokerMachineConfiguration
- Remove-BrokerSiteMetadata

- Remove-BrokerUserFromApplication
- Reset-BrokerLicensingConnection
- Reset-BrokerServiceGroupMembership
- Set-BrokerControllerMetadata
- Set-BrokerDBConnection
- Set-BrokerLeaseMetadata
- Set-BrokerMachineConfiguration
- Set-BrokerMachineConfigurationMetadata
- Set-BrokerSite
- Set-BrokerSiteMetadata
- Test-BrokerDBConnection
- Test-BrokerLicenseServer
- Update-BrokerBrokerLocalLeaseCache

Citrix.Configuration.Admin.V2:

- Export-ConfigFeatureTable
- Get-ConfigDBConnection
- Get-ConfigDBSchema
- Get-ConfigDBVersionChangeScript
- Get-ConfigInstalledDBVersion
- Get-ConfigServiceGroup
- Import-ConfigFeatureTable
- Register-ConfigServiceInstance
- Remove-ConfigRegisteredServiceInstanceMetadata
- Remove-ConfigServiceGroup
- Remove-ConfigServiceGroupMetadata
- Remove-ConfigServiceMetadata
- Remove-ConfigSiteMetadata
- Reset-ConfigServiceGroupMembership
- Set-ConfigDBConnection
- Set-ConfigRegisteredServiceInstance
- Set-ConfigRegisteredServiceInstanceMetadata
- Set-ConfigServiceGroupMetadata
- Set-ConfigServiceMetadata
- Set-ConfigSite
- Set-ConfigSiteMetadata
- Test-ConfigDBConnection
- Unregister-ConfigRegisteredServiceInstance

Citrix.Host.Admin.V2:

- Get-HypDBConnection
- Get-HypDBSchema
- Get-HypDBVersionChangeScript
- Get-HypInstalledDBVersion
- Remove-HypServiceMetadata
- Reset-HypServiceGroupMembership
- Set-HypDBConnection
- Set-HypServiceMetadata
- Test-HypDBConnection

Citrix.ConfigurationLogging.Admin.V1:

- Get-LogDBConnection
- Get-LogDBSchema
- Get-LogDBVersionChangeScript
- Get-LogInstalledDBVersion
- Remove-LogOperation
- Remove-LogServiceMetadata
- Remove-LogSiteMetadata
- Reset-LogDataStore
- Reset-LogServiceGroupMembership
- Set-LogDBConnection
- Set-LogServiceMetadata
- Set-LogSite
- Set-LogSiteMetadata
- Test-LogDBConnection

Citrix.MachineCreation.Admin.V2:

- Get-ProvDBConnection
- Get-ProvDBSchema
- Get-ProvDBVersionChangeScript
- Get-ProvInstalledDBVersion
- Get-ProvServiceConfigurationData
- Remove-ProvServiceConfigurationData
- Remove-ProvServiceMetadata
- Reset-ProvServiceGroupMembership
- Set-ProvDBConnection
- Set-ProvServiceConfigurationData
- Set-ProvServiceMetadata
- Test-ProvDBConnection

Citrix.EnvTest.Admin.V1:

- Get-EnvTestDBConnection
- Get-EnvTestDBSchema
- Get-EnvTestDBVersionChangeScript
- Get-EnvTestInstalledDBVersion
- Remove-EnvTestServiceMetadata
- Reset-EnvTestServiceGroupMembership
- Set-EnvTestDBConnection
- Set-EnvTestServiceMetadata
- Test-EnvTestDBConnection

Citrix.Monitor.Admin.V1:

- Get-MonitorConfiguration
- Get-MonitorDBConnection
- Get-MonitorDBSchema
- Get-MonitorDBVersionChangeScript
- Get-MonitorDataStore
- Get-MonitorDataStore
- Get-MonitorInstalledDBVersion
- Remove-MonitorServiceMetadata
- Reset-MonitorDataStore
- Reset-MonitorServiceGroupMembership
- Set-MonitorConfiguration
- Set-MonitorDBConnection
- Set-MonitorServiceMetadata
- Test-MonitorDBConnection

Citrix.Storefront.Admin.V1:

- Construire-SFCluster
- Get-SfClusters
- Get-SfDBConnection
- Get-SfDBSchema
- Get-SfDBVersionChangeScript
- Get-SfInstalledDBVersion

Avis

Ce logiciel/exemple de code est fourni « en l'état », sans aucune déclaration, garantie ou condition. Vous pouvez l'utiliser, le modifier et le distribuer à vos propres risques. CITRIX EXCLUT TOUTE GARANTIE EXPRESSE, TACITE, ÉCRITE, ORALE OU LÉGALE, Y COMPRIS, MAIS SANS S'Y LIMITER, TOUTE GARANTIE DE QUALITÉ MARCHANDE, D'ADÉQUATION À UN USAGE PARTICULIER, DE PROPRIÉTÉ

ET D'ABSENCE DE CONTREFAÇON. Nonobstant ce qui précède, vous reconnaissez et acceptez (a) que le logiciel/exemple de code peut présenter des erreurs, des défauts de conception ou d'autres problèmes, susceptibles d'entraîner une perte de données ou des dommages à la propriété ; (b) qu'il peut être impossible de rendre le logiciel/exemple de code entièrement opérationnel ; et (c) que Citrix peut, sans préavis ni responsabilité, cesser de mettre à votre disposition la version actuelle et/ou les versions futures du logiciel/exemple de code. En aucun cas le logiciel/code ne devra être utilisé dans le cadre d'activités à haut risque, telles que, mais sans limitation aucune, les activités de maintien en vie ou d'explosion. CITRIX, SES FILIALES OU SES AGENTS NE POURRONT ÊTRE RESPONSABLES, EN VERTU D'UNE RUPTURE DE CONTRAT OU DE TOUTE AUTRE THÉORIE DE RESPONSABILITÉ, DE TOUT DOMMAGE RÉSULTANT DE L'UTILISATION DU LOGICIEL/EXEMPLE DE CODE, Y COMPRIS MAIS SANS LIMITATION AUCUNE, LES DOMMAGES DIRECTS, SPÉCIAUX, ACCESSOIRES, PUNITIFS, INDIRECTS OU AUTRES, MÊME S'ILS ONT ÉTÉ PRÉVENUS DE L'ÉVENTUALITÉ DE TELS DOMMAGES. Vous acceptez d'assurer l'indemnisation et la défense de Citrix contre toute réclamation résultant de l'utilisation, de la modification ou de la distribution du code.

API Monitor Service OData

En plus d'utiliser les fonctions de surveillance pour afficher les données d'historique, vous pouvez interroger les données à l'aide de l'API de Monitor Service. Vous pouvez utiliser l'API pour :

- Analyser des tendances historiques pour la planification
- Effectuer une résolution des problèmes détaillée des échecs de connexion et de machine
- Extraire des informations afin de les envoyer dans d'autres outils et processus ; par exemple, à l'aide des tables PowerPivot de Microsoft Excel pour afficher les données de différentes manières
- Créer une interface utilisateur personnalisée en plus des données offertes par l'API

Pour de plus amples informations, consultez [Monitor Service OData API](#). Pour obtenir des instructions sur l'accès à l'API Monitor Service, consultez la section [Accéder aux données de Monitor Service à l'aide du point de terminaison OData v4 dans Citrix Cloud](#).

Tech Previews des API de Citrix Virtual Apps and Desktops Service

Les Tech Previews des API sont disponibles à l'adresse https://developer.cloud.com/_virtual_apps_and_desktops_service/virtual_apps_and_desktops_service.html.

**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

© 2019 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).