Citrix Cloud

Contents

Accord de niveau de service

November 7, 2018

Date d'entrée en vigueur : 1er août 2018

Citrix Cloud a été développé à l'aide des meilleures pratiques de l'industrie afin de garantir un haut degré de disponibilité du service.

Cet accord de niveau de service (SLA) décrit l'engagement de Citrix envers la disponibilité du service Citrix Cloud. Ce contrat de niveau de service fait partie du Contrat de service de l'utilisateur final Citrix (EUSA) pour les services couverts (« Services »).

L'engagement de service de Citrix (« Engagement de service ») consiste à maintenir une disponibilité mensuelle d'au moins 99,5 % (« Disponibilité mensuelle ») sur les Services. La disponibilité mensuelle est calculée en soustrayant de 100 % le pourcentage de minutes, au cours d'un mois complet de Service, pendant lesquelles l'instance de Service était dans un état « indisponible ». Les services et la mesure de la disponibilité pour chacun sont présentés dans le tableau ci-dessous. Les mesures du pourcentage de disponibilité mensuelle excluent les temps d'arrêt résultant de :

- Fenêtres de maintenance programmées régulièrement.
- Manquement par le client du respect des exigences de configuration du service documentées sur https://docs.citrix.com ou comportement abusif ou saisie incorrecte.
- Utilisation par le client d'un Service après que Citrix a conseillé au client de modifier l'utilisation du Service, si le client n'a pas modifié l'utilisation.
- 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, logiciels installés et contrôlés par le client, équipement réseau ou autre matériel installé ; paramètres de sécurité, stratégies de groupe et autres stratégies de configuration définis et contrôlés par le Client ; défaillances du fournisseur de cloud public, défaillances du fournisseur de services Internet ou autres facteurs de soutien du Client externes au contrôle de Citrix.
- Les employés, agents, sous-traitants ou fournisseurs du Client, ou toute personne ayant accès aux mots de passe ou à l'équipement du client, ou résultant du manquement du Client à suivre les pratiques de sécurité appropriées.
- Les tentatives du client d'effectuer des opérations dépassant les droits du Service.
- Interruption de service due à un cas de force majeure, y compris, mais sans s'y limiter, les catastrophes naturelles, les guerres, les actes de terrorisme, ou les actions du gouvernement.

Aucun engagement de Service n'est offert pour tout essai, Tech Preview, service Labs ou bêta Citrix.

Citrix offre des engagements de Service aux clients qui :

- Ont acheté les Services en utilisant un abonnement basé sur une durée (période d'abonnement minimum d'1 an).

- Disposent d'au moins un abonnement de 100 unités (selon le modèle de licence applicable au Service) au cours de la période.

Les fournisseurs de services Citrix (CSP) ne sont pas éligibles.

Mesures de disponibilité par service

Service	Mesure par disponibilité mensuelle
Citrix Virtual Apps Service	Durée pendant laquelle les utilisateurs peuvent accéder à leur session d'application ou de bureau via le Service.
Citrix Virtual Desktops Service	Durée pendant laquelle les utilisateurs peuvent accéder à leur session d'application ou de bureau via le Service.
Citrix Virtual Apps and Desktops Service	Durée pendant laquelle les utilisateurs peuvent accéder à leur session d'application ou de bureau via le Service.
Content Collaboration	Durée pendant laquelle les utilisateurs peuvent énumérer les fichiers et dossiers associés à leur compte ou télécharger des fichiers hébergés dans des StorageZones gérées par Citrix.
Citrix Endpoint Management	Durée pendant laquelle les utilisateurs peuvent accéder à leurs applications mobiles délivrées par Citrix et aux appareils inscrits via le Service.
WorkSpace Service	Identique à la description ci-dessus pour les services de composants, mais inclut la disponibilité pour chacun. Des crédits peuvent être calculés au prorata si une réclamation concerne un nombre de composants inférieur au nombre total de composants.
Citrix Web App Firewall	Durant pendant laquelle le pare-feu d'applications Web (WAF) traite les données et applique les stratégies de sécurité correspondantes

Service	Mesure par disponibilité mensuelle
Intelligent Traffic Management	Durée pendant laquelle les utilisateurs peuvent accéder aux fonctionnalités de gestion du trafic via des requêtes DNS ou des appels d'API HTTP

Engagement de Service et recours

Si Citrix manque à son Engagement de Service pendant au moins 3 de 5 mois consécutifs à compter de la date d'entrée en vigueur du SLA, le recours exclusif consiste en un crédit de Service de 10 %, sur une base mensuelle, à faire valoir sur la prochaine prolongation annuelle du Service au cours de la période de renouvellement immédiat pour le même Service et le même nombre d'unités impactées.

- Pourcentage de disponibilité mensuelle : < 99,5 %
- Crédit de Service : 10 % (présenté au client sous forme de bon d'achat)

Pour bénéficier du recours ci-dessus, le client doit se conformer à l'EUSA et tout manquement doit être signalé par le client dans les trente (30) jours suivant la fin du dernier mois de la période de cinq mois consécutifs pour laquelle une demande de crédit est présentée. Pour savoir comment signaler d'éventuelles violations de ce contrat SLA, consultez l'article CTX237141.

La demande doit identifier le(s) Service(s), définir les dates, heures et durées d'indisponibilité, ainsi que les journaux ou enregistrements justificatifs corroborant l'indisponibilité et identifier les utilisateurs affectés et leur emplacement géographique, ainsi que l'assistance technique requise ou les réparations mises en œuvre. Un seul crédit de service est autorisé par Service et par mois, avec un maximum de crédit de service pour chaque mois de l'extension. Le client doit présenter le bon lors de l'achat de l'extension.

Si vous achetez l'extension via un revendeur, vous recevrez un crédit auprès du revendeur. Le crédit que nous appliquons pour un achat direct, ou que nous transmettons à votre revendeur pour un achat indirect, sera basé sur le prix de détail suggéré calculé au prorata de l'extension pour le même nombre d'unités. Citrix ne contrôle pas les prix de revente ni les crédits de revente. Les crédits n'incluent aucun de droit de compensation sur les paiements dus à Citrix ou à un revendeur. Citrix mettra occasionnellement à jour ces conditions. En cas de mise à jour, Citrix révisera également la date de publication en haut de l'accord de niveau de service. Toute modification s'applique uniquement à vos nouveaux achats de Service ou extensions de Service à la date de publication actuelle ou après cette dernière.

Avis de tiers

November 7, 2018

- Citrix Cloud - Avis de tiers (PDF)
- Citrix Analytics Service - Avis de tiers (PDF)
- Virtual Apps and Desktops - Avis de tiers (PDF)
- Smart Tools - Avis de tiers
- Citrix ShareFile Sync pour Mac - Avis de tiers (PDF)
- Citrix ShareFile Sync pour Windows - Avis de tiers (PDF)
- Secure Browser Service (PDF)
- Session Manager Service (PDF)
- Citrix Endpoint Management - Avis de tiers (PDF)
- Citrix Cloud Linux VDA Image Service - Avis de tiers (PDF)

Aperçu de l'architecture

November 7, 2018

Citrix Cloud : Architecture de référence de Virtual Apps and Desktops Service pour les nouveaux clients (PDF)

Citrix Cloud : Architecture de référence de Virtual Apps and Desktops Service sur site (PDF)

Évaluations de services Citrix Cloud

November 7, 2018

Les évaluations de services Citrix Cloud individuels sont fournies via la plate-forme Citrix Cloud. Les fonctionnalités disponibles dans la version d'évaluation d'un service sont les mêmes que celles d'un service acheté, par conséquent elles sont appropriées pour une preuve de concept, un projet pilote ou similaire.

Afin de personnaliser votre expérience et fournir les services considérés les plus importants pour vos utilisateurs, l'accès aux évaluations de Citrix Cloud est géré par service.

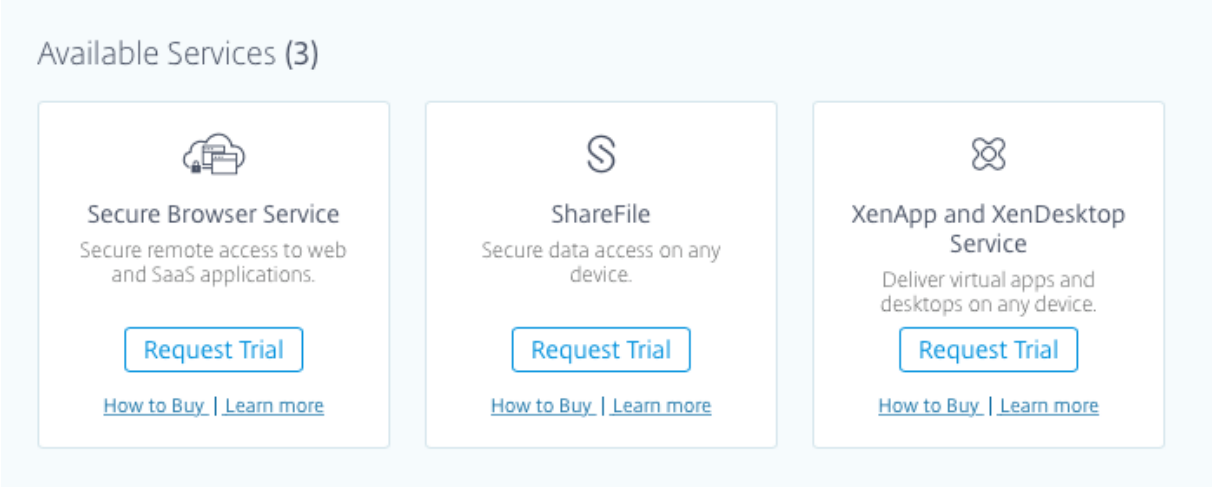
Lorsque vous êtes prêt à acheter des services Citrix Cloud, vous convertirez votre version d'évaluation en compte de production, il n'est donc pas nécessaire de reconfigurer quoi que ce soit, ou de créer un compte de production distinct.

Informations utiles sur les évaluations de service

	Évaluation de Citrix Cloud
Nombre d'abonnés autorisés	25
Durée maximale	60 jours calendaires. Vous ne pouvez demander une évaluation du service qu'une seule fois.
Disponibilité	Disponibilité restreinte
Emplacement de ressources	Fourni et configuré par le client
Durée des sessions utilisateur	Illimitée
Intégration locale à Microsoft Active Directory	Oui
Choix d'emplacements des ressources	Oui
Déploiement sur site	Oui
Virtual Apps and Desktops Service	Ensemble complet de fonctionnalités
Endpoint Management*	Ensemble complet de fonctionnalités
Secure Document Service*	Ensemble complet de fonctionnalités
Smart Tools	Ensemble complet de fonctionnalités
Personnalisable	Oui

*Version d'évaluation non disponible actuellement.

Demander une version d'évaluation de service



Pour demander une version d'évaluation, connectez-vous à votre compte Citrix Cloud. À partir de la

console de gestion, cliquez sur **Demander évaluation** pour le service que vous voulez tester. Une fois votre demande envoyée, le libellé du bouton devient **Version d'évaluation demandée**.

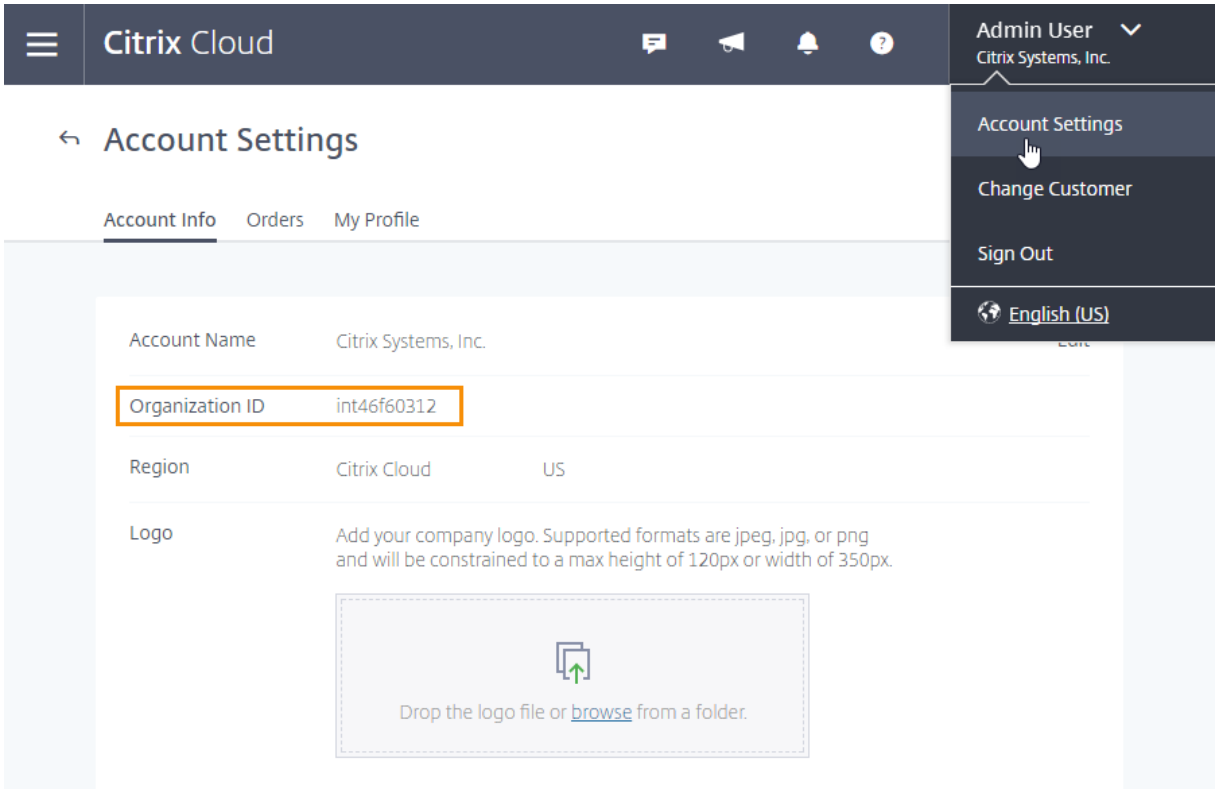
Lorsque votre version d'évaluation est approuvée et prête à être utilisée, vous recevrez une notification par e-mail. Vous avez 60 jours pour utiliser la version d'évaluation.

Remarque : pour garantir la meilleure expérience possible pour ses clients, Citrix se réserve le droit de limiter les évaluations à un certain nombre de participants à la fois.

Acheter des services Citrix Cloud

Lorsque vous êtes prêt à convertir votre version d'évaluation en service de production, consultez la page https://www.citrix.com/products/citrix-cloud/buy.html.

Pour procéder à l'achat, vous aurez besoin de votre ID d'organisation, disponible dans la console de gestion Citrix Cloud.



Important : si vous n'achetez pas avant la fin de votre période d'évaluation de 60 jours, le service prend fin et Citrix archive toutes les données et tous les paramètres pendant 90 jours. Si vous achetez au cours de la période de 90 jours, votre version d'évaluation est réactivée et convertie en service de production.

Prolonger les abonnements aux services de Citrix Cloud

August 1, 2018

Cet article décrit les notifications d'expiration aux services de Citrix Cloud et comment prolonger votre abonnement.

Avant l'expiration

Lorsque l'abonnement à votre service se rapproche de la date d'expiration, Citrix Cloud vous en informe à certains intervalles de façon à ce que vous puissiez prolonger l'abonnement et éviter les interruptions de service. Les notifications suivantes apparaissent dans la console de gestion de Citrix Cloud :

- 90 jours avant l'expiration : une bannière jaune s'affiche, indiquant les services à prolonger et leurs dates d'expiration. Cette notification apparaît dans la console tous les 7 jours ou jusqu'à ce que le service soit prolongé.
- 7 jours avant l'expiration : une bannière rouge s'affiche, indiquant les services à prolonger et leurs dates d'expiration. Cette notification apparaît dans la console jusqu'à ce que le service soit prolongé ou que la période de grâce de 30 jours expire.

Vous pouvez ignorer ces notifications lorsqu'elles apparaissent. Cependant, elles réapparaîtront après sept jours.

Citrix vous envoie également une notification par e-mail contenant une liste des services à prolonger et leurs dates d'expiration. Citrix envoie cette notification aux intervalles suivants :

- 90 jours avant l'expiration
- 60 jours avant l'expiration
- 30 jours avant l'expiration
- Sept jours avant l'expiration
- Un jour avant l'expiration

Après l'expiration : périodes de grâce du service

Lorsque l'abonnement au service expire, Citrix vous permet de continuer à accéder au service pendant 30 jours. Cette période de grâce vous offre un délai supplémentaire pour prolonger le service sans perdre l'accès immédiatement. Si vous choisissez de ne pas prolonger le service, cette période de grâce vous permet de migrer vos utilisateurs hors du service et de supprimer les données que vous avez ajoutées au service.

Si vous ne prolongez pas votre abonnement pendant cette période, Citrix empêche les administrateurs et les utilisateurs d'accéder au service. Pour rappel, Citrix vous envoie une notification par e-mail aux intervalles suivants :

- 15 jours après l'expiration (15 jours avant le blocage du service)
- 22 jours après l'expiration (sept jours avant le blocage du service)
- 29 jours après l'expiration (un jour avant le blocage du service)

La notification par e-mail inclut une liste des services ayant expiré et leurs dates d'expiration.

Si vous prolongez votre abonnement durant cette période de grâce, les modalités de l'abonnement commencent à la date d'expiration initiale du service. Par exemple, si le service expire le 30 mai et que vous prolongez votre abonnement le 25 juin (avant la fin de la période de grâce), votre abonnement prolongé débute le 30 mai.

Après l'expiration : blocage du service et rétention des données

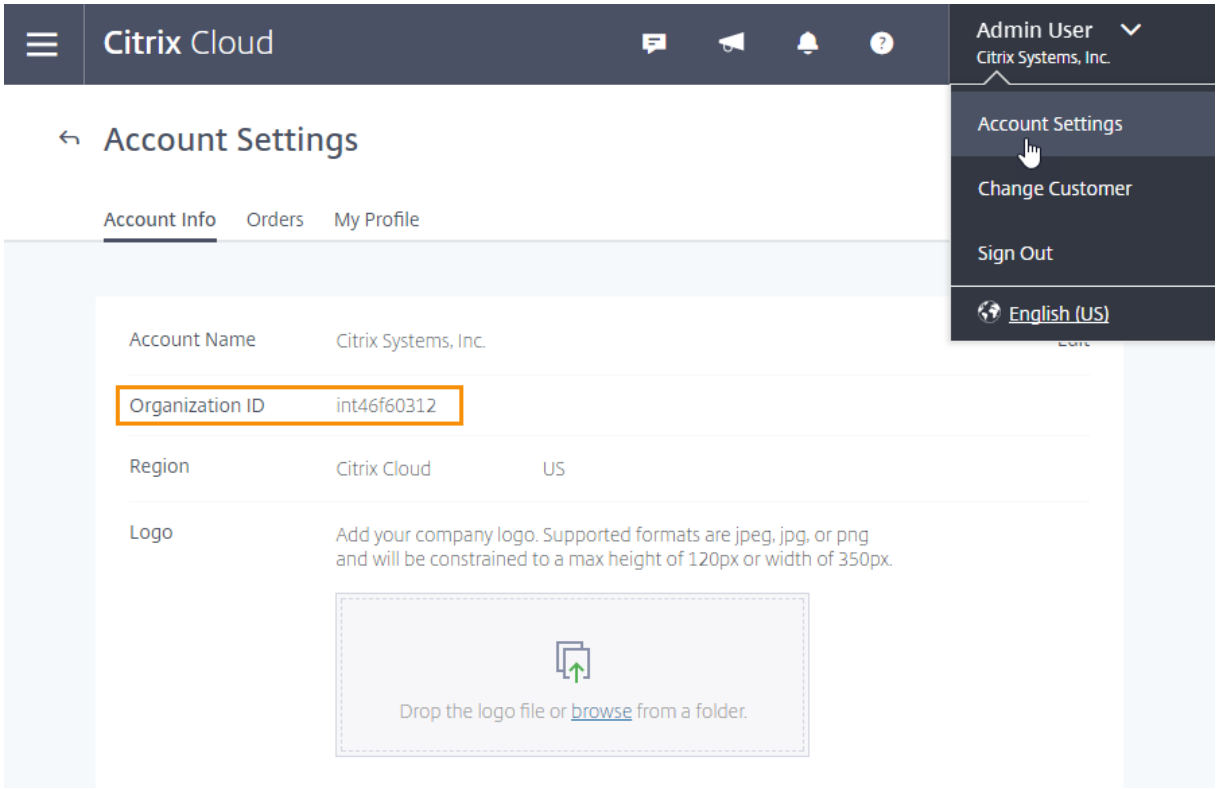
Une fois la période de grâce de 30 jours écoulée, Citrix empêche les administrateurs et les utilisateurs d'accéder au service. Toutes les données que vous avez ajoutées au service sont conservées pendant 90 jours. Si vous prolongez votre abonnement avant la fin de la période de rétention de 90 jours, vos administrateurs et vos utilisateurs peuvent accéder au service et les données sont préservées. La date de début de votre abonnement prolongé est la date à laquelle vous avez acheté l'extension.

Si vous ne prolongez pas votre abonnement avant la fin de la période de 90 jours, Citrix réinitialise le service et supprime les données que vous avez ajoutées.

Acheter des extensions de service

Pour prolonger votre abonnement aux services de Citrix Cloud, accédez à https://www.citrix.com/products/citrix-cloud/buy.html.

Pour procéder à l'achat, vous aurez besoin de votre ID d'organisation, disponible dans la console de gestion Citrix Cloud.



Ouvrir un compte Citrix Cloud

November 7, 2018

Cet article vous guide tout au long du processus d'inscription à Citrix Cloud et d'exécution des tâches requises pour intégrer votre compte avec succès.

Qu'est-ce qu'un compte Citrix ?

Un compte Citrix, également appelé compte Citrix.com ou compte My Citrix, vous permet de gérer l'accès aux licences que vous avez achetées. Votre compte Citrix utilise un ID d'organisation (OrgID) comme identifiant unique. Vous pouvez accéder à votre compte Citrix en vous connectant à https://www.citrix.com avec un nom d'utilisateur (également connu sous le nom de connexion Web) ou votre adresse e-mail, si l'une de ces options est associée à votre compte.

Important : un nom d'utilisateur est associé à un seul compte Citrix, mais une adresse e-mail peut être associée à plusieurs comptes Citrix.

Qu'est-ce qu'un OrgID ?

Un OrgID est l'identifiant unique attribué à votre compte Citrix. Votre OrgID est associé à une adresse de site physique, généralement l'adresse professionnelle de votre entreprise. C'est la raison pour laquelle les entreprises disposent généralement d'un seul OrgID. Cependant, dans certains cas, par exemple, comme avec des succursales ou si différents départements gèrent leurs ressources séparément, Citrix peut permettre à une seule entreprise d'avoir plusieurs OrgID.

Citrix nettoie régulièrement certains OrgID, en fusionnant les doublons dans certains cas. Si votre entreprise dispose de plusieurs OrgID que vous souhaitez fusionner avec un OrgID valide et actif, vous pouvez contacter le service clientèle de Citrix avec les OrgID que vous souhaitez fusionner.

Remarque : les entreprises ont déjà configuré des OrgID en fonction de la façon dont elles souhaitent gérer leurs ressources. Par conséquent, si vous ne savez pas quel OrgID vous devez utiliser ou de combien d'OrgID vous disposez, contactez le service informatique ou l'administrateur Citrix de votre société. Si vous avez besoin d'aide, le service clientèle Citrix peut également vous aider à localiser un OrgID. Vous pouvez contacter le service clientèle de Citrix à l'adresse https://www.citrix.com/contact/support.html.

Qu'est-ce qu'un compte Citrix Cloud ?

Un compte Citrix Cloud vous permet d'utiliser un ou plusieurs services Citrix Cloud de façon à pouvoir distribuer vos applications et vos données en toute sécurité. Un compte Citrix Cloud est également identifié de manière unique par un OrgID, tout comme votre compte Citrix. Il est important d'utiliser le compte Citrix Cloud adéquat, en fonction de la manière dont votre organisation a configuré les OrgID, afin que vos achats et l'accès administrateur puissent continuer à utiliser les mêmes OrgID. Par exemple, si le service de conception d'une société utilisant l'OrgID 1234 utilise une installation sur site de Virtual Apps and Desktops et veut essayer Citrix Cloud, l'un des administrateurs de l'OrgID 1234 doit s'inscrire auprès de Citrix Cloud sur cet OrgID en utilisant une connexion Web ou une adresse e-mail associée à cet OrgID. Ainsi, lorsque la société décide d'acheter un abonnement Virtual Apps and Desktops, la commande peut être placée sur l'OrgID 1234 et la transition est fluide.

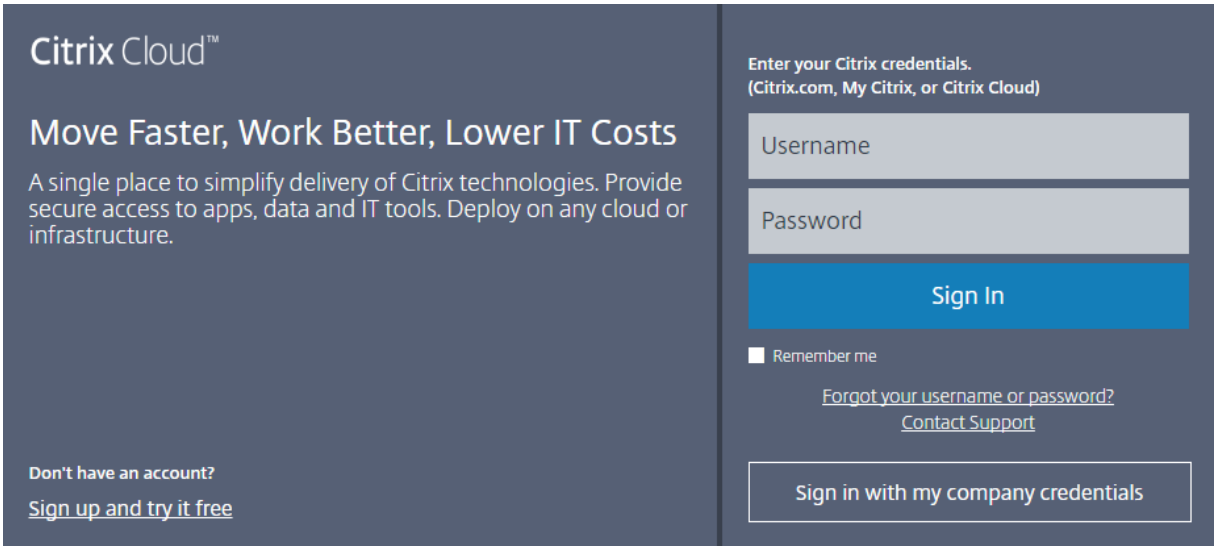
Important : les utilisateurs ayant accès à un compte Citrix particulier n'ont pas automatiquement accès au compte Citrix Cloud associé à l'OrgID de ce compte Citrix. Étant donné que l'accès Citrix Cloud permet aux utilisateurs d'avoir un impact potentiel sur le service, il est important de contrôler qui accède au compte Citrix Cloud.

S’inscrire en tant que client Citrix existant et en tant que nouveau client sur Citrix Cloud

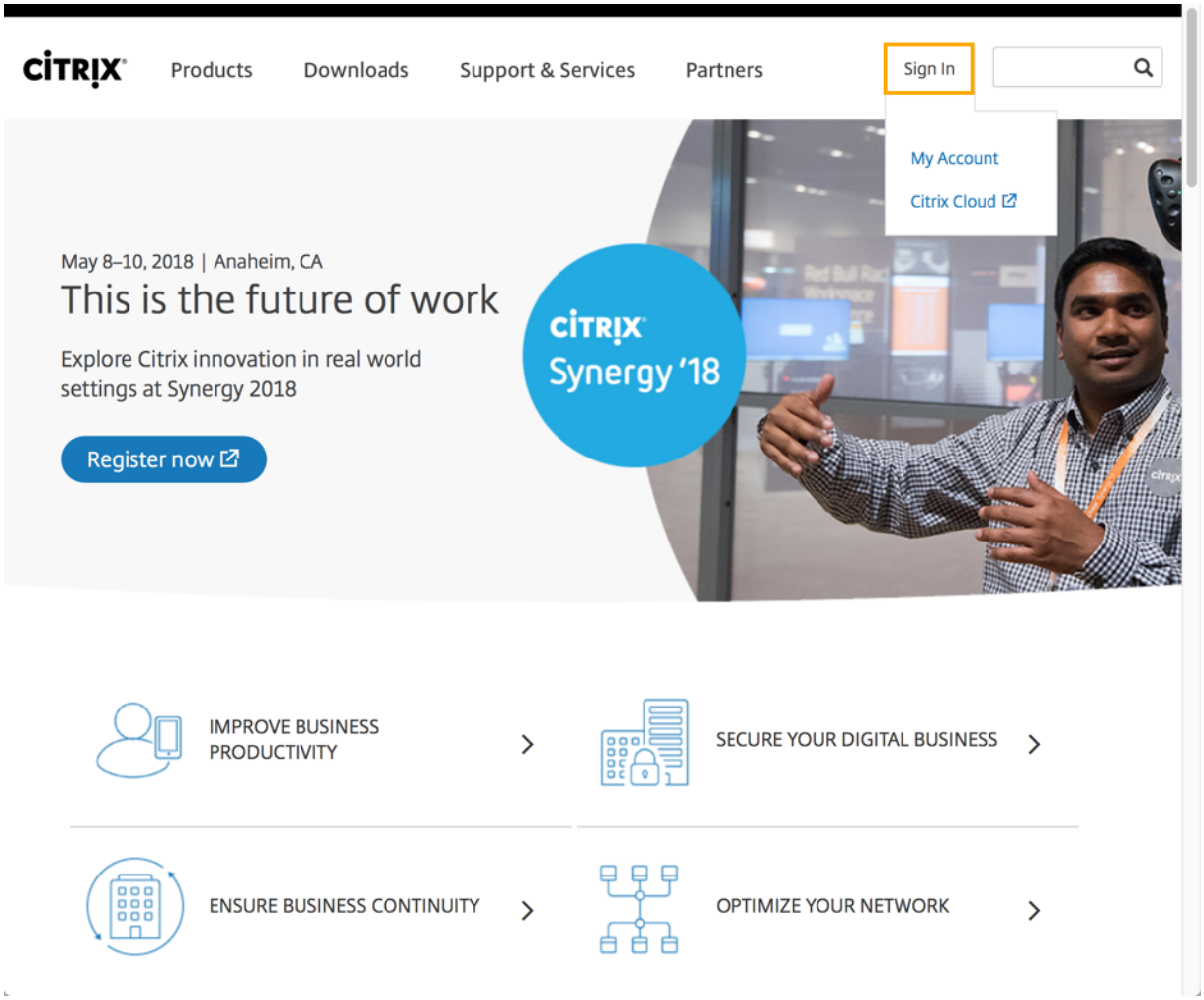
En tant que client Citrix existant, cette section vous aide à créer un compte Citrix Cloud en utilisant l’OrgID approprié afin que vous puissiez continuer à passer des commandes sur les mêmes OrgID que vous avez utilisés, sans modifier la configuration des administrateurs Citrix dans votre société.

Étape 1 : Connectez-vous avec vos informations d’identification Citrix.com pour créer un compte Citrix Cloud

Accédez à https://citrix.cloud.com et connectez-vous à votre compte Citrix Cloud existant. Ce compte est également appelé compte Citrix.com ou My Citrix.



C’est le même compte que celui que vous utilisez pour vous connecter sur Citrix.com. Vous utilisez soit un nom d’utilisateur (également appelé connexion Web) et un mot de passe, soit une adresse e-mail et un mot de passe.

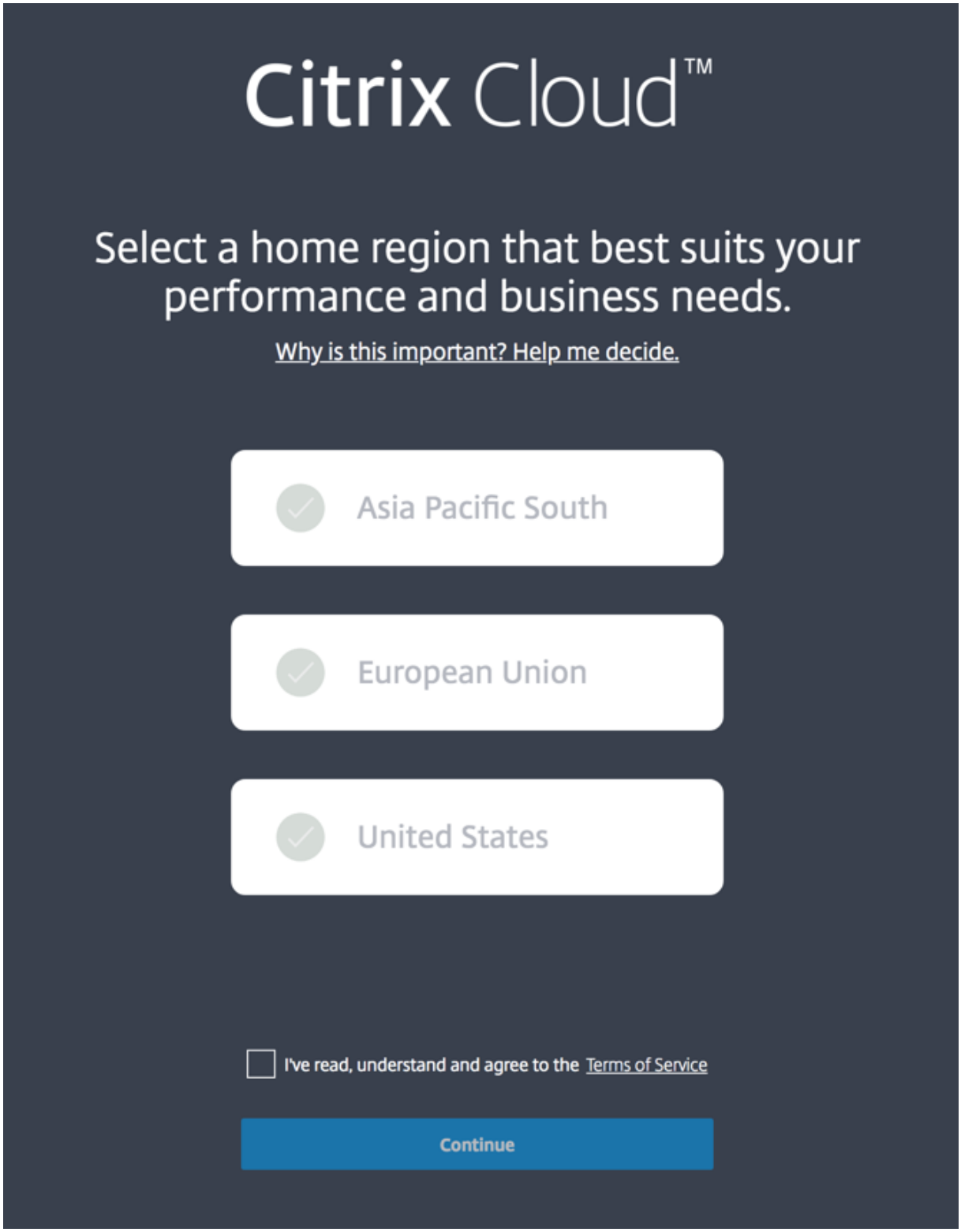


Que se passe-t-il si le compte est déjà utilisé ?

Si vous voyez ce message, cela signifie qu'un autre administrateur de votre compte Citrix a déjà créé le compte Citrix Cloud.

Étant donné qu'un compte Citrix Cloud offre aux administrateurs un plus grand contrôle sur le service, le premier administrateur qui crée le compte Citrix Cloud doit explicitement donner accès à un autre administrateur, même si l'autre administrateur est déjà membre du compte Citrix.

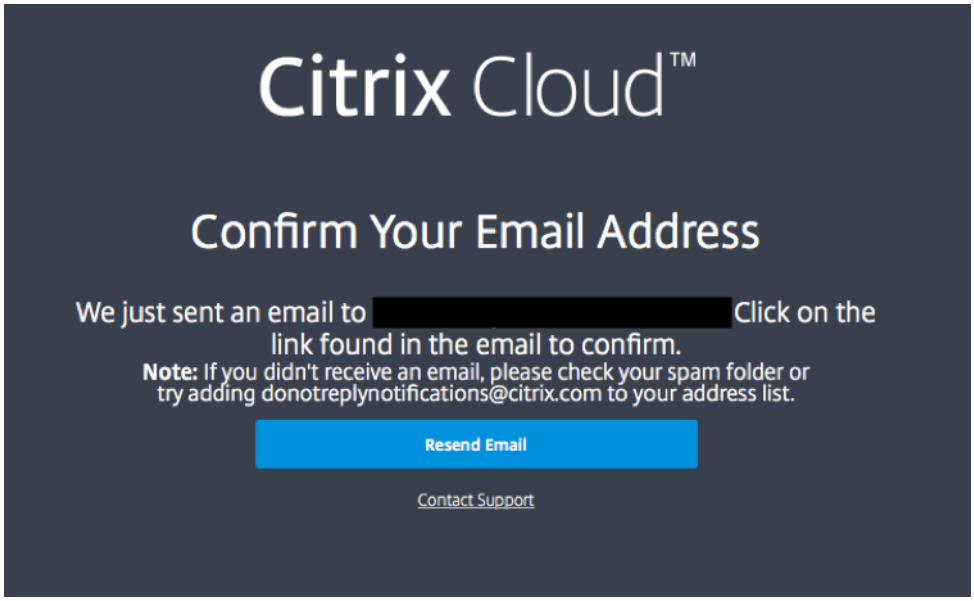
Étape 2 : Choisissez votre région Citrix Cloud



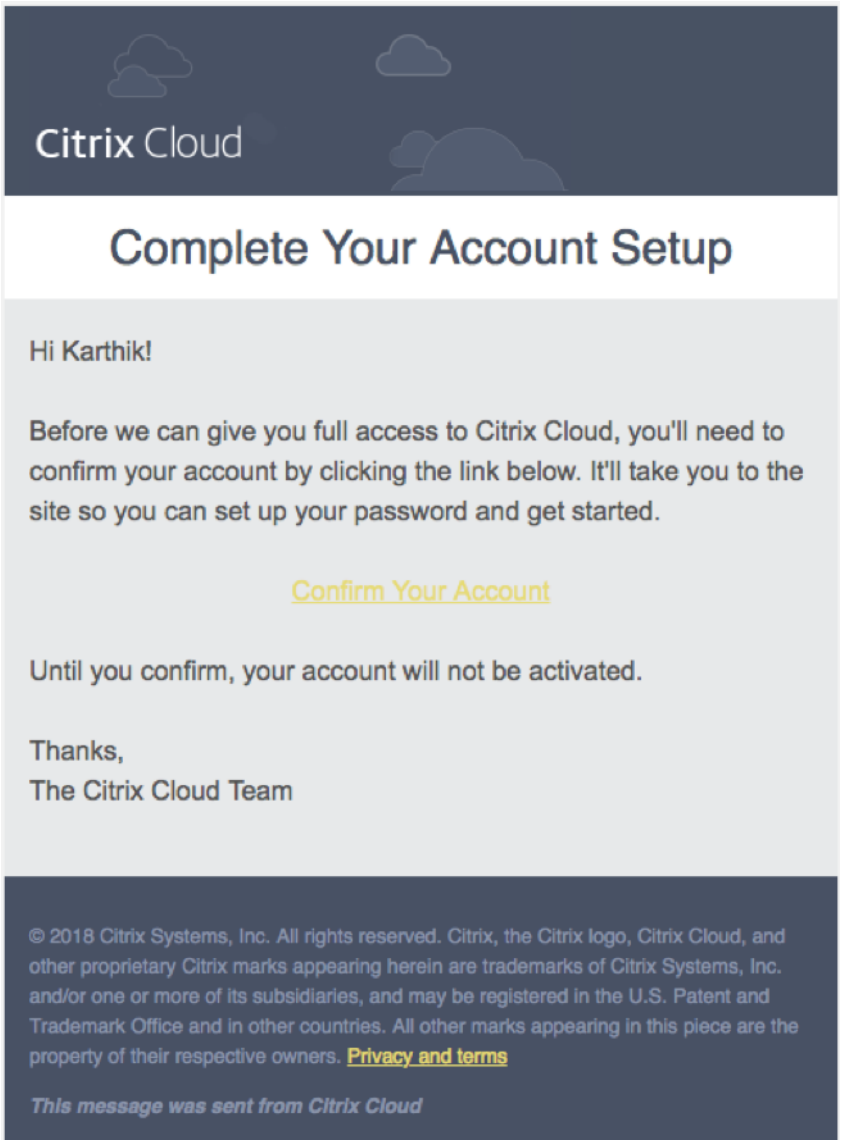
Une région Citrix Cloud est une limite géographique dans laquelle Citrix exploite, stocke et réplique

des services et des données dans le but de mettre à disposition des services Citrix Cloud. Citrix peut utiliser plusieurs clouds publics ou privés situés dans un ou plusieurs pays au sein de la région, y compris des états et des provinces, pour fournir des services. Pour plus d'informations sur les régions de Cloud Citrix, reportez-vous à la section Considérations géographiques.

Étape 3 : Vérifiez votre adresse e-mail



Si vous n'avez pas vérifié votre adresse e-mail, vous pouvez être invité à la valider. Voici un exemple du message que vous recevrez :



Après avoir reçu l'e-mail de vérification et confirmé votre adresse e-mail, votre compte Citrix Cloud est actif.

Étape 4 : Confirmez votre OrgID et invitez des administrateurs

Félicitations, vous avez configuré votre compte Citrix Cloud ! Avant de commencer à utiliser Citrix Cloud, prenez le temps de vérifier votre OrgID et d'inviter d'autres administrateurs pour vous aider à gérer votre compte Citrix Cloud.

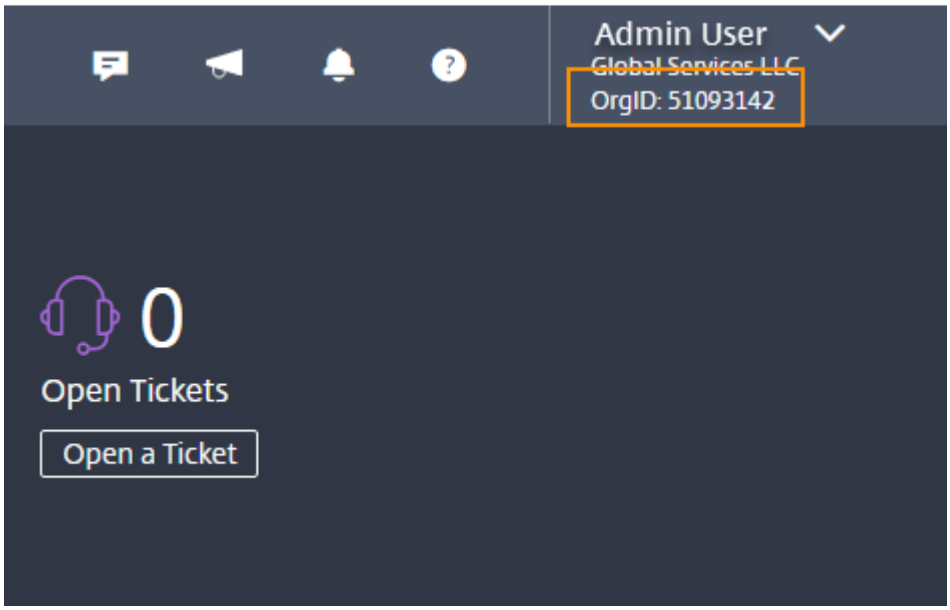
Vérifier l'OrgID de votre compte

Assurez-vous que l'OrgID de votre compte correspond à l'OrgID que vous utilisez pour passer des commandes. L'un des avantages de Citrix Cloud est que si vous testez un service (tel que Virtual Apps and

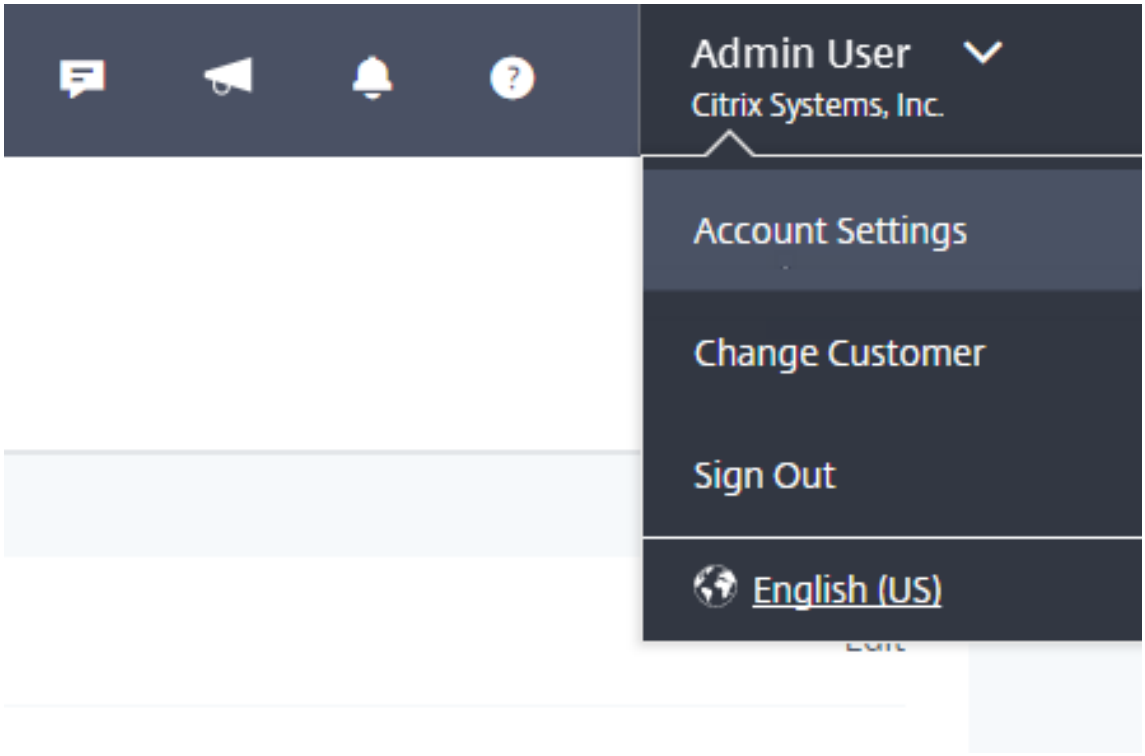
Desktops Service) et décidez de l'acheter, toutes les configurations que vous avez effectuées dans la version d'évaluation sont conservées dans le service acheté, car l'achat s'effectue sous le même compte. Donc, vous assurer que l'évaluation commence avec l'OrgID correct permet de vous faire gagner du temps lorsque vous décidez d'acheter.

Pour vérifier votre OrgID, utilisez l'une des méthodes suivantes :

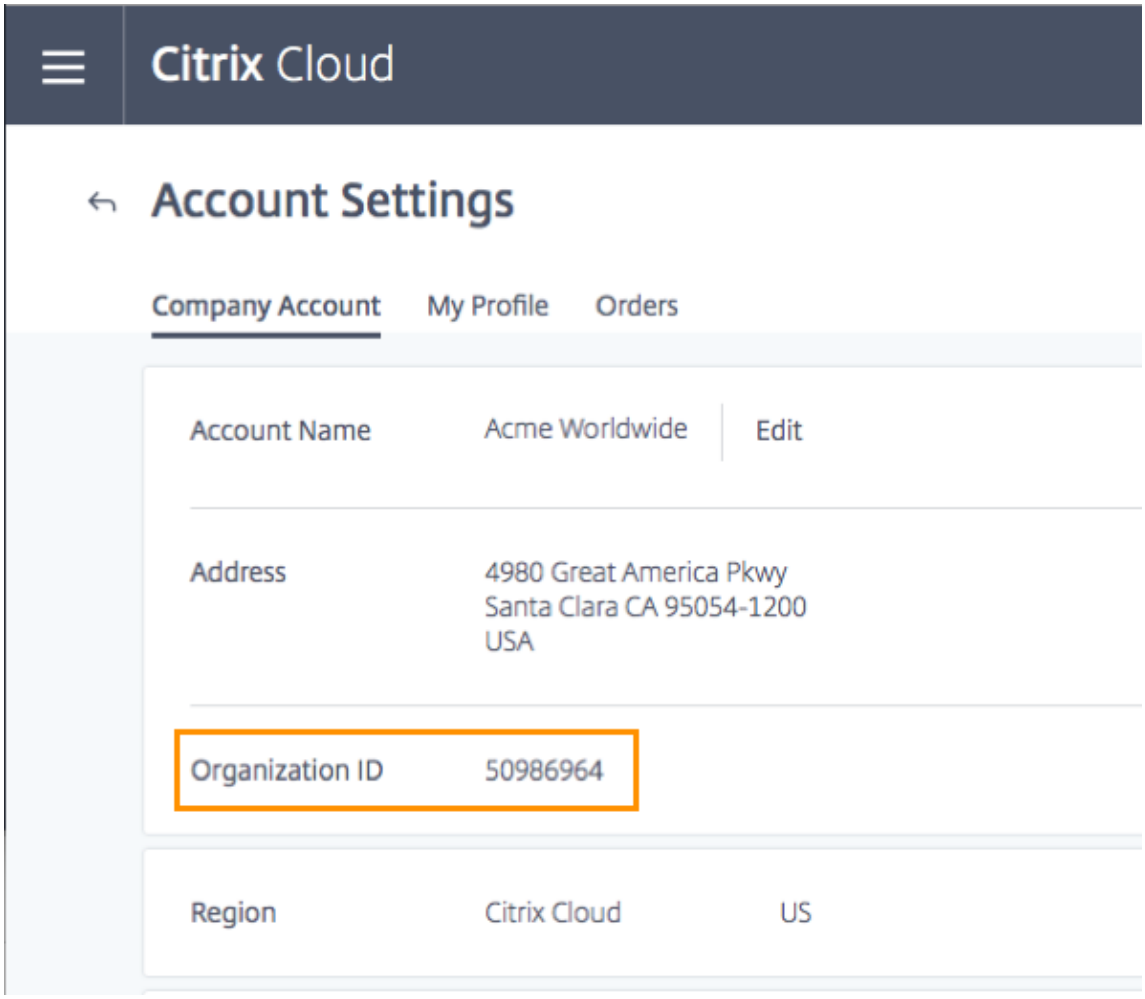
- Dans le coin supérieur droit de la console de gestion, votre OrgID est affiché sous le nom de votre compte.



- Cliquez sur **Paramètres du compte** dans le menu en haut à droite.

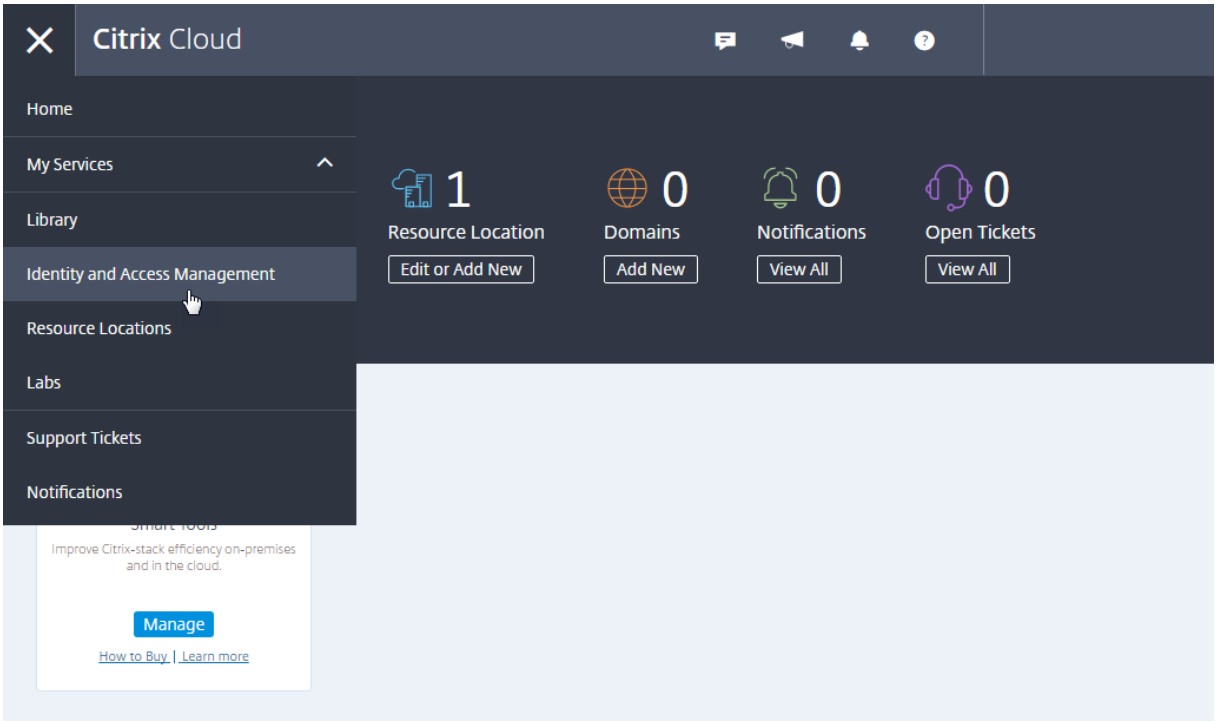


Votre OrgID est affiché dans le champ ID d'organisation.



Inviter un ou plusieurs administrateurs

N'oubliez pas que même si vos autres administrateurs ont accès à votre compte Citrix sur Citrix.com, vous devez quand même les inviter au compte Citrix Cloud. Pour ce faire, dans la console de gestion Citrix Cloud, cliquez sur le bouton de menu dans le coin supérieur gauche et sélectionnez **Gestion des identités et des accès**. Pour de plus amples informations, consultez la section Ajouter des administrateurs à un compte Citrix Cloud.

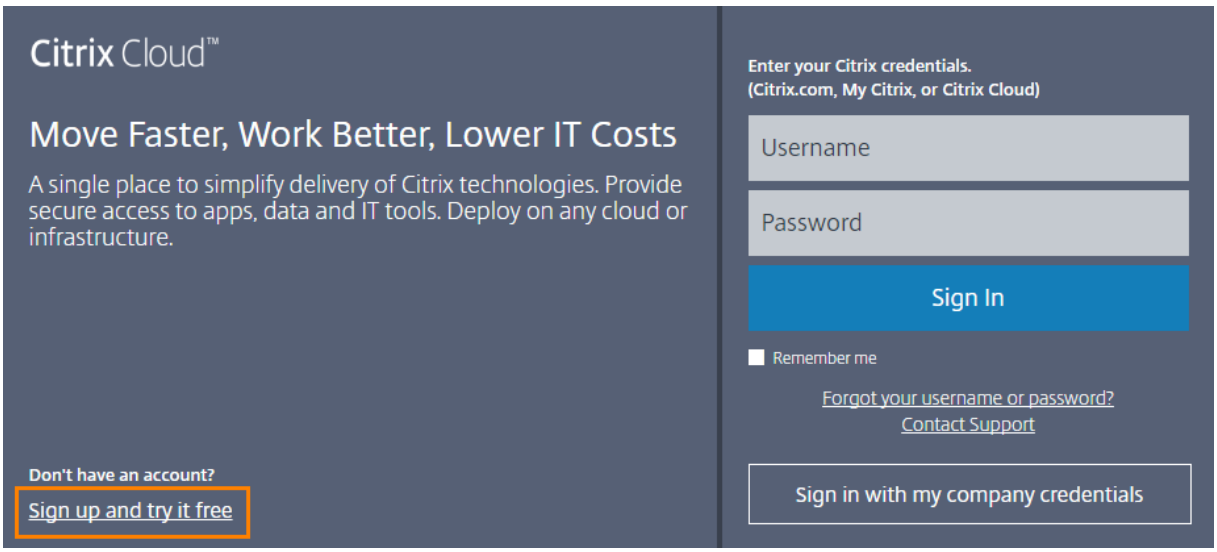


S’inscrire en tant que nouveau client Citrix

Si vous débutez avec Citrix et Citrix Cloud, cette section vous permet de créer un nouveau compte Citrix Cloud et de le configurer.

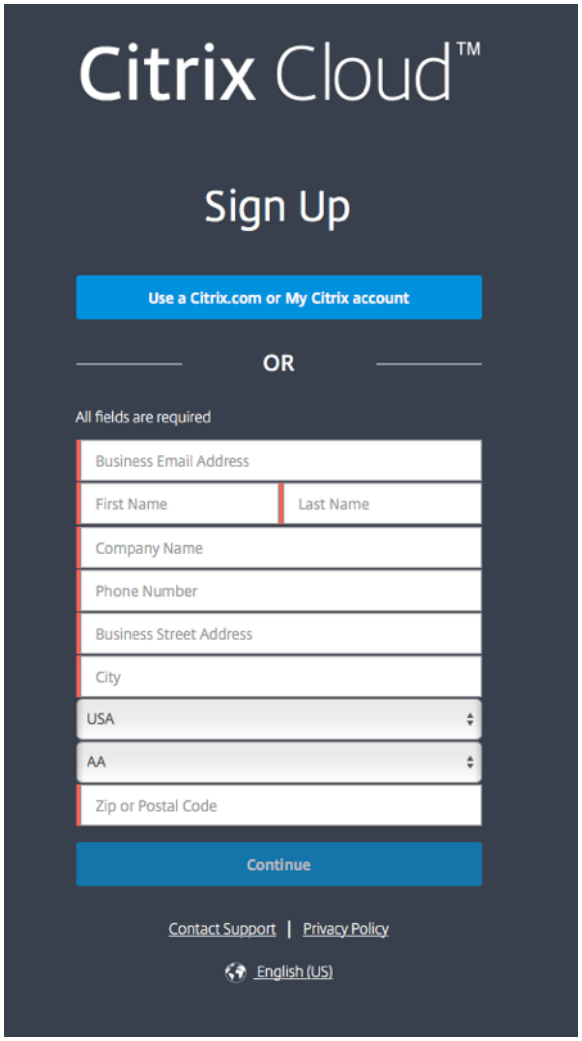
Étape 1 : Cliquez pour ouvrir un nouveau compte

Accédez à `https://citrix.cloud.com` et cliquez sur **Inscrivez-vous pour un essai gratuit**.



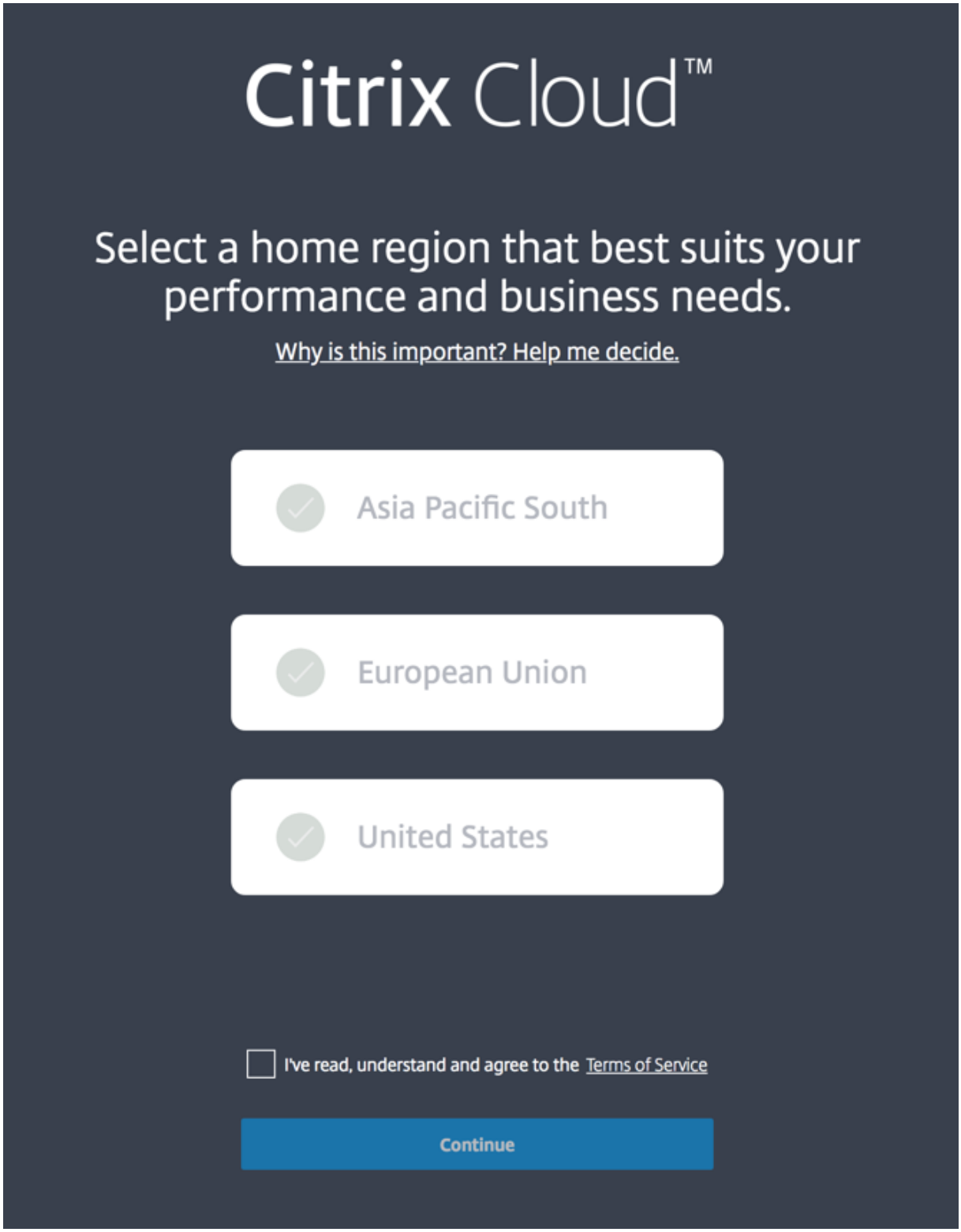
Étape 2 : Remplissez le formulaire d'inscription

Renseignez tous les champs et cliquez sur **Continuer**. N'oubliez pas d'utiliser votre adresse e-mail professionnelle et votre adresse professionnelle. L'utilisation d'une adresse e-mail personnelle ou d'une adresse personnelle peut entraîner des retards lors de la demande de versions d'évaluation.

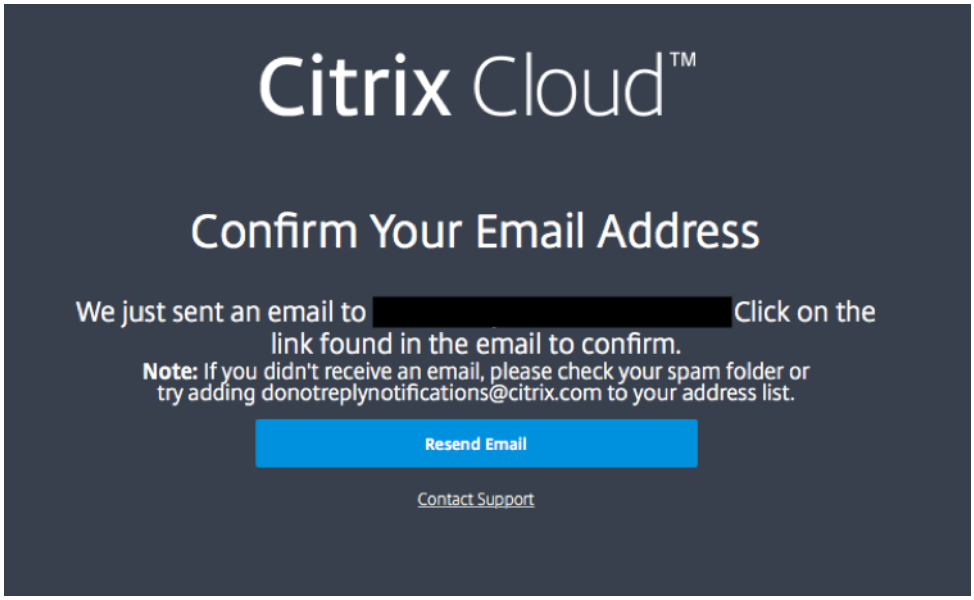


Étape 3 : Choisissez votre région Citrix Cloud

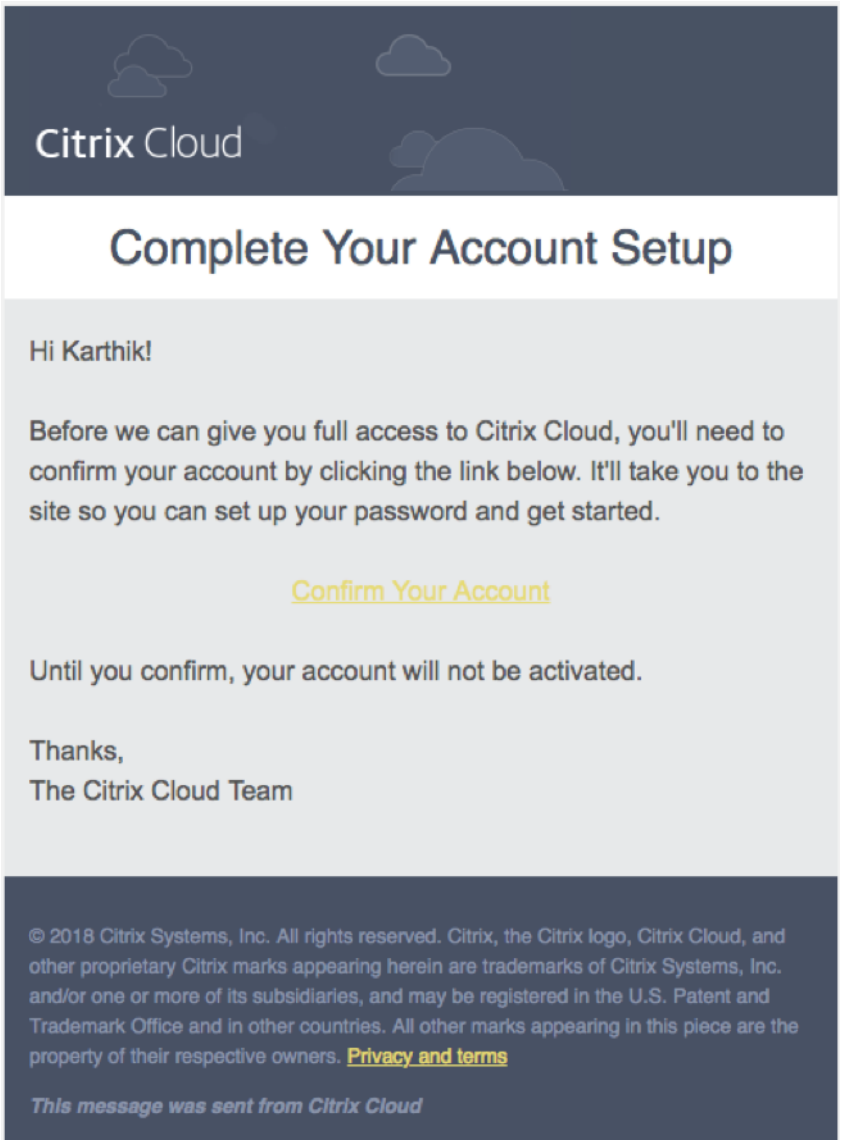
Une région Citrix Cloud est une limite géographique dans laquelle Citrix peut exploiter, stocker et répliquer des services et des données dans le but de mettre à disposition des services Citrix Cloud. Citrix peut utiliser plusieurs clouds publics ou privés situés dans un ou plusieurs pays de la région, y compris des états et des provinces, pour fournir des services. Pour plus d'informations sur les régions de Cloud Citrix, reportez-vous à la section Considérations géographiques.



Étape 4 : Vérifiez votre adresse e-mail



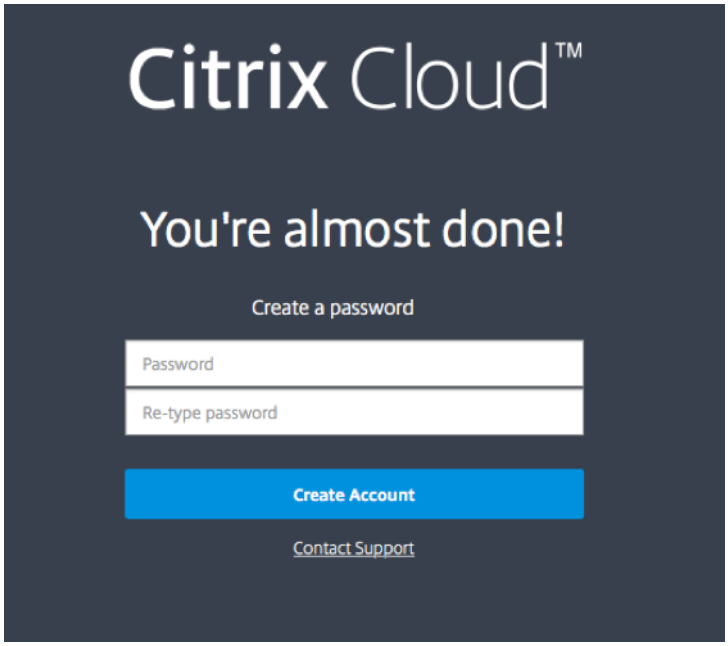
Si vous n’avez pas vérifié votre adresse e-mail, vous pouvez être invité à la valider.



Après avoir reçu l'e-mail de vérification et confirmé votre adresse e-mail, votre compte Citrix Cloud est actif.

Étape 5 : Choisissez un mot de passe

Tapez et confirmez votre mot de passe Citrix Cloud pour terminer la création de votre compte.

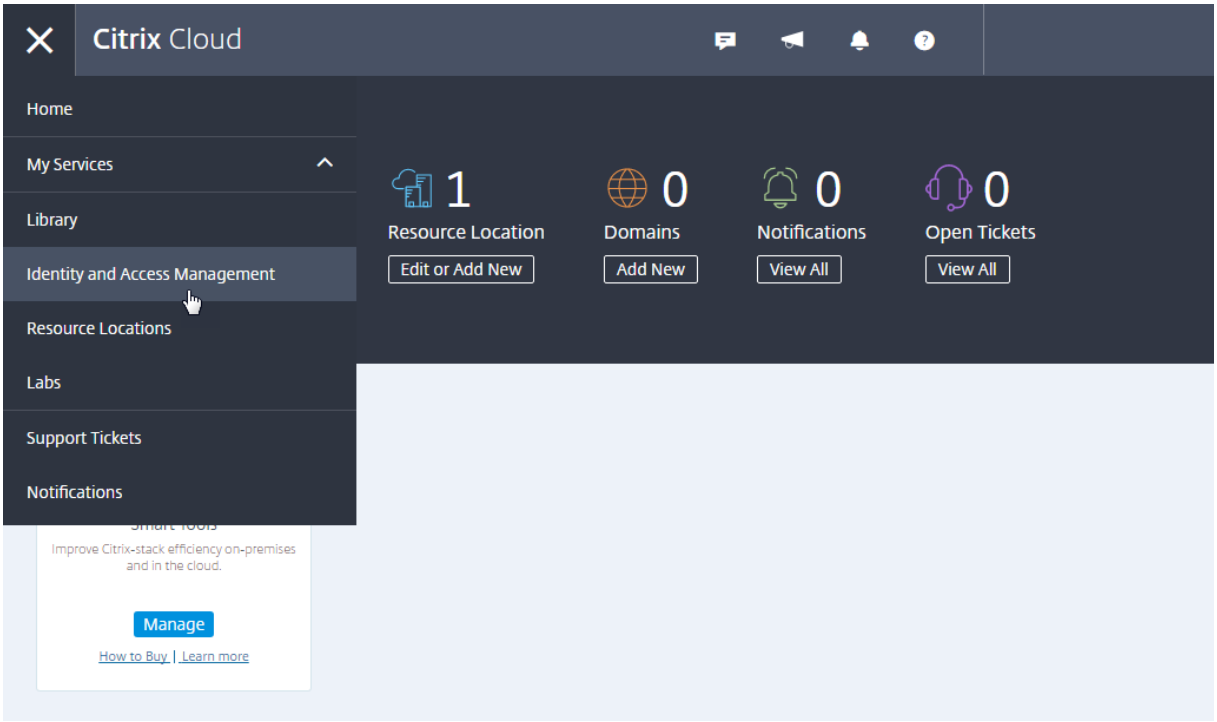


Une fois votre compte créé, vous pouvez vous connecter à Citrix Cloud.

Étape 6 : Invitez des administrateurs

Félicitations, vous avez configuré votre compte Citrix Cloud ! Avant de commencer à utiliser Citrix Cloud, prenez le temps d'inviter au moins un autre administrateur pour vous aider à gérer votre compte Citrix Cloud.

Pour ce faire, dans la console de gestion Citrix Cloud, cliquez sur le bouton de menu et sélectionnez **Gestion des identités et des accès**. Pour de plus amples informations, consultez la section Ajouter des administrateurs à un compte Citrix Cloud.



Demander des versions d'évaluation pour les services de Citrix Cloud

Les évaluations sont conçues pour être testées avec une infrastructure locale ou un cloud public de votre choix, vos applications et votre Microsoft Active Directory. Vous pouvez créer et configurer des services, des espaces de travail et des emplacements de ressources.

Au cours de votre évaluation, si vous décidez d'acheter un abonnement, vous pouvez le faire à tout moment. Toutes vos configurations existantes sont sauvegardées et disponibles pour vous permettre de continuer à utiliser le service sans interruptions.

Pour demander une version d'évaluation, cliquez sur Demander évaluation pour le service que vous souhaitez tester. Pour de plus amples informations, consultez la section Évaluations de services Citrix Cloud.

Considérations géographiques

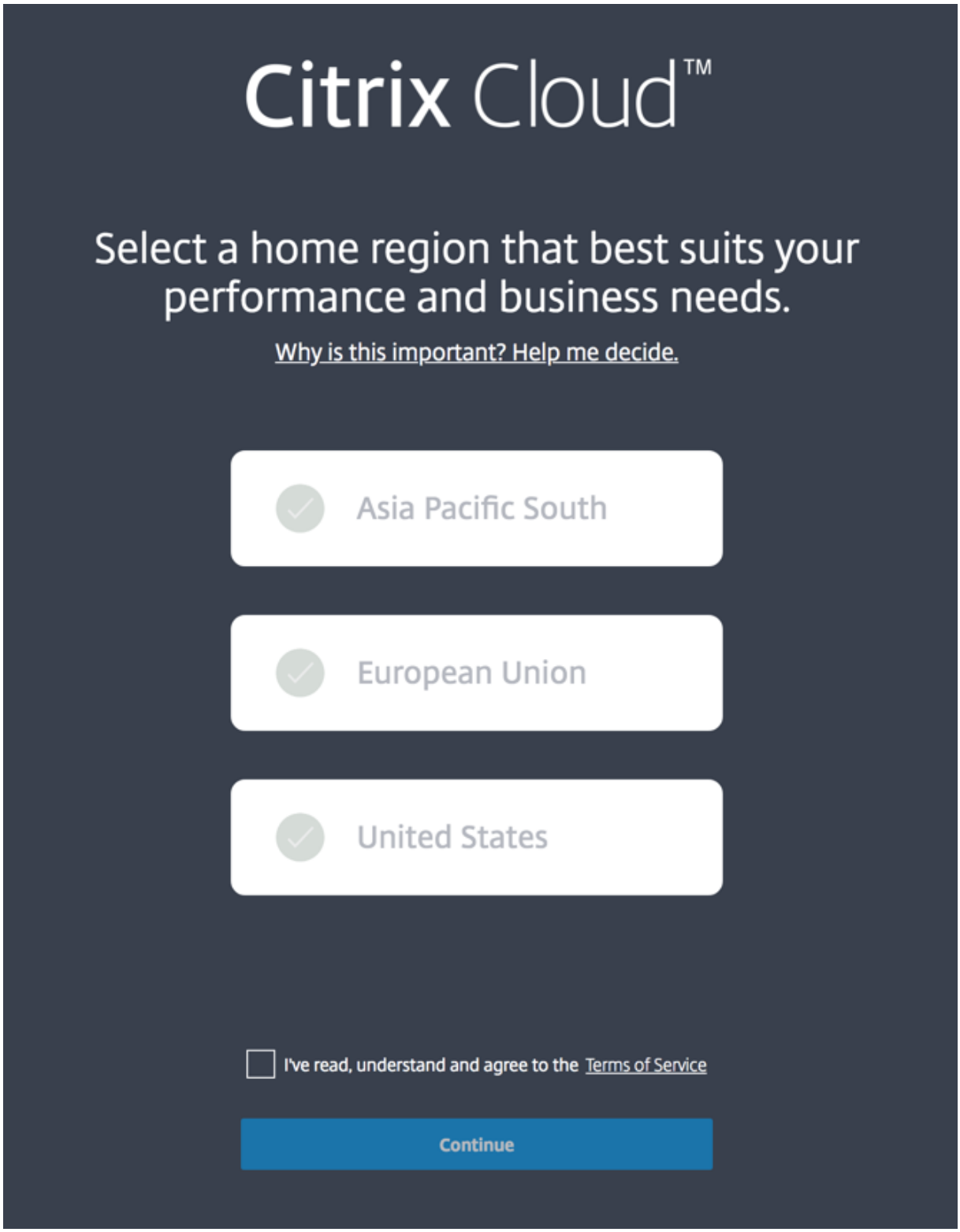
November 7, 2018

Lorsque votre organisation est intégrée à Citrix Cloud et que vous vous connectez pour la première fois, vous êtes invité à choisir l'une des régions suivantes :

- États-Unis
- Union européenne

- Asie Pacifique Sud

Choisissez une région qui correspond à l'emplacement de la plupart de vos utilisateurs et ressources.



Important : le choix de la région s'effectue une seule fois, au moment où votre organisation est intégrée. Vous ne pourrez pas modifier votre région plus tard.

Types de données stockées dans les régions

Votre région correspond à l'emplacement où sont stockées certaines métadonnées concernant votre environnement. Par exemple :

- Détails de l'administrateur de Citrix Cloud, y compris le nom, le nom d'utilisateur et le mot de passe.
- Données résultant du trafic dirigé via votre région par tout Citrix Cloud Connector que vous installez. Par exemple, les données d'authentification utilisant vos contrôleurs de domaine (qu'ils soient gérés sur votre site ou au travers de votre abonnement auprès d'un fournisseur de cloud public) restent dans votre région.
- Données utilisées pour mapper les utilisateurs avec les offres de la bibliothèque. Par exemple, si vous ajoutez Microsoft Office à votre bibliothèque sous forme d'offre pour vos utilisateurs, puis ajoutez cinq utilisateurs à cette offre en tant qu'abonnés, les données liant chaque utilisateur à cette offre (telles que le nom d'utilisateur et le nom de domaine) sont stockées dans votre région.
- Données sur les utilisateurs pour les services disponibles dans votre région. Par exemple, si vous utilisez Endpoint Management dans votre région, les données telles que le nom, l'adresse et le numéro de téléphone sont stockées dans votre région.

Disponibilité du service dans chaque région

Tous les services sont disponibles dans le monde entier, quelle que soit la région sélectionnée pour votre organisation. Certains services, tels que Virtual Apps and Desktops Service, ont des instances régionales dédiées. Cependant, certains services disposent uniquement d'instances basées aux États-Unis.

Dans le cas où un service se situe dans une région différente de celle que vous avez sélectionnée pour votre organisation, certaines informations (telles que les données d'authentification) peuvent être transférées d'une région à l'autre si nécessaire.

Lorsqu'un service est répliqué globalement, toutes les données de ce service sont stockées dans toutes les régions.

Service	États-Unis	UE	Asie Pacifique Sud
Plan de contrôle Citrix Cloud	Oui	Oui	Oui

Service	États-Unis	UE	Asie Pacifique Sud
Citrix Analytics	Oui	Non (Utilise la région États-Unis)	Non (Utilise la région États-Unis)
Citrix App Layering	Oui	Non (Utilise la région États-Unis)	Non (Utilise la région États-Unis)
Application Delivery Management	Oui	Non (Utilise la région États-Unis)	Non (Utilise la région États-Unis)
Citrix Content Collaboration	Oui ***	Oui ***	Non - Sélectionnez États-Unis ou UE **
Citrix Endpoint Management	Oui **	Oui **	Oui **
SD-WAN Zero-Touch Deployment	Oui	Non (Utilise la région États-Unis)	Non (Utilise la région États-Unis)
Secure Browser Service	Oui *	Oui *	Oui *
Citrix Smart Tools	Oui	Non (Utilise la région États-Unis)	Non (Utilise la région États-Unis)
Citrix Virtual Apps and Desktops Service	Oui *	Oui *	Oui *
Citrix Virtual Apps Essentials	Oui *	Oui *	Oui *
Citrix Virtual Desktops Essentials	Oui *	Oui *	Oui *
Web App Firewall	Oui	Oui	Non (Utilise la région États-Unis)
Citrix Workspace	Oui *	Oui *	Oui *
Workspace Environment Management	Oui	Non (Utilise la région États-Unis)	Non (Utilise la région États-Unis)
Citrix Cloud Labs Services	Oui	Non (Utilise la région États-Unis)	Non (Utilise la région États-Unis)
Services de réseau	Oui	Non (Utilise la région États-Unis)	Non (Utilise la région États-Unis)

Service	États-Unis	UE	Asie Pacifique Sud
License Usage Insights (CSP uniquement)	Réplication globale	Réplication globale	Réplication globale
Nœuds d'accès Citrix Gateway/POP	Plusieurs nœuds au niveau global ; trafic routé selon les besoins pour assurer la meilleure expérience	Plusieurs nœuds au niveau global ; trafic routé selon les besoins pour assurer la meilleure expérience	Plusieurs nœuds au niveau global ; trafic routé selon les besoins pour assurer la meilleure expérience

⋆ Le service utilise la région Citrix Cloud.

⋆⋆ Sélectionnez parmi plusieurs emplacements dans plusieurs régions. Veuillez consulter la section ci-dessous.

⋆⋆⋆ StorageZone peut être sélectionné à partir de plusieurs emplacements. Veuillez consulter la section ci-dessous.

Pour plus d'informations sur les données stockées par les différents services, reportez-vous à la page Vue d'ensemble de la sécurité technique de chaque service.

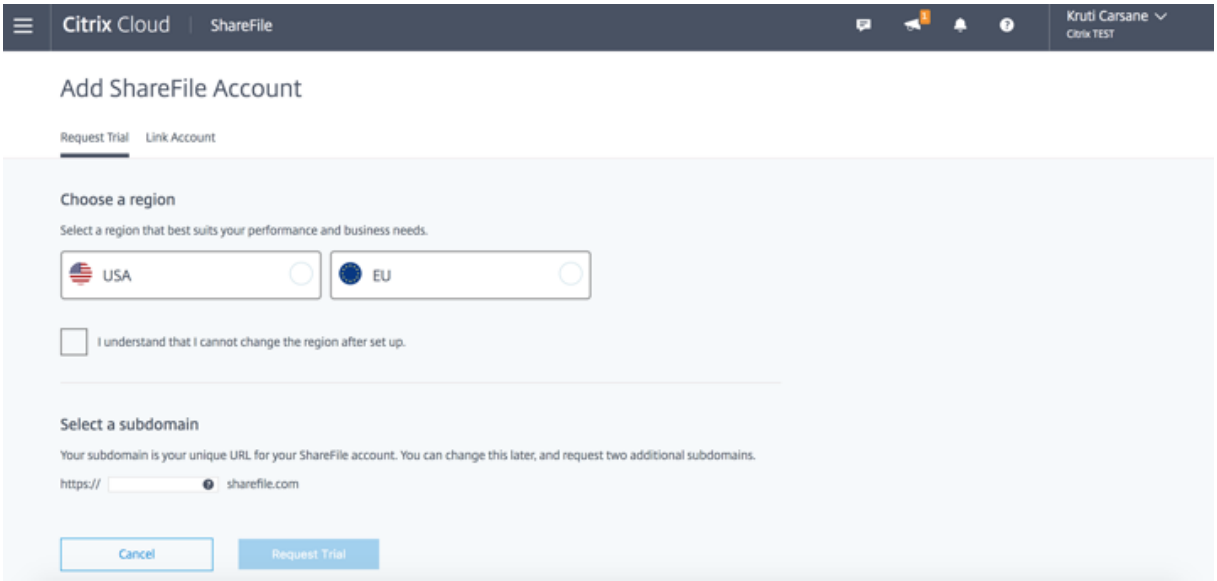
Emplacements de Endpoint Management Service

Vous pouvez sélectionner l'un des emplacements Endpoint Management Service suivants depuis votre région d'origine :

- Est des États-Unis
- Ouest des États-Unis
- Europe occidentale
- Asie du Sud-Est
- Sydney

Emplacements Content Collaboration et StorageZones

Lors de la configuration d'un compte Content Collaboration dans Citrix Cloud, vous pouvez sélectionner une région aux États-Unis ou dans l'UE. Votre région Content Collaboration est distincte de votre région d'origine Citrix Cloud. Toutefois, comme la région d'origine Citrix Cloud, vous ne pouvez pas modifier la région Content Collaboration après la configuration de votre compte Content Collaboration.



Pour les comptes Content Collaboration créés dans Citrix Cloud, votre StorageZone par défaut est initialement située dans la région États-Unis.

Pour les comptes ShareFile Enterprise créés en dehors de Citrix Cloud, votre StorageZone se trouve dans la région que vous sélectionnez, c'est-à-dire États-Unis ou UE. La connexion à Citrix Cloud ne modifie pas votre sélection.

Une fois votre compte Content Collaboration configuré, vous pouvez activer et désactiver des StorageZones dans le monde entier, et même choisir une nouvelle zone par défaut. Vous pouvez également spécifier une valeur par défaut spécifique aux utilisateurs ou aux dossiers individuels en fonction des StorageZones activées dans la console de gestion de Content Collaboration. Vous pouvez choisir parmi les emplacements suivants :

- Japon
- Singapour
- Australie
- Union européenne
- États-Unis - Est
- États-Unis - Ouest
- États-Unis - Nord-Ouest
- Brésil

Questions fréquentes

- **Existe-t-il des répercussions importantes sur les performances si je suis dans une région et que j'utilise un service basé dans une autre région ?** Les services Citrix Cloud sont conçus

pour être utilisés au niveau global. Par exemple, les clients des États-Unis qui ont des utilisateurs et des Cloud Connector en Australie observeront un impact minimal en terme de latence.
- **Si je ne suis pas dans la région États-Unis ou EMEA, puis-je utiliser Citrix Cloud ?** Oui, choisissez simplement la région qui est la plus proche de la plupart de vos utilisateurs ou qui fournit les meilleurs contrôles pour la protection de l'intégrité de vos données.

Vérifier votre adresse e-mail pour Citrix Cloud

April 19, 2018

De temps à autre, Citrix peut vous demander de vérifier votre compte Citrix Cloud. Voici quelques raisons pour lesquelles vous pouvez être invité à vérifier votre e-mail :

- Vous ne vous êtes pas connecté à Citrix Cloud depuis un certain temps.
- Vous avez changé d'adresse e-mail.
- Vous avez ajouté un nouvel administrateur à votre compte Citrix Cloud.

Questions fréquentes

À quelle fréquence serai-je sollicité pour une vérification ? La vérification de votre compte est un événement ponctuel. Citrix ne vous demandera pas de vérifier votre compte chaque fois que vous vous connectez ou que vous modifiez votre compte. Si vous êtes invité à vérifier fréquemment votre compte, contactez le support technique Citrix.

Est-ce que quelque chose est arrivé à mon compte ? Non, la demande de vérification de votre compte ne signifie pas que votre compte ou l'un de vos services Cloud Citrix ne fonctionne pas correctement. C'est une façon pour Citrix de protéger vos informations.

Je n'ai pas reçu d'e-mail. Que dois-je faire ? Procédez comme suit :

- Recherchez dans votre boîte de réception un e-mail provenant de « Citrix ».
- S'il n'est pas dans votre boîte de réception, vérifiez vos dossiers. Si un filtre anti-spam ou une règle de messagerie a déplacé l'e-mail, il se trouve peut-être dans votre dossier de spam ou votre corbeille.
- Assurez-vous que vous vérifiez le bon compte de messagerie. Citrix envoie l'e-mail de vérification à l'adresse e-mail actuellement enregistrée pour votre compte. Généralement, il s'agit de l'adresse e-mail avec laquelle vous vous êtes initialement inscrit auprès de Citrix Cloud ou celle avec laquelle vous avez été invité à rejoindre le compte Citrix Cloud.

Contacter l'assistance technique Citrix

Si vous rencontrez un problème qui n'est pas traité ici, contactez le support technique Citrix pour ouvrir un ticket de support.

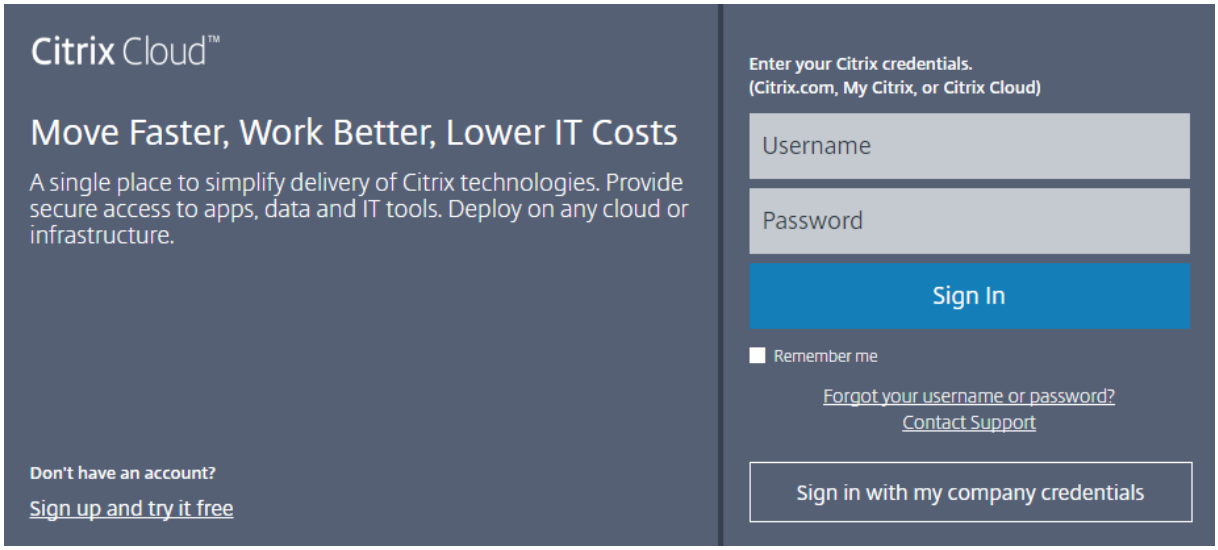
Comment obtenir de l'aide

August 1, 2018

Création d'un compte Citrix Cloud

Si vous rencontrez une erreur lors de votre inscription à un compte Citrix Cloud, contactez le service client Citrix.

Connexion à votre compte



Si vous ne parvenez pas à vous connecter à votre compte Citrix Cloud :

- Assurez-vous que vous vous connectez avec l'adresse e-mail et le mot de passe que vous avez fournis lors de la création votre compte.
- Si votre entreprise autorise les utilisateurs à se connecter à Citrix Cloud à l'aide de leurs informations d'identification d'entreprise au lieu d'un compte Citrix, cliquez sur **Se connecter avec mes identifiants d'entreprise** et entrez l'URL de connexion de votre entreprise. Vous pouvez ensuite entrer vos informations d'identification d'entreprise pour accéder au compte Citrix Cloud de votre entreprise. Si vous ne connaissez pas l'URL de connexion de votre entreprise, contactez l'administrateur de votre entreprise pour obtenir de l'aide.

Si vous avez oublié le mot de passe de votre compte Citrix Cloud ou que vous devez le réinitialiser, cliquez sur **Nom d'utilisateur ou mot de passe oublié ?** et vous pouvez entrer l'adresse e-mail de votre compte. Vous recevrez un e-mail pour réinitialiser votre mot de passe.

Si vous ne recevez pas l'e-mail de réinitialisation du mot de passe ou si vous avez besoin d'une assistance supplémentaire, contactez le service client Citrix.

Forums de support Citrix Cloud

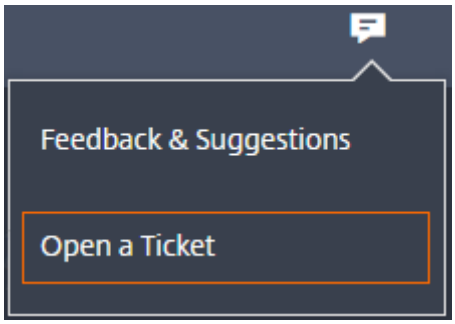
Sur les forums de support Citrix Cloud, vous pouvez obtenir de l'aide, fournir des commentaires et des suggestions d'améliorations, consulter les conversations d'autres utilisateurs ou initier vos propres conversations.

Les membres du personnel de support Citrix suivent ces forums et sont prêts à répondre à vos questions. D'autres membres de la communauté Citrix Cloud peuvent également vous aider ou participer à la discussion.

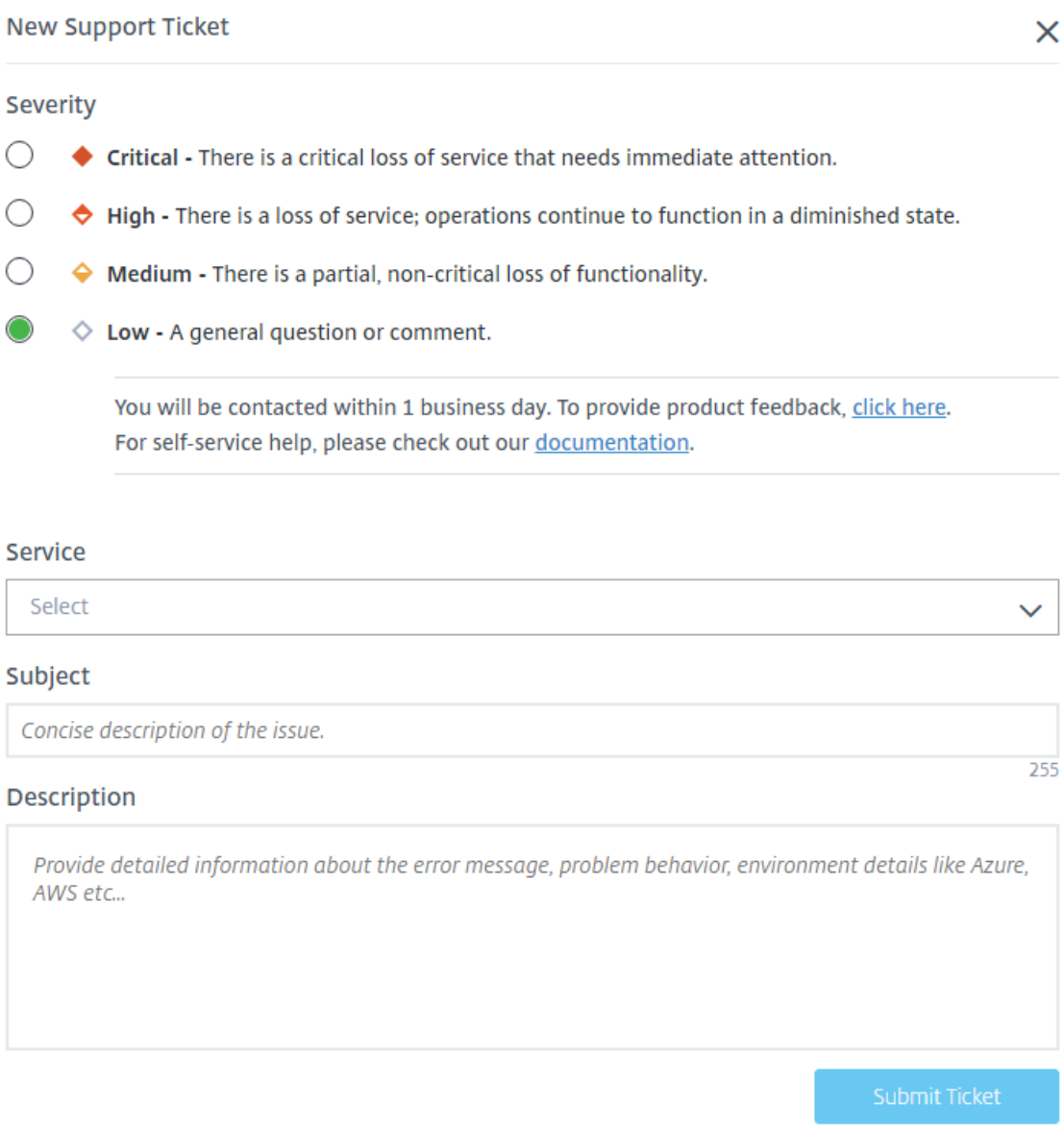
Vous n'avez pas besoin de vous connecter pour lire les sujets du forum. Cependant, vous devez vous connecter pour publier ou répondre. Pour vous connecter, utilisez vos informations d'identification de compte Citrix existantes ou utilisez l'adresse e-mail et le mot de passe que vous avez fournis lors de la création de votre compte Citrix Cloud. Pour créer un nouveau compte Citrix, accédez à Create or request an account (Créer ou demander un compte).

Support technique

Si vous rencontrez un problème nécessitant une assistance technique, cliquez sur l'icône **Commentaires/support** dans le coin supérieur droit de l'écran, puis sélectionnez **Ouvrir un ticket**.



Vous pouvez ensuite entrer les détails du problème dans le formulaire qui apparaît. Le support technique Citrix vous contactera pour résoudre le problème.



Articles de support

Le centre de connaissances Citrix fournit une multitude de contenus de support pour vous aider à résoudre les problèmes que vous pourriez rencontrer avec les produits Citrix.

Pour consulter les articles de support Citrix Cloud, visitez la section Citrix Cloud dans le centre de connaissances.

Configuration système requise

November 7, 2018

Citrix Cloud requiert la configuration minimale suivante :

- Un domaine Active Directory
- Deux machines physiques ou virtuelles pour Citrix Cloud Connector. Pour plus d'informations, consultez la section Détails techniques de Citrix Cloud Connector.
- Des machines physiques ou virtuelles, appartenant à votre domaine, pour l'hébergement des charges de travail et d'autres composants tels que StoreFront. Pour plus d'informations, veuillez consulter la Configuration système requise pour Virtual Apps and Desktops.

Navigateurs Web pris en charge

- Dernière version de Google Chrome
- Dernière version de Mozilla Firefox
- Dernière version de Microsoft Edge
- Microsoft Internet Explorer 11
- Dernière version de Apple Safari

Exigences en terme de connexion Internet

November 7, 2018

Citrix Cloud fournit des fonctions administratives (via un navigateur Web) et des requêtes opérationnelles (provenant d'autres composants installés) qui se connectent aux ressources du déploiement d'un client. Ce document définit la configuration requise et les considérations à prendre en compte pour établir la connexion entre les ressources du client et Citrix Cloud.

Généralités

La connexion à Internet à partir de vos datacenters nécessite l'ouverture du port 443 pour les connexions sortantes. Toutefois, afin de fonctionner dans des environnements contenant un serveur proxy Internet ou des restrictions de pare-feu, une configuration supplémentaire peut être nécessaire. Cet article décrit ces exigences.

Adresses requises

Les adresses suivantes doivent pouvoir être contactées afin d'utiliser et de consommer correctement les services Citrix Cloud.

Citrix Workspace

- `https://*.cloud.com`
- `https://*.citrixdata.com`

Pour Content Collaboration, Citrix Files et Workspace, Citrix recommande de placer les domaines répertoriés dans l'article CTX208318 sur liste blanche.

Smart Tools

Emplacements des ressources/Cloud Connector Citrix :

- `https://*.citrixworkspacesapi.net`
- `https://*.cloud.com`
- Exigences supplémentaires : https://docs.citrix.com/en-us/smart-tools/system-requirements/connectivity-requirements.html

Console d'administration :

- `https://*.citrixworkspacesapi.net`
- `https://*.cloud.com`
- Exigences supplémentaires : https://docs.citrix.com/en-us/smart-tools/system-requirements/connectivity-requirements.html

Content Collaboration

Emplacements des ressources/Cloud Connector Citrix :

- `https://*.sharefile.com`
- Exigences supplémentaires : adresse IP et configuration du pare-feu de ShareFile (CTX208318)

Console d'administration :

- `https://*.citrixworkspacesapi.net`
- `https://*.cloud.com`
- Exigences supplémentaires : adresse IP et configuration du pare-feu de ShareFile (CTX208318)

Secure Browser

Emplacements des ressources/Cloud Connector Citrix :

- https://*.citrixworkspacesapi.net
- https://*.cloud.com
- https://*.servicebus.windows.net

Console d'administration :

- https://*.cloud.com
- https://*.citrixworkspacesapi.net
- https://browser-release-a.azureedge.net
- https://browser-release-b.azureedge.net

Virtual Apps and Desktops Service

Emplacements des ressources/Cloud Connector Citrix :

- https://*.azure.com
- https://*.citrixworkspacesapi.net
- https://*.cloud.com
- https://*.apps.cloud.com
- https://*.blob.core.windows.net
- https://*.nssvc.net- **Si Citrix Gateway Service est activé**
- https://*.servicebus.windows.net
- https://*.xendesktop.net

Console d'administration :

- https://*.citrixworkspacesapi.net
- https://*.cloud.com
- https://*.blob.core.windows.net
- https://*.xendesktop.net

Endpoint Management

Emplacements des ressources/Cloud Connector Citrix :

- https://*.citrixworkspacesapi.net
- https://*.cloud.com
- https://*.blob.core.windows.net
- https://*.servicebus.windows.net

- Exigences supplémentaires : https://docs.citrix.com/fr-fr/citrix-endpoint-management/endpoint-management.html

Console d'administration :

- `https://*.citrix.com`
- `https://*.citrixworkspacesapi.net`
- `https://*.cloud.com`
- `https://*.blob.core.windows.net`
- Exigences supplémentaires : https://docs.citrix.com/fr-fr/citrix-endpoint-management/endpoint-management.html

Gateway

*.netscalergateway.net

Workspace Environment Management

- `https://*.wem.cloud.com`

Console de gestion Citrix Cloud

La console de gestion Citrix Cloud est une console Web à laquelle vous pouvez accéder après la connexion sur https://citrix.cloud.com. Les pages Web qui composent la console peuvent nécessiter d'autres ressources sur Internet, soit lors de la connexion, soit ultérieurement lors de l'exécution d'opérations spécifiques.

Configuration du proxy

Si vous vous connectez via un serveur proxy, la console de gestion fonctionne à l'aide de la même configuration que celle appliquée à votre navigateur Web. La console fonctionne dans le contexte de l'utilisateur, de sorte que toute configuration de serveurs proxy nécessitant l'authentification de l'utilisateur devrait fonctionner comme prévu.

Configuration du pare-feu

Pour que la console de gestion fonctionne, le port 443 doit être ouvert pour les connexions sortantes. Vous pouvez tester la connectivité générale en naviguant dans la console.

Citrix Cloud Connector

Le Citrix Cloud Connector est un package logiciel qui déploie un ensemble de services exécutés sur des serveurs Microsoft Windows. L'ordinateur hébergeant le Cloud Connector se trouve dans le réseau sur lequel résident les ressources que vous utilisez avec Citrix Cloud. Le Cloud Connector se connecte à Citrix Cloud, ce qui lui permet d'utiliser et de gérer vos ressources selon les besoins.

Pour la configuration requise pour l'installation du Cloud Connector, consultez la section Installation de Cloud Connector. Le Cloud Connector requiert une connectivité sortante sur le port 443 pour fonctionner. Après l'installation, le Cloud Connector peut avoir des exigences d'accès supplémentaires en fonction du service Citrix Cloud avec lequel il est utilisé.

> **Important :** l'activation du décryptage SSL sur certains proxies peut empêcher le Cloud Connector de se connecter à Citrix Cloud. Pour plus d'informations sur la résolution de ce problème, consultez l'article CTX221535.

Guide de déploiement sécurisé pour la plate-forme Citrix Cloud

November 7, 2018

Le Guide de déploiement sécurisé de Citrix Cloud fournit une vue d'ensemble des recommandations en matière de sécurité lors de l'utilisation de Citrix Cloud et décrit les informations recueillies et gérées par Citrix Cloud.

Les articles suivants fournissent des informations similaires pour d'autres services dans Citrix Cloud :

- Vue d'ensemble de la sécurité technique de Virtual Apps and Desktops Service
- Vue d'ensemble de la sécurité technique associée à Endpoint Management
- Vue d'ensemble de la sécurité technique de Smart Tools
- Vue d'ensemble de la sécurité technique de ShareFile
- Vue d'ensemble de la sécurité technique de Secure Browser Service

Plan de contrôle

Instructions pour les administrateurs

- Utilisez des mots de passe forts et changez-les régulièrement.
- Tous les administrateurs d'un compte client peuvent ajouter et supprimer d'autres administrateurs. Assurez-vous que seuls des administrateurs de confiance ont accès à Citrix Cloud.
- Les administrateurs d'un client ont, par défaut, un accès complet à tous les services. Certains services permettent de restreindre l'accès d'un administrateur. Pour plus d'informations, consultez la documentation de chaque service.

- L'authentification à deux facteurs pour les administrateurs est assurée grâce à l'intégration de Citrix Cloud avec Azure Active Directory.

Cryptage et gestion des clés

Le plan de contrôle ne stocke pas les informations sensibles du client. Citrix Cloud récupère les informations telles que les mots de passe administrateur sur demande uniquement (en demandant explicitement à l'administrateur). Il n'y a pas de données au repos sensibles ou cryptées, vous n'avez donc pas besoin de gérer les clés.

Pour les données en vol, Citrix utilise la norme standard TLS 1.2 avec les suites de chiffrement les plus puissantes. Les clients ne peuvent pas contrôler le certificat TLS utilisé, car Citrix Cloud est hébergé sur le domaine cloud.com appartenant à Citrix. Pour accéder à Citrix Cloud, les clients doivent utiliser un navigateur compatible TLS 1.2 avec des suites de chiffrement puissantes.

Consultez la documentation spécifique à chaque service pour plus de détails sur le chiffrement et la gestion des clés au sein de chaque service.

Souveraineté des données

Le plan de contrôle Citrix Cloud est hébergé aux États-Unis et dans l'Union Européenne. Les clients ne peuvent pas le gérer.

Le client possède et gère les emplacements de ressources qu'il utilise avec Citrix Cloud. Un emplacement de ressources peut être créé dans un datacenter, un cloud, un emplacement où une zone géographique choisis par le client. Toutes les données stratégiques de l'entreprise (telles que les documents, les feuilles de calcul, etc.) sont stockées dans les emplacements de ressources et contrôlées par le client.

Pour Content Collaboration, consultez les ressources suivantes pour plus d'informations sur l'emplacement sur lequel les données sont stockées :

- Documentation de Content Collaboration Service
- Questions fréquemment posées sur la sécurité de ShareFile
- Sécurité et conformité de Citrix ShareFile
- ShareFile StorageZones

D'autres services peuvent proposer la possibilité de stocker des données dans différentes régions. Consultez les rubriques Considérations géographiques ou Vue d'ensemble de la sécurité technique (répertoriées au début de cet article) pour chaque service.

Audit et contrôle des modifications

Il n'existe actuellement aucun contrôle d'audit ou de modification visible par les clients dans l'interface utilisateur ou les API de Cloud Citrix.

Citrix dispose d'informations d'audit internes complètes. Si un client a des préoccupations, nous lui recommandons de contacter Citrix dans un délai de 30 jours. Citrix va vérifier les journaux d'audit pour déterminer l'administrateur qui a effectué une opération, la date à laquelle elle a été effectuée, l'adresse IP associée à l'opération et ainsi de suite.

Aperçu des problèmes de sécurité

Le site Web status.cloud.com offre une vue globale des problèmes de sécurité qui ont un impact continu sur le client. Ce site enregistre l'état et les informations de disponibilité. Il existe une option pour vous abonner aux mises à jour de la plateforme ou de services individuels.

Citrix Cloud Connector

Installation du Cloud Connector

Pour des raisons de sécurité et de performance, Citrix recommande de ne pas installer le logiciel Cloud Connector sur un contrôleur de domaine.

Par ailleurs, les machines sur lesquelles le logiciel Cloud Connector est installé doivent se trouver à l'intérieur du réseau privé du client et non dans la DMZ. Pour la configuration système et réseau requise et des instructions sur l'installation du Cloud Connector, consultez la section Citrix Cloud Connector.

Configuration du Cloud Connector

Le client est responsable de l'installation des mises à jour de sécurité de Windows sur les machines sur lesquelles le Cloud Connector est installé.

Les clients peuvent utiliser un anti-virus avec le Cloud Connector. Citrix effectue des tests avec McAfee VirusScan Enterprise + AntiSpyware Enterprise 8.8. Citrix apportera son assistance aux clients qui utilisent d'autres antivirus standard.

Dans l'Active Directory (AD) du client, le compte d'ordinateur du Cloud Connector doit être limité à un accès en lecture seule. Il s'agit de la configuration par défaut dans Active Directory. En outre, le client peut activer la journalisation et l'audit AD sur le compte d'ordinateur du Cloud Connector pour surveiller toute activité d'accès à AD.

Connexion à l'ordinateur hébergeant le Cloud Connector

Le Cloud Connector contient des informations de sécurité sensibles telles que les mots de passe d'administration. Seuls les administrateurs les plus privilégiés doivent être en mesure de se connecter aux machines hébergeant le Cloud Connector (par exemple, pour réaliser des opérations de maintenance). En général, il n'est pas nécessaire qu'un administrateur se connecte à ces machines pour gérer des produits Citrix. Le Cloud Connector se gère tout seul.

N'autorisez pas les utilisateurs à se connecter à des machines hébergeant le Cloud Connector.

Installation de logiciels supplémentaires sur des machines Cloud Connector

Les clients peuvent installer des logiciels antivirus et des outils d'hyperviseur (si installés sur une machine virtuelle) sur les machines sur lesquelles le Cloud Connector est installé. Toutefois, Citrix recommande aux clients de ne pas installer d'autres logiciels sur ces machines. D'autres logiciels créent d'autres vecteurs d'attaque et peuvent réduire la sécurité de la solution globale de Citrix Cloud.

Configuration des ports entrants et sortants

Le Cloud Connector nécessite que le port sortant 443 soit ouvert avec accès à Internet. Le Cloud Connector ne doit pas disposer de ports entrants accessibles depuis Internet.

Les clients peuvent placer le Cloud Connector derrière un proxy Web pour surveiller ses communications Internet sortantes. Cependant, le proxy Web doit fonctionner avec une communication cryptée SSL/TLS.

Le Cloud Connector peut avoir des ports sortants supplémentaires avec accès à Internet. Le Cloud Connector négociera sur une large gamme de ports pour optimiser la bande passante et les performances du réseau si des ports supplémentaires sont disponibles.

Le Cloud Connector doit avoir une large gamme de ports entrants et sortants ouverts dans le réseau interne. Le tableau ci-dessous répertorie les ports ouverts requis.

Ports client	Port du serveur	Service
49152 -65535/UDP	123/UDP	W32Time
49152 -65535/TCP	135/TCP	Mappeur de points de terminaison RPC
49152 -65535/TCP	464/TCP/UDP	Changement de mot de passe Kerberos
49152 -65535/TCP	49152-65535/TCP	RPC pour LSA, SAM, Netlogon (*)

Ports client	Port du serveur	Service
49152 -65535/TCP/UDP	389/TCP/UDP	LDAP
49152 -65535/TCP	636/TCP	LDAP SSL
49152 -65535/TCP	3268/TCP	LDAP GC
49152 -65535/TCP	3269/TCP	LDAP GC SSL
53, 49152 -65535/TCP/UDP	53/TCP/UDP	DNS
49152 -65535/TCP	49152 -65535/TCP	FRS RPC (*)
49152 -65535/TCP/UDP	88/TCP/UDP	Kerberos
49152 -65535/TCP/UDP	445/TCP	SMB

Chacun des services utilisés dans Citrix Cloud étendra la liste des ports ouverts requis. Pour plus d'informations, veuillez consulter les ressources suivantes :

- Vue d'ensemble de la sécurité technique pour chaque service (répertoriée au début de cet article)
- Exigences en terme de connexion Internet pour les services Citrix Cloud
- Exigences requises par Application Delivery Management Service en matière de port
- Exigences requises par Endpoint Management en matière de port

Contrôle des communications sortantes

Le Cloud Connector communique vers Internet sur le port 443, à la fois vers les serveurs Citrix Cloud et vers les serveurs Microsoft Azure Service Bus.

Le Cloud Connector communique avec les contrôleurs de domaine du réseau local se trouvant au sein de la forêt Active Directory sur laquelle résident les machines hébergeant le Cloud Connector.

Pendant un fonctionnement normal, le Cloud Connector communique uniquement avec les contrôleurs de domaine des domaines apparaissant sous **Utiliser pour les abonnements** sur la page **Gestion des identités et des accès** de l'interface utilisateur Citrix Cloud.

En sélectionnant les domaines à configurer sous **Utiliser pour les abonnements**, le Cloud Connector communique avec les contrôleurs de domaine dans tous les domaines de la forêt Active Directory sur laquelle résident les machines hébergeant le Cloud Connector.

Chaque service dans le Citrix Cloud étend la liste des serveurs et des ressources internes que le Cloud Connector peut contacter au cours de ses opérations normales. En outre, les clients ne peuvent pas contrôler les données que le Cloud Connector envoie à Citrix. Pour plus d'informations sur les ressources internes des services et les données envoyées à Citrix, consultez les ressources suivantes :

- Vue d'ensemble de la sécurité technique pour chaque service (répertoriée au début de cet article)
- Exigences en terme de connexion Internet pour les services Citrix Cloud

Affichage des journaux Cloud Connector

Toute information pertinente ou exploitable par un administrateur est disponible dans le journal des événements Windows sur la machine Cloud Connector.

Afficher les journaux d'installation du Cloud Connector dans les répertoires suivants :

- %AppData%\Local\Temp\CitrixLogs\CloudServicesSetup
- %windir%\Temp\CitrixLogs\CloudServicesSetup

Les journaux que le Cloud Connector envoie au cloud figurent dans : %ProgramData%\Citrix\WorkspaceCloud\Log

Les journaux du répertoire WorkspaceCloud\Logs sont supprimés lorsqu'ils dépassent un seuil de taille spécifié. L'administrateur peut contrôler ce seuil de la taille en réglant la valeur de clé de Registre pour HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CloudServices\AgentAdministration\MaximumLogSpaceMegabyt

Configuration de SSL/TLS

La configuration du Cloud Connector de base n'a pas besoin d'une configuration SSL/TLS spéciale.

Le Cloud Connector doit faire confiance à l'autorité de certification utilisée par les certificats SSL/TLS de Citrix Cloud et les certificats SSL/TLS de Microsoft Azure Service Bus. Citrix et Microsoft pourront changer les certificats et les autorités de certification à l'avenir, mais utiliseront toujours des autorités de certification qui font partie de la liste des éditeurs approuvés Windows standard.

Chaque service de Citrix Cloud peut avoir différentes exigences de configuration SSL. Pour de plus amples informations, consultez la Vue d'ensemble de la sécurité technique pour chaque service (répertoriée au début de cet article).

Conformité aux normes de sécurité

Pour assurer la conformité aux normes de sécurité, le Cloud Connector s'auto-gère. Ne désactivez pas les redémarrages et ne placez pas d'autres restrictions sur le Cloud Connector. Ces actions empêchent le Cloud Connector de se mettre à jour lorsqu'il y a une mise à jour critique.

Le client n'est pas tenu de prendre d'autres mesures pour réagir aux problèmes de sécurité. Le Cloud Connector applique automatiquement les correctifs de sécurité.

Conseils de gestion des comptes compromis

- Vérifiez la liste des administrateurs de Citrix Cloud et supprimez ceux qui ne sont pas approuvés.
- Désactivez tous les comptes compromis dans l'annuaire Active Directory de votre entreprise.
- Contactez Citrix et demandez-leur d'alterner les secrets d'autorisation stockés pour tous les Cloud Connector du client. En fonction de la gravité du problème de sécurité, effectuez les actions suivantes :
  - **Faible risque :** Citrix peut alterner progressivement les secrets. Les Cloud Connector continueront à fonctionner normalement. Les anciens secrets d'autorisation deviendront invalides dans un délai de 2 à 4 semaines. Surveillez le Cloud Connector pendant ce temps pour vous assurer qu'aucune opération inattendue n'est effectuée.
  - **Risque élevé continu :** Citrix peut révoquer tous les anciens secrets. Les Cloud Connector existants ne fonctionneront plus. Pour reprendre le fonctionnement normal, le client doit désinstaller et réinstaller le Cloud Connector sur toutes les machines applicables.

Terminologie

November 7, 2018

Citrix Cloud : plan de contrôle basé sur le cloud appartenant à Citrix et pouvant être utilisé par les clients pour fournir des services dans leurs propres datacenters ou dans des clouds.

Citrix Cloud Connector : assure la communication entre les ressources de l'emplacement de ressources et Citrix Cloud. Pour de plus amples informations sur le fonctionnement et les exigences du Cloud Connector, consultez la section Citrix Cloud Connector.

Service de cloud : les services de cloud fournissent les fonctionnalités qui permettent de proposer les services dont les abonnés ont besoin pour effectuer leur travail. Cela inclut la création et la gestion des ressources d'infrastructure nécessaires.

Bibliothèque : contient les applications, bureaux ou données qui constituent les offres mises à la disposition des abonnés. Les administrateurs utilisent la bibliothèque pour créer et gérer leurs offres et accorder l'accès aux abonnés. Pour de plus amples informations, consultez Attribuer des utilisateurs et des groupes à des offres de services à l'aide de la bibliothèque.

Offres (fournies par le client pour les abonnés) : applications, bureaux ou données dans la bibliothèque qu'un administrateur Citrix Cloud alloue aux abonnés. Les offres peuvent être créées via un service Citrix Cloud, comme Virtual Apps and Desktops Service. Les abonnés peuvent uniquement accéder aux applications, bureaux et données auxquels ils sont affectés.

Emplacement de ressources : définit l'emplacement qui contient les ressources que vous utilisez avec les services Citrix Cloud. Les emplacements de ressources peuvent résider dans un cloud public ou privé où dans votre datacenter local. Il n'existe aucune limite au nombre d'emplacements de

ressources que vous pouvez créer. Les ressources dans un emplacement de ressources se trouvent toutes au sein d'un périmètre de communication/réseau défini, dans lequel il est possible d'accéder à ces ressources à partir de Citrix Cloud et à toute autre infrastructure client nécessaire au fonctionnement. La connexion à Citrix Cloud s'effectue via le Citrix Cloud Connector. Pour de plus amples informations, consultez la section Emplacements des ressources.

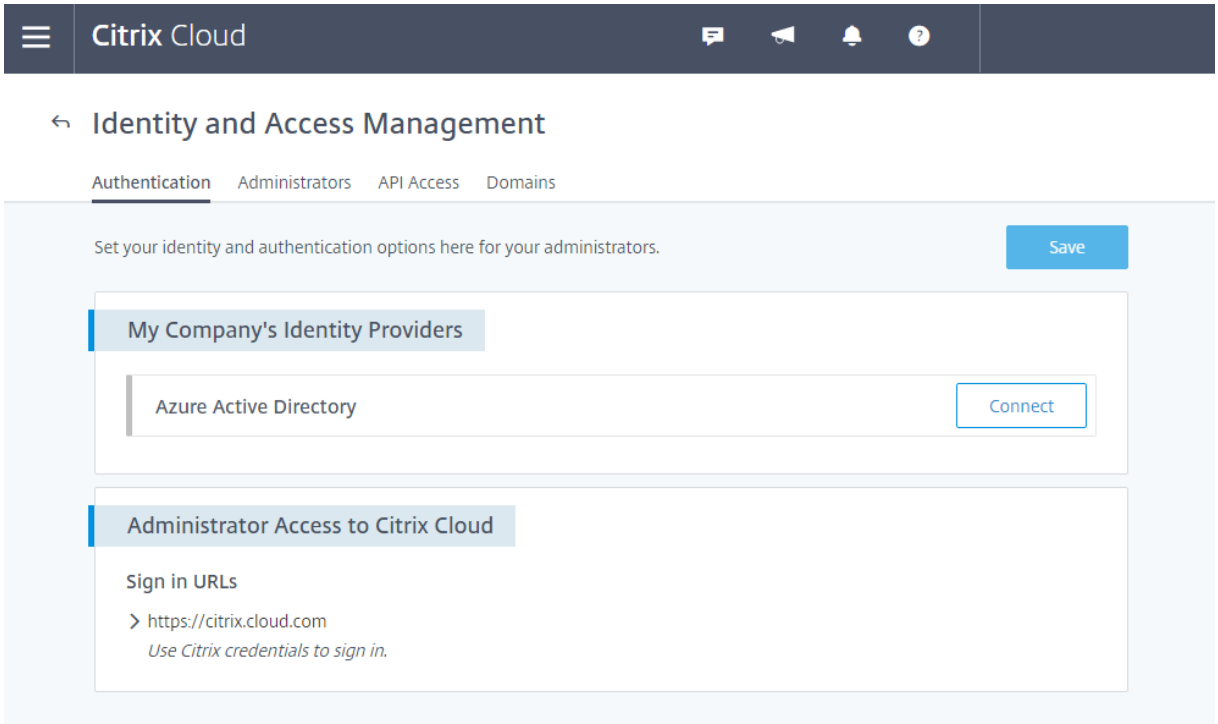
Ressources : composants utilisés pour fournir l'infrastructure aux services Citrix Cloud que vous utilisez. Ces ressources peuvent être des hyperviseurs, des serveurs, des appliances réseau, des VDA pour Virtual Apps and Desktops, etc. Ces composants résident généralement dans les emplacements de ressources dans Citrix Cloud. Pour de plus amples informations, consultez la section Emplacements des ressources.

Abonné : personne qui utilise les offres de bibliothèque qui lui ont été affectées par un administrateur Citrix Cloud. Un abonné peut accéder à ses offres à l'aide de Citrix Receiver ou d'un espace de travail disponible dans le cadre de Citrix Virtual Apps Essentials Service.

Espace de travail : se compose d'offres auxquelles les abonnés peuvent accéder. Les espaces de travail sont disponibles dans le cadre de Citrix Virtual Apps Essentials Service. Pour plus d'informations sur l'utilisation d'espaces de travail, consultez la section Configuration de l'espace de travail.

Gestion des identités et des accès

November 7, 2018



La fonction Gestion des identités et des accès définit les fournisseurs d'identité et les comptes utilisés pour les administrateurs et les abonnés à Citrix Cloud et ses offres.

Fournisseurs d'identité

Par défaut, Citrix Cloud utilise le fournisseur d'identité Citrix pour gérer les informations d'identité de tous les utilisateurs de votre compte Citrix Cloud. Vous pouvez modifier ce comportement pour utiliser Azure Active Directory ou Active Directory sur site.

Pour obtenir des instructions sur l'utilisation d'Azure Active Directory, consultez la rubrique Connecter Azure Active Directory à Citrix Cloud.

Pour obtenir des instructions sur l'utilisation d'Active Directory, consultez la rubrique Connecter Active Directory à Citrix Cloud.

Administrateurs

Les administrateurs utilisent leur identité pour accéder à Citrix Cloud, effectuer des activités de gestion et installer Citrix Cloud Connector.

Un mécanisme d'identité Citrix fournit une authentification pour les administrateurs à l'aide d'une adresse e-mail et d'un mot de passe. Les administrateurs peuvent également utiliser leurs informations d'identification My Citrix pour se connecter à Citrix Cloud.

Ajouter de nouveaux administrateurs

Lors du processus de création d'un compte, un administrateur initial est créé. L'administrateur peut ensuite inviter d'autres administrateurs à rejoindre Citrix Cloud. Ces nouveaux administrateurs peuvent utiliser leurs informations d'identification de compte Citrix existantes ou configurer un nouveau compte si nécessaire. Vous pouvez également ajuster les autorisations d'accès des administrateurs que vous invitez. Cela vous permet de définir un accès en phase avec le rôle de l'administrateur dans votre organisation.

Pour inviter d'autres administrateurs et personnaliser leur accès au Citrix Cloud, consultez la section Ajouter des administrateurs à un compte Citrix Cloud.

Réinitialiser votre mot de passe

Si vous avez oublié ou que vous souhaitez réinitialiser votre mot de passe, cliquez sur **Nom d'utilisateur ou mot de passe oublié ?** sur la page de connexion à Citrix Cloud. Après avoir entré

votre adresse e-mail ou nom d'utilisateur pour trouver votre compte, Citrix vous envoie un e-mail contenant un lien permettant de réinitialiser votre mot de passe.

Conseil : ajoutez **customerservice@citrix.com** à votre liste blanche pour vous assurer que l'e-mail ne finisse pas dans votre dossier de spam ou la corbeille.

Supprimer des administrateurs

Vous pouvez supprimer des administrateurs de votre compte Citrix Cloud sur l'onglet Administrateur. Lorsque vous supprimez un administrateur, il ne peut plus se connecter à Citrix cloud.

Si un administrateur est connecté lorsque vous supprimez le compte, l'administrateur reste actif pendant au maximum 1 minute. L'accès à Citrix Cloud est ensuite refusé.

Remarque :

- Si le compte ne dispose que d'un seul administrateur, vous ne pouvez pas supprimer cet administrateur. Citrix Cloud requiert au moins un administrateur pour chaque compte client.
- Les connecteurs Citrix Cloud Connector ne sont pas liés à des comptes d'administrateur. Les Cloud Connector continueront à fonctionner même si vous supprimez l'administrateur qui les a installés.

Abonnés

L'identité d'un abonné définit les services auxquels il a accès dans Citrix Cloud. Cette identité provient de comptes de domaine Active Directory fournis à partir des domaines dans l'emplacement de ressources. L'attribution d'un abonné à une offre de bibliothèque autorise l'abonné à accéder à cette offre.

Les administrateurs peuvent contrôler les domaines qui sont utilisés pour fournir ces identités sur l'onglet Domaines. Si vous prévoyez d'utiliser des domaines de plusieurs forêts, installez au moins deux Cloud Connector dans chaque forêt. Citrix recommande au moins deux Cloud Connector pour garantir un environnement de haute disponibilité.

Remarque :

- La désactivation de domaines empêche uniquement la sélection de nouvelles identités. Cela n'empêche pas les abonnés d'utiliser des identités déjà allouées.
- Chaque Cloud Connector peut énumérer et utiliser tous les domaines de la forêt unique dans laquelle il est installé.

Gérer l'utilisation des abonnés

Vous pouvez ajouter des abonnés aux offres à l'aide de comptes individuels ou de groupes Active Directory. L'utilisation de groupes Active Directory ne nécessite pas la gestion via Citrix Cloud une fois que vous avez affecté le groupe à une offre.

Lorsqu'un administrateur supprime un abonné individuel ou un groupe d'abonnés d'une offre, ces abonnés ne peuvent plus accéder au service. Pour plus d'informations sur la suppression d'abonnés de services spécifiques, reportez-vous à la documentation du service sur le site Web Documentation produit de Citrix.

Emplacements de ressources principaux

Un emplacement de ressources principal est un emplacement de ressources que vous désignez comme étant « l'emplacement préféré » pour les communications entre votre domaine et Citrix Cloud. L'emplacement de ressources que vous sélectionnez comme « principal » doit disposer de Cloud Connector qui offrent les meilleures performances et la meilleure connectivité à votre domaine. Cela permet à vos utilisateurs de se connecter rapidement à Citrix Cloud.

Pour de plus amples informations, consultez la section Sélectionner un emplacement de ressources principal.

Connecter Active Directory à Citrix Cloud

November 7, 2018

Par défaut, Citrix Cloud utilise le fournisseur d'identité Citrix pour gérer les informations d'identité de tous les utilisateurs de votre compte Citrix Cloud. Vous pouvez cependant choisir d'utiliser Active Directory (AD).

La connexion de votre Active Directory à Citrix Cloud implique l'installation de Cloud Connector dans votre domaine. Citrix recommande d'installer deux Cloud Connector pour garantir une haute disponibilité. Pour consulter la configuration requise et les instructions, voir Installation de Cloud Connector.

Pour connecter Azure Active Directory à Citrix Cloud

1. Dans le menu Citrix Cloud, sélectionnez **Gestion des identités et des accès**.
2. Dans l'onglet **Authentification**, dans **Active Directory**, cliquez sur le menu des points de suspension et sélectionnez **Connecter**.
3. Cliquez sur **Installer connecteur** pour télécharger le logiciel Cloud Connector.

4. Lancez le programme d'installation de Cloud Connector et suivez les instructions de l'assistant d'installation.
5. Dans la page **Se connecter à Active Directory**, cliquez sur **Détecter**. Après vérification, Citrix Cloud affiche un message indiquant que votre Active Directory est connecté.
6. Cliquez sur **Revenir à l'authentification**. L'entrée **Active Directory** est marquée **Activé** dans l'onglet **Authentification**.

Connecter Azure Active Directory à Citrix Cloud

November 7, 2018

Par défaut, Citrix Cloud utilise le fournisseur d'identité Citrix pour gérer les informations d'identité de tous les utilisateurs de votre compte Citrix Cloud. Vous pouvez cependant choisir d'utiliser Azure Active Directory (AD).

En utilisant Azure AD avec Citrix Cloud, vous pouvez :

- Tirer parti de votre propre Active Directory, afin de contrôler l'audit, les stratégies de mot de passe et désactiver facilement les comptes en cas de besoin.
- Configurer l'authentification à plusieurs facteurs. Cela offre un niveau de sécurité plus élevé afin de se protéger contre le vol d'informations d'identification de connexion.
- Utiliser une page de connexion personnalisée, de façon à ce que vos utilisateurs sachent qu'ils se connectent au site approprié.
- Utiliser la fédération avec un fournisseur d'identité de votre choix, y compris ADFS, Okta et Ping, entre autres.

Citrix Cloud comprend une application Azure AD qui permet à Citrix Cloud de se connecter à Azure AD sans que vous ayez à vous connecter à une session Azure AD active. Depuis août 2018, cette application a été mise à niveau pour améliorer les performances et vous permettre d'être prêt pour les versions futures. Si vous avez déjà connecté votre Azure AD à Citrix Cloud (avant août 2018), vous devrez peut-être mettre à jour votre connexion Azure AD dans Citrix Cloud. Pour plus d'informations, consultez Se reconnecter à Azure AD pour l'application mise à niveau dans cet article.

Préparer votre Active Directory et Azure AD

Avant de pouvoir utiliser Azure AD, les conditions suivantes doivent être remplies :

- Vous devez disposer d'un compte Microsoft Azure. Azure AD est fourni gratuitement avec chaque compte Azure. Si vous ne disposez pas d'un compte Azure, inscrivez-vous sur https://azure.microsoft.com/en-us/free/?v=17.36.
- Vous disposez du rôle d'administrateur global dans Azure AD. Ce rôle est requis pour donner à Citrix Cloud l'autorisation de se connecter à Azure AD.

- La propriété « mail » des comptes d'administrateur doit être configurée dans Azure AD. Pour ce faire, vous pouvez synchroniser les comptes de vos Active Directory locaux avec Azure AD à l'aide de l'outil Azure AD Connect de Microsoft. Vous pouvez également configurer des comptes Azure AD non synchronisés avec la messagerie Office 365.

Synchroniser des comptes avec Azure AD Connect

1. Assurez-vous que la propriété utilisateur Adresse de messagerie est configurée pour les comptes Active Directory :
   a) Ouvrez Utilisateurs et ordinateurs Active Directory.
   b) Dans le dossier **Utilisateurs**, recherchez le compte que vous souhaitez vérifier, cliquez avec le bouton droit et sélectionnez **Propriétés**. Sur l'onglet **Général**, vérifiez que le champ **E-mail** a une entrée valide. Citrix Cloud exige que les administrateurs ajoutés depuis Azure AD possèdent des adresses de messagerie différentes de celles des administrateurs qui se connectent à l'aide d'une identité hébergée par Citrix.
2. Installez et configurez Azure AD Connect. Pour plus d'informations, consultez la section Intégrer des répertoires locaux à Azure Active Directory sur le site web de Microsoft Azure.

Connecter Citrix Cloud à Azure AD

Lorsque vous connectez votre compte Citrix Cloud à votre Azure AD, Citrix Cloud doit être autorisé à accéder à votre profil utilisateur (où le profil de l'utilisateur connecté) ainsi qu'aux profils de base des utilisateurs dans votre Azure AD. Citrix requiert cette autorisation afin de pouvoir acquérir votre nom et adresse e-mail (en tant qu'administrateur) et vous permettre de rechercher d'autres utilisateurs et les ajouter en tant qu'administrateurs plus tard.

> **Important :** Vous devez être un administrateur global dans Azure AD pour effectuer cette tâche.

1. Connectez-vous à Citrix Cloud sur https://citrix.cloud.com.
2. Cliquez sur le bouton de menu dans le coin supérieur gauche de la page et sélectionnez **Gestion des identités et des accès**.
3. Sous **Fournisseurs d'identité de mon entreprise**, cliquez sur **Connecter** pour Azure Active Directory.
4. Lorsque vous y êtes invité, entrez un identifiant d'URL convivial et court pour votre entreprise et cliquez sur **Connecter**. L'identifiant que vous choisissez doit être globalement unique au sein de Citrix Cloud.
5. Lorsque vous y êtes invité, connectez-vous au compte Azure avec lequel vous souhaitez vous connecter. Azure affiche les autorisations requises par Citrix Cloud pour accéder au compte et obtenir les informations nécessaires à la connexion. Ces autorisations en lecture seule permettent à Citrix Cloud de collecter des informations de base depuis Microsoft Graph, telles que les

groupes et les profils utilisateur. Si vous êtes un client XME, vous devrez accorder des autorisations de lecture-écriture liées à Microsoft Intune.

6. Cliquez sur **Accepter** pour accepter la demande d'autorisations.

Ajouter des administrateurs à Citrix Cloud depuis Azure AD

1. Dans Citrix Cloud, à partir de la page **Gestion des identités et des accès**, cliquez sur l'onglet **Administrateurs**.
2. À partir du menu **Ajouter admin. de**, sélectionnez l'option Azure AD.
3. Dans la zone de recherche, commencez à taper le nom de l'utilisateur que vous souhaitez ajouter et inviter au compte, comme décrit dans Ajouter des administrateurs à un compte Citrix Cloud. Citrix Cloud envoie à l'utilisateur un e-mail contenant un lien permettant d'accepter l'invitation.

Après avoir cliqué sur le lien dans l'e-mail, l'utilisateur se connecte au Azure Active Directory de l'entreprise. Cela vérifie l'adresse e-mail de l'utilisateur et valide la connexion entre le compte utilisateur Azure AD et Citrix Cloud.

Se connecter à Citrix Cloud à l'aide d'Azure AD

Une fois que les comptes d'utilisateur Azure AD sont connectés, les utilisateurs peuvent se connecter à Citrix Cloud à l'aide d'une des méthodes suivantes :

- Accédez à l'URL de connexion administrateur que vous avez configurée lorsque vous vous êtes connecté initialement au fournisseur d'identité Azure AD pour votre entreprise. Exemple : `https://citrix.cloud.com/go/mycompany`
- À partir de la page de connexion de Citrix Cloud, cliquez sur **Se connecter avec mes identifiants d'entreprise**, entrez l'identifiant que vous avez créé lorsque vous vous êtes initialement connecté à Azure AD (par exemple, « monentreprise ») et cliquez sur **Continuer**.

Activer l'authentification Azure AD pour les espaces de travail

Une fois que vous avez connecté Azure AD à Citrix Cloud, vous pouvez permettre à vos abonnés de s'authentifier auprès de leurs espaces de travail via Azure AD.

> **Important :** Avant d'activer l'authentification Azure AD pour les espaces de travail, passez en revue la section Azure Active Directory relative aux considérations relatives à l'utilisation d'Azure AD avec des espaces de travail.

1. Dans Citrix Cloud, cliquez sur le bouton de menu situé dans le coin supérieur gauche et sélectionnez **Configuration de l'espace de travail**.

2. Dans l'onglet **Authentification**, sélectionnez **Azure Active Directory**.
3. Cliquez sur **Confirmer** pour accepter les modifications apportées à l'expérience d'espace de travail lorsque l'authentification Azure AD est activée.

Activer les fonctionnalités avancées d'Azure AD

Azure AD offre une authentification à plusieurs facteurs avancée, des fonctionnalités de sécurité de pointe, une fédération avec 20 différents fournisseurs d'identité, et la modification et réinitialisation en libre-service du mot de passe, parmi beaucoup d'autres fonctionnalités. L'activation de ces fonctionnalités pour vos utilisateurs Azure AD permet à Citrix Cloud de tirer parti de ces fonctionnalités automatiquement.

Pour comparer les fonctionnalités par niveau de service et la tarification Azure AD, consultez la page https://azure.microsoft.com/en-us/pricing/details/active-directory/.

Se reconnecter à Azure AD pour l'application mise à niveau

Si vous avez déjà connecté votre Azure AD à Citrix Cloud (avant août 2018), il est possible que Citrix Cloud n'utilise pas l'application la plus récente pour se connecter à Azure AD. Par conséquent, Citrix Cloud peut vous demander de reconnecter votre Azure AD et d'accorder des autorisations supplémentaires en lecture seule. Pour accorder ces autorisations au niveau de l'application, vous devez être un administrateur global. Ces autorisations permettent à Citrix Cloud d'effectuer une recherche en arrière-plan des utilisateurs et des groupes dans votre Azure AD. En vous reconnectant à Azure AD, vous accordez des autorisations en lecture seule au niveau de l'application à Citrix Cloud et autorisez Citrix Cloud à se reconnecter à Azure AD en votre nom.

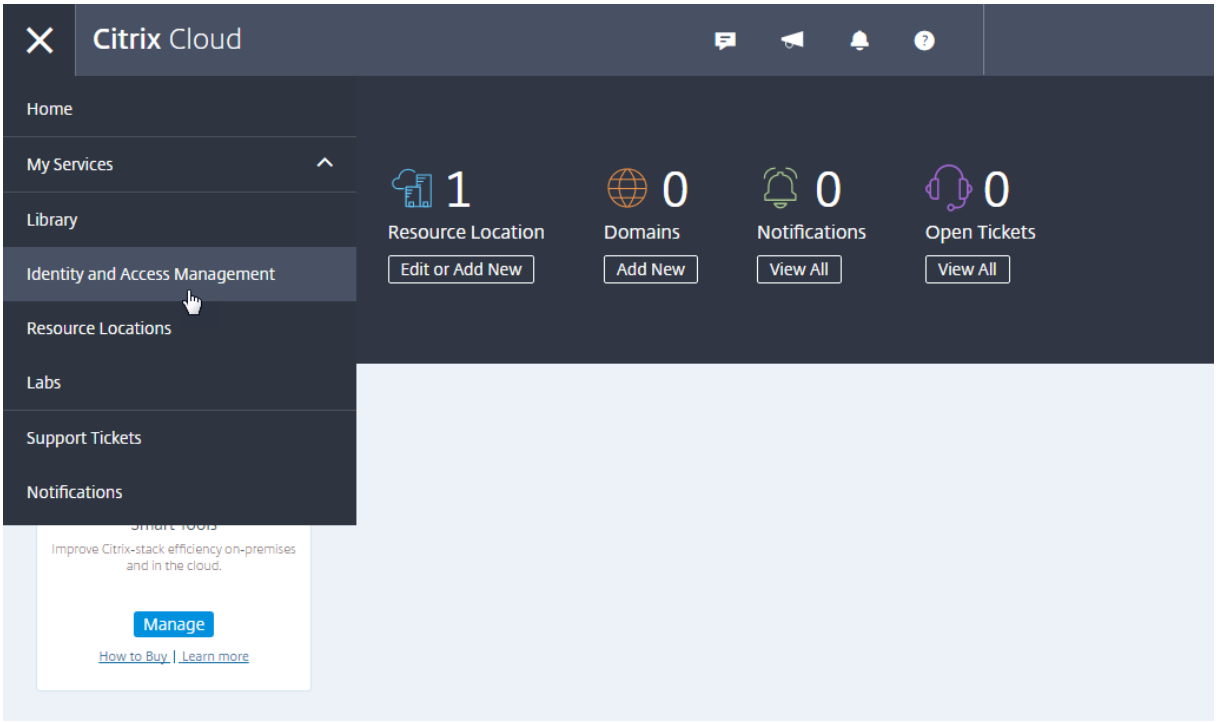
Ajouter des administrateurs à un compte Citrix Cloud

November 7, 2018

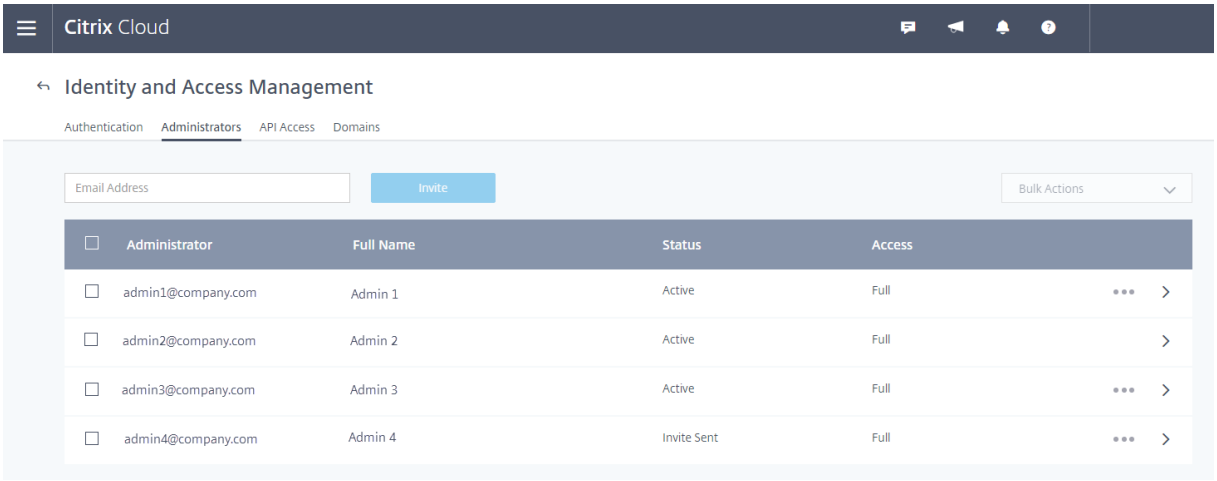
Les administrateurs sont gérés à partir de la console Citrix Cloud. Si vous souhaitez être ajouté en tant qu'administrateur à un compte Citrix Cloud existant, vous devez être invité par un administrateur du compte.

Inviter de nouveaux administrateurs

Après vous être connecté à Citrix Cloud, sélectionnez **Gestion des identités et des accès** à partir du menu.



Sur la page **Gestion des identités et des accès**, cliquez sur **Administrateurs**. La console affiche tous les administrateurs actuels du compte.



Pour inviter un administrateur, entrez son adresse e-mail et cliquez sur **Inviter**. Citrix Cloud envoie une invitation à l'adresse e-mail que vous avez spécifiée et ajoute l'administrateur à la liste. L'e-mail est envoyé depuis cloud@citrix.com et explique comment accéder au compte.

Lorsqu'un administrateur reçoit l'e-mail, il clique sur le lien **Joindre** pour accepter l'invitation. Une fenêtre de navigateur s'ouvre également à partir de laquelle il peut créer son mot de passe.

Remarque : si l'administrateur dispose déjà d'un compte, Citrix Cloud l'invite à utiliser son mot de passe et à se connecter. Après avoir accepté l'invitation, l'administrateur reçoit un e-mail de bienvenue et Citrix Cloud affiche l'administrateur comme « Actif » dans la console.

Configurer les autorisations d'administrateur

Lorsque vous ajoutez des administrateurs à votre compte Citrix Cloud, vous devrez peut-être leur attribuer des niveaux d'accès différents, tels que :

- Accès au service d'assistance pour Virtual Apps and Desktops Service
- Accès pour gérer un ou plusieurs services de cloud spécifiques
- Accès limité aux administrateurs de partenaires
- Accès en lecture seule

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 définir les autorisations d'accès

Seuls les administrateurs Citrix possédant un accès complet peuvent définir des autorisations d'accès pour d'autres d'administrateurs.

1. Connectez-vous à Citrix Cloud sur https://citrix.cloud.com.
2. Cliquez sur le bouton de menu dans le coin supérieur gauche de la page et sélectionnez **Gestion des identités et des accès**.
3. Cliquez sur l'onglet **Administrateurs**.
4. Recherchez l'administrateur que vous souhaitez gérer, cliquez sur le bouton **Plus d'options** et sélectionnez **Modifier l'accès**.
5. Pour autoriser ou interdire des autorisations spécifiques, sélectionnez **Accès personnalisé**. Par défaut, les administrateurs ont un accès complet à toutes les fonctions de Citrix Cloud.
6. Pour chaque autorisation, sélectionnez ou désélectionnez la case à cocher selon vos besoins.
7. Cliquez sur **Enregistrer**.

Sélectionner un emplacement de ressources principal

April 19, 2018

Si vous disposez de plusieurs emplacements de ressources dans votre domaine, vous pouvez choisir l'emplacement « principal » ou « préféré » pour Citrix Cloud. L'emplacement de ressources principal offre les meilleures performances et la meilleure connectivité entre Citrix Cloud et votre domaine, ce qui permet aux utilisateurs de se connecter rapidement.

Lorsque vous sélectionnez un emplacement de ressources principal, les Cloud Connector dans cet emplacement de ressources sont utilisés pour les ouvertures de session des utilisateurs et les opérations d'approvisionnement. Si les Cloud Connector de l'emplacement de ressources principal ne sont pas disponibles, ces opérations sont effectuées à l'aide d'un autre Cloud Connector du domaine.

Remarque : pour garantir que les Cloud Connector sont toujours disponibles dans tous les emplacements de ressources, Citrix recommande d'installer au moins deux (2) Cloud Connector.

Pour décider quel emplacement de ressources vous souhaitez utiliser pour votre emplacement de ressources principal, tenez compte des éléments suivants :

- L'emplacement de ressources offre-t-il la meilleure connectivité à votre domaine ?
- L'emplacement de ressources est-il le plus proche de la région géographique dans laquelle vous utilisez la console de gestion Citrix Cloud ? Par exemple, si votre console Citrix Cloud est sur https://us.cloud.com, vous choisiriez l'emplacement de ressources le plus proche de la région des États-Unis.

Pour sélectionner un emplacement de ressources principal

1. Dans la console de gestion Citrix Cloud, cliquez sur le bouton de menu et sélectionnez **Gestion des identités et des accès**.
2. Cliquez sur **Domaines**, puis développez le domaine contenant l'emplacement de ressources que vous souhaitez utiliser.
3. Cliquez sur **Définir l'emplacement de ressources principal**, puis sélectionnez l'emplacement de ressources que vous voulez désigner comme principal.
4. Cliquez sur **Enregistrer**. Citrix Cloud affiche « Principal » à côté de l'emplacement de ressources que vous avez sélectionné.

Remarque : assurez-vous de sauvegarder vos sélections dans un domaine avant de développer un domaine différent. Lorsque vous développez un domaine, puis développez un autre domaine, le domaine précédemment développé se réduit et supprime toutes les sélections non enregistrées.

Sélectionner un emplacement de ressources principal différent

1. Dans la console de gestion Citrix Cloud, cliquez sur le bouton de menu et sélectionnez **Gestion des identités et des accès**.
2. Cliquez sur **Domaines**, puis développez le domaine contenant l'emplacement de ressources que vous souhaitez modifier.
3. Cliquez sur **Changer l'emplacement de ressources principal**, puis sélectionnez l'emplacement de ressources que vous voulez utiliser.
4. Cliquez sur **Enregistrer**.

Réinitialiser un emplacement de ressources principal

La réinitialisation de l'emplacement de ressources principal vous permet de supprimer la désignation « Principal » attribuée à un emplacement de ressources sans en sélectionner un autre. Lorsque vous

supprimez la désignation « Principal », tous les Cloud Connector du domaine peuvent gérer les opérations d'ouverture de session utilisateur. Par conséquent, certains utilisateurs peuvent rencontrer des connexions plus lentes.

1. Dans la console de gestion Citrix Cloud, cliquez sur le bouton de menu et sélectionnez **Gestion des identités et des accès**.
2. Cliquez sur **Domaines**, puis développez le domaine contenant l'emplacement de ressources principal que vous souhaitez modifier.
3. Choisissez **Changer l'emplacement de ressources principal**, puis **Réinitialiser**. Une notification s'affiche, vous avertissant que les performances d'ouverture de session peuvent être affectées.
4. Sélectionnez **Je comprends l'impact potentiel pour les abonnés**, puis cliquez sur **Confirmer la réinitialisation**.

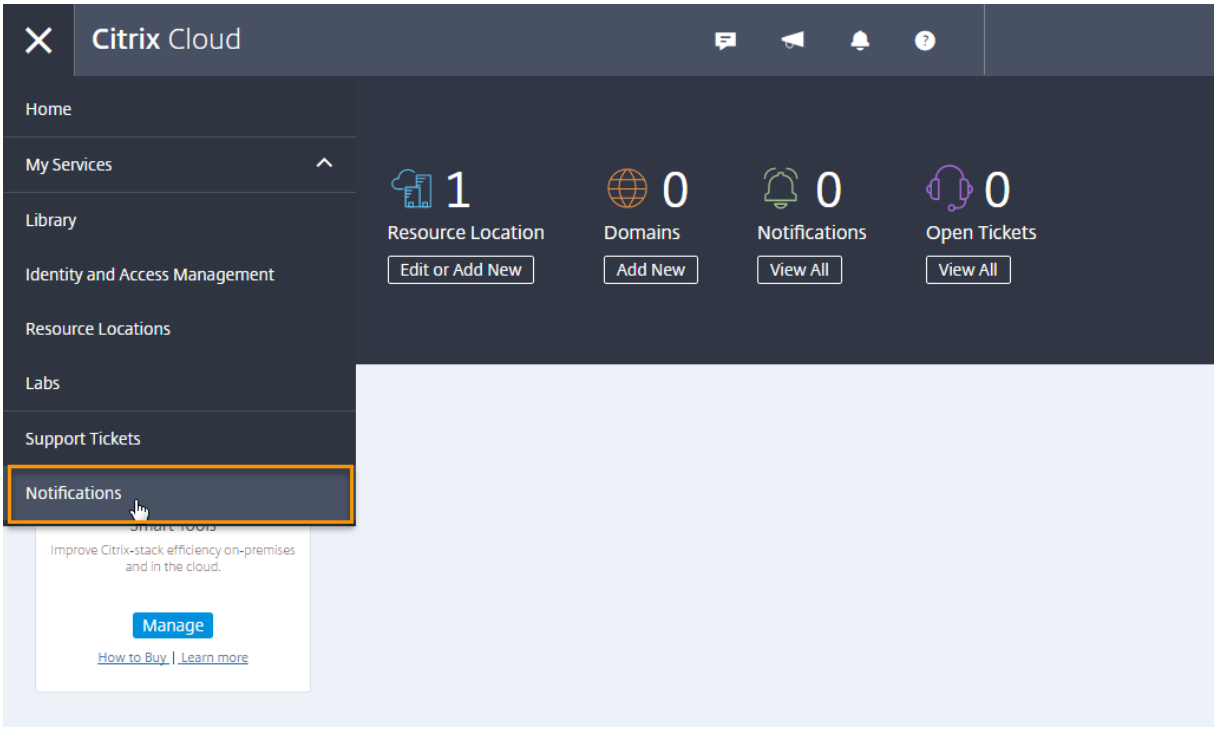
Notifications

August 1, 2018

Les notifications fournissent des informations sur des problèmes ou événements susceptibles d'intéresser les administrateurs, tels que de nouvelles fonctionnalités Citrix Cloud ou des problèmes rencontrés sur une machine dans un emplacement de ressources. Les notifications peuvent provenir de n'importe quel service de Citrix Cloud.

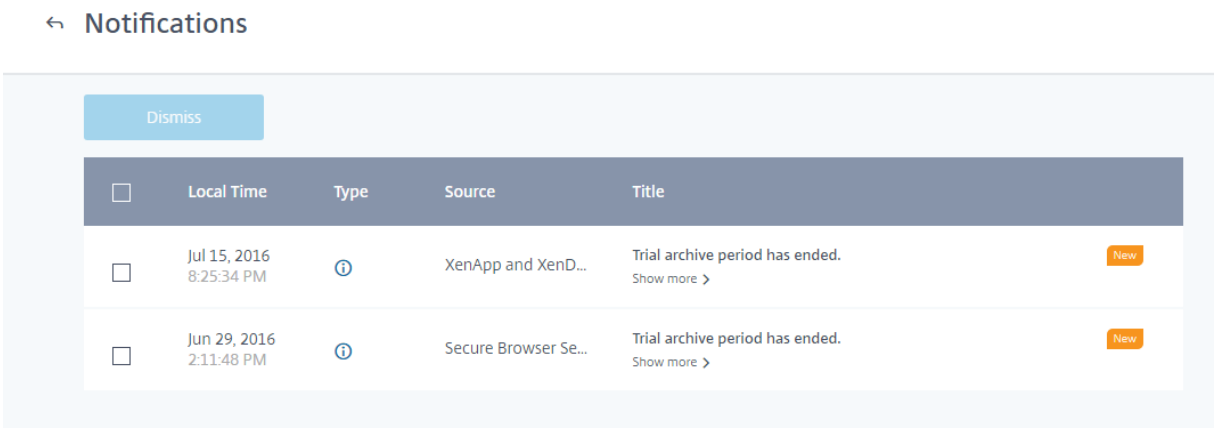
Afficher les notifications

Le nombre de notifications apparaît en haut de la page de la console Citrix Cloud. Pour plus de détails, cliquez sur **Tout afficher** sous **Notifications** dans la console ou sélectionnez **Notifications** dans le menu de la console.



Ignorer les notifications

Une fois que vous avez lu une notification et que vous y avez donné suite (si nécessaire), sélectionnez la notification et cliquez sur **Ignorer**. La fermeture des notifications supprime ces dernières de votre liste et Citrix Cloud met à jour le nombre de notifications lorsque vous revenez sur la page d'accueil de la console.



Les administrateurs reçoivent leurs propres notifications dans Citrix Cloud. Par conséquent, la suppression de notifications n'empêche pas d'autres administrateurs de voir leurs notifications.

Recevoir des notifications par e-mail

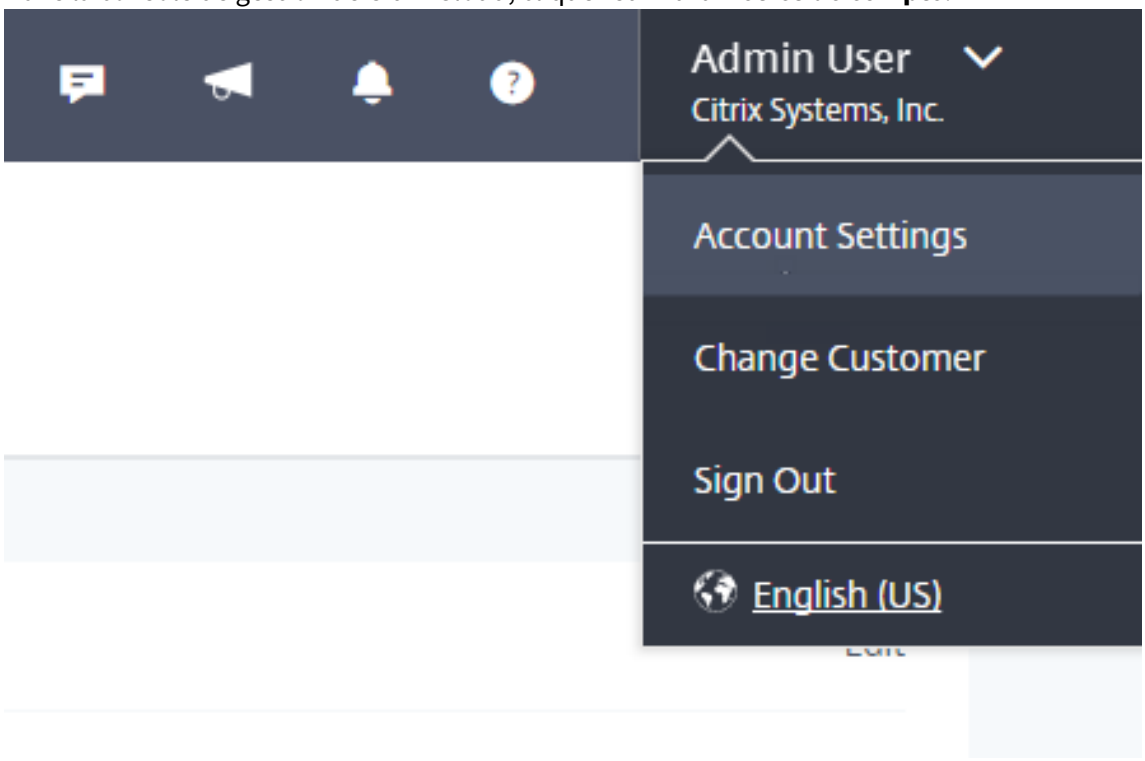
Vous pouvez choisir de recevoir des notifications par e-mail au lieu de vous connecter pour les voir. Par défaut, les notifications par e-mail sont désactivées.

Lorsque vous activez les notifications par e-mail, Citrix Cloud vous envoie un e-mail pour chaque notification. Les notifications sont envoyées dès que possible. Elles ne sont ni regroupées dans un seul e-mail ni groupées pour être envoyées ultérieurement.

Après avoir lu une notification par e-mail, vous pouvez la supprimer via la page **Notifications** dans Citrix Cloud.

Pour activer les notifications par e-mail

1. Dans la console de gestion de Citrix Cloud, cliquez sur **Paramètres de compte**.



2. Sélectionnez **Mon profil**.
3. Cliquez sur le bouton **Notifications par e-mail** pour activer les notifications par e-mail.
4. Sélectionnez les notifications que vous souhaitez recevoir. Par défaut, tous les types de notification sont sélectionnés.

Nettoyage automatique des notifications

Citrix Cloud supprime automatiquement les notifications de plus de 90 jours, qu'elles aient été lues ou non. Cela garantit que la page Notifications ne soit pas encombrée et permet aux administrateurs de se concentrer uniquement sur les notifications les plus importantes.

Surveiller l'utilisation des licences pour les services cloud

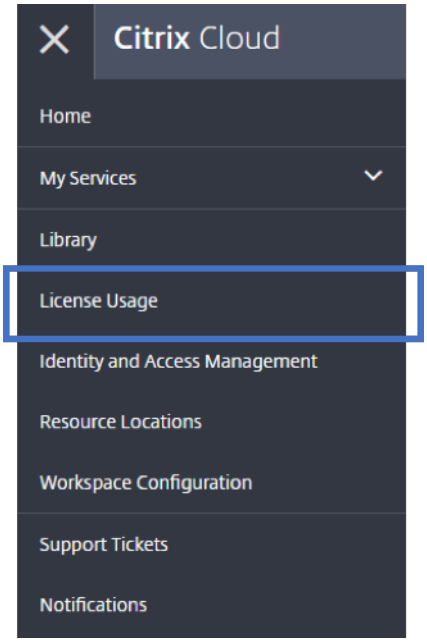
November 7, 2018

L'utilisation des licences dans Citrix Cloud vous permet de surveiller de près la consommation de licences des services cloud que vous avez achetés. Les rapports de synthèse et détaillé vous permettent :

- D'afficher la disponibilité et les affectations de licences
- D'explorer les détails d'attribution de licence individuelle et les tendances d'utilisation
- D'exporter les données d'utilisation de licence au format CSV

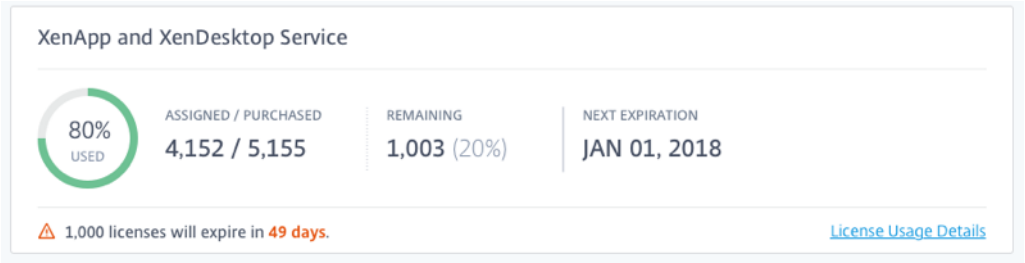
Remarque : l'utilisation des licences est disponible pour Virtual Apps and Desktops Service dans les régions suivantes : États-Unis, Union Européenne et Asie Pacifique Sud.

Pour afficher les données de licence de vos services cloud, sélectionnez **Utilisation des licences** dans le menu de la console.



Résumé et détails d'utilisation des licences

Le résumé Utilisation des licences fournit une vue d'ensemble des informations suivantes :



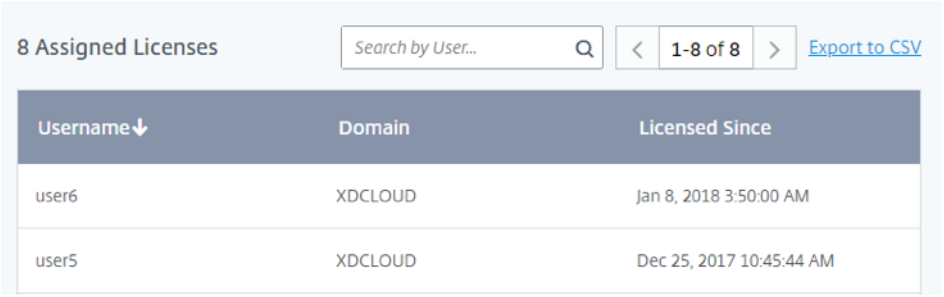
- Pourcentage du nombre total de licences achetées attribuées. Les utilisateurs se voient attribuer une licence lors de la première utilisation du service de cloud. Lorsque le pourcentage approche 100 %, le pourcentage passe du vert au jaune. Si le pourcentage dépasse 100 %, il devient rouge.
- Ratio entre le nombre de licences attribuées et le nombre de licences achetées.
- Temps restant avant expiration de l'abonnement au service de cloud. Si l'abonnement expire dans les 90 jours suivants, un message d'avertissement apparaît.

Pour obtenir une vue détaillée des licences de votre service de cloud, cliquez sur Détails d'utilisation des licences. Vous pouvez ensuite voir une ventilation des tendances d'utilisation mensuelles et des utilisateurs individuels qui consomment des licences de service cloud.

Cette ventilation vous montre les informations suivantes :

- **Nombre total de licences :** nombre total de licences achetées pour le service cloud pour toutes les prestations.
- **Attribution cumulée :** licences de service cloud déjà attribuées au début de chaque mois. Par exemple, si une licence est attribuée à un utilisateur en juillet, cette attribution est comptabilisée dans le nombre d'attributions cumulées du mois d'août.
- **Nouvellement attribuées :** nombre de licences de service cloud qui ont été attribuées chaque mois. Par exemple, un utilisateur qui accède au service cloud pour la première fois en juillet se voit attribuer une licence. Cette licence est comptabilisée dans le nombre de licences nouvellement attribuées pour juillet.

La vue Détails d'utilisation des licences affiche également une liste des utilisateurs individuels auxquels des licences ont été attribuées et quand ces licences ont été attribuées.



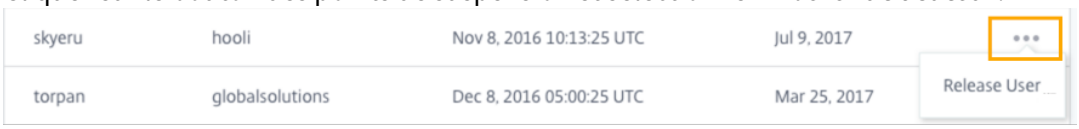
Libérer des licences attribuées

Une licence attribuée peut être libérée si l'utilisateur n'a pas utilisé le service de cloud pendant 30 jours consécutifs. Pour Virtual Apps and Desktops Service, vous pouvez libérer des licences pour les utilisateurs qui n'ont pas lancé d'applications ou de postes de travail au cours des 30 derniers jours. Après libération d'une licence d'utilisateur, l'utilisateur peut acquérir une autre licence en se connectant et en utilisant le service de cloud.

Sur la page Détails d'utilisation des licences, la liste des utilisateurs affiche des boutons de points de suspension cliquables pour les utilisateurs dont les licences peuvent être libérées. Le bouton des points de suspension est inactif pour les utilisateurs qui ont utilisé le service de cloud au cours des 30 derniers jours. Lorsqu'une licence est libérée, le nombre de licences restantes augmente et le nombre de licences attribuées diminue en conséquence.

Pour libérer des licences attribuées

1. Sur la page **Détails d'utilisation des licences**, faites défiler jusqu'à la liste des utilisateurs.
2. Pour libérer la licence d'utilisateur individuel :
   a) Localisez l'utilisateur que vous voulez gérer.
   b) Cliquez sur le bouton des points de suspension et sélectionnez **Libérer utilisateur**.



3. Pour libérer plusieurs utilisateurs à la fois :
   a) Cliquez sur **Libérer utilisateurs**. Une liste affiche tous les utilisateurs dont les licences peuvent être libérées.
   b) Sélectionnez les utilisateurs que vous souhaitez gérer et cliquez sur **Continuer**.
4. Lorsque vous êtes invité à confirmer la libération, cliquez sur **Libérer**.

Questions fréquentes

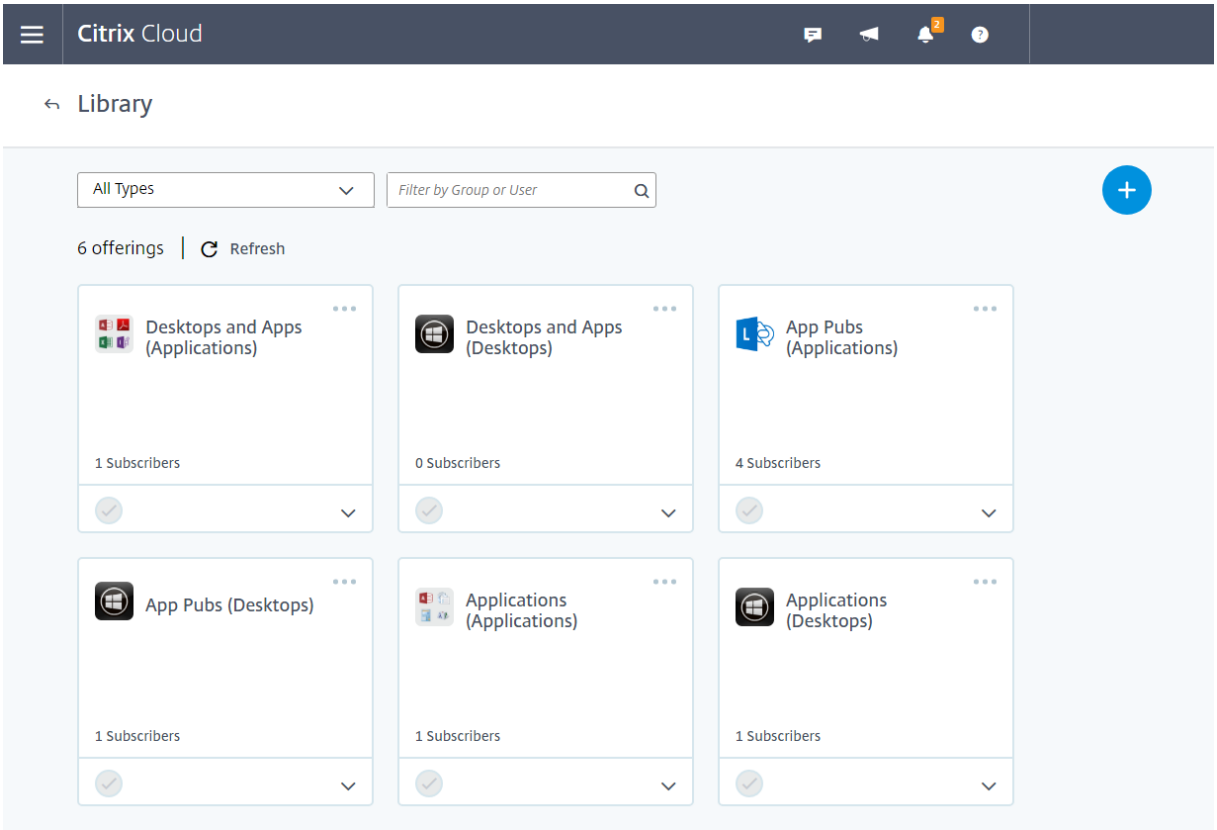
- **Qu'est-ce qu'une attribution de licence ?** En général, l'attribution de licence se produit lorsqu'un utilisateur accède et utilise le service cloud pour la première fois. Pour Virtual Apps and Desktops Service, une licence est attribuée lorsqu'un utilisateur lance une application ou un poste de travail pour la première fois.
- **Citrix empêche-t-il l'utilisation du service cloud si les licences attribuées dépassent le nombre de licences achetées ?** Non, Citrix n'empêche le lancement d'aucun service en cas de dépassement du nombre de licences de cloud que vous achetées. L'utilisation des licences fournit des informations permettant de suivre votre consommation de licences cloud. Citrix s'attend donc à ce que vous surveilliez vos attributions de licences et que vous respectiez les limites. Si, à un moment donné, vous pensez que vous allez consommer plus de licences que ne le permet votre service, Citrix vous encourage à contacter votre représentant commercial pour discuter de vos besoins en matière de licences.
- **Quelles informations de licence sont-elles capturées ?** Actuellement, seules les informations de licence associées aux connexions utilisateur sont capturées.

Attribuer des utilisateurs et des groupes à des offres de services à l'aide de la bibliothèque

November 7, 2018

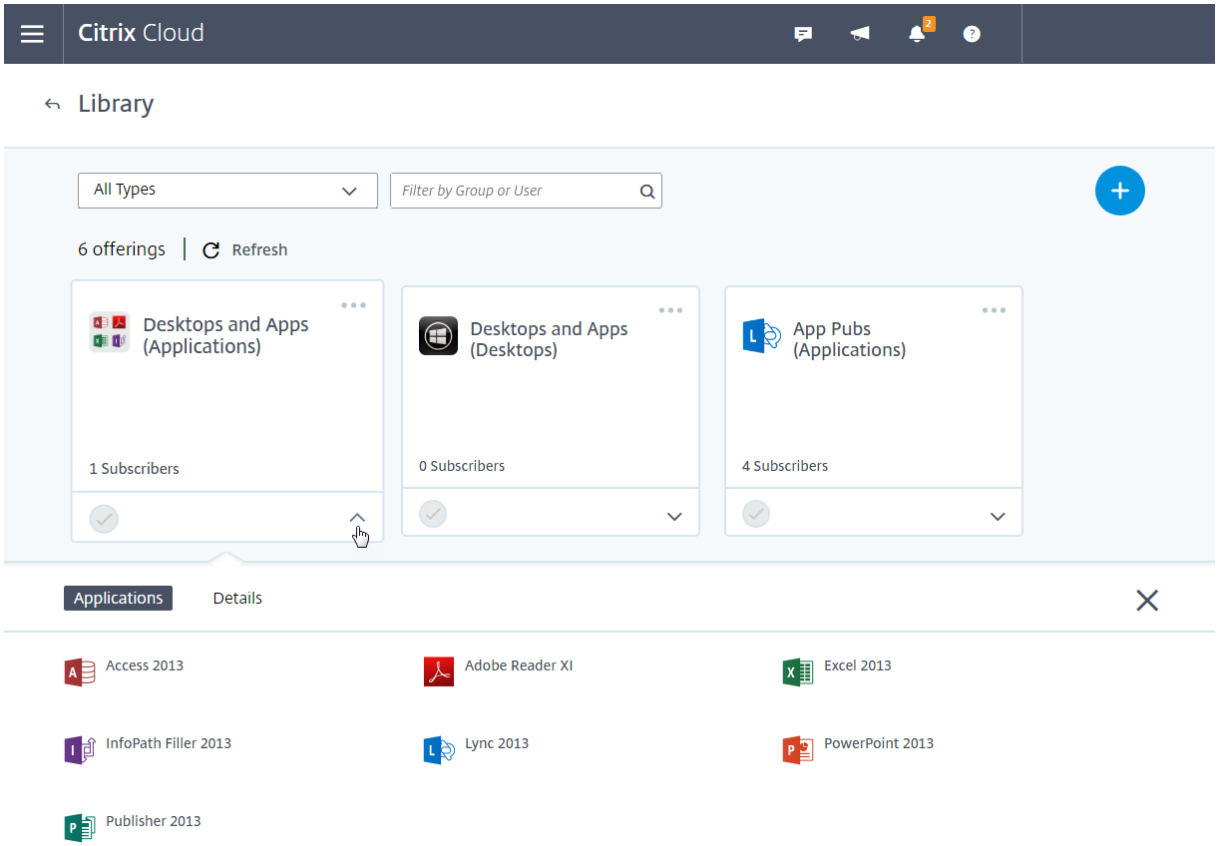
Vous pouvez attribuer des ressources ou d'autres éléments que vous configurez dans un service (par exemple, les bureaux ou les applications configurés dans Virtual Apps and Desktops Service) à vos utilisateurs et groupes Active Directory à l'aide de la bibliothèque.

Les offres peuvent comporter des applications, des postes de travail, des partages de données et des applications web que vous créez via un service Citrix. La bibliothèque affiche toutes vos offres dans une seule vue.



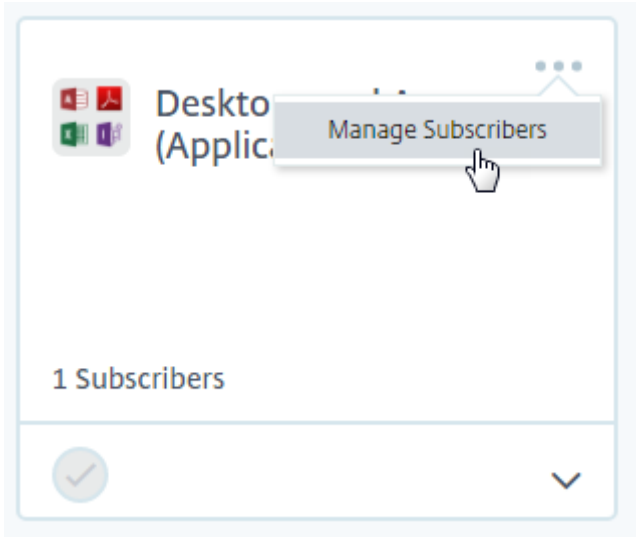
Afficher les détails d’une offre

Pour afficher les applications, les postes de travail, les stratégies et toute autre information relative à l’offre, cliquez sur la flèche sur la carte d’offre.



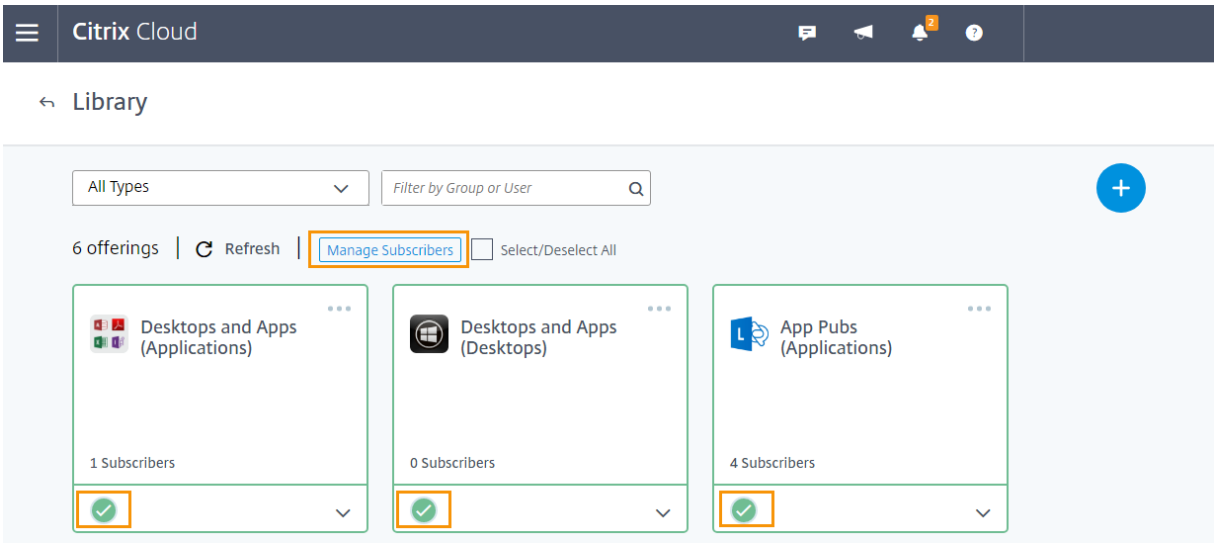
Ajouter ou supprimer des abonnés

Pour gérer les utilisateurs ou groupes d'une seule offre, cliquez sur **Gérer les abonnés** dans le menu de la carte d'offre.

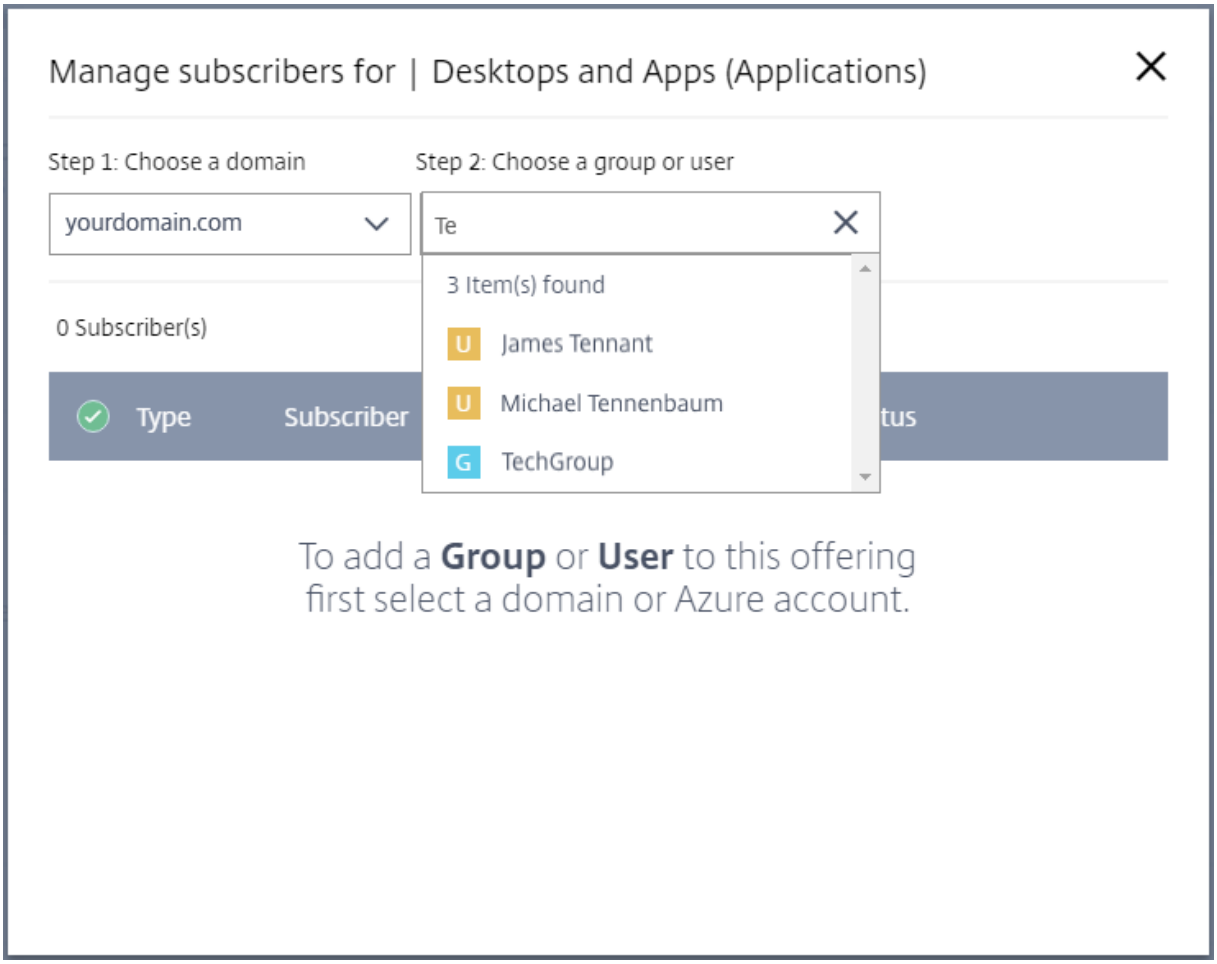


Pour gérer les abonnés pour plusieurs offres, sélectionnez la coche de chaque offre et cliquez sur

Gérer les abonnés.

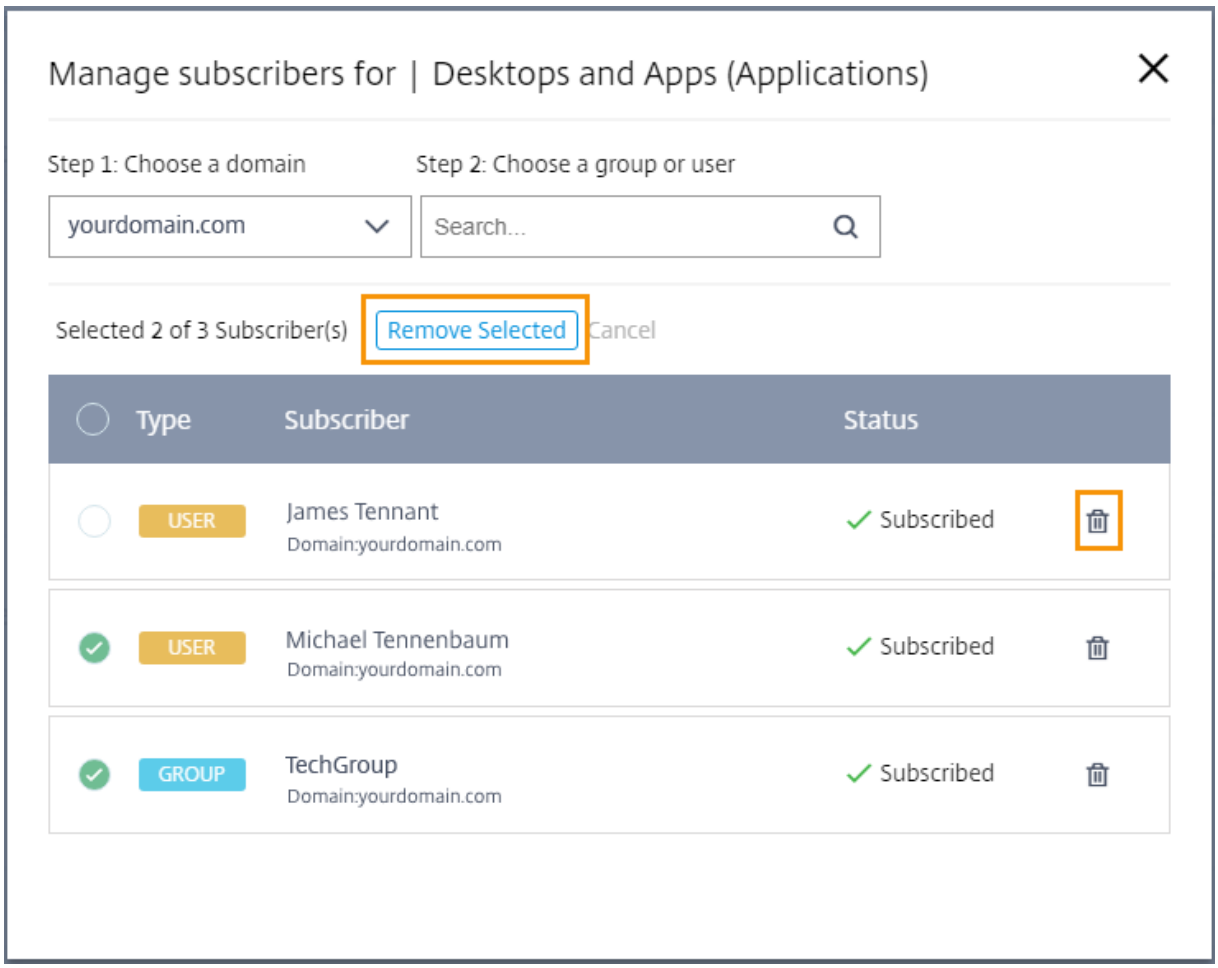


Pour ajouter des abonnés à l'offre, choisissez un domaine et sélectionnez les utilisateurs ou groupes que vous souhaitez ajouter.



Pour supprimer un seul abonné, cliquez sur l'icône de corbeille pour un utilisateur ou groupe. Pour

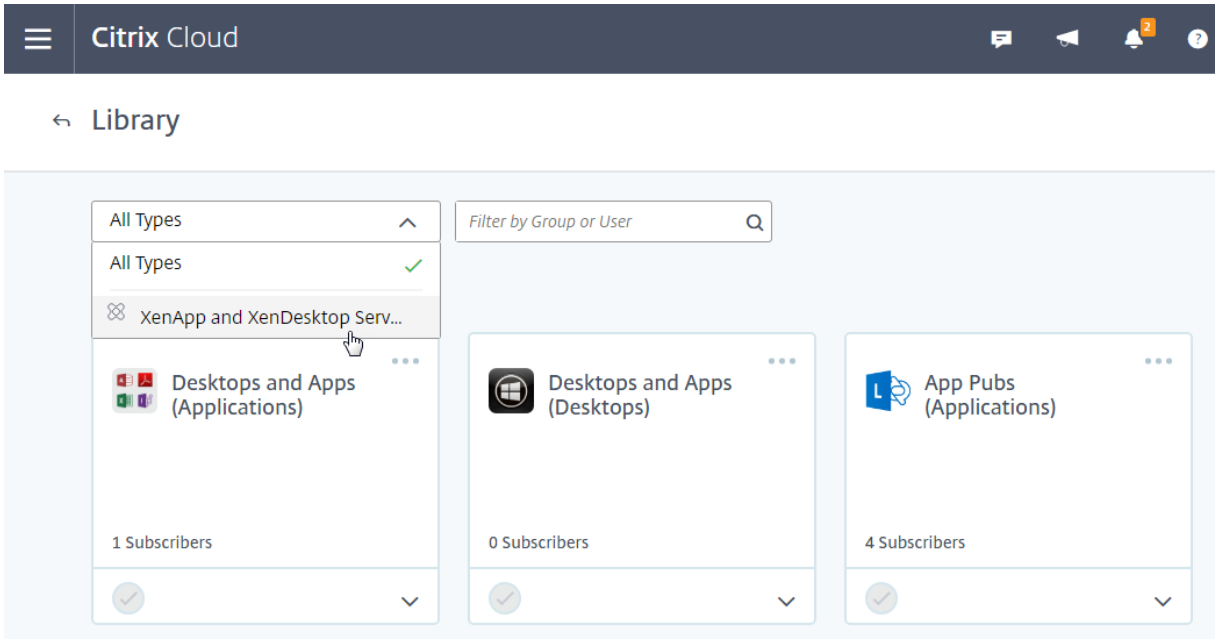
supprimer plusieurs abonnés, sélectionnez les utilisateurs ou groupes et cliquez sur **Supprimer la sélection**.



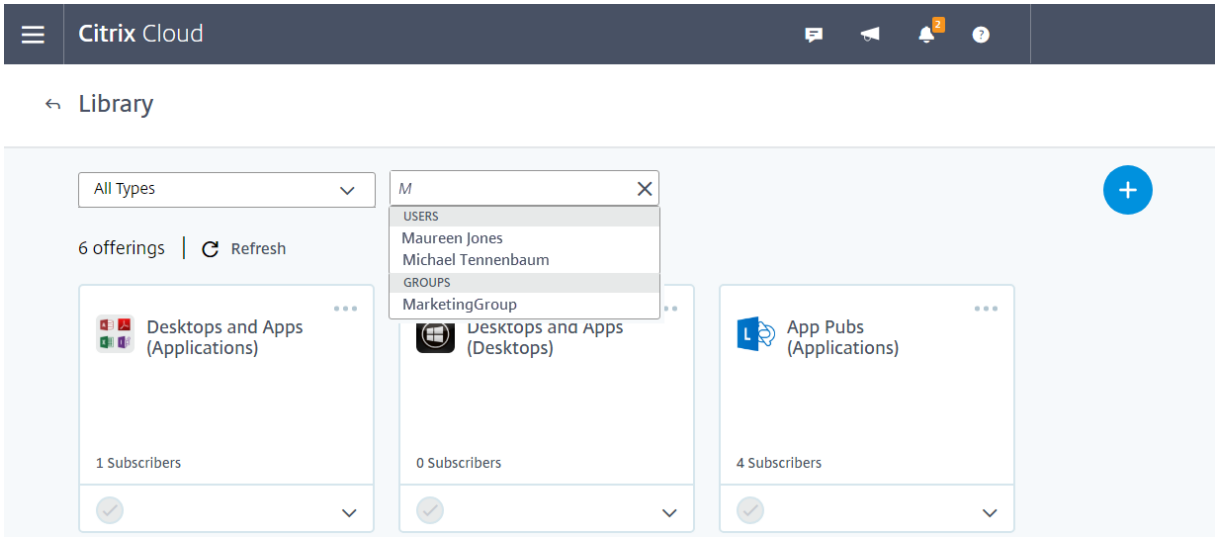
Après avoir ajouté ou supprimé des abonnés d'une offre, la carte d'offre affiche le nombre actuel d'abonnés.

Filtrer les offres

Par défaut, la bibliothèque affiche toutes les offres. Pour afficher rapidement toutes les offres d'un service spécifique, sélectionnez le filtre de ce service.



Vous pouvez également rechercher un utilisateur ou un groupe actuellement abonné à une offre dans la bibliothèque. Citrix Cloud affiche uniquement les offres appartenant à l'utilisateur ou au groupe que vous sélectionnez. Pour voir les offres de tous les utilisateurs, cliquez sur le X pour effacer le filtre.



Fonctionnalités pour les partenaires Citrix

August 1, 2018

Citrix Cloud propose des services, des fonctionnalités et des expériences conçus pour les clients et les partenaires. Cette section présente les fonctionnalités à disposition des partenaires Citrix qui les aideront à collaborer avec leurs clients sur les services et les solutions Citrix Cloud.

Identification des partenaires

Les partenaires sont identifiés dans Citrix Cloud en fonction de leur ID d'organisation Citrix. Chaque compte Citrix Cloud est associé à un ID d'organisation Citrix pouvant être affiché dans les détails du compte Citrix Cloud.

Si l'ID d'organisation du compte est membre actif d'un programme partenaire Citrix (tel que Citrix Solution Advisor ou Citrix Service Provider), le badge du programme s'affiche, indiquant que ce compte appartient à un partenaire Citrix. L'identification du partenaire est ensuite utilisée pour déterminer l'accès à des services ou fonctionnalités cloud supplémentaires.

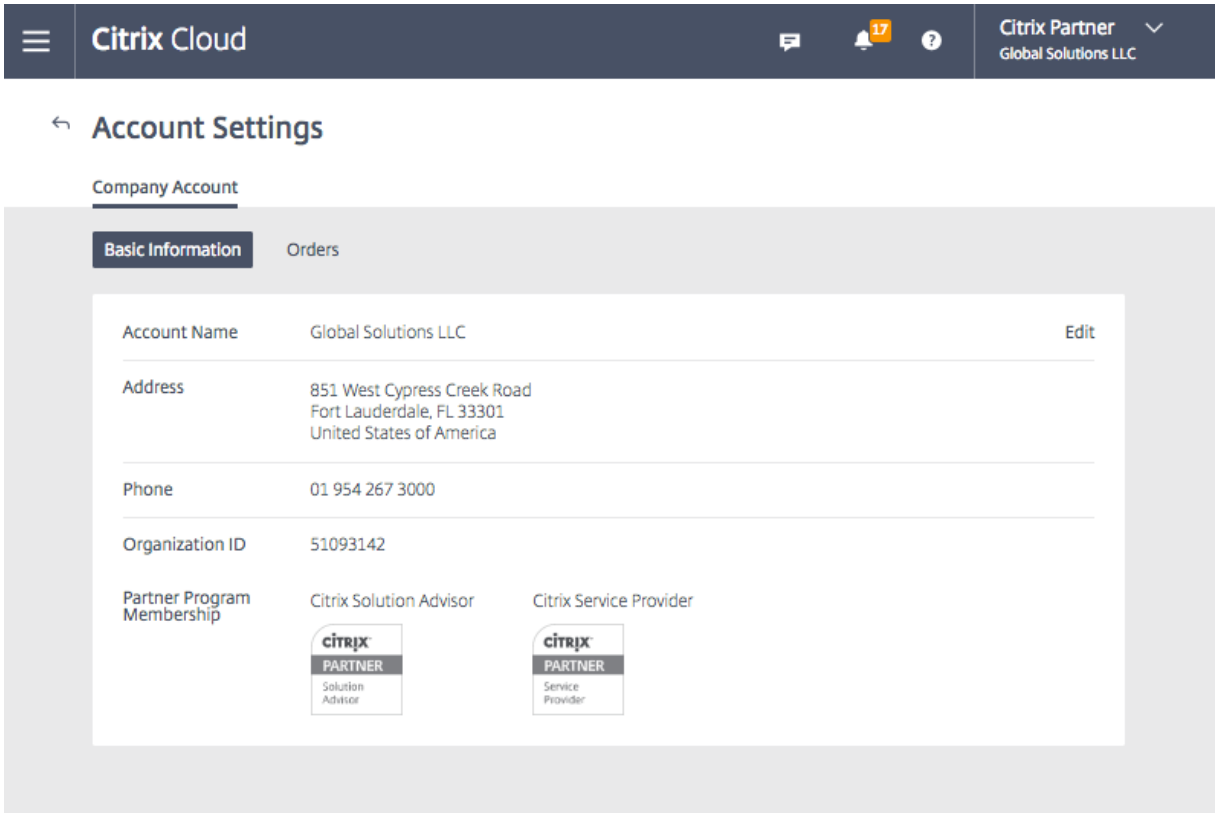
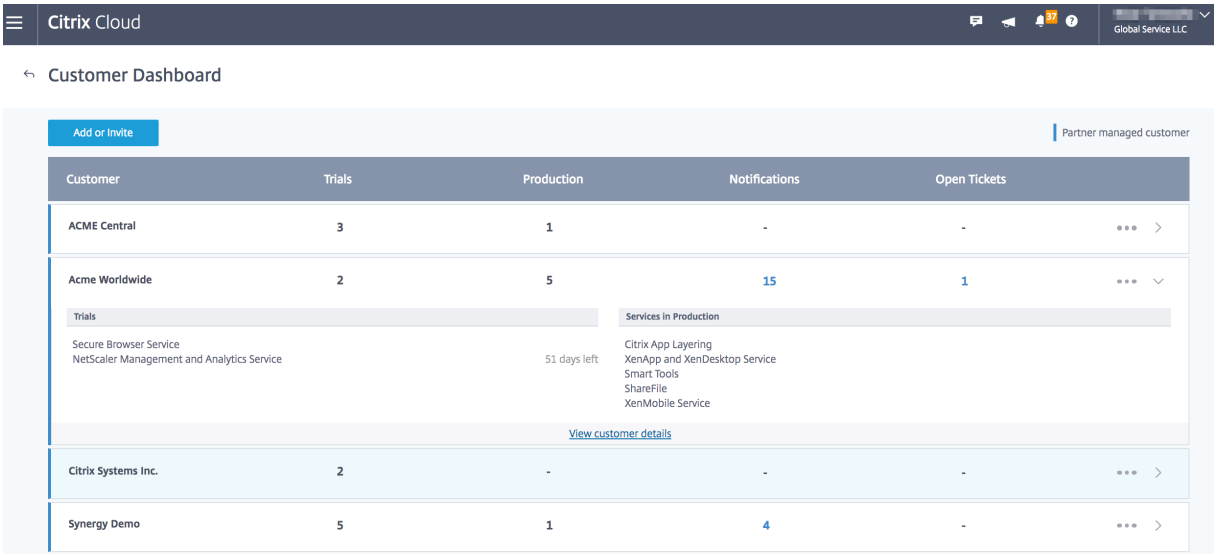


Tableau de bord client

Le tableau de bord client est conçu pour permettre aux partenaires d'afficher l'état de leurs clients Citrix Cloud dans une vue consolidée. Pour qu'un client apparaisse sur le tableau de bord, une connexion doit être établie entre le partenaire et le client. Le tableau de bord client est disponible sur les comptes Citrix Cloud avec badge partenaire.



Connexion avec les clients

Les partenaires qui collaborent avec leurs clients sur les solutions Citrix Cloud peuvent établir un lien de confiance entre leurs comptes. Cette relation au niveau du compte permet à un client de partager facilement des informations spécifiques avec un partenaire. En acceptant de se connecter à un partenaire, un client autorise le partenaire à voir des informations sur son compte Citrix Cloud et sa relation avec Citrix.

Lorsqu'une connexion de partenaire est établie :

- Le client apparaît sur le tableau de bord du partenaire
- Le partenaire apparaît en tant que connexion active dans les paramètres du compte client
- Les partenaires voient les droits d'utilisation des services Citrix Cloud

Informations supplémentaires sur les connexions de partenaire :

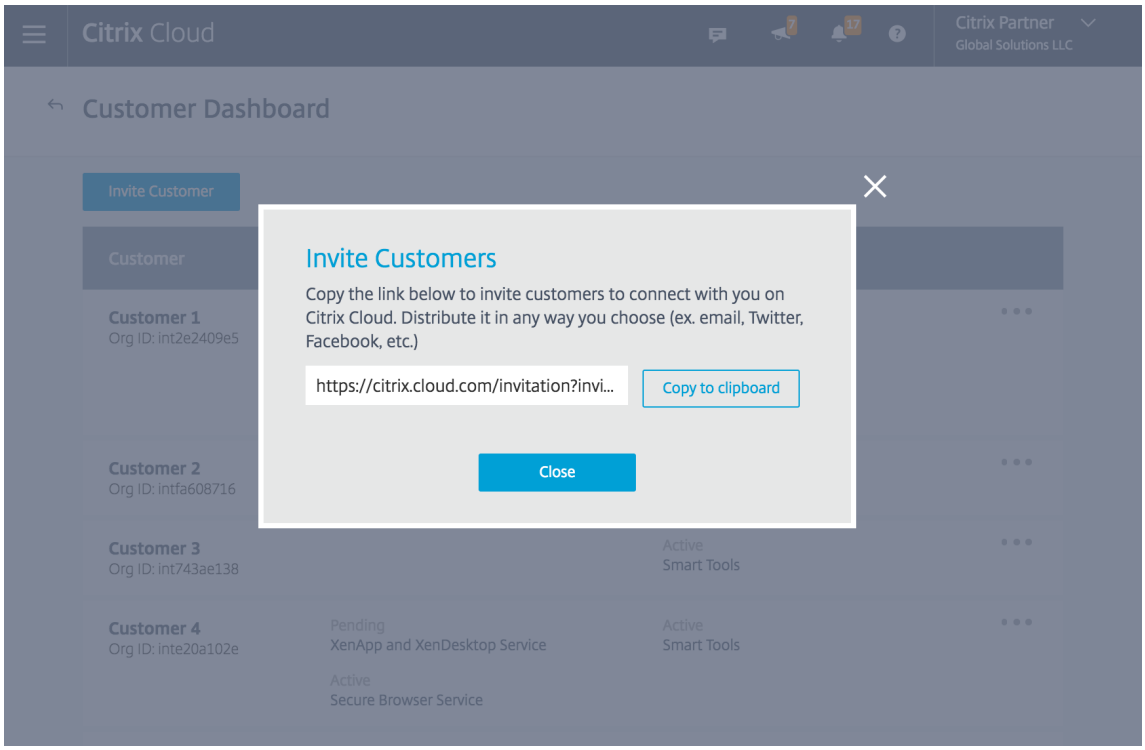
- Les partenaires peuvent établir des connexions avec plusieurs clients
- Les clients peuvent établir des connexions avec plusieurs partenaires
- Il n'y a pas de limite au nombre de connexions client-partenaire
- Les connexions peuvent être annulées à tout moment par le client ou le partenaire
  - Par le client dans la page d'informations de compte
  - Par le partenaire à l'aide du tableau de bord client
- Des notifications Cloud Citrix sont envoyées en fonction du workflow de connexion
  - Le partenaire est averti lorsqu'une connexion client est établie
  - Le partenaire est informé si le client met fin à la connexion
  - Le client est informé si le partenaire met fin à la connexion
- Les connexions partenaire-client n'expirent pas

Une fois que la connexion est établie entre le partenaire et le client, les administrateurs de partenaire ont accès aux informations de base sur le compte du client, aux commandes passées par le client ainsi qu'aux informations sur les droits telles que les services, le nombre de licences, les dates d'expiration et ainsi de suite.

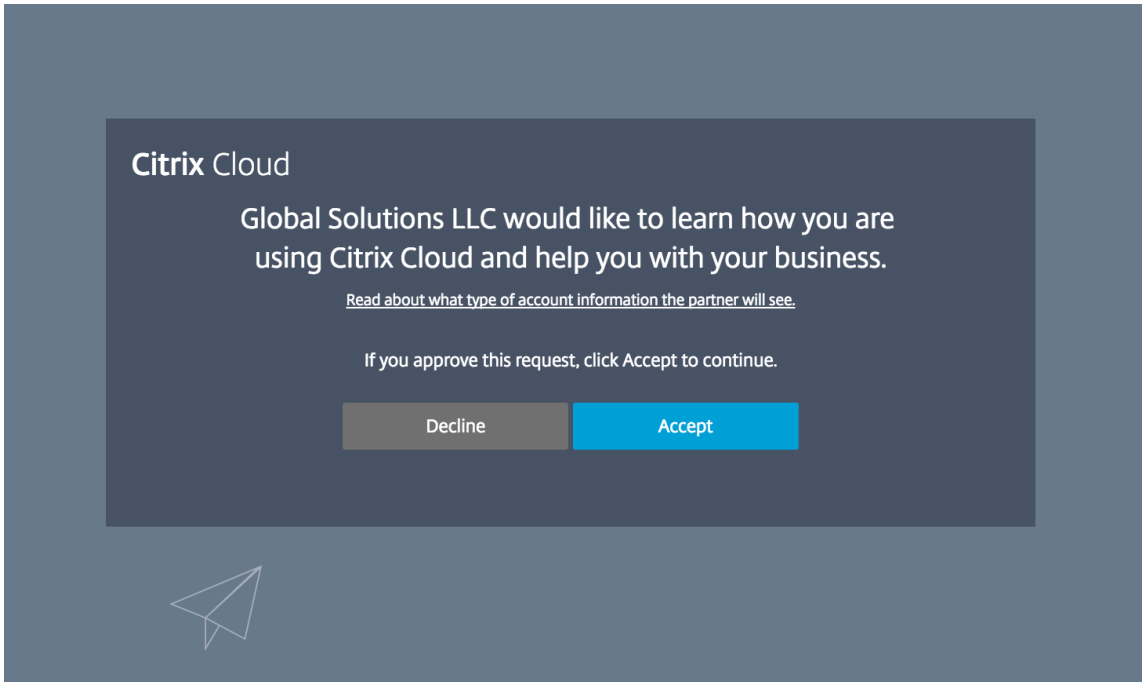
Inviter un client à se connecter

Les partenaires se connectent avec les clients en trois étapes simples :

1. Le partenaire récupère son lien d'invitation à partir du tableau de bord client



2. Le partenaire copie le lien d'invitation et le fournit au client
3. Le client clique sur le lien, se connecte (ou s'inscrit) et accepte la demande de connexion



Informations supplémentaires sur les liens d'invitation :

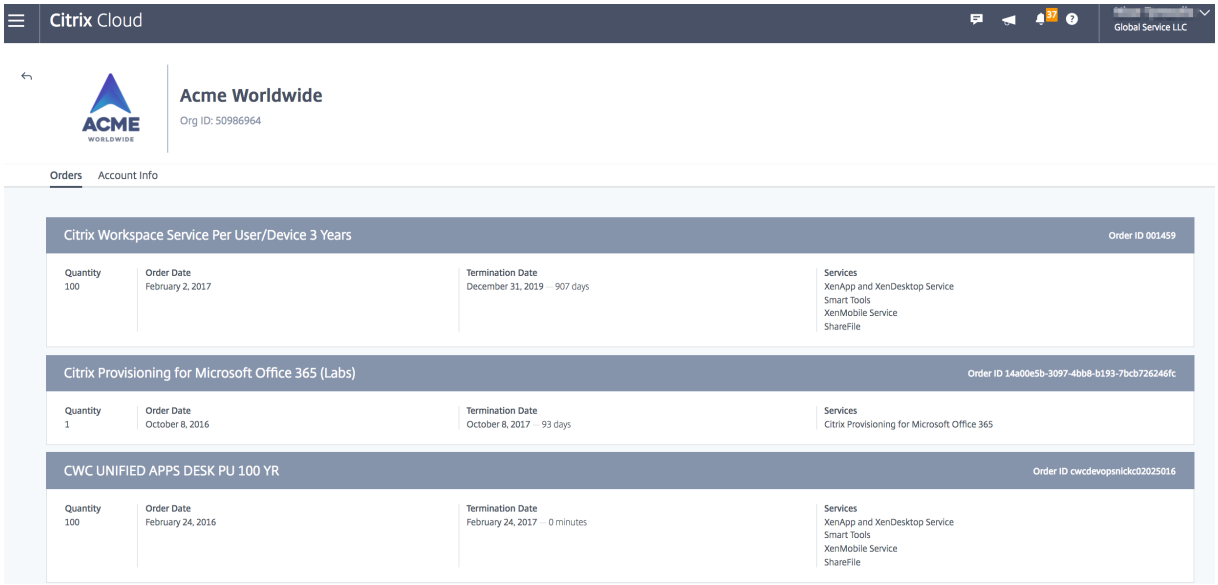
- Les partenaires disposent d'un seul lien d'invitation ; le lien est fixe et ne peut être ni personnalisé ni modifié.
- Il n'existe aucune limite au nombre de fois que le lien peut être utilisé pour établir une connexion.
- Le lien peut être réutilisé si une connexion doit être recréée.
- Le lien n'expire pas.

Partage des informations de compte avec des partenaires

Les partenaires voient les droits d'utilisation des services Citrix Cloud

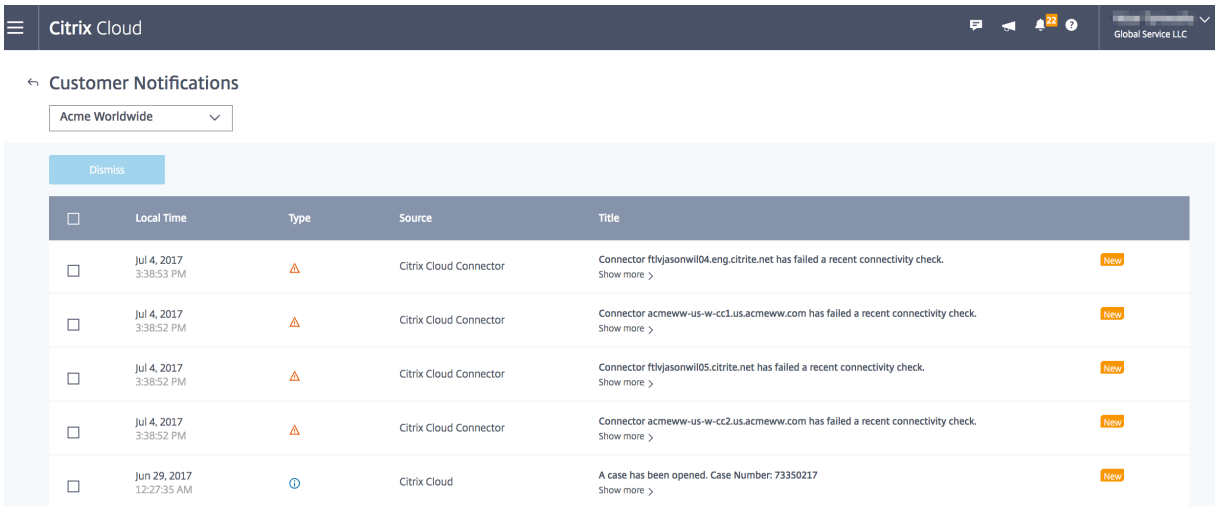
Lorsqu'un client accepte l'invitation de connexion d'un partenaire Citrix, le partenaire peut voir des informations de base sur les droits d'utilisation des services Citrix Cloud pour ce client. Ces informations incluent l'état des droits d'utilisation des versions d'évaluation et standard. Informations supplémentaires :

- Évaluations de service en cours
- Demandes d'évaluation de service en attente
- Évaluations de service qui ont expiré
- Droits d'utilisation en cours (services achetés ou autrement autorisés/activés pour le client)
- Nombre de licences et date d'expiration des droits

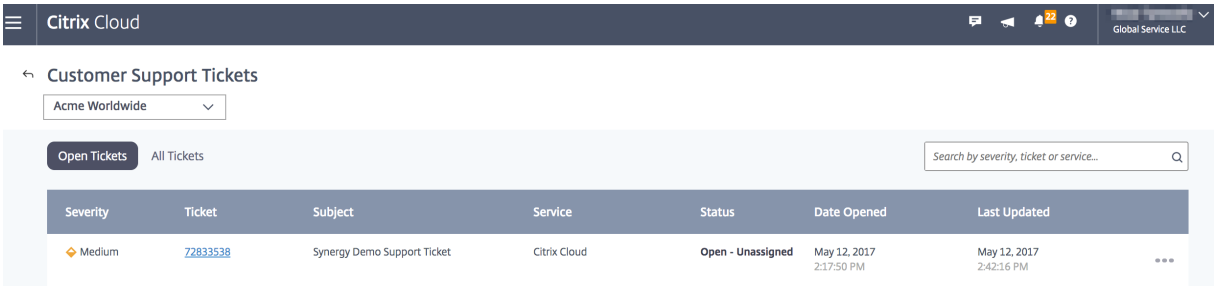


Visibilité des partenaires sur les tickets de support et les notifications des clients

Les partenaires peuvent afficher les tickets de support et les notifications des clients connectés. Les partenaires peuvent également filtrer les notifications spécifiques au client et prendre des mesures comme ignorer une notification. Le partenaire ne verra plus cette notification ; toutefois, les clients pourront toujours la voir dans leur compte après s'être connectés à Citrix Cloud.



La visibilité des tickets de support des clients aidera les partenaires à résoudre les problèmes de leurs clients, garantissant ainsi une expérience simplifiée et sans erreur pour leurs utilisateurs.

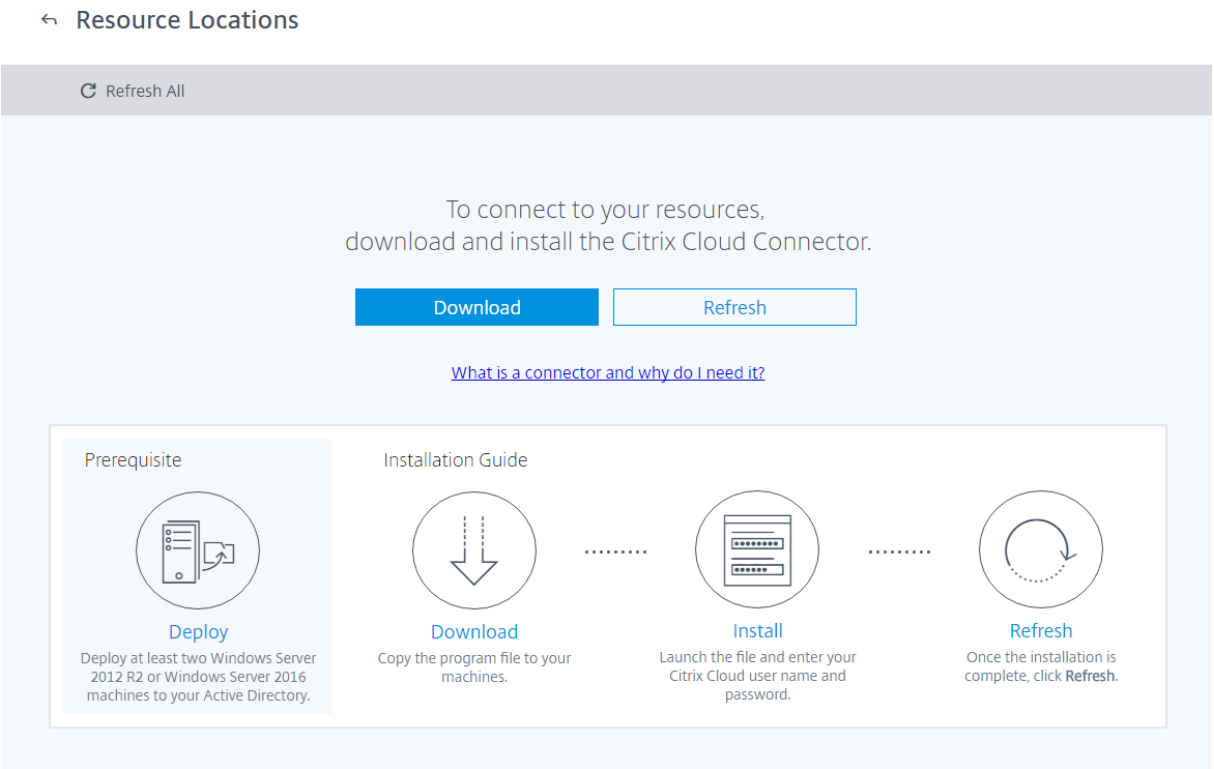


Emplacements des ressources

November 7, 2018

Les emplacements de ressources contiennent les ressources requises pour fournir des services à vos abonnés. Vous pouvez gérer ces ressources à partir de la console Citrix Cloud.

Types de ressources



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 abonnés.

Les ressources sont souvent les suivantes :

- Domaines Active Directory
- Appliances Citrix ADC
- Hyperviseurs tels que Citrix XenServer
- VDA
- Serveurs StoreFront
- Machines hébergeant l'agent Citrix Smart Tools

Les emplacements de ressources contiennent également les Citrix Cloud Connector nécessaires pour établir la communication entre vos ressources et Citrix Cloud. Pour plus de détails sur l'utilisation des Cloud Connector dans votre emplacement de ressources, voir Citrix Cloud Connector.

Emplacement des ressources

Votre emplacement de ressources est l'endroit où vos ressources résident, qu'il s'agisse d'un cloud public ou privé, d'une succursale ou d'un datacenter. Si vous disposez déjà de ressources dans votre propre cloud ou datacenter, vos ressources restent là où elles sont. Il n'est pas nécessaire de les déplacer pour les utiliser avec Citrix Cloud.

Le choix de l'emplacement peut être influencé par les facteurs suivants :

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

Il n'existe aucune restriction sur le nombre d'emplacements de ressources dont vous pouvez disposer. Les frais afférents à un emplacement de ressources sont faibles.

Restrictions de dénomination

Les caractères suivants ne sont pas autorisés lors de la création de noms pour des emplacements de ressources :

- ##, $, %, ^, &, ?
- Accolades : [], { }
- Barres verticales (|)
- Symbole inférieur à (<)
- Barres obliques et barres obliques inverses (/, \)

Emplacements de ressources principaux

Un emplacement de ressources principal est un emplacement de ressources que vous désignez comme étant « l'emplacement préféré » pour les communications entre votre domaine et Citrix

Cloud. L'emplacement de ressources que vous sélectionnez comme « principal » doit disposer de Cloud Connector qui offrent les meilleures performances et la meilleure connectivité à votre domaine. Cela permet à vos utilisateurs de se connecter rapidement à Citrix Cloud.

Pour de plus amples informations, consultez la section Sélectionner un emplacement de ressources principal.

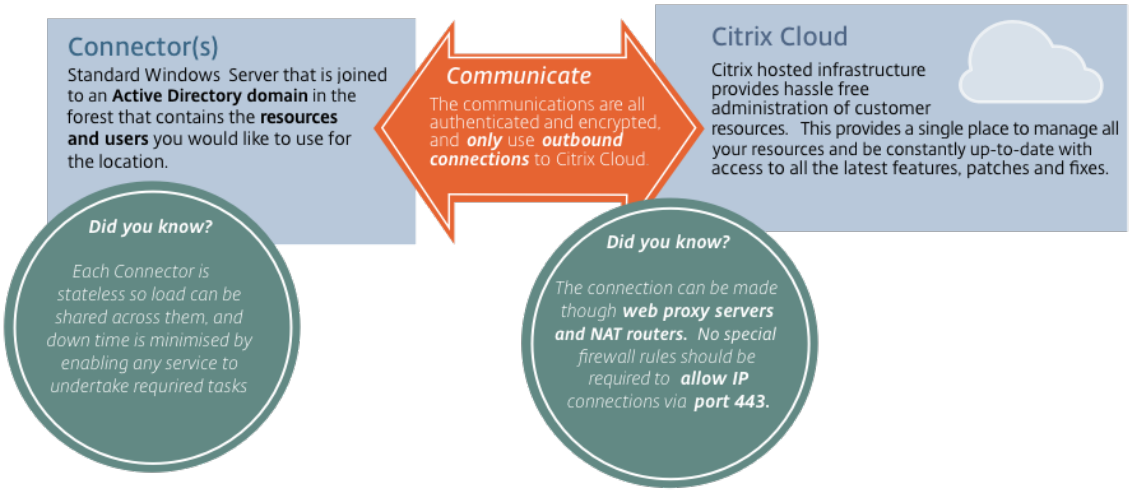
Exemple de déploiement d'un emplacement de ressources

- Créez votre premier emplacement de ressources dans votre datacenter pour le siège social en fonction des applications et des abonnés qui doivent être proches des données.
- Ajoutez un second emplacement de ressources pour vos utilisateurs internationaux dans un cloud public. Ou créez des emplacements de ressources distincts dans les succursales pour fournir les applications les plus utilisées à proximité des employés de la succursale.
- Ajoutez un autre emplacement de ressources sur un réseau distinct qui fournit des applications restreintes. Ceci offre une visibilité limitée aux autres ressources et abonnés sans avoir à ajuster les autres emplacements de ressources.

Citrix Cloud Connector

November 7, 2018

Le Citrix Cloud Connector est un composant Citrix qui sert de canal de communication entre Citrix Cloud et vos emplacements de ressources, ce qui permet d'administrer le cloud sans qu'il soit nécessaire d'effectuer des configurations réseau ou d'infrastructure complexes. Il élimine les contraintes qu'implique la gestion d'une infrastructure de mise à disposition. Il vous permet de gérer et d'axer la priorité sur les ressources qui apportent de la valeur à vos utilisateurs.



Services qui requièrent le Cloud Connector

Virtual Apps and Desktops Service requiert le Cloud Connector. Citrix Endpoint Management requiert le Cloud Connector pour la connectivité d'entreprise au Endpoint Management Service.

Où obtenir le Cloud Connector ?

Vous pouvez télécharger le logiciel Cloud Connector à partir de Citrix Cloud.

1. Connectez-vous à Citrix Cloud.
2. Dans le menu en haut à gauche de l'écran, sélectionnez **Emplacements des ressources**.
3. Si vous ne disposez d'aucun emplacement de ressources, cliquez sur **Télécharger** sur la page Emplacements des ressources. Lorsque vous y êtes invité, enregistrez le fichier **cwcconnector.exe**.
4. Si vous disposez déjà d'un emplacement de ressources, mais qu'aucun Cloud Connector n'est installé, cliquez sur la barre Cloud Connector et cliquez sur **Télécharger**. Lorsque vous y êtes invité, enregistrez le fichier **cwcconnector.exe**.

Où dois-je installer le Cloud Connector ?

Installez le Cloud Connector sur une machine exécutant Windows Server 2012 R2 ou Windows Server 2016. Cette machine doit être jointe à votre domaine et capable de communiquer avec les ressources que vous souhaitez gérer depuis Citrix Cloud.

Chaque emplacement de ressources doit contenir suffisamment de Cloud Connector pour supporter votre charge, et au moins un connecteur supplémentaire pour garantir une haute disponibilité. Citrix recommande au moins deux Cloud Connector dans chaque emplacement de ressources.

Comment automatiser l'installation du Cloud Connector ?

L'installation silencieuse ou les déploiements en push du connecteur à l'aide d'une stratégie de groupe ou d'autres systèmes de déploiement est prise en charge. Reportez-vous à la section Détails techniques sur Citrix Cloud Connector pour connaître les paramètres requis pour l'installation silencieuse.

Communication avec le Cloud Connector

Le Cloud Connector authentifie et crypte toutes les communications entre Citrix Cloud et vos emplacements de ressources. Toutes les communications entre le Cloud Connector et Citrix Cloud sont sortantes. Toutes les connexions sont établies depuis le Cloud Connector vers le cloud à l'aide du port HTTPS standard (443) et du protocole TCP. Aucune connexion entrante n'est acceptée.

Fonctions du Cloud Connector

- **Active Directory (AD) :** autorise la gestion d'Active Directory, ce qui permet d'utiliser des forêts et des domaines Active Directory au sein de vos emplacements de ressources. Cela supprime le besoin d'ajouter des approbations Active Directory supplémentaires.
- **Publication de Virtual Apps and Desktops :** permet la publication depuis des ressources dans vos emplacements de ressources.
- **Endpoint Management** : offre un environnement de gestion de la flotte mobile (MDM) et des applications mobiles (MAM) afin de gérer les stratégies d'appareil et d'application et mettre à disposition des applications aux utilisateurs.
- **Provisioning de groupe de mise à disposition :** permet le provisioning de machines directement dans vos emplacements de ressources.

Remarque : bien qu'opérationnelle, cette fonctionnalité peut être limitée pendant la période de temps pendant laquelle la connexion à Citrix Cloud n'est pas disponible. Vous pouvez surveiller l'intégrité du Cloud Connector à partir de la console Citrix Cloud.

Disponibilité du Cloud Connector

Pour garantir une disponibilité continue, installez plusieurs Cloud Connector dans chacun de vos emplacements de ressources. Citrix recommande au moins deux (2) Cloud Connector dans chaque emplacement de ressources. Si un Cloud Connector est indisponible pendant une période de temps, les autres Cloud Connector peuvent prendre en charge la connexion.

Tant qu'un Cloud Connector est disponible, la communication avec Citrix Cloud ne sera pas interrompue. La connexion de l'utilisateur aux ressources dans l'emplacement de ressources ne repose pas sur une connexion à Citrix Cloud, dans la mesure du possible. Cela permet à l'emplacement de ressources d'offrir aux utilisateurs un accès à leurs ressources, qu'une connexion soit établie ou non avec Citrix Cloud.

Gestion de la charge

Gérez la charge en installant plusieurs Cloud Connector dans chaque emplacement de ressources. Étant donné que chaque Cloud Connector est sans état, la charge peut être distribuée sur tous les Cloud Connector disponibles. Il n'est pas nécessaire de configurer cette fonction d'équilibrage de charge. Elle est complètement automatisée.

Prise en charge du Cloud Connector

Tant que vous assurez la disponibilité continue du Cloud Connector dans chaque emplacement de ressources, vous pouvez gérer les machines sur lesquelles ils sont installés une à la fois pour éviter les

périodes d'arrêt. Vous pouvez surveiller l'intégrité des Cloud Connector à partir de la console Citrix Cloud.

Détails techniques sur Citrix Cloud Connector

November 7, 2018

Le Citrix Cloud Connector est un composant comprenant divers services Windows installés sur Windows Server 2012 R2 ou Windows Server 2016.

Configuration système requise

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

- Systèmes d'exploitation : Windows Server 2012 R2, Windows Server 2016

  > **Remarque :** Le Cloud Connector n'est pas pris en charge pour une utilisation avec Windows Server Core.

- 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.

Niveaux fonctionnels Active Directory pris en charge

Le Citrix Cloud Connector prend en charge les niveaux fonctionnels de forêt et de domaine suivants dans Active Directory.

Niveau fonctionnel de la forêt	Niveau fonctionnel du domaine	Contrôleurs de domaine pris en charge
Windows Server 2008 R2	Windows Server 2008 R2	Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016
Windows Server 2008 R2	Windows Server 2012	Windows Server 2012, Windows Server 2012 R2, Windows Server 2016
Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2012 R2, Windows Server 2016
Windows Server 2008 R2	Windows Server 2016	Windows Server 2016
Windows Server 2012	Windows Server 2012	Windows Server 2012, Windows Server 2012 R2, Windows Server 2016
Windows Server 2012	Windows Server 2012 R2	Windows Server 2012 R2, Windows Server 2016
Windows Server 2012	Windows Server 2016	Windows Server 2016
Windows Server 2012 R2	Windows Server 2012 R2	Windows Server 2012 R2, Windows Server 2016
Windows Server 2012 R2	Windows Server 2016	Windows Server 2016
Windows Server 2016	Windows Server 2016	Windows Server 2016

Prise en charge de la norme FIPS (Federal Information Processing Standard)

Le Citrix Cloud Connector n'est pas pris en charge sur les machines compatibles FIPS. Ces machines utilisent uniquement des algorithmes cryptographiques certifiés FIPS que le logiciel Cloud Connector ne prend pas en charge. Si vous tentez d'installer le Cloud Connector sur une machine compatible FIPS, l'installation échoue. Installez Cloud Connector uniquement sur des machines sur lesquelles FIPS n'est pas activé.

Afficher l'état du Cloud Connector

La page Emplacements des ressources dans Citrix Cloud affiche l'état de tous les Cloud Connector dans vos emplacements de ressources.

Messages d'événements

Des messages d'événements sont disponibles dans l'Observateur d'événements Windows sur la machine connecteur. Les journaux d'événements Windows générés par le Cloud Connector se trouvent dans les documents suivants :

- Connector Agent Provider [format XML]
- Connector AgentWatchDog Provider [format XML]

Journaux d'événements

Par défaut, les journaux d'événements figurent dans le répertoire C:\ProgramData\Citrix\WorkspaceCloud\Logs de la machine hébergeant le Cloud Connector.

Résoudre les problèmes liés au Cloud Connector

La première chose à faire pour diagnostiquer des problèmes avec le Cloud Connector est de vérifier les messages d'événements et les journaux d'événements. Si le Cloud Connector n'est pas répertorié dans votre emplacement de ressources ou qu'il n'est « pas en contact », les journaux d'événements fourniront des informations initiales.

Si le Cloud Connector est « déconnecté » et que les journaux d'événements n'indiquent pas pourquoi la connexion ne peut pas être établie entre le Cloud Connector et Citrix Cloud, contactez le support Citrix.

Si le Cloud Connector indique un état « d'erreur », il est possible qu'il y ait un problème d'hébergement du Cloud Connector. Installez le Cloud Connector sur une nouvelle machine. Si le problème persiste, contactez le support Citrix.

Pour résoudre les problèmes d'installation ou d'utilisation de Cloud Connector, reportez-vous à l'article CTX221535.

Installation de Cloud Connector

November 7, 2018

Vous pouvez installer le logiciel Cloud Connector de manière interactive ou à l'aide de l'installation silencieuse ou automatisée.

Lors de l'installation, le Cloud Connector requiert l'accès au cloud pour authentifier l'utilisateur effectuant l'installation, valider les autorisations du programme d'installation et télécharger et configurer les services fournis par le Cloud Connector. L'installation s'effectue avec les privilèges de l'utilisateur qui lance l'installation.

Exigences

- Assurez-vous que chaque machine sur laquelle vous installez le Cloud Connector répond à la configuration système requise décrite dans Détails techniques sur Citrix Cloud Connector.
- Assurez-vous que les machines sur lesquelles vous allez installer le Cloud Connector remplissent les Exigences en terme de connexion Internet.
- Si vous installez le Cloud Connector dans un environnement doté d'un proxy Web ou de règles de pare-feu strictes, consultez la section Configuration du pare-feu et du proxy d'un Cloud Connector pour prendre connaissance des exigences avant de poursuivre l'installation.
- Vous pouvez uniquement installer le Cloud Connector sur une machine appartenant au domaine. Si la machine n'appartient pas à un domaine, le programme d'installation du Cloud Connector empêche l'installation.
- Le Cloud Connector doit pouvoir accéder aux contrôleurs de domaine parent (racine) ainsi qu'aux contrôleurs de domaine enfant de l'infrastructure Active Directory (pour compléter les workflows Active Directory) dans lesquels le Cloud Connector est installé. Pour plus d'informations, consultez les articles de support de Microsoft suivants :
  - Comment faire pour configurer un pare-feu pour les domaines et les approbations
  - Ports des services système
- La machine sur laquelle vous installez le Cloud Connector doit être synchronisée avec l'heure UTC.
- Le programme d'installation du Cloud Connector est téléchargé depuis Citrix Cloud. Par conséquent, votre navigateur doit autoriser le téléchargement de fichiers exécutables.
- Désactivez la configuration de sécurité renforcée d'Internet Explorer (IE ESC). Si cette configuration est activée, le Cloud Connector ne pourra pas se connecter à Citrix Cloud.
- Assurez-vous que FIPS n'est pas activé sur la machine sur laquelle vous installez le Cloud Connector. Le Cloud Connector n'est pas pris en charge sur les machines compatibles FIPS. Si vous tentez d'installer le Cloud Connector sur une machine compatible FIPS, l'installation échoue.

Remarques importantes

- Conservez tous les Cloud Connector sous tension à tout moment pour garantir une connexion permanente à Citrix Cloud.
- N'installez pas le Cloud Connector sur un contrôleur de domaine Active Directory ou toute autre machine critique à votre infrastructure d'emplacement de ressources. La maintenance régulière du Cloud Connector exécute des opérations qui entraîneraient un arrêt de ces ressources supplémentaires.
- Ne téléchargez et n'installez pas d'autres produits Citrix sur les machines hébergeant le Cloud Connector.
- Ne téléchargez pas et n'installez pas le Cloud Connector sur des machines faisant partie d'autres

déploiements de produits Citrix (par exemple, Delivery Controller dans un déploiement Citrix Virtual Apps and Desktops).

- Ne mettez pas à niveau un Cloud Connector précédemment installé vers une version plus récente. Au lieu de cela, désinstallez l'ancien Cloud Connector et installez la nouvelle version.
- Citrix recommande vivement d'activer Windows Update sur toutes les machines hébergeant le Cloud Connector. Lors de la configuration de Windows Update, téléchargez et installez automatiquement les mises à jour, mais n'autorisez pas les redémarrages automatiques. La plateforme Citrix Cloud se charge des redémarrages, et ne les autorise que pour un seul Cloud Connector à la fois, au besoin. Vous pouvez également contrôler quand la machine est redémarrée après une mise à jour à l'aide de la stratégie de groupe. Pour plus d'informations, voir https://docs.microsoft.com/en-us/windows/deployment/update/waas-restart.
- Citrix recommande l'installation d'au moins deux (2) Cloud Connector dans chaque emplacement de ressources. En règle générale, le nombre de Cloud Connector que vous devez installer est de N+1, où N est la capacité nécessaire pour prendre en charge l'infrastructure dans votre emplacement de ressources. Ceci garantit la continuité de la connexion entre Citrix Cloud et votre emplacement de ressources au cas où un Cloud Connector devient indisponible.
- Chaque forêt Active Directory que vous prévoyez d'utiliser avec Citrix Cloud doit être accessible par deux Cloud Connector à tout moment.
- Après l'installation, ne déplacez pas la machine qui héberge le Cloud Connector dans un autre domaine. Si la machine doit être jointe à un autre domaine, désinstallez le Cloud Connector et réinstallez-le une fois que la machine est jointe à l'autre domaine.

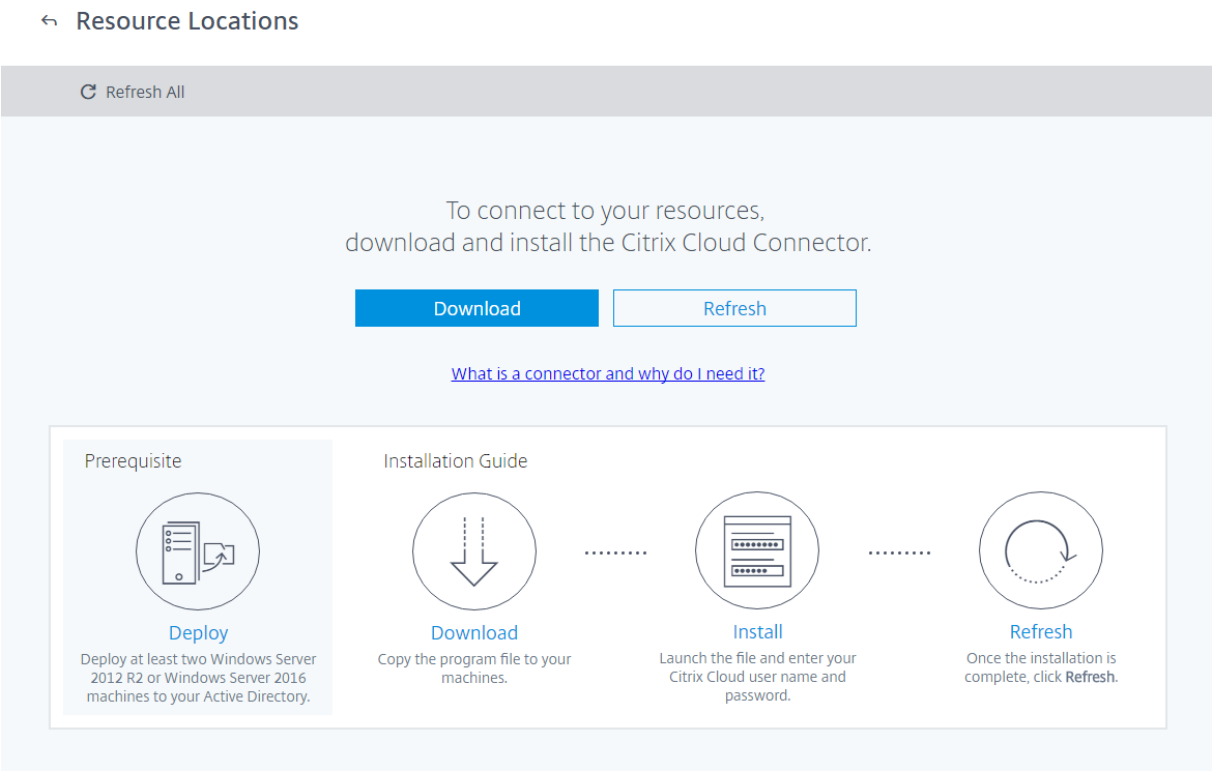
Considérations liées aux machines clonées

Chaque machine qui héberge le Cloud Connector doit avoir un SID et un ID de connecteur uniques afin que Citrix Cloud puisse communiquer de manière fiable avec les machines dans votre emplacement de ressources. Si vous avez l'intention d'héberger le Cloud Connector sur plusieurs machines dans votre emplacement de ressources et souhaitez utiliser des machines clonées, effectuez les opérations suivantes :

1. Préparez le modèle de machine en fonction des exigences de votre environnement.
2. Provisionnez le nombre de machines que vous prévoyez d'utiliser en tant que Cloud Connector.
3. Installez le Cloud Connector sur chaque machine, soit manuellement soit à l'aide du mode d'installation silencieuse.

L'installation du Cloud Connector sur un modèle de machine (avant le clonage) n'est pas pris en charge. Si vous clonez une machine sur laquelle le Cloud Connector est installé, les services du Cloud Connector ne fonctionneront pas et la machine ne pourra pas se connecter à Citrix Cloud.

Installation interactive



Pour créer votre premier emplacement de ressources

1. Ouvrez une session en tant qu'administrateur sur la machine sur laquelle vous allez installer le Cloud Connector. Windows Server 2012 R2 ou Windows Server 2016 doit être installé sur la machine, elle doit être jointe à un domaine et avoir un accès sortant à Internet.
2. Visitez https://citrix.cloud.com et connectez-vous avec les informations d'identification que vous avez reçues dans l'e-mail de Citrix Cloud. La console de gestion Citrix Cloud s'affiche.
3. À partir du bouton de menu dans le coin supérieur gauche, sélectionnez **Emplacements des ressources**.
4. Sur la page Emplacements des ressources, cliquez sur **Télécharger** pour télécharger le logiciel Cloud Connector.
5. Lancez le programme d'installation de Cloud Connector. Le programme d'installation vérifie la connectivité pour s'assurer que vous pouvez vous connecter à Citrix Cloud.
6. Connectez-vous à Citrix Cloud lorsque vous y êtes invité.
7. Suivez l'assistant pour installer et configurer le Cloud Connector. Une fois l'installation terminée, le programme d'installation vérifie une dernière fois la connectivité pour vérifier la communication du connecteur avec le cloud.
8. Répétez les étapes 1 à 4 sur les autres machines que vous voulez utiliser en tant que Cloud Con-

nector.

Après l'installation, Citrix Cloud enregistre votre domaine dans **Gestion des identités et des accès**. Pour de plus amples informations, consultez la section Gestion des identités et des accès.

Installation avec plusieurs clients et des emplacements de ressources existants

Si vous êtes l'administrateur de plusieurs comptes utilisateur, Citrix Cloud vous invite à sélectionner le compte client que vous souhaitez associer au Cloud Connector.

Si votre compte client dispose de plusieurs emplacements de ressources, Citrix Cloud vous invite à sélectionner l'emplacement de ressources à associer au Cloud Connector.

Installation avec ligne de commande (non interactif)

L'installation silencieuse ou automatisée est prise en charge. Toutefois, il n'est pas recommandé d'utiliser le même programme d'installation pour des installations répétées sur une période donnée. Téléchargez un nouveau Cloud Connector à partir de la page Emplacements des ressources de la console Citrix Cloud.

Utilisez **Start /Wait CWCConnector.exe /parameter:value** pour examiner les codes d'erreur potentiels en cas de défaillance. Cette opération peut être effectuée à l'aide du mécanisme standard d'exécution de **echo %ErrorLevel%** une fois l'installation terminée.

Paramètres pris en charge

Vous pouvez récupérer une liste des paramètres pris en charge en exécutant **CWCConnector /?**.

- **/Customer:** requis. ID du client affiché sur la page Accès aux API dans la console Citrix Cloud (sous Gestion des identités et des accès).
- **/ClientId:** requis. ID de client sécurisé qu'un administrateur peut créer, situé sur la page Accès aux API
- **/ClientSecret:** requis. Clé secrète sécurisée du client qui peut être téléchargée après création du client sécurisé. Située sur la page Accès aux API.
- **/ResourceLocationId:** requis. Identificateur unique d'un emplacement de ressources existant. Pour récupérer l'ID, cliquez sur le bouton d'ID de l'emplacement de ressources sur la page Emplacements des ressources dans la console Citrix Cloud. Si aucune valeur n'est spécifiée, Citrix Cloud utilise l'ID du premier emplacement de ressources dans le compte.
- **/AcceptTermsOfService:** requis. La valeur par défaut est **Yes**.

Exemple de ligne de commande avec tous les paramètres requis :


```
CWCConnector.exe /q /Customer:\*Customer\*  /ClientId:\*ClientId\*  /
    ClientSecret:\*ClientSecret\*  /ResourceLocationId:\*
    ResourceLocationId\*  /AcceptTermsOfService:\*true\*
```

Codes de sortie

- 1603 - An unexpected error occured (Une erreur inattendue s'est produite).
- 2 - A prerequiste check failed (Échec de vérification des conditions requises).
- 0 - Installation completed successfully (Installation terminée avec succès).

Journaux d'installation

Les journaux d'installation se trouvent dans **%LOCALAPPDATA%\Temp\CitrixLogs\CloudServicesSetup**.

En outre, les journaux sont ajoutés à **%ProgramData%\Citrix\WorkspaceCloud\InstallLogs** après l'installation.

Configuration du pare-feu et du proxy d'un Cloud Connector

November 7, 2018

Port 443 avec trafic HTTP, en sortie uniquement. Pour des informations complètes sur la connectivité, consultez la section Exigences en terme de connexion Internet.

Configuration du Connector en vue de prendre en charge un proxy Web

Le Cloud Connector prend en charge la connexion à Internet via un serveur proxy Web. Le programme d'installation et les services installés par le connecteur doivent être connectés à Citrix Cloud. Un accès Internet doit être disponible sur ces deux points.

> **Important :** l'activation du décryptage SSL sur certains proxies peut empêcher le Cloud Connector de se connecter à Citrix Cloud. Pour plus d'informations sur la résolution de ce problème, consultez l'article CTX221535.

Programme d'installation

Le programme d'installation utilise les paramètres configurés pour les connexions Internet. Si vous pouvez accéder à Internet à partir de la machine, le programme d'installation devrait également fonctionner.

Consultez la page Changing proxy server settings in Internet Explorer pour plus de détails sur la manière de configurer les paramètres proxy.

Services lors de l'exécution

Le service d'exécution fonctionne dans le contexte d'un service local. Il n'utilise pas le paramètre défini pour l'utilisateur (comme décrit ci-dessus). Vous devez importer le paramètre depuis le navigateur.

Pour configurer les paramètres de proxy à cette fin, ouvrez une fenêtre d'invite de commandes et utilisez **netsh** comme suit :

```
1 netsh winhttp import proxy source =ie
```

Après l'exécution de la commande, redémarrez la machine Cloud Connector de façon à ce que les services démarrent avec ces paramètres de proxy.

Pour plus de détails, consultez Netsh Commands for Windows Hypertext Transfer Protocol (WINHTTP).

Remarque : la détection automatique ou les scripts PAC ne sont pas pris en charge.

Plate-forme Citrix Workspace

November 7, 2018

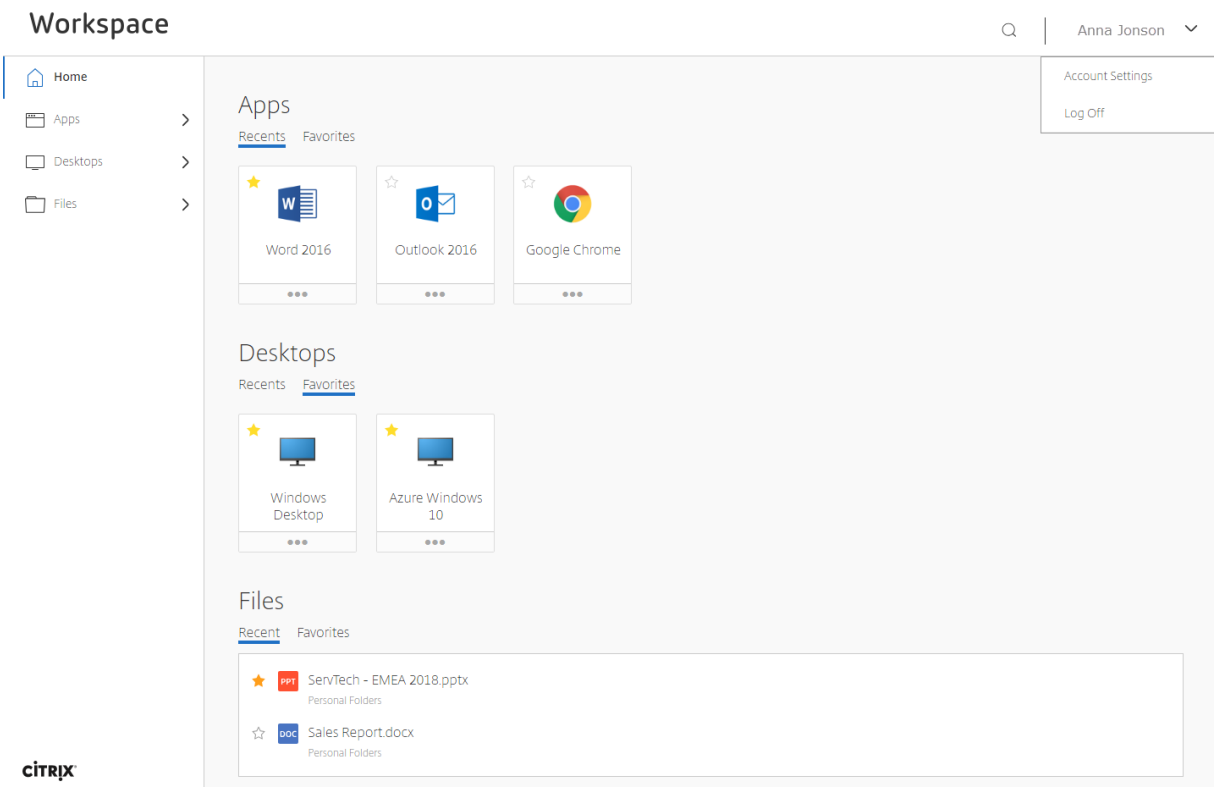
La plate-forme Citrix Workspace est un composant fondamental de Citrix Cloud qui énumère et fournit toutes vos ressources d'espace de travail numérique à l'expérience Citrix Workspace.

> **Important :**
>
> Les adresses suivantes doivent pouvoir être contactées afin d'utiliser et de consommer correctement Citrix Workspace :
>
> - `https://*.cloud.com`
> - `https://*.citrixdata.com`
>
> Pour une liste complète des exigences de connectivité de Citrix Cloud, consultez Exigences en terme de connexion Internet.

Présentation de Workspace

Cette capture d'écran est un exemple de ce que Citrix Workspace ressemble pour vos utilisateurs. Cette interface évolue et peut différer de celle avec laquelle ils travaillent aujourd'hui. Par exemple, elle n'inclura Files que si votre organisation a soucrit à Content Collaboration Service.

Pour un aperçu des nouveautés présentes dans Citrix Workspace, consultez Expérience Citrix Workspace et les blogs Citrix Cloud: What's New.



Exemple de cas d'utilisation :

Votre entreprise gère actuellement un parc hétéroclite d'applications Microsoft Office via Citrix Virtual Apps and Desktops Service ainsi que des applications SaaS telles que Workday via Citrix Gateway Service.

Vous disposez également d'anciennes applications provenant d'un déploiement Virtual Apps and Desktops local. Vous pouvez maintenant fournir toutes ces applications au sein d'une seule expérience utilisateur intégrée.

L'utilisateur peut accéder à son espace de travail contenant toutes les applications dont il a besoin à partir d'un navigateur ou d'une application - **l'application Citrix Workspace**. Vous pouvez personnaliser l'expérience dans une console simplifiée (**Configuration de l'espace de travail**) dans Citrix Cloud et choisir la méthode à utiliser par les utilisateurs pour s'authentifier.

Pour ce cas d'utilisation, complétez d'abord la configuration des **services** individuels. Basculez vers la **configuration de l'espace de travail** pour personnaliser davantage le comportement global de l'expérience utilisateur de Workspace. La configuration de l'espace de travail (sous l'onglet **Sites**) vous permet également de connecter votre déploiement Virtual Apps and Desktops local à l'expérience utilisateur de Workspace (appelée *agrégation de sites*). Partagez l'**URL**

> **de l'espace de travail** avec vos utilisateurs pour un accès sans client et guidez-les à travers l'installation de l'**application Citrix Workspace** pour une expérience optimale.

Utilisateurs de l'espace de travail

> **Remarque :**
>
> Lorsque vous vous abonnez à l'un des services suivants, l'intégration à Citrix Workspace est désactivée par défaut pour vos utilisateurs. Vous pouvez activer chaque service à partir de l'onglet Intégrations de services dans Citrix Cloud > Configuration de l'espace de travail.

Les espaces de travail sont initialement disponibles aux abonnés à :

- **Citrix Virtual Apps Essentials Service**. Citrix Virtual Apps Essentials offre un accès sécurisé aux applications virtuelles Windows. Ce service inclut une URL d'espace de travail, activée par défaut, généralement au format : `https://yourcompanyname.cloud.com`. Suivez les étapes pour configurer Citrix Virtual Apps Essentials, puis testez et partagez le lien de l'URL de l'espace de travail avec vos abonnés pour leur donner accès à leurs applications.
- **Citrix Virtual Desktops Essentials Service**. Citrix Virtual Desktops Essentials offre un accès sécurisé aux postes virtuels Windows 10. Ce service inclut une URL d'espace de travail, activée par défaut, généralement au format : `https://yourcompanyname.cloud.com`. Suivez les étapes pour configurer Citrix Virtual Desktops Essentials, puis testez et partagez le lien de l'URL de l'espace de travail avec vos abonnés pour leur donner accès à leurs postes de travail.
- **Citrix Virtual Apps and Desktops Service**. Citrix Virtual Apps and Desktops Service offre un accès sécurisé aux applications et postes virtuels. Ce service inclut une URL d'espace de travail, activée par défaut, généralement au format : `https://yourcompanyname.cloud.com`. Suivez les étapes pour configurer Citrix Virtual Apps and Desktops Service, puis testez et partagez le lien de l'URL de l'espace de travail avec vos abonnés pour leur donner accès à leurs applications et postes de travail. Vos abonnés peuvent accéder à l'URL de l'espace de travail sans aucune configuration supplémentaire.
- **Endpoint Management**. Pour les clients Endpoint Management dont l'expérience Workspace est activée, les utilisateurs qui ouvrent Secure Hub et cliquent sur **Ajouter des applications** sont dirigés vers l'App Store Workspace au lieu du magasin Secure Hub. Cette fonctionnalité est disponible uniquement pour les **nouveaux clients**. La migration des clients existants n'est pas prise en charge. Pour utiliser cette fonctionnalité, effectuez les tâches suivantes :
  - Activez les stratégies Mise en cache du mot de passe et Authentification par mot de passe. Pour de plus amples informations sur la configuration de ces stratégies, veuillez consulter la section Synopsis des stratégies MDX.
  - Configurez l'authentification Active Directory en tant qu'AD ou AD+Cert. Il s'agit des deux modes que nous prenons en charge. Pour plus d'informations sur la configuration de

l'authentification, consultez Authentification domaine ou domaine + jeton de sécurité.

- Activez l'intégration de Workspace pour XenMobile Service. Pour plus d'informations sur l'intégration de Workspace, consultez la section Configuration de l'espace de travail.

  > **Important :**
  >
  > Une fois cette fonctionnalité activée, le SSO ShareFile se produit via Workspace et non XenMobile. Nous vous recommandons de désactiver l'intégration de ShareFile dans la console XenMobile avant d'activer l'intégration de Workspace.

- **Citrix Gateway Service**. Citrix Gateway Service (anciennement NetScaler Gateway Service) fournit un accès distant sécurisé avec des fonctionnalités de gestion des identités et des accès (IdAM), tout en offrant une expérience unifiée aux applications SaaS (Software as a Service) et aux applications et bureaux virtuels. Suivez les étapes pour configurer Citrix Gateway Service, puis testez et partagez le lien de l'URL de l'espace de travail avec vos abonnés pour leur donner un accès à distance. Pour plus d'informations sur la configuration des applications SaaS dans Citrix Gateway Service, consultez Prise en charge des applications SaaS.
- **Content Collaboration Service**. Content Collaboration Service (anciennement ShareFile) permet d'accéder aux données en toute sécurité, de synchroniser et de partager des fichiers à partir de n'importe quel appareil. Suivez les étapes pour configurer Content Collaboration Service, puis testez et partagez le lien de l'URL de l'espace de travail avec vos abonnés pour leur donner accès à Files.
- **Secure Browser Service**. Le Secure Browser Service protège le réseau de l'entreprise contre les attaques via navigateur en isolant la navigation sur le Web. Lorsque des abonnés (utilisateurs) accèdent à l'URL fournie par l'administrateur, leurs navigateurs publiés sont affichés, ainsi que d'autres applications et postes de travail configurés pour eux dans d'autres services Citrix Cloud. Suivez les étapes pour configurer Secure Browser Service, puis testez et partagez le lien de l'URL de l'espace de travail avec vos abonnés pour leur donner accès à un navigateur sécurisé.

> **Important :**
>
> Certains clients continuent d'utiliser StoreFront comme indiqué dans l'article StoreFront et dans l'article Citrix Virtual Desktops Essentials.

Configuration de l'espace de travail

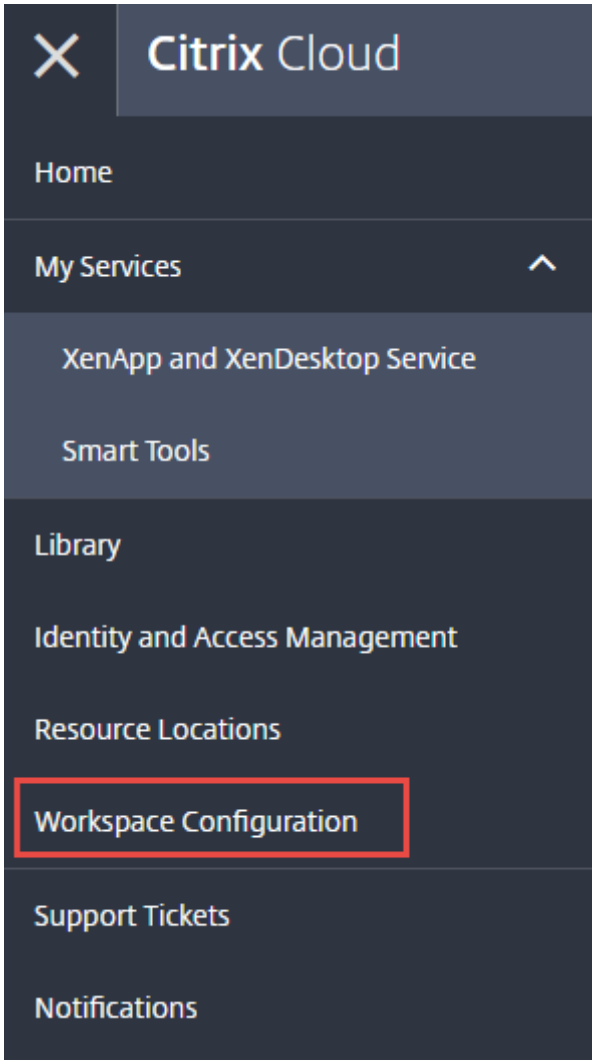
November 7, 2018

Cet article explique aux administrateurs comment configurer des espaces de travail pour les abonnés, qui peuvent utiliser un ou plusieurs services disponibles auprès de Citrix Cloud.

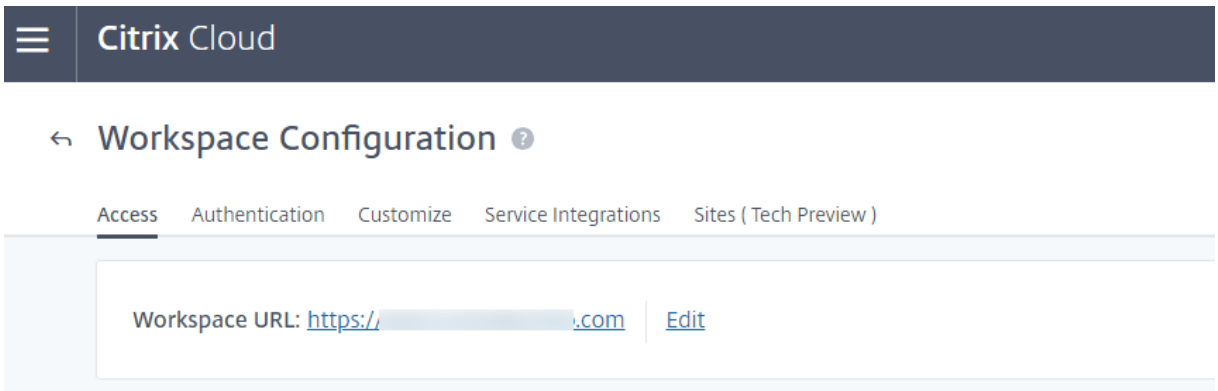
> **Important :**
>
> Les adresses suivantes doivent pouvoir être contactées afin d'utiliser et de consommer correctement Citrix Workspace :
>
> - `https://*.cloud.com`
> - `https://*.citrixdata.com`
>
> Pour une liste complète des exigences de connectivité de Citrix Cloud, consultez Exigences en terme de connexion Internet.

Modifier l'accès à l'espace de travail

Dans **Citrix Cloud > Configuration de l'espace de travail > Accès**, l'URL de l'espace de travail est activée et prête à l'emploi. Vous activez la disponibilité de ressources de service individuelles auprès de vos utilisateurs, par exemple Citrix Virtual Apps and Desktops Service, à partir de l'onglet **Intégrations de services**. Tous les nouveaux services auxquels votre organisation est abonnée sont désactivés par défaut.



> **Remarque :** dans Citrix Virtual Apps Essentials, la configuration de l'espace de travail est disponible dans le menu Citrix Cloud **après** la création du premier catalogue.



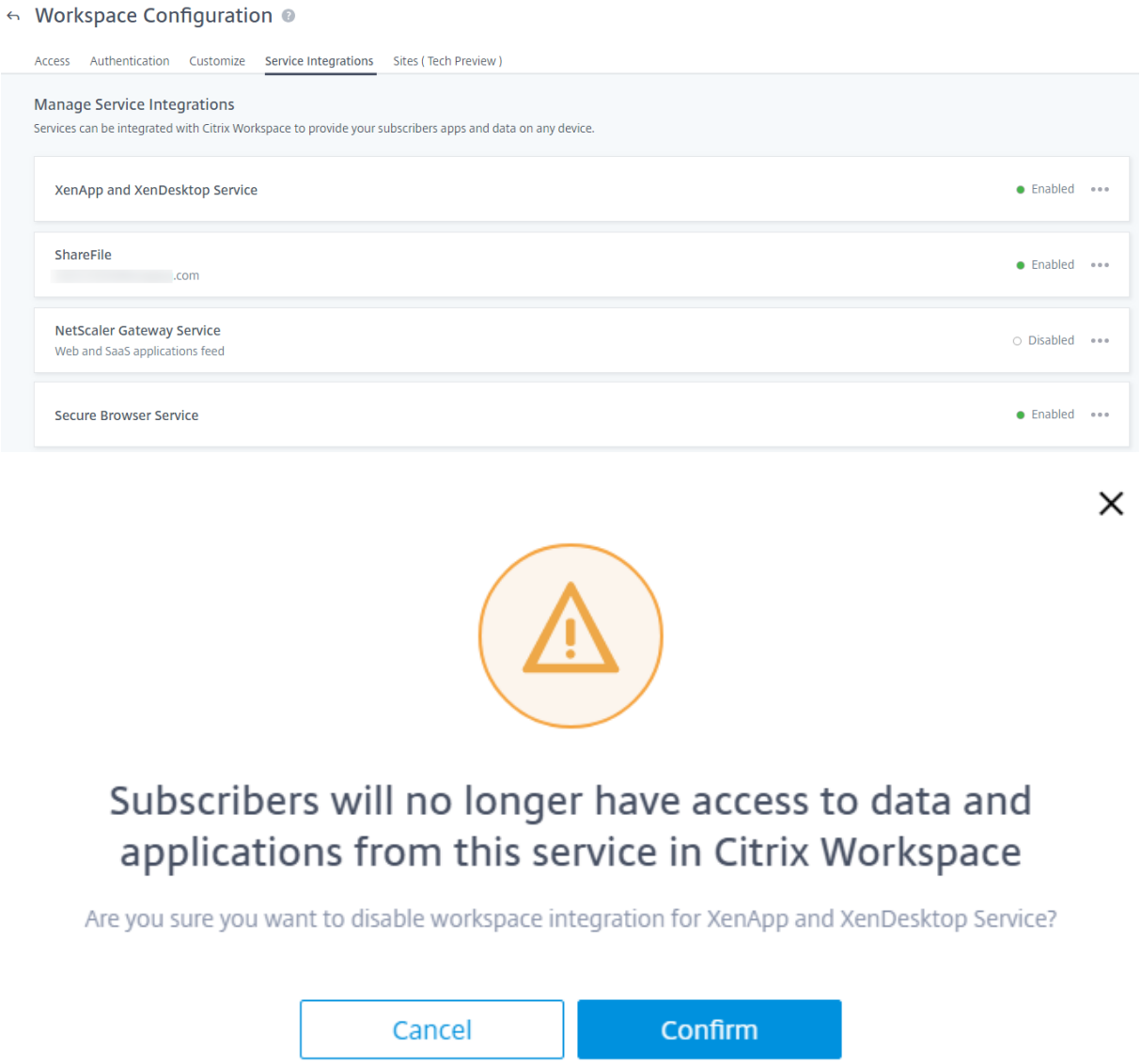
Désactiver l'intégration de l'espace de travail pour un service

Vous pouvez désactiver l'intégration de l'espace de travail pour des services spécifiques. Cela ne désactive pas l'URL de l'espace de travail, mais désactive les données et les applications d'un service.

Pour désactiver l'intégration de l'espace de travail pour un service :

1. Accédez à **Configuration de l'espace de travail > Intégrations de services**.
2. Sélectionnez le bouton d'ellipse (…) à côté du service et **Désactiver**.

> **Important :** la désactivation de l'intégration de l'espace de travail bloque l'accès des abonnés à ce service. Les abonnés n'auront plus accès aux données et applications de ce service dans Citrix Workspace.



> **Remarque :** Citrix App Essentials Service, Citrix Desktop Essentials Service et Citrix Virtual Apps and Desktops Service s'affichent en tant que « Citrix Virtual Apps and Desktops Service » dans l'onglet Gérer les intégrations de services.

Personnaliser l'URL de l'espace de travail

La première partie de l'URL de l'espace de travail est personnalisable. Vous pouvez modifier l'URL, par exemple, de `https://example.cloud.com` à `https://newexample.cloud.com`.

> **Important :** la première partie de l'URL de l'espace de travail représente la société ou l'organisation qui utilise le compte Citrix Cloud et doit respecter le Contrat des services de l'utilisateur final de Citrix. Toute utilisation abusive des droits de propriété intellectuelle d'un tiers, y compris les marques, peut entraîner la révocation et la réaffectation de l'URL de l'espace de travail et/ou la suspension du compte Citrix Cloud.

Dans le menu Citrix Cloud, accédez à **Configuration de l'espace de travail > Accès**, puis sélectionnez le lien **Modifier** en regard de l'URL de l'espace de travail.

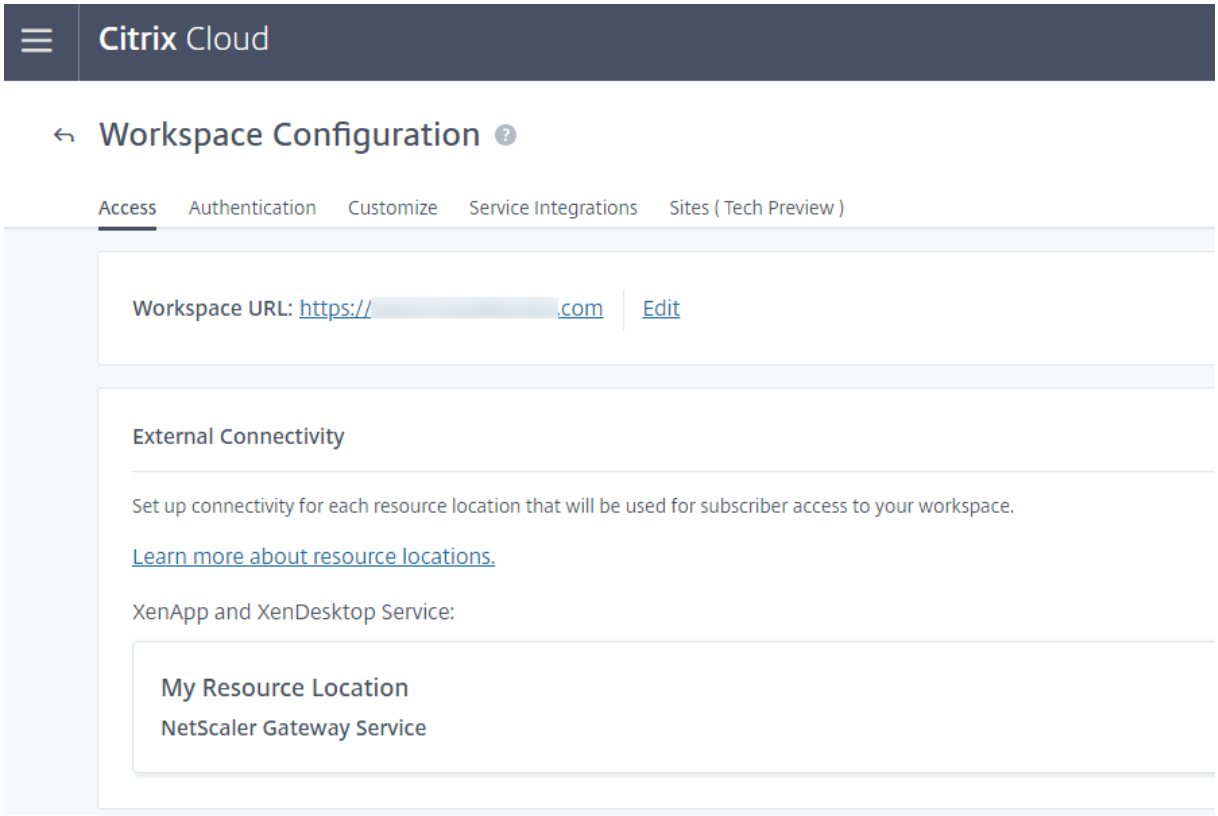
Conseils pour créer de nouvelles URL :

- La partie personnalisable de l'URL (« nouvelexemple ») doit comporter entre 6 et 63 caractères. Si vous souhaitez modifier la partie personnalisable de l'URL en utilisant moins de 6 caractères, veuillez ouvrir un ticket dans Citrix Cloud.
- Elles doivent être composées uniquement de lettres et de chiffres.
- Elles ne peuvent pas contenir de caractères Unicode.
- Lorsque vous renommez une URL, l'ancienne URL est immédiatement supprimée et n'est plus disponible.
- Si vous modifiez l'URL de l'espace de travail, vos abonnés ne peuvent pas accéder à leurs espaces de travail tant que la nouvelle URL n'est pas active (environ 10 minutes). Vous devrez également leur communiquer la nouvelle URL et mettre à jour manuellement toutes les applications Citrix Receiver locales pour utiliser la nouvelle URL.

Connectivité externe

Fournissez un accès sécurisé à vos abonnés distants en ajoutant des Citrix Gateway ou Citrix Gateway Service aux emplacements de ressources.

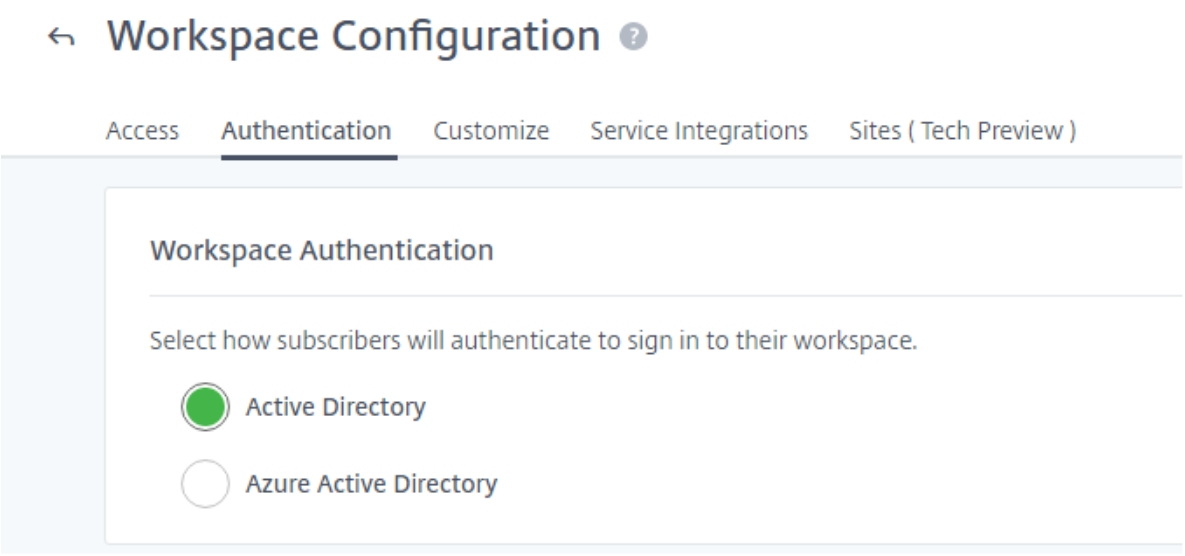
Vous pouvez ajouter des Citrix Gateway à partir de **Configuration de l'espace de travail > Accès > Connectivité externe** ou à partir de **Citrix Cloud > Emplacements des ressources**.



> **Remarque :** la partie Connectivité externe de la page **Configuration de l'espace de travail > Accès** n'est pas disponible dans Citrix Virtual Apps Essentials. Citrix Virtual Apps Essentials Service utilise Citrix Gateway Service, qui ne nécessite aucune configuration supplémentaire.

Modifier l'authentification aux espaces de travail

Modifiez la façon dont les abonnés s'authentifient auprès de leur espace de travail dans **Configuration de l'espace de travail > Authentification > Authentification de l'espace de travail**.



En tant qu'administrateur, vous pouvez exiger que vos abonnés (utilisateurs finaux) s'authentifient auprès de leurs espaces de travail à l'aide d'Active Directory ou d'Azure Active Directory. Ces options d'authentification sont disponibles pour tous les services Citrix Cloud, y compris le contrôle d'accès.

Le contrôle d'accès est une fonctionnalité qui permet aux utilisateurs finaux d'accéder aux applications SaaS, Web et virtuelles avec une expérience d'authentification unique (SSO).

> **Important :** Le changement de mode d'authentification peut prendre jusqu'à 5 minutes et entraîne une interruption pour vos abonnés pendant cette période. Citrix recommande de modifier les méthodes d'authentification uniquement pendant les périodes de faible utilisation. Si vous avez des abonnés connectés à Citrix Workspace à l'aide d'un navigateur ou d'une application Citrix Workspace, veuillez leur indiquer de fermer le navigateur ou de quitter l'application. Après avoir attendu environ cinq minutes, ils peuvent se reconnecter à l'aide de la nouvelle méthode d'authentification.

Active Directory

Par défaut, Citrix Cloud utilise Active Directory pour gérer l'authentification des abonnés aux espaces de travail. L'utilisation d'Active Directory nécessite l'installation d'un Citrix Cloud Connector dans le domaine Active Directory local. Pour de plus amples informations sur l'installation du Cloud Connector, consultez la section Installation de Cloud Connector.

Azure Active Directory

L'utilisation d'Azure Active Directory (AD) pour gérer l'authentification des abonnés aux espaces de travail satisfait aux exigences suivantes :

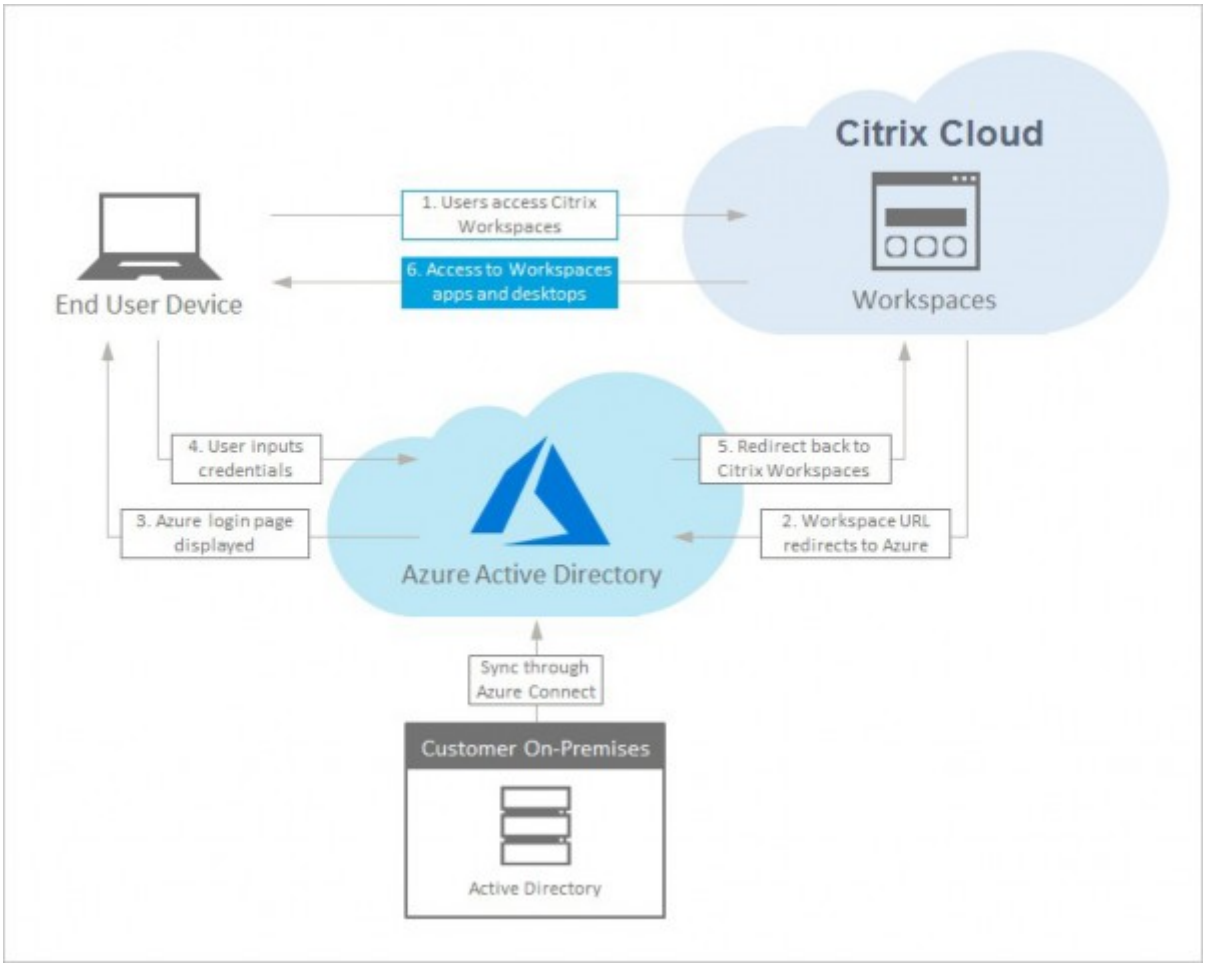
- Azure AD avec un utilisateur disposant d'autorisations d'administrateur général.
- Un Citrix Cloud Connector installé dans le domaine Active Directory local. La machine doit également être jointe au domaine qui se synchronise avec Azure AD.
- VDA version 7.15.2000 LTSR CU VDA ou version actuelle 7.18 ou supérieure.
- Une connexion entre Azure AD et Citrix Cloud. Pour de plus amples informations, consultez la section Connecter Azure Active Directory à Citrix Cloud. Lors de la synchronisation de votre Active Directory avec Azure AD, les entrées UPN et SID doivent être incluses dans la synchronisation. Si ces entrées ne sont pas synchronisées, certains flux de travail échoueront dans Citrix Workspace.

> **Avertissement :**
>
> - Si vous utilisez Azure AD, ne modifiez pas le Registre comme décrit dans l'article CTX225819. Cette modification peut entraîner l'échec du lancement de sessions pour les utilisateurs Azure AD.
> - L'ajout d'un groupe en tant que membre d'un autre groupe (imbrication) n'est pas pris en charge pour l'authentification fédérée à l'aide d'Azure AD. Si vous affectez un groupe imbriqué à un catalogue, les membres de ce groupe ne peuvent pas accéder aux applications du catalogue.

Après l'activation de l'authentification Azure AD :

- **Gérer les utilisateurs et les groupes d'utilisateurs à l'aide de la bibliothèque de Citrix Cloud :** utilisez uniquement la bibliothèque de Citrix Cloud pour gérer les utilisateurs et les groupes d'utilisateurs. (Ne spécifiez pas d'utilisateurs et de groupes d'utilisateurs lors de la création ou de la modification de groupes de mise à disposition.)
- **Sécurité accrue :** les utilisateurs sont invités à se reconnecter lorsqu'ils lancent une application ou un bureau. Ceci est intentionnel et offre plus de sécurité, car les informations de mot de passe circulent directement de l'appareil de l'utilisateur vers le VDA qui héberge la session.
- **Expérience de connexion :** les utilisateurs ont une expérience de connexion différente dans Azure AD. La sélection de l'authentification Azure AD fournit une connexion fédérée et non SSO. Les utilisateurs se connectent à l'espace de travail à partir d'une page de connexion Azure, toutefois, ils peuvent être amenés à s'authentifier une seconde fois lors de l'ouverture d'une application ou d'un bureau à partir de Citrix Virtual Apps and Desktops Service. Vous pouvez personnaliser l'expérience de connexion pour Azure AD. Pour de plus amples informations, veuillez consulter la documentation de Microsoft. Les personnalisations de connexion (logo) effectuées dans la configuration de Workspace n'affectent pas l'expérience de connexion d'Azure AD.

Le diagramme suivant montre la séquence de l'authentification Azure AD.



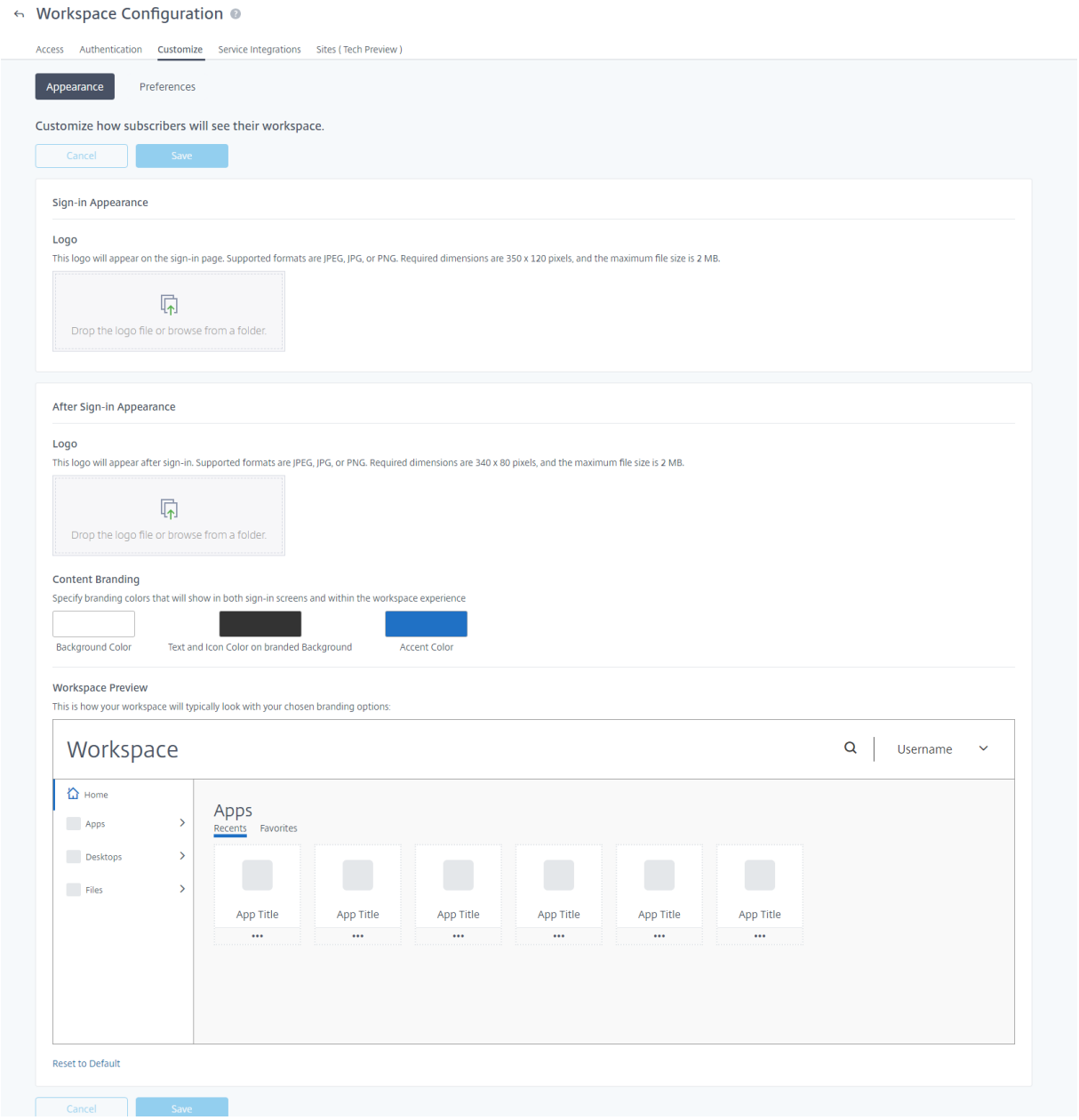
Expérience de déconnexion

Important : si Citrix Workspace expire dans le navigateur en raison d'une inactivité, les abonnés restent connectés à Azure AD. Ce comportement est conçu pour empêcher l'expiration d'un Citrix Workspace ce qui entraînerait la fermeture d'autres applications Azure AD.

Pour fermer Citrix Workspace, utilisez **Paramètres > Déconnexion**. Cette option met fin au processus de déconnexion de l'espace de travail et d'Azure AD. Si les abonnés ferment le navigateur au lieu d'utiliser l'option **Déconnexion**, ils peuvent rester connectés à Azure AD.

Personnaliser l'apparence des espaces de travail

Pour personnaliser l'apparence des espaces de travail de vos abonnés, modifiez les paramètres dans **Configuration de l'espace de travail > Personnaliser > Apparence** et **Enregistrer**.



Les modifications apportées à l'apparence de l'espace de travail prennent effet immédiatement. Il faut environ cinq minutes pour que l'interface utilisateur mise à jour s'affiche dans les applications Citrix Receiver locales.

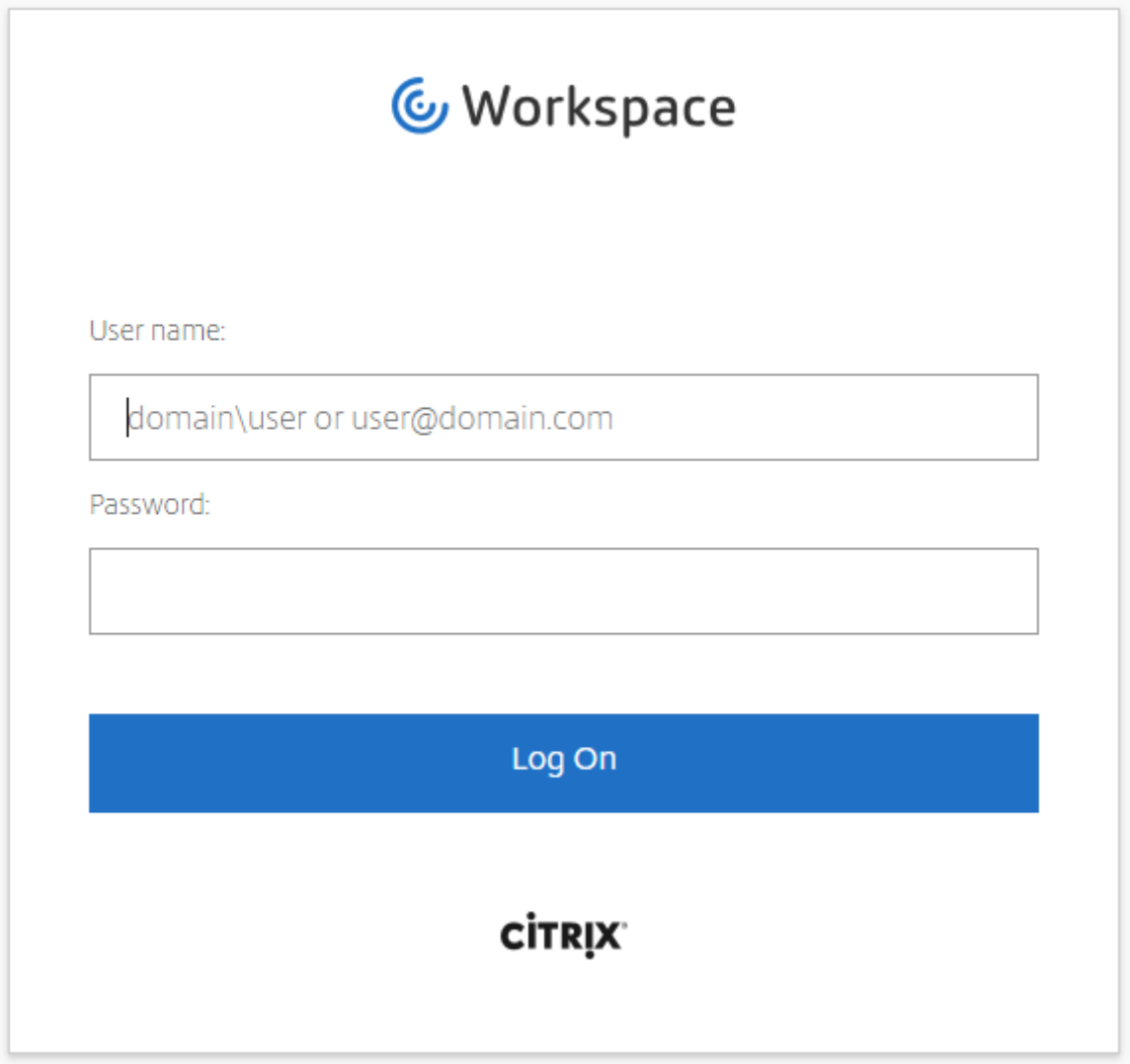
> **Remarque** : l'aperçu de l'espace de travail n'affiche pas d'aperçu si vous travaillez actuellement avec l'ancienne interface utilisateur de couleur mauve.

Logo	Dimensions requises	Taille maximale	Formats pris en charge
Logo de connexion	350 x 120 pixels	2 Mo	JPEG, JPG ou PNG

Logo	Dimensions requises	Taille maximale	Formats pris en charge
Logo après la connexion	340 x 80 pixels	2 Mo	JPEG, JPG ou PNG

Les logos non conformes aux dimensions requises peuvent apparaître déformés.

Le logo **Connexion** apparaît sur le formulaire de connexion à l'espace de travail. Vous pouvez remplacer le logo Workspace par le vôtre. Les couleurs et le branding du reste de la page de connexion ne sont pas affectés.



Les modifications apportées au logo de connexion n'ont aucun impact sur les utilisateurs qui s'authentifient auprès de leur espace de travail à l'aide d'Azure Active Directory. Pour plus d'informations sur l'ajout du branding d'entreprise à votre page de connexion dans Azure AD,

consultez la documentation de Microsoft.

Le logo **Après la connexion** apparaît en haut à gauche de l'espace de travail.

Les couleurs du **Contenu de marque** changent la couleur de l'arrière-plan d'en-tête, du texte et de l'icône ainsi que la couleur d'accentuation dans l'espace de travail.

Personnaliser les préférences de l'espace de travail

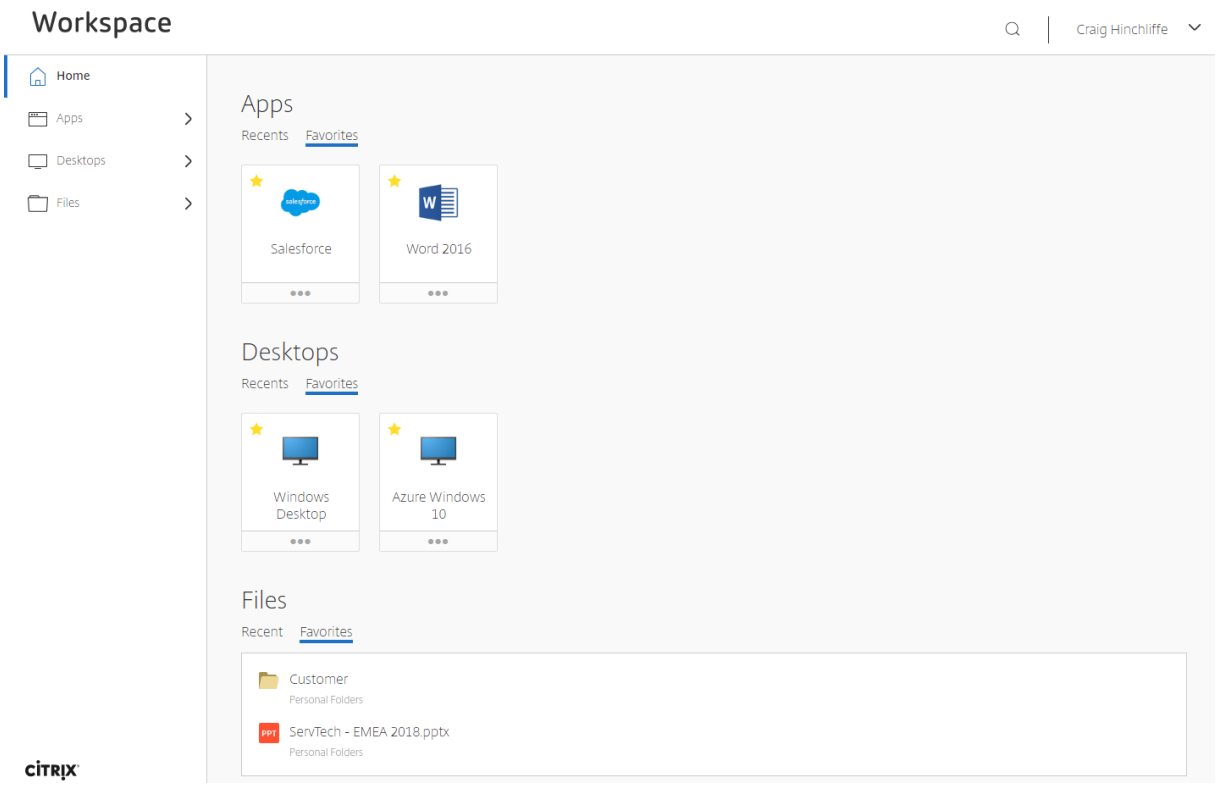
Personnalisez la manière dont les abonnés interagissent avec leur espace de travail dans **Configuration de l'espace de travail** > **Personnaliser** > **Préférences**.

Autoriser les favoris

L'option Autoriser les favoris est disponible pour les clients qui ont accès à la configuration de l'espace de travail et à la nouvelle expérience de l'espace de travail.

Onglet Préférences des favoris

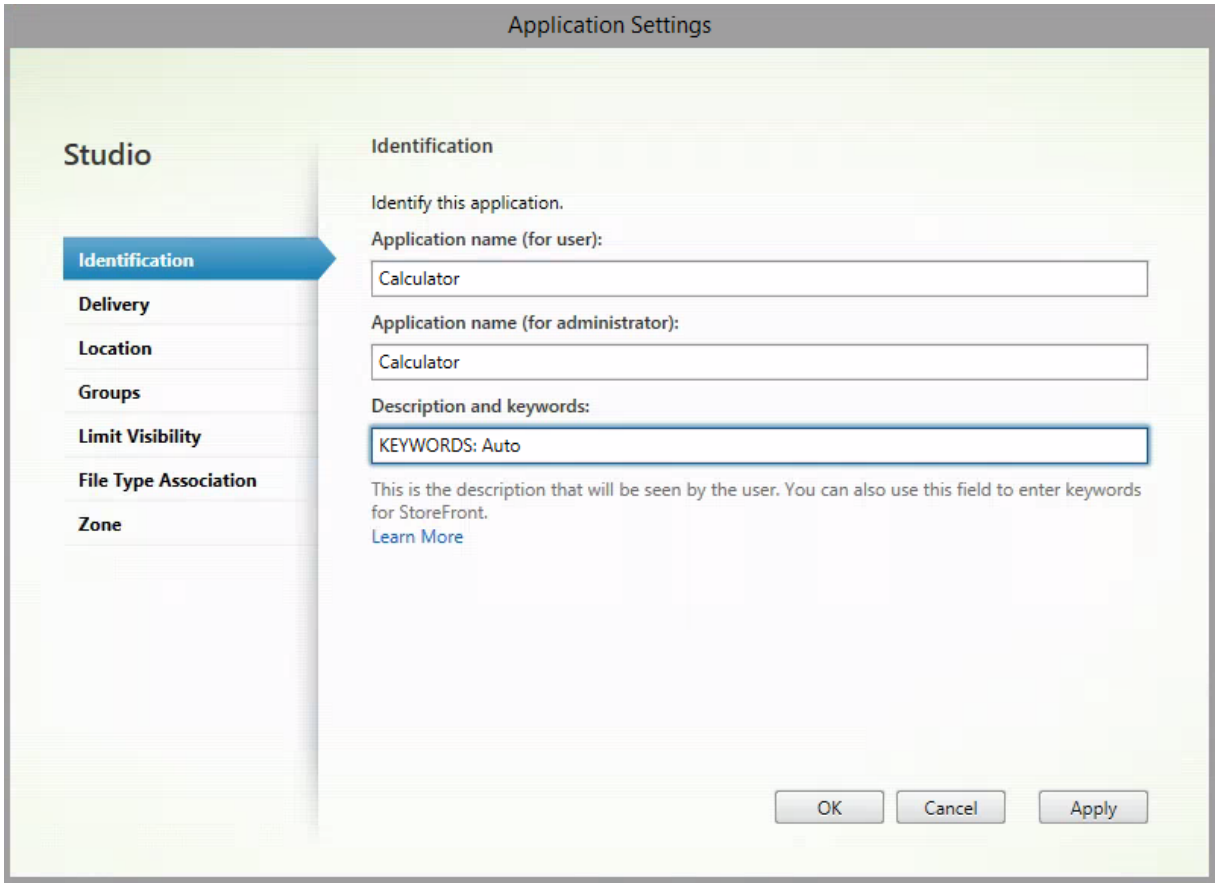
Activé (valeur par défaut). Les abonnés à l'espace de travail peuvent ajouter des applications favorites (maximum de 250) en sélectionnant l'icône d'étoile.



Désactivé. Les abonnés ne peuvent pas sélectionner d'applications en tant que favoris. Les favoris ne sont pas supprimés et peuvent être récupérés si vous réactivez les favoris.

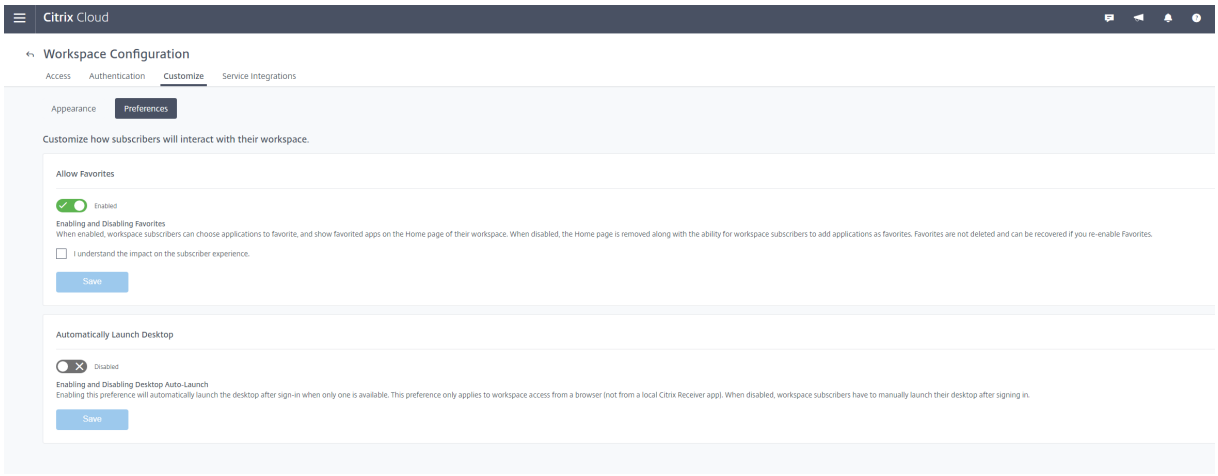
> **Remarque :** pour certains clients existants (nouveaux dans l'espace de travail entre décembre 2017 et avril 2018), l'option **Autoriser les favoris** est désactivée par défaut. L'administrateur peut décider quand activer cette fonctionnalité pour ses abonnés.

- Si un abonné ajoute plus d'applications favorites que le maximum (250) autorisé, l'application « favorite la plus ancienne » sera supprimée (ou aussi proche que possible pour conserver les favoris les plus récents).
- Les administrateurs peuvent ajouter automatiquement des applications favorites pour les abonnés en utilisant les mots-clés KEYWORDS: Auto et KEYWORDS: Mandatory. Ces paramètres sont disponibles dans Virtual Apps and Desktops Service dans **Gérer** > **Configuration complète** > **Applications**.
  - **KEYWORDS: Auto**. L'application est ajoutée en tant que favori, mais les abonnés peuvent supprimer le favori.
  - **KEYWORDS: Mandatory**. L'application est ajoutée en tant que favori, mais les abonnés ne peuvent pas supprimer le favori. Les applications obligatoires n'affichent pas une icône d'étoile.



Lancer bureau automatiquement

L'option Lancer bureau automatiquement est disponible pour les clients qui ont accès à la configuration de l'espace de travail et à la nouvelle expérience de l'espace de travail. Cette préférence s'applique uniquement à l'accès à l'espace de travail à partir d'un navigateur.



Désactivé (défaut). Empêche Citrix Workspace de démarrer automatiquement un poste de travail lorsqu'un abonné se connecte. Les abonnés doivent lancer manuellement leur poste de travail après la connexion.

Activé. Si un abonné ne dispose que d'un poste de travail disponible, le poste se lance automatiquement lorsque l'abonné se connecte à l'espace de travail. Les applications de l'abonné ne sont pas reconnectées, quelle que soit la configuration du contrôle de l'espace de travail.

> **Remarque :**
>
> pour permettre à Citrix Workspace de lancer automatiquement des postes, les abonnés qui accèdent au site via Internet Explorer doivent ajouter l'URL de l'espace de travaile à la zone Intranet local ou Sites de confiance.

Ajouter un site local à Workspace

August 1, 2018

Si vous disposez d'un déploiement local de XenApp et XenDesktop, vous pouvez ajouter votre site à Citrix Workspace. Ce processus est appelé *Agrégation de sites*. Vous pouvez ensuite créer des espaces de travail pour vos utilisateurs, en affichant les applications locales disponibles, et vos utilisateurs peuvent accéder à ces applications via Citrix Cloud.

> **Important :** cette fonctionnalité est une version d'évaluation technique qui est initialement disponible pour les clients Citrix existants qui sont déjà autorisés à accéder à la nouvelle expérience Workspace.

Environnements pris en charge

L'agrégation de sites est prise en charge uniquement pour les déploiements locaux de XenApp 6.5 et XenApp et XenDesktop 7.x. Les sites locaux exécutant des versions antérieures de XenApp ou XenApp et XenDesktop ne sont pas pris en charge avec Citrix Workspace.

Vue d'ensemble des tâches

Lorsque vous ajoutez votre site local à Citrix Workspace, l'assistant Ajouter un site vous guide à travers les tâches suivantes :

- Découverte de votre site et sélection de l'emplacement de ressources par défaut. L'emplacement de ressources par défaut spécifie le domaine et la méthode de connectivité pour tous les utilisateurs qui accèdent à votre site. Au cours de ce processus, Citrix Cloud effectue un test de connectivité pour vérifier que votre site est accessible et affiche vos emplacements de ressources. Si vous disposez d'emplacements de ressources sans Cloud Connector, vous pouvez télécharger et installer le logiciel requis.
- Détection des domaines Active Directory sur lesquels vos Cloud Connector sont installés. Pour XenApp 6.5, Citrix Cloud détecte également si des applications publiées sont affectées à des comptes d'utilisateurs locaux sur des serveurs XenApp. Pour utiliser Workspace, les utilisateurs de l'application doivent pouvoir s'authentifier avec Active Directory. Citrix Cloud fournit une liste des comptes d'utilisateurs locaux détectés afin que vous puissiez vous assurer qu'ils peuvent s'authentifier auprès de Workspace.
- Spécification de la connectivité à utiliser entre Citrix Cloud et votre site. Pour une connectivité externe, vous pouvez utiliser votre propre NetScaler Gateway ou NetScaler Gateway Service. Pour vous assurer que seuls les utilisateurs sur le même réseau que votre site peuvent accéder aux applications, vous pouvez spécifier un accès uniquement en interne.

Conditions préalables

Cloud Connector

Vous devez disposer d'au moins deux (2) serveurs sur lesquels installer le logiciel Citrix Cloud Connector. Ces serveurs doivent satisfaire aux exigences suivantes :

- Répondre aux exigences système décrites dans Détails techniques sur Cloud Connector.

- Aucun autre composant Citrix ne doit être installé sur ces serveurs, ils ne doivent pas être un contrôleur de domaine Active Directory ou une machine critique à votre infrastructure d'emplacement de ressources.
- Être joints au domaine sur lequel réside votre site. Si les utilisateurs accèdent aux applications de votre site dans plusieurs domaines, vous devez installer au moins deux Cloud Connector dans chaque domaine.
- Être connectés à un réseau pouvant contacter votre site.
- Être connectés à Internet. Pour de plus amples informations, consultez la section Exigences en terme de connexion Internet.
- Citrix recommande deux serveurs pour garantir la haute disponibilité de Cloud Connector. Après l'installation, les Cloud Connector permettent à Citrix Cloud de localiser et de communiquer avec votre site.

Pour de plus amples informations sur l'installation du Cloud Connector, consultez la section Installation de Cloud Connector.

Bien que vous puissiez installer les Cloud Connector pendant le processus d'ajout de votre site à Citrix Workspace, Citrix recommande de les installer préalablement pour veiller à ce que votre site soit ajouté avec une interruption minimale.

Active Directory

L'agrégation de sites prend en charge les sites qui utilisent un Active Directory local. Azure Active Directory n'est pas pris en charge.

Approbations Active Directory

Si vous disposez de forêts d'utilisateurs et de ressources distinctes dans Active Directory, des Cloud Connector doivent être installés dans chaque forêt avant d'ajouter votre site local. Lorsque vous ajoutez votre site, Citrix Cloud détecte ces forêts au cours du processus de détection du site via les Cloud Connector. Vous pouvez ensuite utiliser les utilisateurs et les ressources des forêts pour créer des espaces de travail pour vos utilisateurs.

Limitations :

- Vous ne pouvez pas utiliser des forêts d'utilisateurs et de ressources distinctes lorsque vous définissez l'emplacement de ressources par défaut pendant l'ajout de votre site. Étant donné que les Cloud Connector ne participent pas aux approbations inter-forêts qui pourraient être établies, Citrix Cloud ne peut pas détecter votre site via les Cloud Connector dans ces forêts. Vous pouvez utiliser ces forêts lorsque vous définissez un emplacement de ressources secondaire afin d'offrir une option de connectivité différente à vos utilisateurs. Pour de plus

amples informations, consultez Ajouter des plages d'adresses IP pour différentes options de connectivité.

- Les forêts non approuvées ne sont pas prises en charge pour l'agrégation de sites. Bien que Citrix Cloud et Workspace prennent en charge les utilisateurs issus de forêts non approuvées, ces utilisateurs ne peuvent pas utiliser Workspace après l'ajout d'un site local via l'agrégation de sites. Seuls les utilisateurs situés dans des forêts approuvées par le site peuvent se connecter et utiliser Workspace. Si les utilisateurs d'une forêt non approuvée tentent de se connecter à Workspace, ils reçoivent le message d'erreur « Votre ouverture de session a expiré. Rouvrez une session pour continuer. »

Connectivité interne et externe aux ressources d'un espace de travail

Au cours du processus d'ajout de votre site à Workspace, vous pouvez spécifier si vous souhaitez fournir un accès interne ou externe aux ressources que vous mettez à la disposition des utilisateurs via Workspace. Si vous avez l'intention d'autoriser uniquement les utilisateurs internes à accéder à votre site via Workspace, les utilisateurs doivent être sur le même réseau que le site pour accéder à leurs applications.

Si vous avez l'intention d'autoriser des utilisateurs externes à accéder à ces ressources, vous disposez des options suivantes :

- Utiliser votre NetScaler Gateway existant pour gérer le trafic entre votre site local et Citrix Cloud. Pour utiliser cette option, votre NetScaler Gateway doit être configuré pour utiliser des Cloud Connector en tant que serveurs STA (Secure Ticket Authority) **avant** d'ajouter votre site à Workspace. Pour obtenir des instructions, veuillez consulter l'article CTX232640.
- Utiliser le NetScaler Gateway Service si vous préférez autoriser Citrix à gérer le trafic entre votre site et Citrix Cloud. Vous pouvez activer une évaluation du service et configurer le service lorsque vous ajoutez votre site. Si vous êtes déjà inscrit au NetScaler Gateway Service, Citrix Cloud détecte votre abonnement lorsque vous sélectionnez cette option.

> **Remarque :** pour que Citrix Cloud détecte votre abonnement au service NetScaler Gateway Service lors de l'ajout de votre site à Workspace, vous devez utiliser le même OrgID que celui que vous avez utilisé lors de votre inscription à NetScaler Gateway Service. Pour plus d'informations sur les OrgID dans Citrix Cloud, voir Qu'est-ce qu'un OrgID ?.

Informations d'identification et ports pour la détection du site

Au cours du processus d'ajout de votre site à Workspace, Citrix Cloud détecte votre site et s'assure que le Controller que vous spécifiez est disponible. Avant d'ajouter votre site local, effectuez les tâches suivantes :

- Vérifiez que vous disposez d'informations d'identification d'administrateur Citrix avec au minimum des autorisations Lecture seule. Au cours du processus d'ajout de votre site à Workspace, Citrix Cloud vous invite à fournir ces informations d'identification. Citrix Cloud utilise uniquement ces informations d'identification pour le processus de détection. Citrix Cloud ne stocke pas ces informations d'identification et ne les utilise pas pour apporter des modifications à votre site.
- **XenApp 6.5 uniquement :** assurez-vous que le port 2513 sur le serveur XenApp est accessible depuis les machines Cloud Connector de votre environnement. Au cours du processus de détection, les Cloud Connector contactent le Citrix XenApp Remoting Service sur le serveur XenApp que vous spécifiez. Ce service est à l'écoute sur le port 2513. Si ce port est bloqué, Citrix Cloud ne peut pas détecter votre déploiement.

Pour activer la détection de site sans les informations d'identification de site

XenApp et XenDesktop 7.x uniquement : si vous ne souhaitez pas fournir les informations d'identification de votre site pour des raisons de sécurité, vous pouvez activer Citrix Cloud pour qu'il détecte votre site sans demander les informations d'identification du site. Effectuez cette tâche **avant** d'ajouter votre site à Citrix Workspace.

1. Installez au moins deux Cloud Connector dans le domaine de votre site.
2. Créez un groupe de sécurité Active Directory et ajoutez-y les Cloud Connector de votre domaine.
3. Dans Studio, accordez au minimum les autorisations Lecture seule au groupe de sécurité.

Tâche 1 : Détecter votre site

Dans cette étape, vous fournissez les informations dont Citrix Cloud a besoin pour localiser votre site et vous sélectionnez votre emplacement de ressources par défaut. L'emplacement de ressources par défaut spécifie le domaine et la connectivité pour tous les utilisateurs qui accèdent à votre site. Si vous devez installer des Cloud Connector dans le domaine de votre site, vous pouvez le faire maintenant. Si vous avez déjà installé des Cloud Connector, vous pouvez les sélectionner lorsque vous y êtes invité.

1. Dans le menu Citrix Cloud, cliquez sur **Configuration de l'espace de travail**, puis sur **Sites > Ajouter un site**.
2. Dans **Sélectionner le type de site**, sélectionnez la version XenApp ou XenDesktop du site que vous souhaitez ajouter. Citrix Cloud tente de détecter les Cloud Connector dans votre domaine et les affiche dans l'onglet suivant.
3. Dans **Détecter le site XenApp** ou **Détecter le site XenApp et XenDesktop**, effectuez l'une des actions suivantes :

    a) Si vous n'avez installé aucun Cloud Connector dans le domaine de votre site, cliquez sur **Installer connecteur**. Citrix Cloud vous invite à télécharger le logiciel Cloud Connector et

à compléter l'assistant d'installation.

b) Si vous avez installé des Cloud Connector, Citrix Cloud affiche les connecteurs dans les domaines dans lesquels ils ont été détectés. Sélectionnez l'emplacement de ressources que vous souhaitez ajouter à Workspace. Cet emplacement de ressources devient l'emplacement de ressources par défaut.

c) Si vous avez installé des Cloud Connector mais qu'ils ne sont pas affichés, cliquez sur **Détecter**.

4. Dans **Entrer l'adresse du serveur**, entrez l'adresse IP ou le nom de domaine complet d'un Controller dans le site.
5. **XenApp 6.5 uniquement :** entrez le port du serveur XML. Si le port du serveur XML utilise SSL, sélectionnez **Utiliser SSL**.

   > **Remarque :** pour les sites XenApp et XenDesktop 7.x, Citrix Cloud détecte automatiquement le port du serveur XML.

6. Cliquez sur **Découvrir**.
7. Si vous y êtes invité, entrez des informations d'identification d'administrateur Citrix pour le site et cliquez sur **Continuer**. Citrix Cloud effectue un test de connectivité pour vérifier que votre site est accessible. La découverte peut prendre quelques minutes, selon le type et la taille du site.
8. Cliquez sur **Continuer**.

Tâche 2 : Vérifier la connexion Active Directory

Dans **Vérifier la connexion Active Directory**, Citrix Cloud affiche les domaines utilisés avec votre site et indique si des Cloud Connector sont installés dans ces domaines. Pour XenApp 6.5, Citrix Cloud affiche également une alerte si des applications sont affectées à des comptes d'utilisateurs locaux sur des serveurs XenApp.

S'il n'y a pas de Cloud Connector dans un domaine, les utilisateurs dans ce domaine ne peuvent pas utiliser Citrix Workspace pour accéder aux applications publiées dans ce domaine. Si un seul Cloud Connector est installé, la connexion de votre site à Citrix Cloud est plus vulnérable à une panne, ce qui empêche les utilisateurs d'utiliser Workspace. Pour garantir la haute disponibilité de votre site, Citrix recommande d'installer au moins deux (2) Cloud Connector dans chaque domaine.

XenApp 6.5 : si des comptes d'utilisateurs locaux sont affectés à des applications publiées, ces utilisateurs doivent être affectés à des applications à l'aide de leur compte Active Directory. Sinon, ils ne peuvent pas utiliser Workspace pour accéder à leurs applications. Citrix Cloud fournit une liste téléchargeable au format CSV des applications et des comptes d'utilisateurs locaux qui leur sont affectés.

1. Pour installer des Cloud Connector supplémentaires, cliquez sur **Installer connecteur**. Si votre domaine ne dispose que d'un seul Cloud Connector et que vous choisissez de continuer sans installer davantage de Cloud Connector, sélectionnez **Je comprends que la haute disponibilité nécessite l'installation de deux connecteurs dans chaque domaine**.
2. Si des utilisateurs locaux sont affectés à des applications de votre site, cliquez sur **Télécharger la liste des utilisateurs (.csv)**.
3. Cliquez sur **Continuer**.

Tâche 3 : Configurer la connectivité et confirmer les paramètres

Au cours de cette étape, vous indiquez si vous souhaitez autoriser uniquement les utilisateurs internes à accéder à votre site via Workspace ou les utilisateurs externes. La connectivité interne nécessite que vos utilisateurs soient sur le même réseau que votre site. Pour une connectivité externe, vous pouvez utiliser votre NetScaler Gateway existant ou Citrix NetScaler Gateway Service.

1. Dans **Configurer la connectivité**, sous **Sélectionner le type de connectivité**, sélectionnez l'une des options suivantes :
   - **Ajouter Netscaler Gateway existant :** sélectionnez cette option pour utiliser votre NetScaler Gateway existant pour fournir un accès externe.
   - **NetScaler Gateway Service :** sélectionnez cette option pour activer une évaluation du service ou utiliser votre abonnement existant avec votre site.
   - **Interne uniquement :** si cette option est sélectionnée, aucune autre configuration n'est requise. Cliquez sur **Continuer**.
2. Si **Ajouter NetScaler Gateway existant** est sélectionné, effectuez les actions suivantes :
   a) Cliquez sur **Modifier** et tapez l'URL publique de NetScaler Gateway.
   b) Vérifiez que NetScaler Gateway est configuré pour utiliser vos Cloud Connector en tant que serveurs STA comme décrit dans l'article CTX232640.
   c) Cliquez sur **Tester STA**. Lorsque le test est réussi, cliquez sur **Continuer**. Si le test échoue, reportez-vous à l'article CTX232517 pour les étapes de dépannage.
3. Si **NetScaler Gateway Service** est sélectionné, mais que le service n'est pas activé pour votre compte Citrix Cloud en tant qu'évaluation ou en tant qu'achat, cliquez sur **Commencer une version d'évaluation de 60 jours**. Citrix Cloud active le service en tant que version d'évaluation. Si le service a été activé plus tôt, Citrix Cloud détecte le service et affiche le nombre de jours restants, le cas échéant.
4. Cliquez sur **Continuer**.
5. Dans **Confirmer l'agrégation de sites**, vérifiez le port XML, les serveurs XML, les domaines Active Directory et le type de connectivité que vous avez choisis précédemment.

> **Remarque :** Citrix Cloud affiche jusqu'à cinq des serveurs XML auxquels il peut se connecter. Si vous avez plusieurs serveurs XML sur votre site mais qu'un seul s'affiche, Citrix Cloud affiche une alerte. Pour résoudre ce problème, reportez-vous à l'article CTX232516.

6. Cliquez sur **Enregistrer et terminer**. La page Sites affiche le site que vous venez d'ajouter.

> **Remarque :** si vous souhaitez spécifier différents serveurs XML, cliquez sur **Enregistrer et terminer**. Vous pouvez ensuite modifier votre site pour changer ces valeurs.

Modifier la configuration de votre site

Redétecter votre site

Si vous ajoutez des Delivery Controller à votre site ou si vous modifiez les ports XML, vous pouvez initier une nouvelle détection pour vérifier que votre site est toujours accessible dans Workspace.

1. Sur la page **Sites**, cliquez sur le bouton à points du site que vous souhaitez mettre à jour, puis sur **Modifier site**.
2. Dans **Adresse du serveur**, tapez l'adresse IP ou le nom de domaine complet d'un Delivery Controller dans le site et cliquez sur **Redétecter**.

Ajouter ou modifier des serveurs XML

Lorsque vous ajoutez un nouveau site à Workspace, Citrix Cloud détecte automatiquement les serveurs XML de votre site et affiche jusqu'à cinq serveurs XML dans la configuration de votre site. Vous pouvez ajouter et supprimer des serveurs XML selon les besoins de configuration de site, jusqu'à la limite d'affichage de cinq serveurs XML.

Pour ajouter un serveur XML

1. Sur la page **Sites**, cliquez sur le bouton à points du site que vous souhaitez mettre à jour, puis sur **Modifier site**.
2. Dans la section **Serveurs XML**, tapez le port du serveur XML et sélectionnez **Utiliser SSL** si nécessaire.
3. Sélectionnez une méthode de connectivité :
   - **Équilibrage de charge :** cette option permet à Citrix Cloud de sélectionner un serveur XML aléatoire dans la liste.
   - **Basculement :** cette option permet à Citrix Cloud d'utiliser les serveurs XML répertoriés dans l'ordre dans lequel ils apparaissent dans la liste. Vous pouvez réorganiser la liste en faisant glisser et en déposant chaque serveur si nécessaire.
4. Cliquez sur **Enregistrer**.

Si vous rencontrez une erreur lors de l'ajout d'un serveur XML, reportez-vous à l'article CTX232516 pour les étapes de dépannage.

Ajouter des plages d'adresses IP pour différentes options de connectivité

Si vous avez des VDA ou des hôtes de session dans différents sous-réseaux, vous pouvez spécifier des plages d'adresses IP avec un type de connectivité différent pour chacun. Chaque plage d'adresses IP peut également être associée à un emplacement de ressources différent. Par exemple, vous pouvez avoir une plage d'adresses IP pour les machines situées en Europe où les utilisateurs se connectent uniquement en interne, une plage d'adresse IP pour les machines en Europe où les utilisateurs se connectent via votre NetScaler Gateway existant et une plage d'adresses IP pour les machines aux États-Unis où les utilisateurs se connectent via le NetScaler Gateway Service.

1. Sur la page **Sites**, cliquez sur le bouton à points du site que vous souhaitez mettre à jour, puis sur **Modifier site**.
2. Dans la section **Connectivité**, cliquez sur **Ajoutez une plage d'adresses IP avec une option de connectivité différente**.
3. Tapez une plage d'adresses IP au format CIDR.
4. Pour créer un nouvel emplacement de ressources pour votre plage d'adresses IP, effectuez les actions suivantes :
    a) Sélectionnez **Ajouter un nouvel emplacement de ressources** et entrez un nom convivial.
    b) Dans **Sélectionner votre connectivité**, indiquez si vous souhaitez fournir un accès interne uniquement ou autoriser un accès externe à l'aide de votre NetScaler Gateway existant ou de NetScaler Gateway Service.
5. Pour attribuer un emplacement de ressources existant à la plage d'adresses IP, choisissez **Sélectionner un emplacement de ressources existant**, puis sélectionnez l'emplacement de ressources que vous souhaitez utiliser. Si vous choisissez un emplacement de ressources avec un seul Cloud Connector installé, sélectionnez **Je comprends que la haute disponibilité nécessite l'installation de deux connecteurs dans un emplacement de ressources**.
6. Cliquez sur **Ajouter**.

Ajouter des domaines Active Directory supplémentaires

Si vous installez des Cloud Connector dans des domaines supplémentaires avec des utilisateurs Active Directory sur votre site, vous pouvez vous assurer qu'ils sont ajoutés à la configuration de votre site dans Workspace.

1. Sur la page **Sites**, cliquez sur le bouton à points du site que vous souhaitez mettre à jour, puis sur **Modifier site**.
2. Sous Active Directory, cliquez sur **Actualiser**.

Supprimer un site de Workspace

Si vous n'avez plus besoin de la configuration de votre site local dans Workspace, vous pouvez supprimer le site. Lorsque vous supprimez un site, seule la configuration du site dans Workspace est supprimée. Citrix Cloud n'apporte aucune modification à votre site.

1. Sur la page **Sites**, cliquez sur le bouton à points du site que vous souhaitez supprimer.
2. Cliquez sur **Supprimer**.

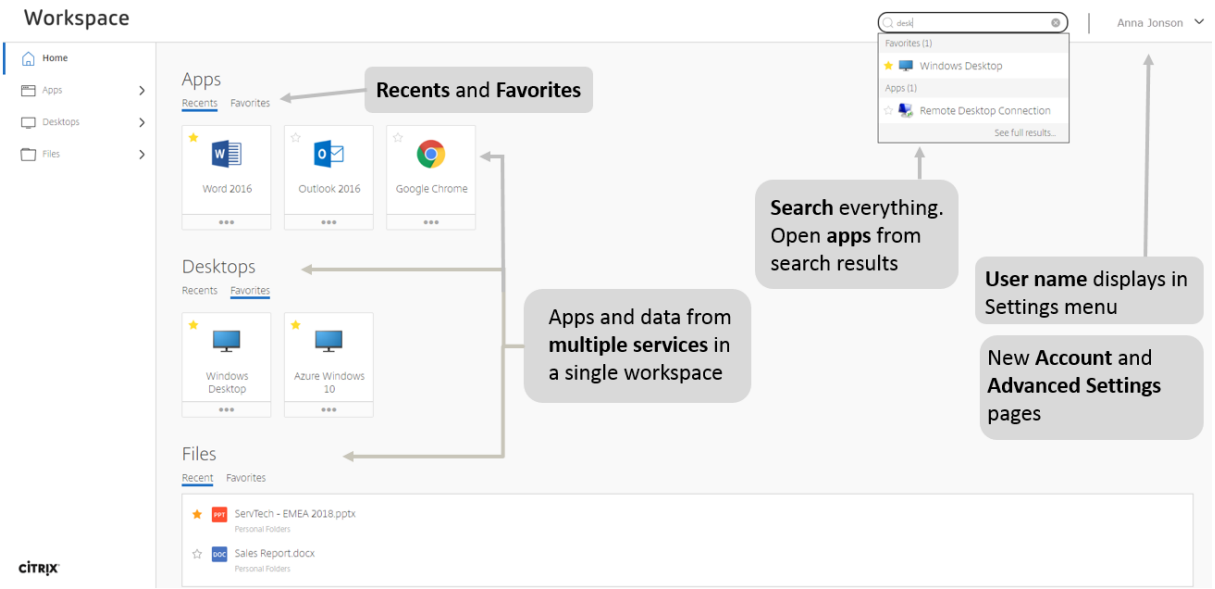
Expérience d'espace de travail

November 7, 2018

Cette article donne un aperçu de l'expérience Citrix Workspace, y compris les modifications récentes.

> **Important :**
>
> Les adresses suivantes doivent pouvoir être contactées afin d'utiliser et de consommer correctement Citrix Workspace :
>
> - `https://*.cloud.com`
> - `https://*.citrixdata.com`
>
> Pour une liste complète des exigences de connectivité de Citrix Cloud, consultez Exigences en terme de connexion Internet.

Améliorations apportées à l'expérience d'espace de travail



Prise en charge des navigateurs

Accédez à l'espace de travail à l'aide d'Internet Explorer 11 ou de la dernière version de Edge, Chrome, Firefox ou Safari.

Disposition de la carte

Les applications et les postes de travail de votre espace de travail sont représentés sous forme de « carte ». Une fenêtre contextuelle affiche plus de détails et d'actions.

Rechercher

Recherchez tout ce que vous voulez dans votre espace de travail et ouvrez des applications directement à partir des résultats de la recherche.

> **Remarque** : la recherche nécessite un minimum de trois caractères.

Récents

Récents affiche les applications, les bureaux et les fichiers récemment ouverts. Pour les applications et les ordinateurs de bureau, en fonction de la taille de l'écran, jusqu'à 30 entrées peuvent s'afficher (dans chaque). Pour les fichiers, vous verrez jusqu'à 15 entrées.

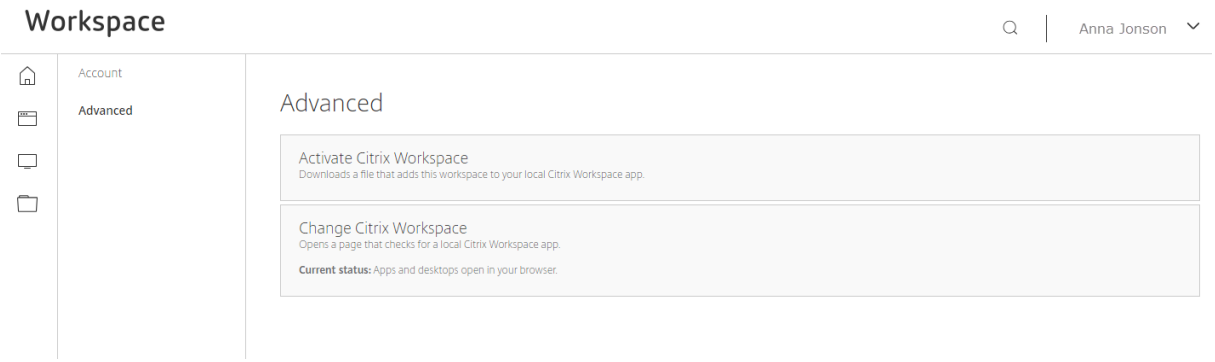
Favoris

Sélectionnez l'icône en forme d'étoile pour ajouter une application aux favoris (250 max.). Cette option est configurable par votre administrateur et peut ne pas être disponible.

Paramètres

Accédez aux paramètres depuis le menu déroulant. Le menu contient le nom d'utilisateur. Le nom d'utilisateur provient du nom d'affichage Active Directory. Si le nom d'affichage est laissé vide (non recommandé), le domaine et le nom du compte s'affichent.

Sélectionnez **Paramètres de compte** pour plus d'options.



- **Activer Citrix Workspace**. Télécharge un fichier qui ajoute cet espace de travail à votre application Citrix Receiver locale.
- **Changer Citrix Workspace**. Ouvre une page qui recherche une application Citrix Workspace locale. Non disponible dans Internet Explorer 11. **Remarque :** cette option est uniquement disponible avec les services Citrix Virtual Apps and Desktops. L'option **Changer Citrix Workspace** n'est pas disponible si, par exemple, vous n'utilisez que des applications SaaS via Citrix Gateway Service.
- **Télécharger Citrix Workspace**. Télécharge un fichier d'installation de Citrix Receiver sur votre ordinateur. Exécutez le fichier pour installer une application Citrix Workspace locale pour Windows ou Mac.

Citrix Receiver et l'application Citrix Workspace

Cette section guide les clients existants qui utilisent Citrix Receiver via la migration vers l'application Citrix Workspace.

La dernière expérience Citrix Workspace est disponible avec les services suivants dans Citrix Cloud :

- Virtual Apps Essentials
- Virtual Desktops Essentials
- Virtual Apps and Desktops Service (inclut l'agrégation de sites à partir des ressources locales de Virtual Apps and Desktops)
- Citrix Gateway Service (mise à disposition d'applications Web et SaaS sécurisées)
- Content Collaboration (anciennement ShareFile)
- Secure Browser Service

Nouveaux clients. Si c'est la première fois que vous utilisez un espace de travail, vous obtiendrez la dernière version de l'interface utilisateur dès qu'elle est disponible. Vous pouvez accéder à l'espace de travail depuis votre navigateur ou depuis une application Citrix Workspace locale.

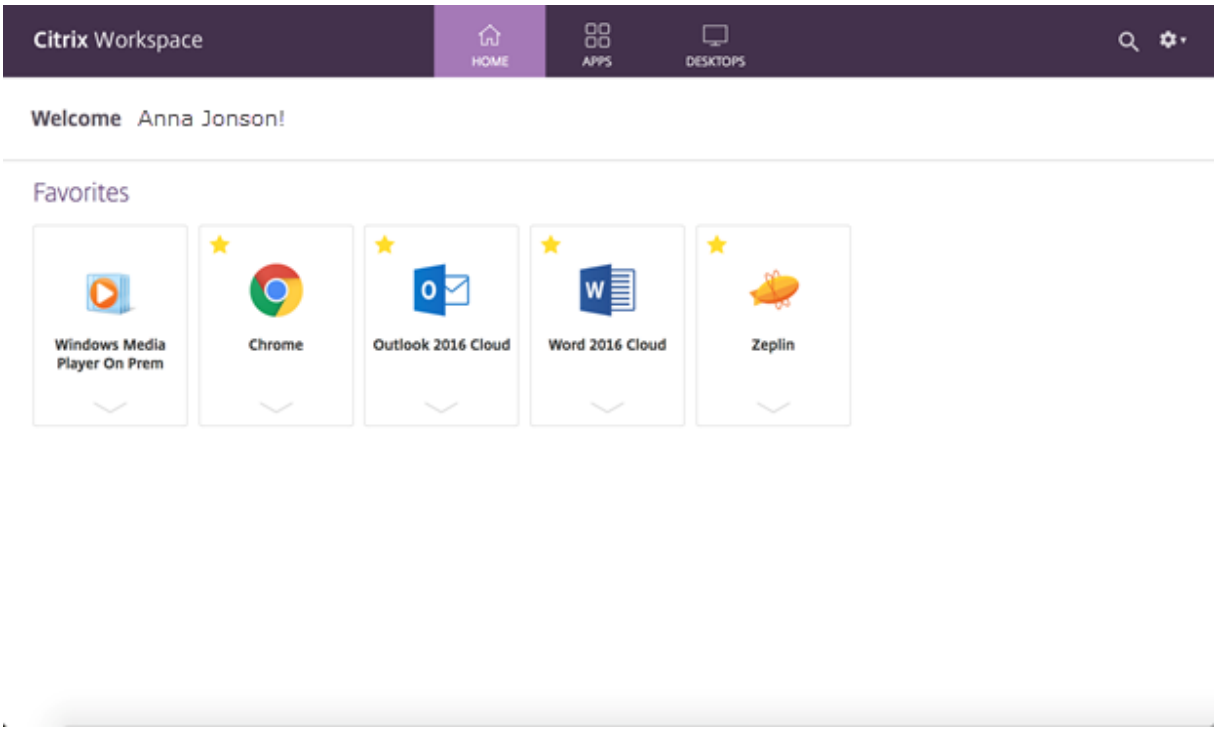
Clients existants. Si vous avez utilisé une version antérieure de Citrix Workspace, l'interface utilisateur mise à jour peut prendre environ cinq minutes à s'afficher dans les applications Citrix Workspace

locales. Vous pouvez voir temporairement une ancienne version de l'interface utilisateur. Vous pouvez également cliquer sur le bouton **Actualiser** de votre navigateur Web pour mettre à jour l'interface utilisateur si nécessaire. Si vous avez utilisé Citrix Receiver en tant qu'application locale, vous devez guider vos utilisateurs pour qu'ils mettent à niveau vers l'application Citrix Workspace afin de tirer parti de toutes les fonctionnalités des services Citrix Cloud.

Les scénarios ci-dessous illustrent ce que les utilisateurs sont susceptibles de voir.

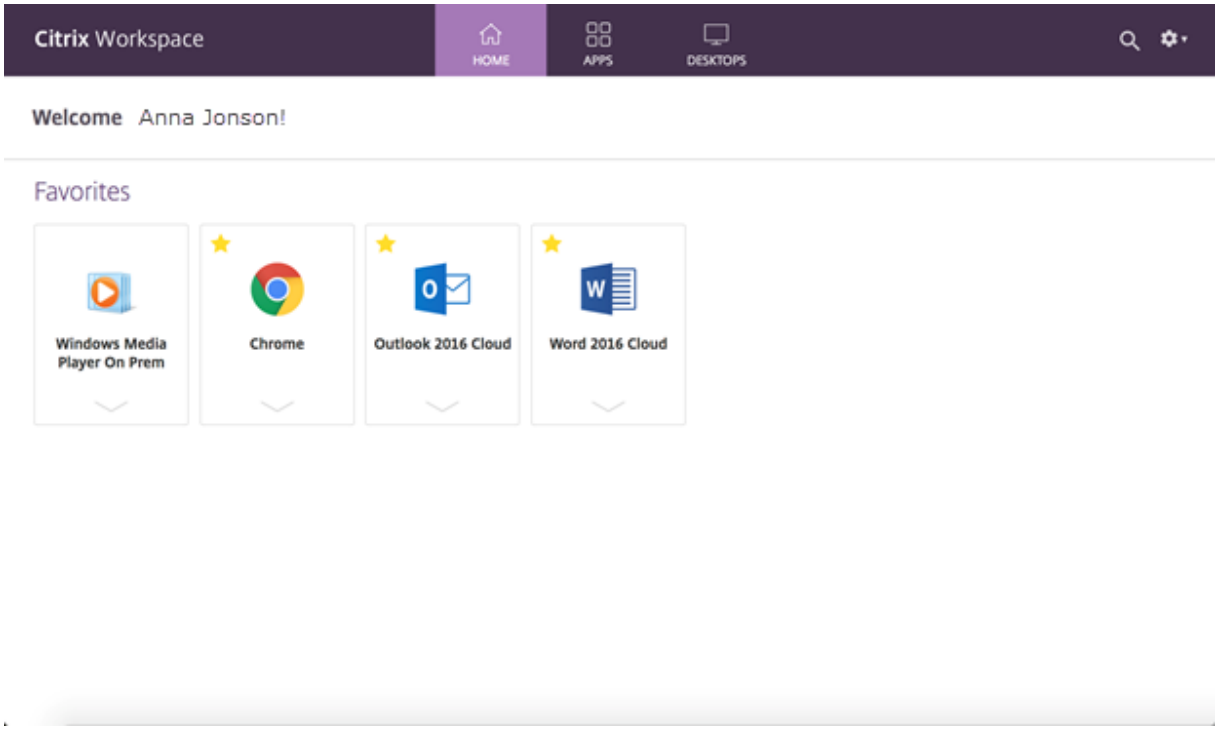
Citrix Receiver

Si vos utilisateurs accèdent à Workspace avec Citrix Receiver, et que les intégrations de services ci-dessus sont activées, ils verront l'interface utilisateur de couleur mauve illustrée ci-dessous. Ils verront les applications Virtual Apps and Desktops ainsi que les applications Web et SaaS provenant de Citrix Gateway Service. Les fichiers ne sont pas pris en charge dans Citrix Receiver et les utilisateurs ne pourront pas y accéder de cette manière.



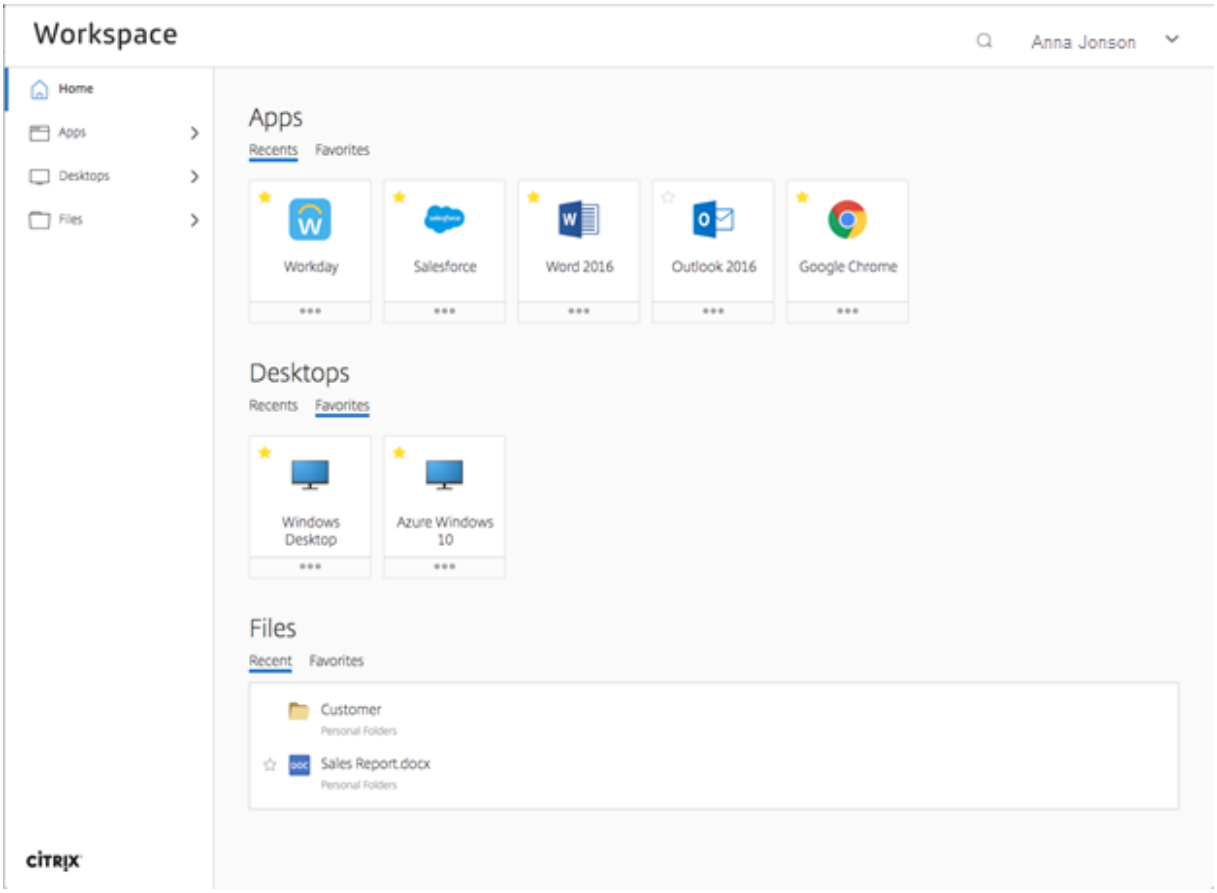
Avec les mêmes services activés et le **contrôle d'accès** activé, les utilisateurs verront toujours l'interface utilisateur mauve, mais sans applications Web et SaaS, car la fonction de contrôle d'accès n'est pas prise en charge dans Citrix Receiver.

Le contrôle d'accès est une fonctionnalité qui permet aux utilisateurs finaux d'accéder aux applications SaaS, Web et virtuelles avec une expérience d'authentification unique (SSO).



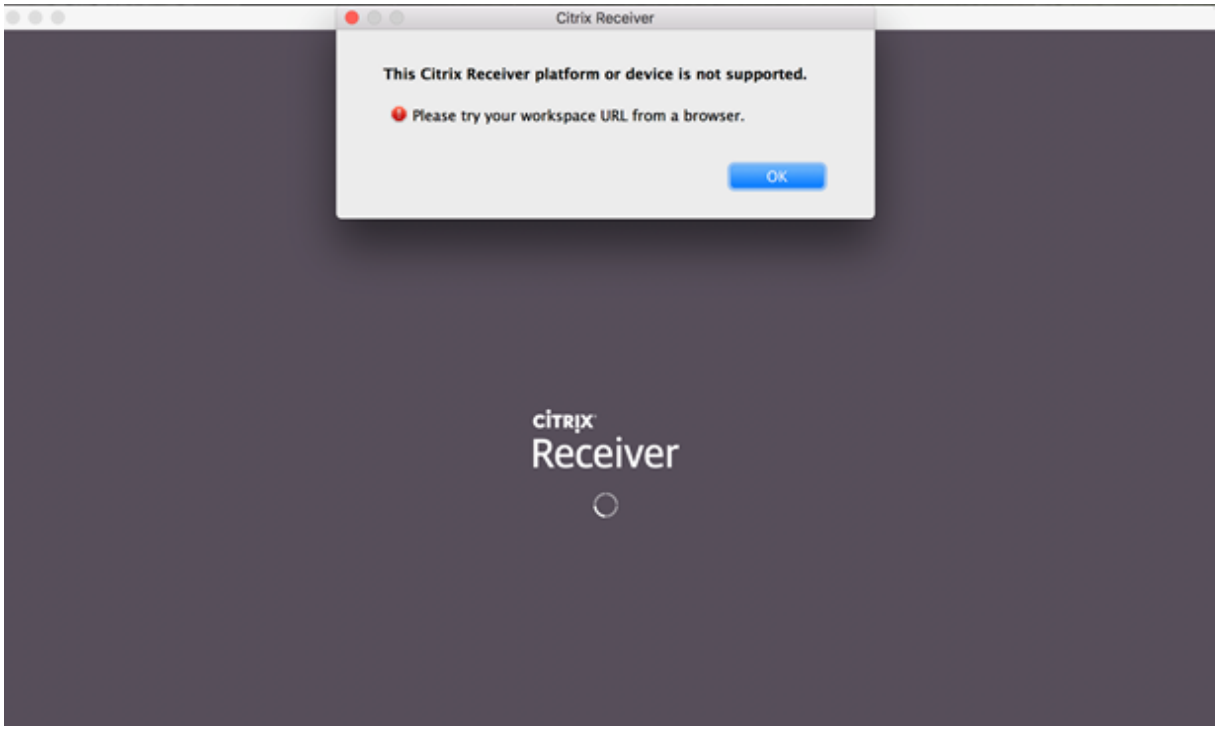
Application Citrix Workspace ou navigateur

Lorsque vos utilisateurs mettent à niveau vers l'application Citrix Workspace ou qu'ils utilisent un navigateur Web pour accéder à Workspace, ils voient la nouvelle interface utilisateur et peuvent utiliser toutes les nouvelles fonctionnalités, y compris Fichiers.



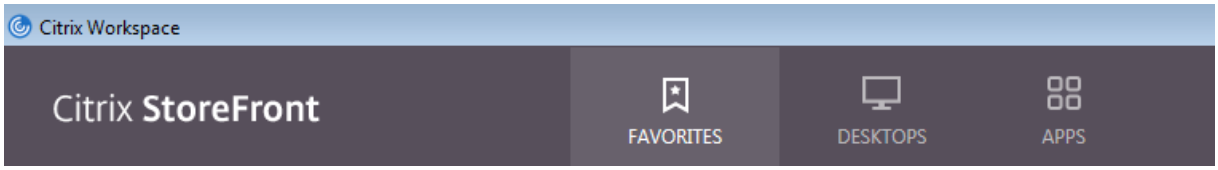
Azure Active Directory (AAD)

Ce scénario s'applique lorsque AAD est activé comme méthode d'authentification de Workspace. Si vos utilisateurs essaient de se connecter à l'aide de Citrix Receiver, ils verront un message indiquant que l'appareil n'est pas pris en charge et qu'ils doivent utiliser un navigateur. Une fois qu'ils ont mis à niveau vers l'application Citrix Workspace, ils peuvent accéder à Workspace. Pour le tableau montrant les méthodes d'authentification prises en charge avec l'application Citrix Workspace, voir le tableau à la fin de cet article.



StoreFront (déploiement sur site)

Si vous disposez d'un environnement local de StoreFront et que les utilisateurs choisissent de mettre à niveau Citrix Receiver vers l'application Citrix Workspace, le seul changement sera l'icône permettant d'ouvrir l'application Citrix Workspace.



Utilisateurs du gouvernement

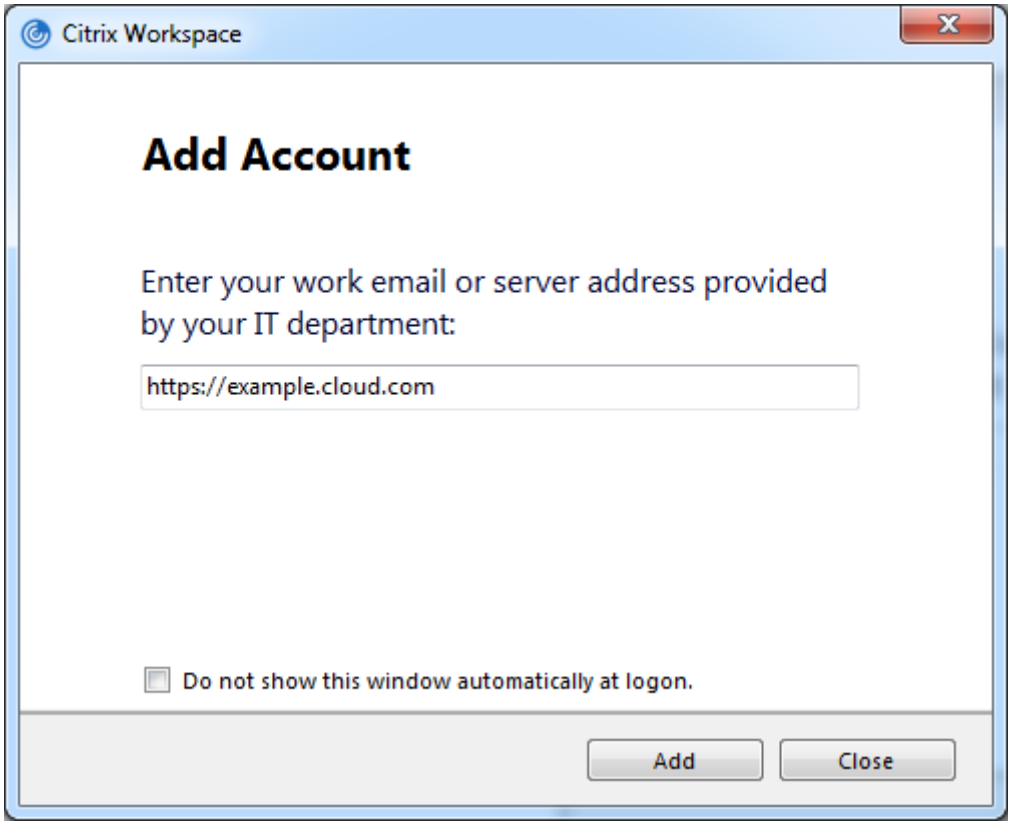
Les utilisateurs de Citrix Cloud Government continueront d'utiliser l'interface utilisateur de couleur « mauve » lorsqu'ils utilisent l'application Workspace ou lors de l'accès à partir d'un navigateur Web.

Modification de votre abonnement au service

Si vous avez modifié l'abonnement à votre service, vous devrez peut-être actualiser l'application Workspace locale manuellement. Dans l'application Citrix Workspace pour Windows :

1. Depuis la barre d'état système Windows, cliquez avec le bouton droit sur l'icône de Citrix Workspace et cliquez sur **Préférences avancées > Réinitialiser Citrix Workspace**.

2. Ouvrez l'application Citrix Workspace pour Windows, sélectionnez **Comptes > Ajouter** et entrez l'adresse de l'espace de travail, par exemple, `https://example.cloud.com`.



Au lieu de suivre l'étape 2, vous pouvez utiliser un navigateur pour entrer l'URL de l'espace de travail et vous connecter. Ensuite, activez Citrix Workspace à partir de **Paramètres > Paramètres du compte > Activer Citrix Workspace**. L'activation de Citrix Workspace télécharge un fichier avec une extension .cr qui ajoute l'espace de travail à votre application Citrix Workspace locale.

Changement de la méthode d'authentification

Si vous êtes connecté à Citrix Workspace et que votre administrateur modifie la méthode d'authentification, par exemple d'Active Directory à Azure Active Directory, des erreurs risquent de se produire dans Citrix Workspace. Si cela vous arrive, déconnectez-vous de Citrix Workspace et fermez le navigateur ou l'application Citrix Workspace. Attendez environ 5 minutes et reconnectez-vous. Citrix Workspace devrait de nouveau être disponible. Vous pouvez vous connecter à l'aide de la nouvelle méthode d'authentification.

Authentification et l'application Citrix Workspace

Le tableau suivant répertorie les méthodes d'authentification prises en charge par l'application Citrix Workspace. Nous recommandons aux abonnés à Workspace d'utiliser la dernière version de

l'application Citrix Workspace.

Certains clients continuent à utiliser Citrix Receiver. Citrix Receiver est pris en charge sur toutes les plates-formes de bureau (Windows, Mac et Linux). Citrix Receiver pour HTML5 et Citrix Receiver pour Chrome sont également pris en charge. Pour un aperçu de la prise en charge de TLS et SHA2 avec les Citrix Receiver, consultez l'article CTX23226.

Le tableau suivant répertorie les méthodes d'authentification prises en charge par Citrix Workspace.

Application Citrix Workspace	Authentification Active Directory	Authentification Azure Active Directory
Citrix Workspace pour Windows	Oui	Oui (application Workspace ; Receiver 4.9 LTSR CU2 et versions ultérieures uniquement ; Receiver 4.11 CR et versions ultérieures uniquement)
Citrix Workspace pour Linux	Oui	Oui (application Workspace ; Receiver 13.8 ou versions ultérieures uniquement)
Citrix Workspace pour Mac	Oui	Non
Citrix Workspace pour Android	Oui	Oui (application Workspace ; Receiver 13.13 et versions ultérieures uniquement)

Pour plus d'informations sur la prise en charge par l'application Workspace de fonctionnalités spécifiques, reportez-vous au tableau des fonctionnalités de l'application Citrix Workspace.

Service Contrôle d'accès

November 7, 2018

Le service Contrôle d'accès permet aux administrateurs d'offrir une expérience homogène, intégrant Single Sign-on, accès distant et inspection du contenu dans une solution unique pour un contrôle d'accès de bout en bout. Les administrateurs informatiques peuvent gérer l'accès aux applications SaaS approuvées avec une expérience de connexion unique simplifiée. Grâce au service Contrôle d'accès, les administrateurs peuvent également protéger le réseau de l'organisation et les machines des utilisateurs contre les logiciels malveillants et les fuites de données en filtrant l'accès à des sites Web et des catégories de sites Web spécifiques. Les administrateurs peuvent appliquer des stratégies

de sécurité d'accès renforcées pour un accès sécurisé aux applications SaaS. Une fois authentifiés, les employés ont accès à toutes les applications critiques de l'entreprise, qu'ils se trouvent dans les bureaux, à la maison ou en voyage.

Les administrateurs peuvent surveiller les activités des utilisateurs, telles que les sites Web malveillants, dangereux ou inconnus visités, la bande passante consommée et les comportements de chargement et de téléchargement risqués. En utilisant les statistiques sur les sites Web et les catégories de sites Web consultées, les administrateurs peuvent prendre des mesures correctives pour protéger le réseau de l'entreprise. Parallèlement, le service fournit aux utilisateurs un accès transparent et sécurisé à toutes leurs applications hébergées.

Les administrateurs peuvent également limiter des actions, telles que l'impression, les téléchargements et l'accès au Presse-papiers (copier-coller).

Le diagramme suivant est une représentation visuelle du service Contrôle d'accès.

Fonctionnalités principales du service Contrôle d'accès

Certaines des tâches principales que vous pouvez effectuer avec le service Contrôle d'accès sont les suivantes :

- Publier des applications SaaS avec un accès SSO.
- Définir des stratégies de sécurité améliorées pour les applications SaaS. (Par exemple, filigrane, restriction du copier-coller et blocage des téléchargements.)
- Définir la stratégie d'accès pour les catégories de sites Web et les sites Web à bloquer.
- Définir la stratégie d'accès pour les catégories de sites Web et les sites Web à rediriger vers Secure Browser Service.
- Comprendre l'activité des utilisateurs et des sites Web dans le contexte des applications SaaS et la mettre en corrélation avec les stratégies définies.
- Apporter des modifications aux stratégies pour autoriser ou bloquer l'accès à des sites Web et activer l'accès dans une session de Secure Browser Service.

Mise en route

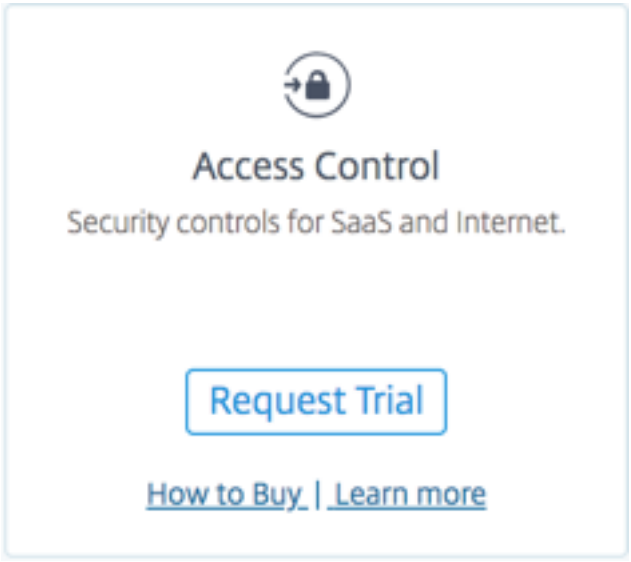
November 7, 2018

Cette page vous explique comment commencer à intégrer et configurer le service Contrôle d'accès pour la première fois. En tant qu'administrateur, vous devez configurer l'authentification, configurer l'accès aux applications SaaS et spécifier les paramètres d'accès au contenu dans le service Contrôle

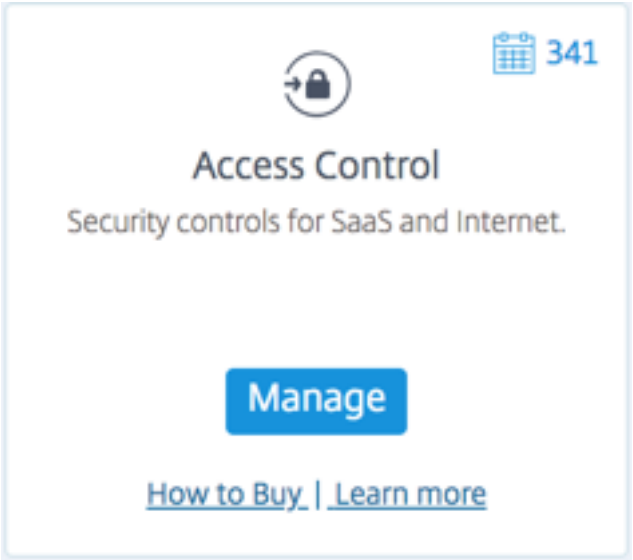
d'accès. Une fois les paramètres terminés, les utilisateurs peuvent accéder au service à partir de l'application Citrix Workspace ou de l'URL de l'espace de travail.

Conditions préalables et limitations

1. Vous devez disposer d'un compte Citrix Cloud. Pour des instructions détaillées sur la manière de procéder, voir Inscription à Citrix Cloud.
2. Vous devez disposer du droit d'accès au service Contrôle d'accès. Sur l'écran Cloud Citrix, dans la section **Services disponibles**, cliquez sur **Demander évaluation**.



Une fois que vous avez reçu le droit d'accès au service, la vignette est disponible dans **Mes services**. Cliquez sur **Gérer** pour accéder à l'interface utilisateur du service.



3. Pour que vos utilisateurs puissent utiliser l'espace de travail et accéder aux applications, ils doivent télécharger et utiliser l'application Citrix Workspace ou utiliser l'URL de l'espace de travail. Vous devez avoir quelques applications SaaS publiées sur votre espace de travail pour tester la solution de contrôle d'accès. L'application Workspace peut être téléchargée depuis https://www.citrix.com/downloads. Dans la liste **Rechercher des téléchargements**, sélectionnez **Application Citrix Workspace**.
4. Si un pare-feu sortant est configuré, assurez-vous que l'accès aux domaines suivants est autorisé.

> - *.cloud.com
> - *.nssvc.net
> - *.netscalergateway.net

Vous trouverez plus de détails dans Configuration du pare-feu et du proxy d'un Cloud Connector et Exigences en terme de connexion Internet.

Limitation : vous ne pouvez ajouter qu'un seul compte Workspace.

Paramètres d'administration

Le diagramme suivant montre les étapes principales à suivre pour démarrer avec le service Contrôle d'accès.

1. Configurez l'authentification de l'utilisateur. Vous devez d'abord configurer l'espace de travail de l'utilisateur avec le fournisseur d'identité préféré de l'organisation, à savoir Identité Citrix (une identité unique avec Citrix Cloud), Active Directory, Active Directory + jeton ou Azure Active Directory. Pour plus d'informations sur les différentes méthodes d'authentification et leur sélection, voir Configuration de l'espace de travail et Gestion des identités et des accès.
2. Configurez l'accès de l'utilisateur aux applications SaaS et virtuelles. Pour connaître la procédure détaillée de configuration et de publication des applications SaaS, voir Prise en charge des applications SaaS.
3. Configurez le filtrage Web pour l'accès Internet à partir des applications SaaS. Si vous avez ajouté une application SaaS à partir de Citrix Gateway Service, pour revenir au service Contrôle d'accès, cliquez sur l'icône de hamburger en haut à gauche du volet de navigation. Dans la liste **Mes services**, sélectionnez **Contrôle d'accès**. Click **Configurer paramètres d'accès au contenu**.

Configurer le filtrage Web pour l'accès Internet à partir des applications SaaS

Vous êtes maintenant prêt à configurer les paramètres d'accès au contenu pour les utilisateurs qui accèdent aux applications SaaS. Par exemple, un lien dans une application SaaS pourrait pointer vers

un site Web malveillant. Avec les paramètres d'accès au contenu, un administrateur peut autoriser, bloquer ou rediriger la demande d'accès à une URL de site Web ou une catégorie de site Web spécifique vers une instance de navigateur hébergée et sécurisée, empêchant ainsi les attaques par navigateur. Pour plus d'informations sur le Secure Browser Service, consultez la documentation Secure Browser Standard Service sur Secure Browser Standard Service.

Remarque : par défaut, les clients de Secured Browser Standard Service (organisation) reçoivent par défaut 5000 heures d'utilisation par an. Pour ajouter des heures supplémentaires, ils doivent acheter des modules Secure Browser complémentaires. Vous pouvez suivre l'utilisation de Secure Browser Service. Pour plus d'informations, consultez la section Surveiller l'utilisation.

L'illustration suivante explique le flux de trafic de l'utilisateur.

Lorsqu'une demande arrive, les vérifications suivantes sont effectuées et les actions correspondantes sont exécutées :

1. La demande correspond-elle à la liste d'autorisation globale ?
    a) Si elle correspond, l'utilisateur peut accéder au site Web demandé.
    b) Si elle ne correspond pas, les listes de sites Web sont vérifiées.
2. La demande correspond-elle à la liste de sites Web configurée ?
    a) Si elle correspond, la séquence suivante détermine l'action.
        i. Bloquer
        ii. Rediriger
        iii. Autoriser
    b) Si elle ne correspond pas, les catégories de sites Web sont vérifiées.
3. La demande correspond-elle à la catégorie de site Web configurée ?
    a) Si elle correspond, la séquence suivante détermine l'action.
        i. Bloquer
        ii. Rediriger
        iii. Autoriser
    b) Si elle ne correspond pas, l'action par défaut (AUTORISER) est appliquée. L'action par défaut ne peut pas être modifiée.

Procédez comme suit pour configurer les paramètres de sécurité améliorés.

1. Cliquez sur Configurer l'accès au contenu.
2. Configurez le filtrage des catégories de sites Web et/ou des listes de sites Web.

Configurer le filtrage des catégories de sites Web

La classification des sites Web restreint l'accès des utilisateurs à des catégories de sites Web spécifiques. Les administrateurs peuvent sélectionner une catégorie dans une liste prédéfinie ou personnaliser les catégories en fonction du déploiement. La liste prédéfinie permet aux organisations de filtrer le trafic Web en utilisant une base de données de classification commerciale. Cette base de données à mise à jour automatique classifie des milliards de sites Web au sein de différentes catégories, telles que réseaux sociaux, jeux d'argent, contenu pour adultes, nouveaux médias et achats. Outre la classification, chaque site Web dispose d'un score de réputation actualisé en fonction du profil de risque historique du site. Les paramètres prédéfinis sont classés comme stricts, modérés, indulgents, inexistants et personnalisés. Les administrateurs peuvent modifier les paramètres prédéfinis pour ajouter ou supprimer des catégories de sites Web.

- Des paramètres prédéfinis strictes minimisent le risque d'accéder à des sites Web non sécurisés ou malveillants. Les utilisateurs peuvent toujours accéder aux sites Web qui présentent de faibles risques. Comprend la plupart des sites Web de voyages d'affaires et de réseaux sociaux.
- Un paramètre prédéfini modéré minimise les risques tout en autorisant des catégories supplémentaires affichant une faible probabilité d'exposition à des sites non sécurisés ou malveillants. Comprend la plupart des sites Web de voyages d'affaires, de loisirs et de réseaux sociaux.
- Le paramètre prédéfini Indulgent maximise l'accès tout en contrôlant les risques liés aux sites Web illégaux et malveillants.
- Le paramètre prédéfini Inexistant autorise toutes les catégories.
- Personnalisé permet de configurer un filtrage personnalisé des catégories.

Procédez comme suit pour configurer le filtrage des catégories de sites Web.

1. Activez **Filter website categories**.
2. Cliquez sur **Add** dans la section correspondante pour bloquer des catégories de sites Web, autoriser des catégories de sites Web ou rediriger l'utilisateur vers un navigateur sécurisé. Par exemple, pour bloquer des catégories, dans la section des catégories bloquées, cliquez sur **Add**.
3. Sélectionnez les catégories à bloquer dans la liste et cliquez sur **Add**.
4. Pour autoriser des catégories, dans la section des catégories autorisées, cliquez sur **Add**. Sélectionnez les catégories à autoriser dans la liste et cliquez sur **Add**.
5. Pour rediriger des utilisateurs vers un navigateur sécurisé, dans la section des catégories redirigées vers un navigateur sécurisé, cliquez sur **Add**. Sélectionnez les catégories dans la liste et cliquez sur **Add**.
6. Cliquez sur **Enregistrer**.

Configurer le filtrage des listes de sites Web

La fonctionnalité de liste de sites Web vous permet de contrôler l'accès à des sites Web spécifiques. Vous pouvez utiliser des caractères génériques, tels que *.exemple.com/*, pour contrôler l'accès à tous les domaines de ce site Web et à toutes les pages dans ce domaine.
Procédez comme suit pour configurer le filtrage des listes de sites Web.

1. Activez **Filter website list**. Cliquez sur **Add** dans la section correspondante pour bloquer, autoriser ou rediriger des sites Web vers un navigateur sécurisé. Par exemple, pour bloquer des sites Web, dans la section des catégories bloquées, cliquez sur **Add**.
2. Entrez un site Web auquel les utilisateurs ne peuvent pas accéder et cliquez sur **Add**.
3. Pour autoriser des sites Web, dans la section des sites Web autorisés, cliquez sur **Add**. Entrez le site Web auquel les utilisateurs peuvent accéder et cliquez sur **Add**.
4. Pour rediriger des utilisateurs vers un navigateur sécurisé, dans la section des sites Web redirigés vers un navigateur sécurisé, cliquez sur **Add**. Entrez un site Web auquel les utilisateurs peuvent uniquement accéder à partir d'un navigateur hébergé par Citrix et cliquez sur **Add**.
5. Cliquez sur **Save** pour que les modifications prennent effet.

Workflow de l'utilisateur

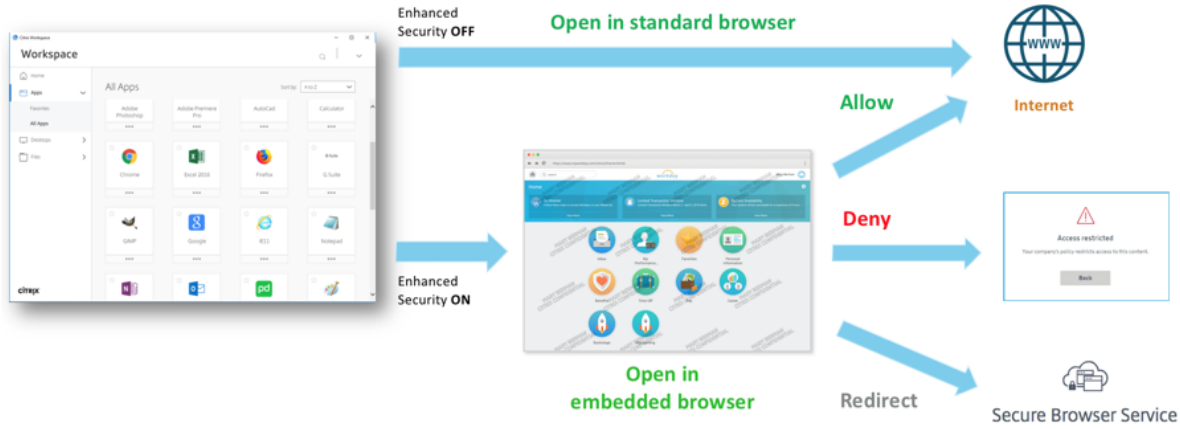
En tant qu'utilisateur, vous devez effectuer les opérations suivantes :

1. Téléchargez l'application Citrix Workspace depuis https://www.citrix.com/downloads. Dans la liste **Find Downloads** (Recherche de téléchargements), sélectionnez **Application Citrix Workspace**.
2. Connectez-vous et recherchez vos applications SaaS. Cliquez sur l'application pour la lancer.

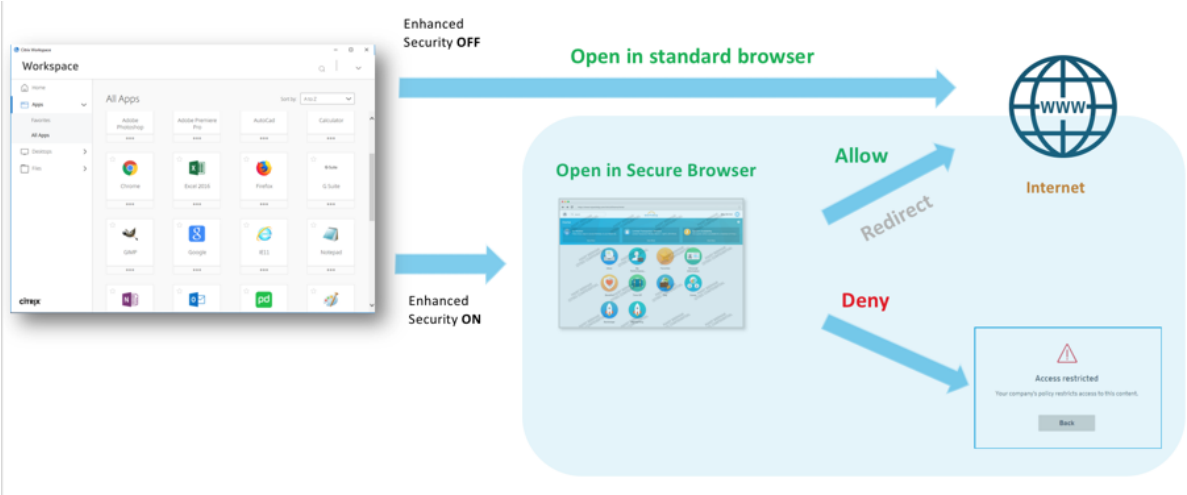
Vous pouvez désormais utiliser l'application SaaS depuis l'application Citrix Workspace ou depuis le portail Web de Citrix Workspace.

Selon les paramètres configurés par l'administrateur, vos applications SaaS s'ouvrent à l'aide du moteur de navigateur de l'application Workspace ou vous êtes redirigé vers un navigateur sécurisé.

Le diagramme suivant montre le flux de haut niveau de l'application Citrix Workspace.



Le diagramme suivant illustre le flux de haut niveau du portail Web de Citrix Workspace.



Systèmes d'exploitation pris en charge

L'application Citrix Workspace est prise en charge sous Windows 7, 8, 10 et Mac 10.11 et versions supérieures.

Prise en charge des navigateurs

Accédez aux espaces de travail à l'aide d'Internet Explorer 11 ou des dernières versions de Edge, Chrome, Firefox ou Safari.

Prise en charge de Citrix Workspace

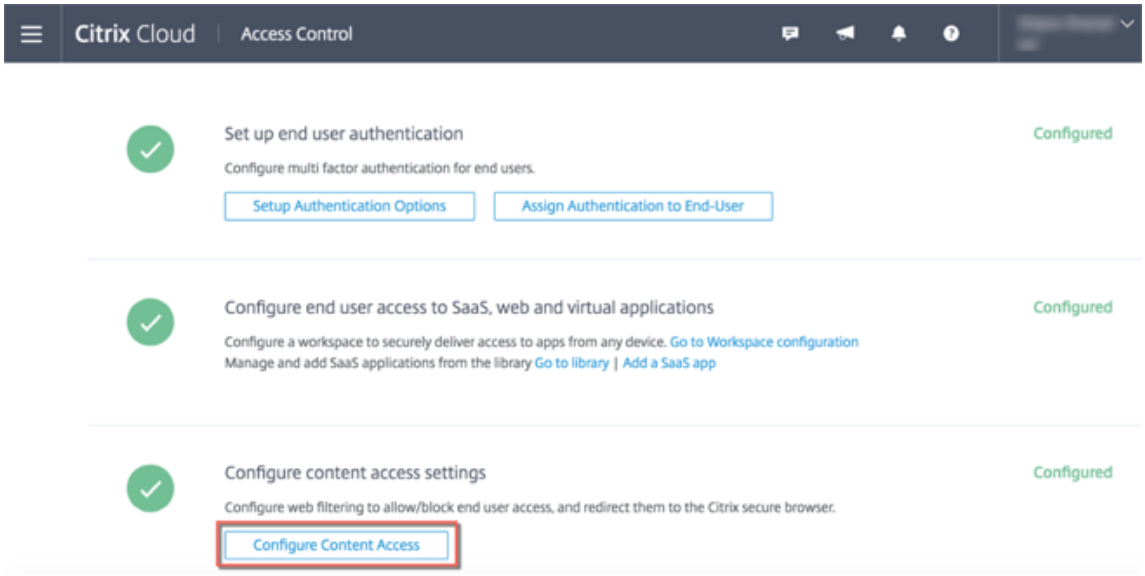
Accédez aux espaces de travail à l'aide de Citrix Workspace pour toutes les plates-formes de bureau (Windows, Mac).

Gérer les paramètres

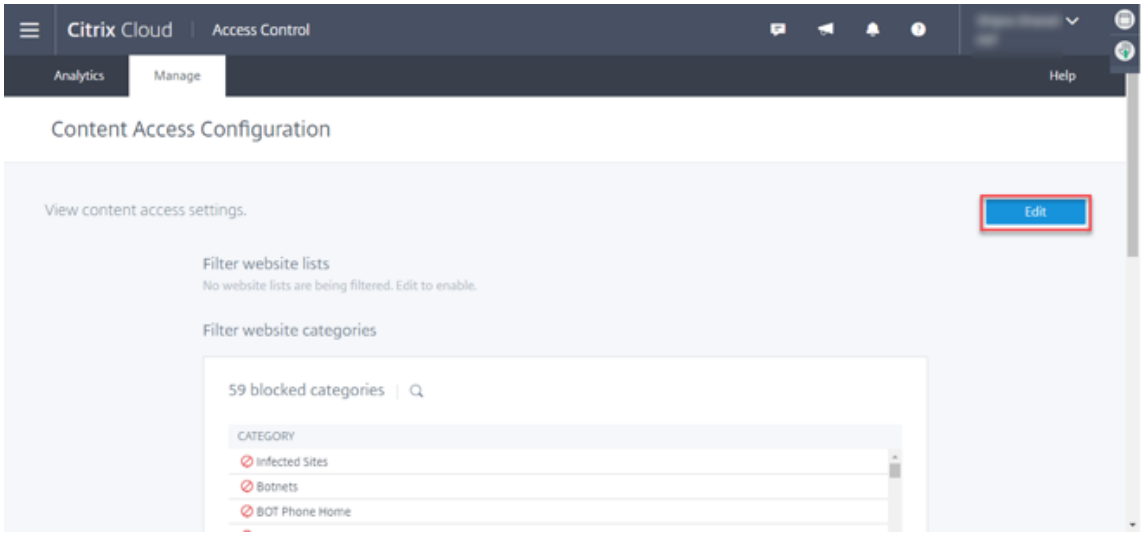
November 7, 2018

Vous pouvez modifier les paramètres de sécurité améliorés pour les utilisateurs à tout moment en fonction de vos besoins.

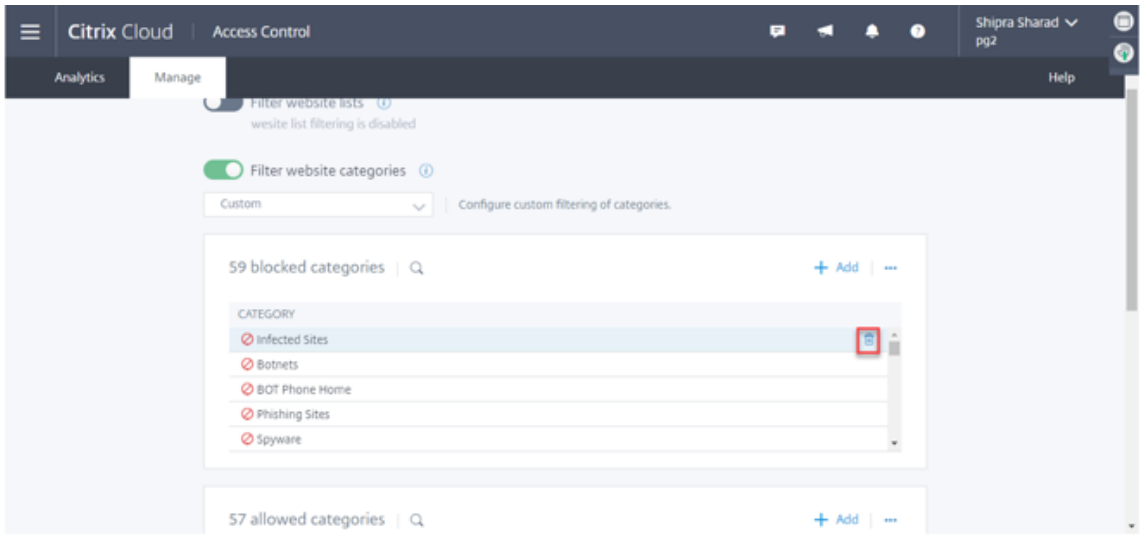
1. Sur la page Get Started, cliquez sur **Configure Content Access**.



2. Dans l'onglet Manage, dans la page Content Access Configuration, cliquez sur **Edit**.



3. Cliquez sur la corbeille pour la catégorie ou le site Web que vous souhaitez supprimer.



4. Cliquez sur **Add** pour bloquer, autoriser ou rediriger vers un navigateur sécurisé une catégorie de site Web ou un site Web.
5. Cliquez sur **Save** pour que les modifications prennent effet.

Catégories

November 7, 2018

Les catégories restreignent l'accès des utilisateurs à des sites Web et à des catégories de sites Web spécifiques. Les clients d'entreprise peuvent filtrer le trafic Web à l'aide d'une base de données de classification commerciale disponible dans le service Contrôle d'accès. Cette base de données contient un très grand nombre d'URL classées dans différentes catégories, telles que réseaux sociaux,

jeux d'argent, contenu pour adultes, nouveaux médias et achats. Lorsque vous sélectionnez des catégories pour ajouter, bloquer ou rediriger vers un navigateur sécurisé, des règles avancées sont créées en interne pour filtrer votre trafic.

Par exemple, vous pouvez bloquer l'accès à des sites dangereux, tels que des sites connus pour être infectés par des logiciels malveillants. Vous souhaiterez peut-être restreindre de manière sélective l'accès à du contenu, tel que du contenu pour adultes ou du contenu multimédia de divertissement pour les utilisateurs de l'entreprise.

Liste des catégories tierces et des groupes de catégories :

- Adulte
  - Adulte/pornographie
  - Nudité
  - Services sexuels
  - Recherche/liens pour adultes
  - Activités illégales
  - Rencontres
  - Grotesque
  - Magazine/actualités pour adultes
  - Fétiche
  - Expression sexuelle (texte)
  - Éducation sexuelle
- Entreprises et industries
  - Maillots de bain et lingerie
  - Entreprises et industries
  - Traducteurs
  - Enchères
  - Shopping/vente au détail
  - Immobilier
  - Achats informatiques en ligne
  - Activités parallèles
  - Fumer
  - Produits alcoolisés
  - Automobile
  - Affaires et Commercial
  - Sonneries
  - Émoticônes
  - Opérateurs mobiles
  - Agriculture
  - Associations/groupements d'affiliation/syndicats
  - Livres/livres électroniques

  - Piratage et usurpation de droits d'auteur
  - Service de transport et fret
- Informatique et Internet
  - Publicités/bannières
  - Informatique et Internet
  - Applications mobiles et éditeurs
  - Réseaux de distribution de contenu et infrastructure
  - Sites d'hébergement
  - Domaines parqués
  - DDNS
- Téléchargements
  - Téléchargements
  - Téléchargements de programmes
  - Services de stockage
  - App Stores pour mobiles
- E-mail
  - Messagerie Internet
  - Abonnements par e-Mail
- Finances
  - Taux du marché
  - Négoce en ligne
  - Assurance
  - Produits financiers
- Jeux d'argent
  - Jeux d'argent en général
  - Loterie
  - Concours/prix
- Santé
  - Santé
  - Haine
- Illégal/dangereux
  - Activités illégales
  - Drogues illicites
  - Médicaments
  - Marijuana
  - Terrorisme/extrémistes
  - Armes
  - Haine/calomnie
  - Violence/suicide

  - Défense d'intérêts en général
- Emplois et CV
  - LinkedIn
  - LinkedIn : Mises à jour
  - LinkedIn : Messages
  - LinkedIn : Connexions
  - LinkedIn : Emplois
  - Emploi
  - Avancement professionnel
- Malware et SPAM
  - Piratage/décodage
  - Malware
  - SPAM
  - Spyware
  - Botnets
  - Sites infectés
  - Sites de phishing
  - Keyloggers
  - Malware sur mobiles
  - Bot de type rappel (phone home)
- Messagerie/chat/téléphonie
  - Chat en ligne
  - Messages instantanés
  - Téléphonie Internet
  - Militaire
  - Services de téléphonie mobile et SMS
- Actualités/divertissement/société
  - Jeux en ligne
  - Jeux
  - Pages Web personnelles/blogs
  - Pages Web personnelles/blogs
  - Streaming de multimédia
  - Événements spéciaux
  - Sujets populaires
  - Boissons
  - Expression sexuelle (texte)
  - Costume/divertissement
  - Occulte
  - Maison et famille

- Sports professionnels
- Sports en général
- Événements de la vie
- Voyage et tourisme
- Agence publique de tourisme
- Transport public
- Hébergement
- Musique
- Horoscope /astrologie/voyance
- Artiste/célébrité
- Restaurant/gestronomie
- Divertissements/lieux/activités
- Religions traditionnelles
- Religions
- Politique
- Actualités
- Éducation
- Gouvernement
- Militaire
- Loisirs et hobbies
- Référence
- Sites pour enfants
- Événements artistiques et culturels
- Organisations philanthropiques à but non lucratif
- Mode et beauté
- Aucun contenu
- URL non prise en charge
- Loi
- Communautés locales
- Divers
- Magazines en ligne
- Animaux/vétérinaire
- Recyclage/environnement
- Science
- Société et culture
- Photographie et film
- Musées et histoire
- Formation en ligne
- Wordpress

    - Wordpress : Publication
    - Wordpress : Charger
- Adresse IP privée
    - Adresses IP privées
- Peer-to-Peer/Torrents
    - Peer to Peer/Torrents
- Proxies distants
    - Proxies distants
- Rechercher
    - Caches du moteur de recherche
    - Ask.fm
    - Ask.fm : Demander
    - Ask.fm : Répondre
    - Moteurs de recherche et portails
- Réseaux sociaux
    - Réseaux sociaux en général
    - Facebook
    - Facebook : Publication
    - Facebook : Commenter
    - Facebook : Amis
    - Facebook : Charger des photos
    - Facebook : Événements
    - Facebook : Applications
    - Facebook : Chat
    - Facebook : Questions
    - Facebook : Chargement de vidéos
    - Facebook : Groupes
    - Facebook : Jeux
    - Twitter
    - Twitter : Publication
    - Twitter : Messages
    - Twitter : Suivre
    - Youtube
    - YouTube : Commenter
    - YouTube : Chargement de vidéos
    - YouTube : Partage
    - Instagram
    - Instagram : Charger
    - Instagram : Commenter

- Instagram : Message privé
- Tumblr
- Tumblr : Publication
- Tumblr : Commenter
- Tumblr : Chargement de photos ou de vidéos
- Google+
- Google+ : Publication
- Google+ : Commenter
- Google+ : Chargement de photos
- Google+ : Chargement de vidéos
- Google+ : chat vidéo
- Pinterest
- Pinterest : Code PIN
- Pinterest : Commenter
- Vine
- Vine : Charger
- Vine : Commenter
- Vine : Message
- YikYak
- YikYak : Publication
- YikYak : Commenter
- Sites de recherche et de partage de photos
- Bulletins électroniques
- Bulletins informatiques

Cas d'utilisation : configurer une stratégie d'accès pour permettre un accès sélectif aux applications

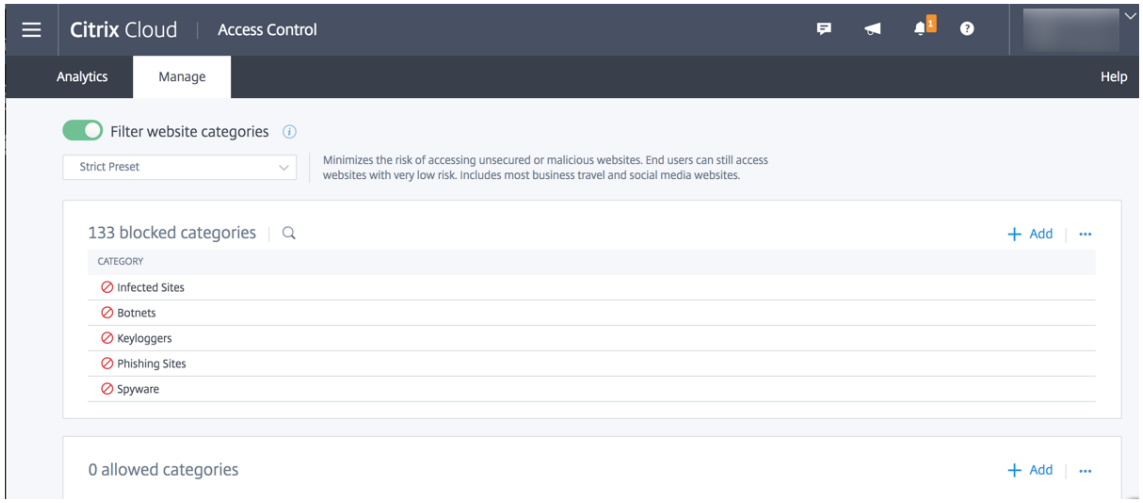
November 7, 2018

Certaines organisations souhaitent restreindre l'accès aux programmes de messagerie Web ou aux sites de réseaux sociaux, dans le cadre d'une stratégie, pour des raisons de sécurité ou autres. Pour configurer cela, ils peuvent sélectionner `strict preset` dans les catégories de filtres de site Web. Des paramètres prédéfinis strictes minimisent le risque d'accéder à des sites Web non sécurisés ou malveillants. Les utilisateurs peuvent toujours accéder aux sites Web qui présentent de faibles risques.

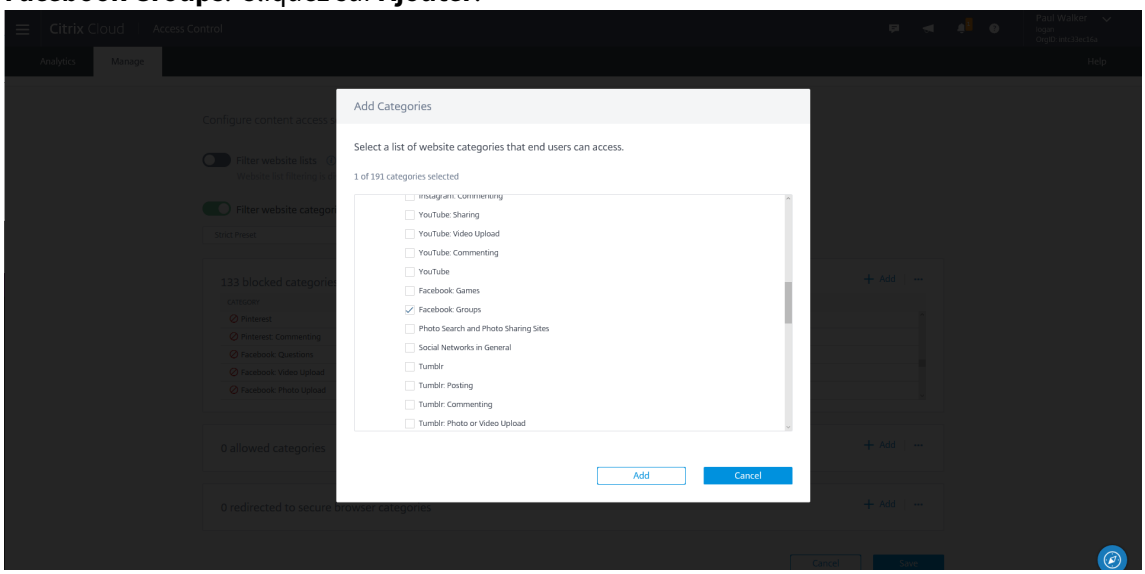
Si la stratégie de votre organisation impose des préréglages stricts, mais souhaite autoriser un accès sélectif aux applications qui ne sont pas liées à la productivité, mais qui sont nécessaires à l'interaction sociale, procédez comme suit pour configurer les paramètres du service Contrôle

d'accès. Dans la configuration suivante, des paramètres prédéfinis strictes sont sélectionnés, mais ils sont personnalisés pour autoriser l'accès aux groupes facebook et accéder à Instagram via un navigateur sécurisé.

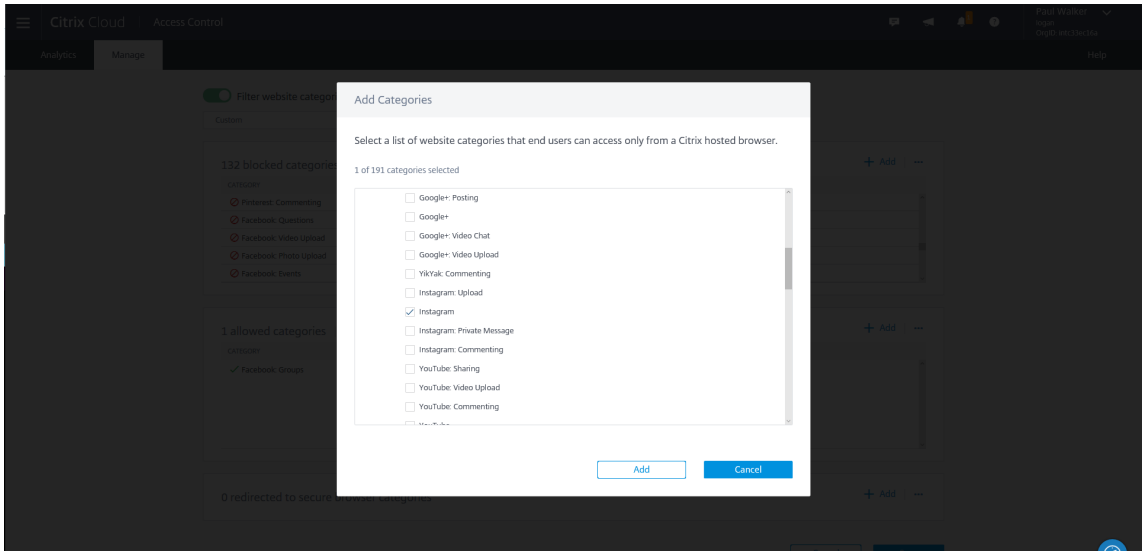
1. Connectez-vous à Citrix Cloud.
2. Sur la vignette **Contrôle d'accès**, cliquez sur **Gérer**.
3. Cliquez sur **Configure Content Access**.
4. Activez **Filter website categories**.
5. Sélectionnez **Strict Preset**.



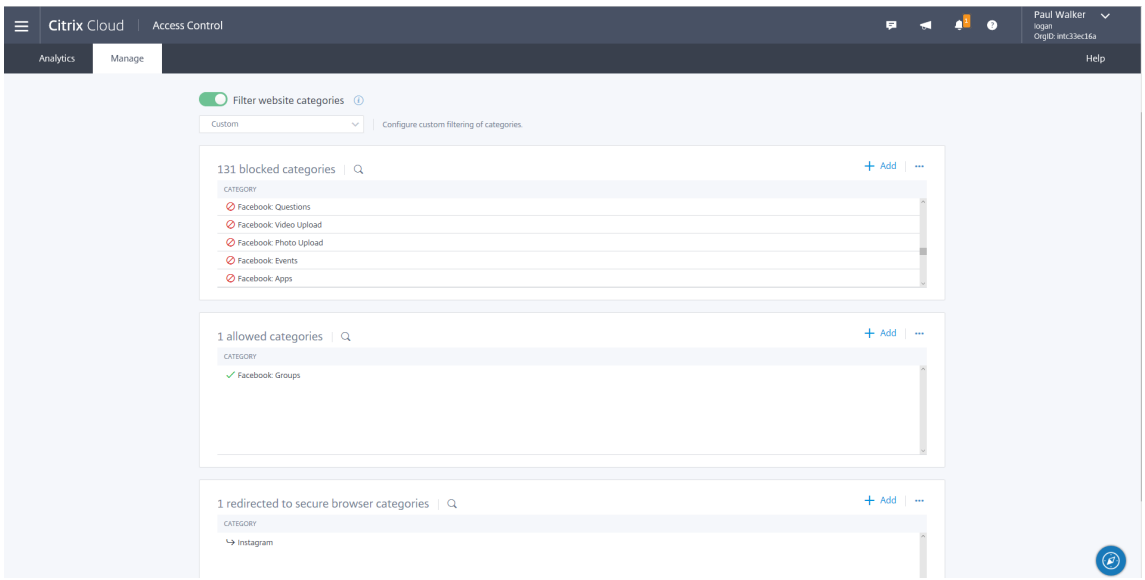
6. Dans la section des catégories autorisées, cliquez sur **Add**. Dans **Add Categories**, sélectionnez **Facebook Groups**. Cliquez sur **Ajouter**.



7. Dans la section des catégories redirigées vers un navigateur sécurisé, cliquez sur **Add**. Dans **Add Categories**, sélectionnez **Instagram**. Cliquez sur **Ajouter**.



8. Vos paramètres apparaissent dans les catégories autorisées et redirigées. Cliquez sur **Enregistrer**.



Validation

Pour valider votre configuration, vous pouvez publier une application SaaS pour https://www.google.com avec SSO désactivé et souscrire certains utilisateurs à l'application.

- Lancez l'application SaaS à partir de l'application Citrix Workspace (ou de Citrix Workspace pour Web).
- Une fois l'application ouverte, recherchez facebook et cliquez sur le lien renvoyé dans la recherche. L'application devrait se lancer.

- Recherchez Instagram et cliquez sur le lien renvoyé dans la recherche. L'application devrait se lancer dans un navigateur sécurisé.
- Recherchez une URL dans la catégorie bloquée et cliquez sur le lien renvoyé. L'accès refusé devrait être refusé.

Analytics

November 7, 2018

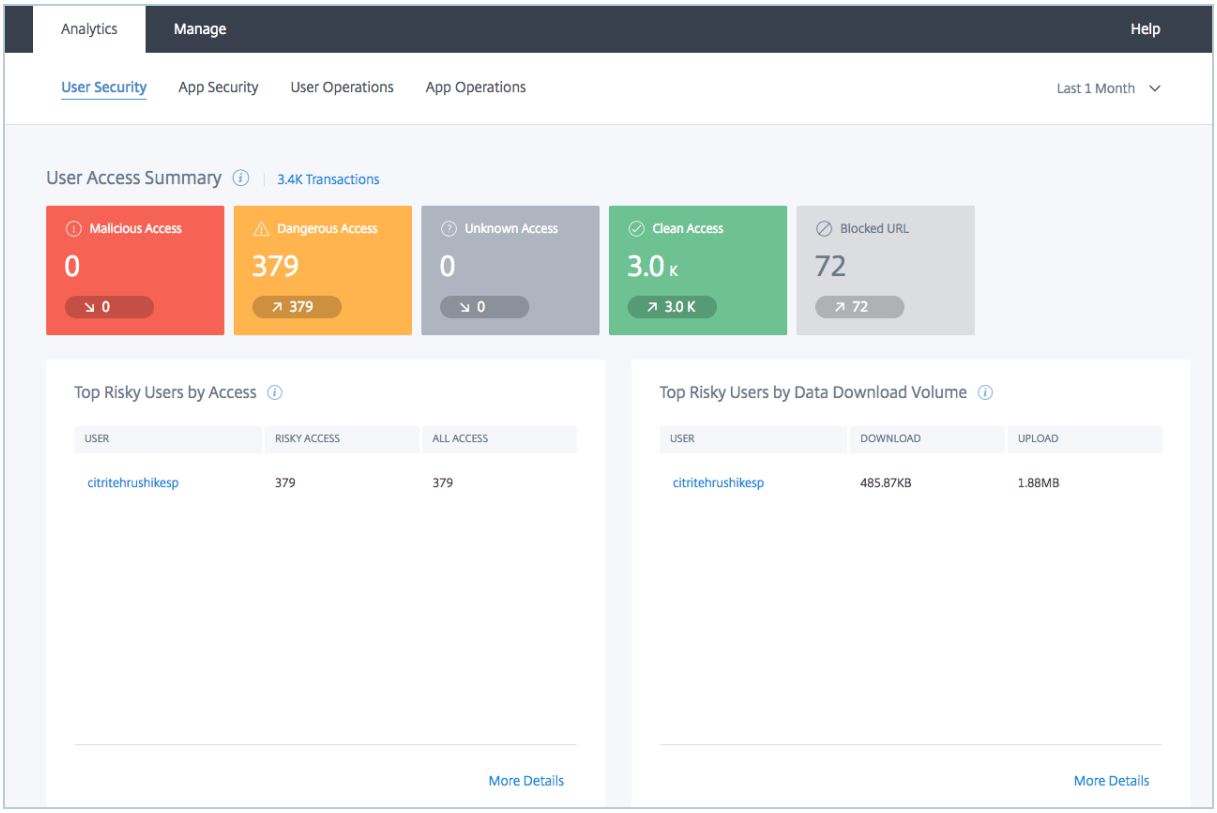
Le service Contrôle d'accès rassemble et présente des informations sur les activités des utilisateurs, telles que les sites Web visités et la bande passante utilisée. Il signale également l'utilisation de la bande passante et les menaces détectées, telles que les logiciels malveillants et les sites de phishing. Vous pouvez utiliser ces indicateurs clés pour surveiller votre réseau et prendre des mesures correctives.

Tableaux de bord

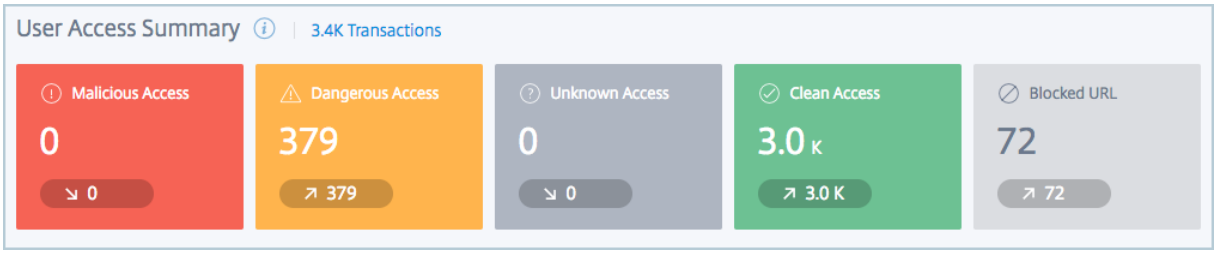
Le service Contrôle d'accès propose quatre tableaux de bord : tableau de bord sur la sécurité des utilisateurs, tableau de bord sur la sécurité des applications, tableau de bord sur les opérations des utilisateur et tableau de bord sur les opérations des applications. Ces tableaux de bord affichent plusieurs sections qui dressent la liste des applications ou des sites Web auxquels les utilisateurs ont accédé à partir du réseau d'entreprise, ainsi que les activités effectuées par les utilisateurs du réseau.

Sécurité des utilisateurs

Les domaines auxquels accèdent les utilisateurs de votre réseau sont classés en fonction de la configuration de la catégorisation d'URL dans le service Contrôle d'accès. Le tableau de bord **User Security** indique le nombre de domaines potentiellement dangereux auxquels les utilisateurs ont accédé et le volume de données chargées et téléchargées par les utilisateurs de votre réseau.
Pour accéder au tableau de bord **User Security**, sous l'onglet **Analytics**, cliquez sur **User Security**.



Pour la période sélectionnée, dans la section **User Access Summary**, le tableau de bord fournit un aperçu des domaines malveillants, des domaines dangereux, des domaines inconnus, des domaines propres et des URL bloquées auxquels les utilisateurs de votre réseau ont accédé, de même que la tendance d'accès à ces domaines par les utilisateurs.

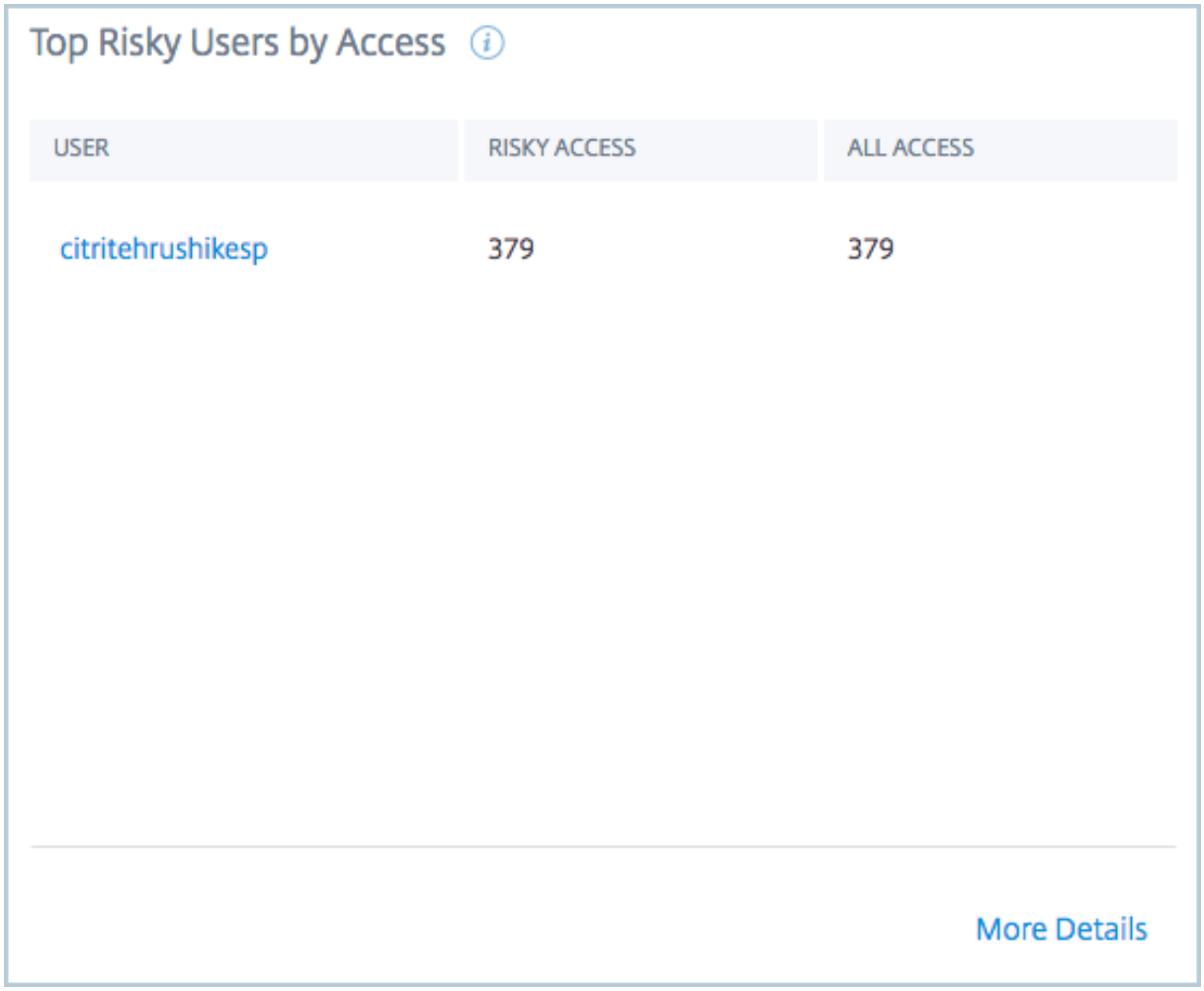


Les widgets sont représentés en fonction du score de réputation des domaines auxquels les utilisateurs ont accédé. Le score de réputation des domaines est attribué en fonction de la configuration de la catégorisation des URL dans le service Contrôle d'accès. Les widgets sont représentés comme suit :

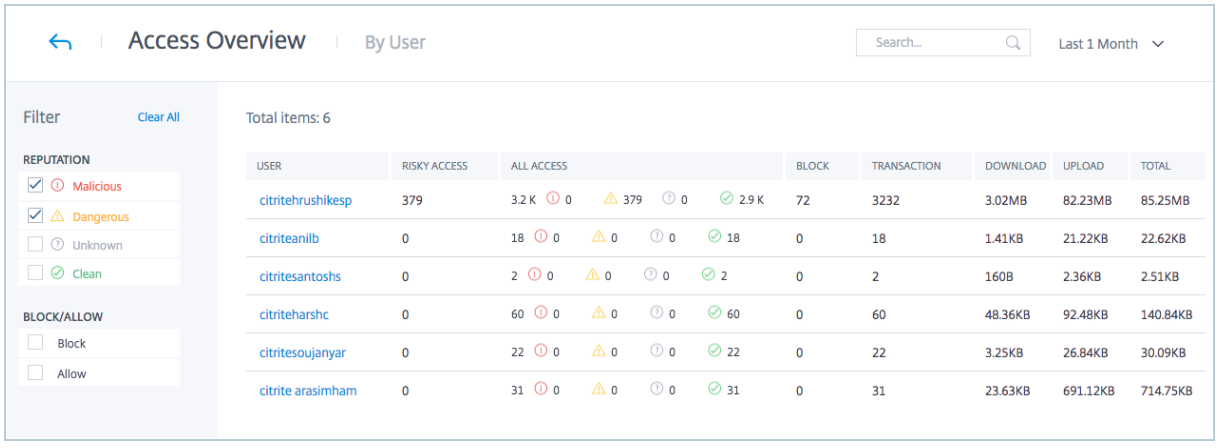
Widgets	Détails
Malicious Access	Affiche le nombre de domaines ayant un score de réputation 4 auxquels les utilisateurs ont accédé.
Dangerous Access	Affiche le nombre de domaines ayant un score de réputation 3 auxquels les utilisateurs ont accédé.
Unknown Access	Affiche le nombre de domaines ayant un score de réputation 2 auxquels les utilisateurs ont accédé.
Clear Access	Affiche le nombre de domaines ayant un score de réputation 1 auxquels les utilisateurs ont accédé.
Blocked URL	Affiche le nombre de domaines ou d'URL bloqués par le service Contrôle d'accès.

Principaux utilisateurs à risque par accès

Dans la section **Top Risky Users by Access**, le tableau de bord fournit les détails des principaux utilisateurs ayant accédé aux URL ou aux domaines classés comme malveillants ou dangereux par le service de contrôle d'accès. Il fournit le nom du compte d'utilisateur, le nombre de domaines potentiellement dangereux auxquels l'utilisateur a accédé et le nombre total de domaines auxquels l'utilisateur a accédé.

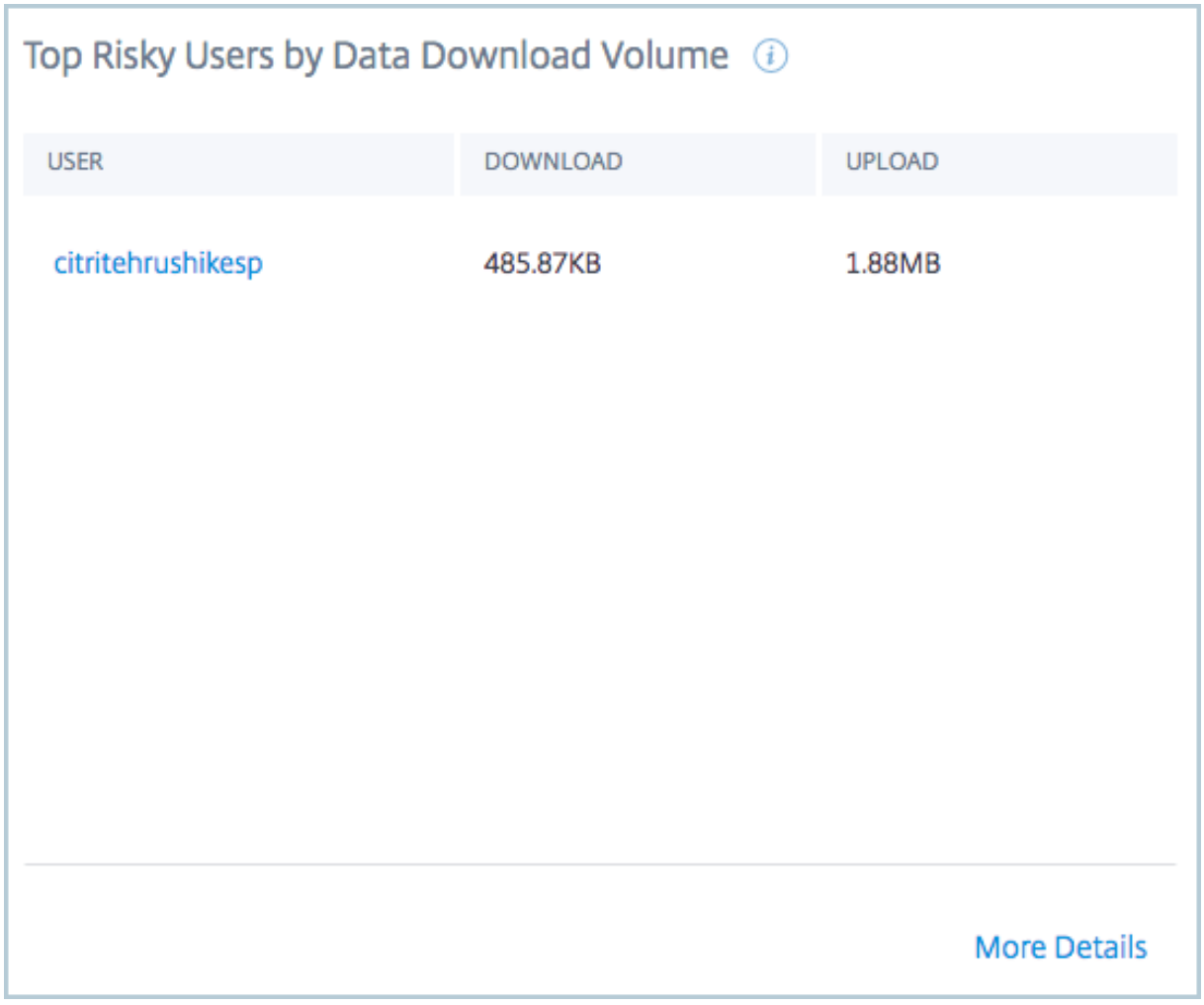


Vous pouvez cliquer sur **More Details** pour afficher la liste complète des utilisateurs ayant accédé à des domaines potentiellement dangereux.

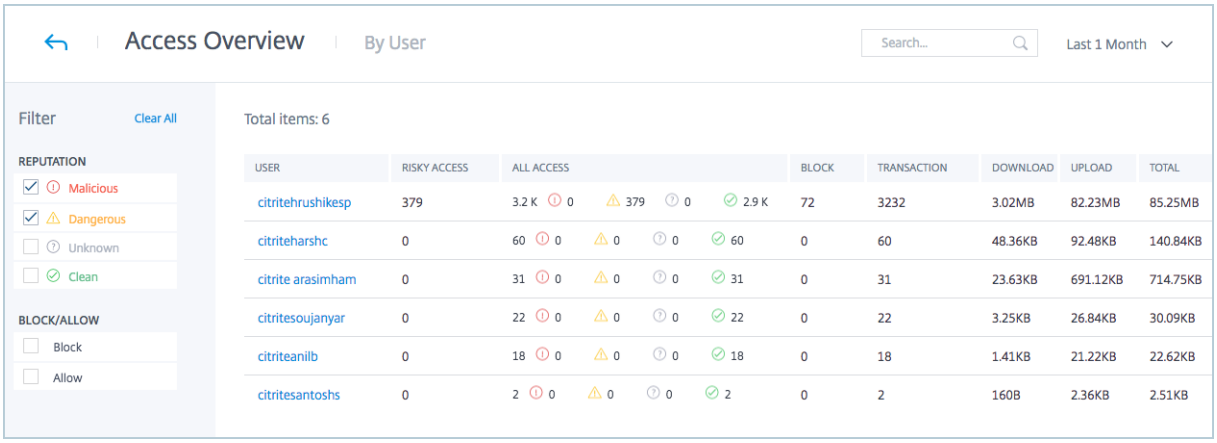


Principaux utilisateurs à risque par volume de données téléchargées

Dans la section **Top Risky Users by Data Download Volume**, le tableau de bord fournit les détails des principaux utilisateurs ayant chargé ou téléchargé un volume important de données à partir des domaines classés comme malveillants ou dangereux par le service de contrôle d'accès. Il fournit le nom du compte d'utilisateur, le volume de données chargées ou téléchargées par l'utilisateur depuis des domaines potentiellement dangereux.

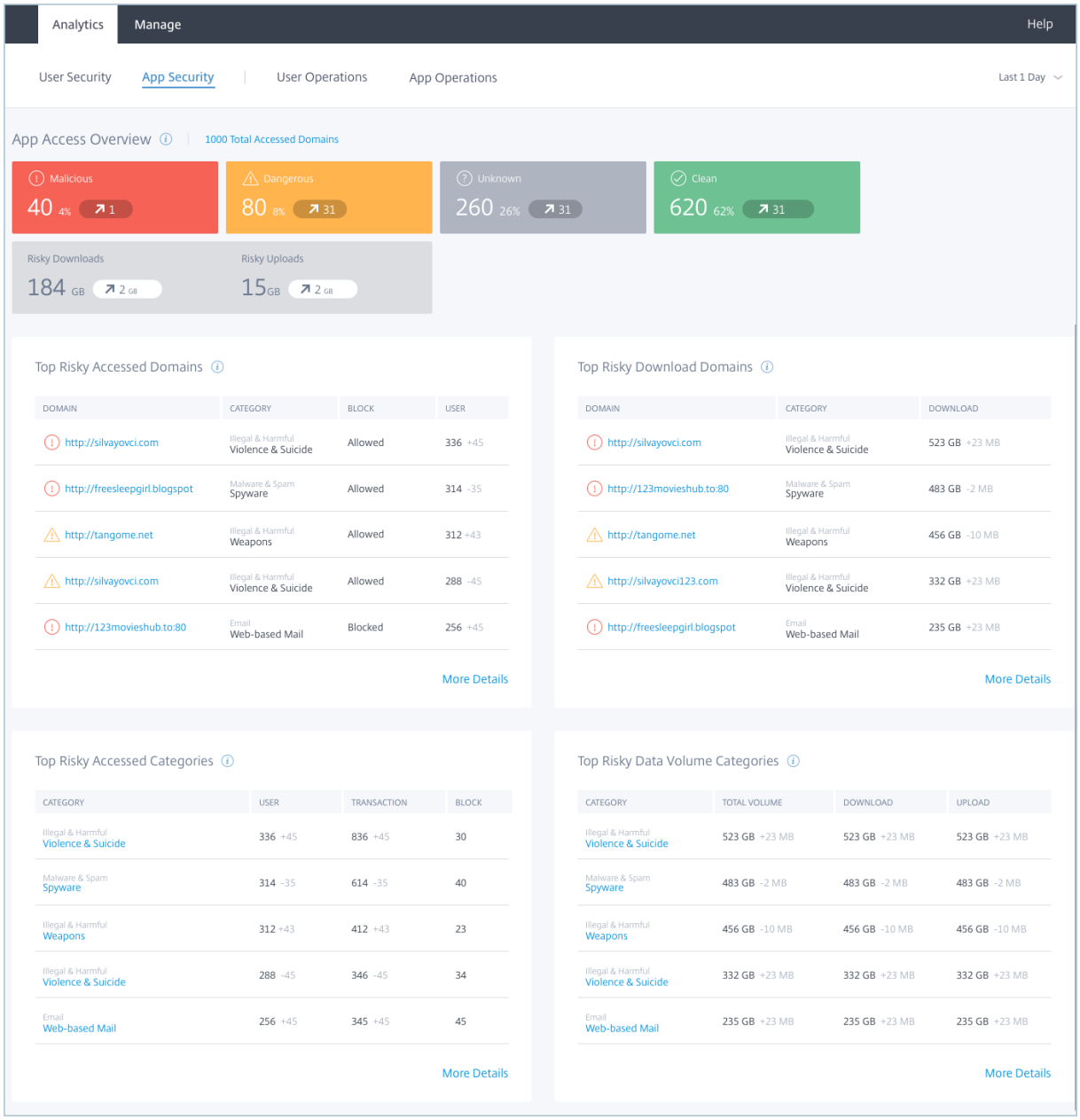


Vous pouvez cliquer sur **More Details** pour afficher la liste complète des utilisateurs ayant chargé ou téléchargé des données depuis des domaines potentiellement dangereux.

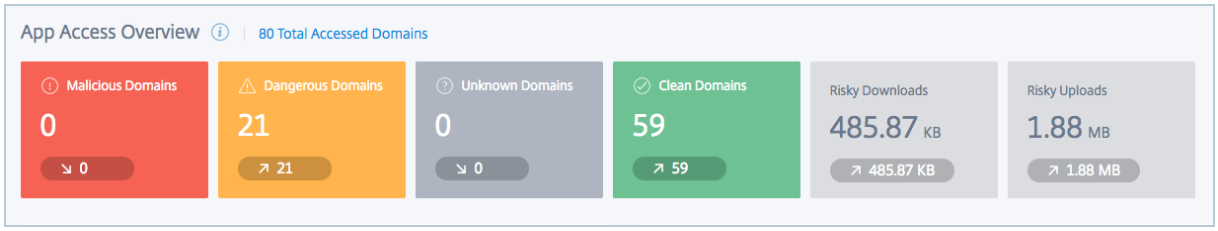


Sécurité des applications

Le tableau de bord **App Security** récapitule les détails des domaines, des URL et des applications auxquels les utilisateurs de votre réseau ont accédé. Pour accéder au tableau de bord **App Security**, sous l'onglet **Analytics**, cliquez sur **App Security**.



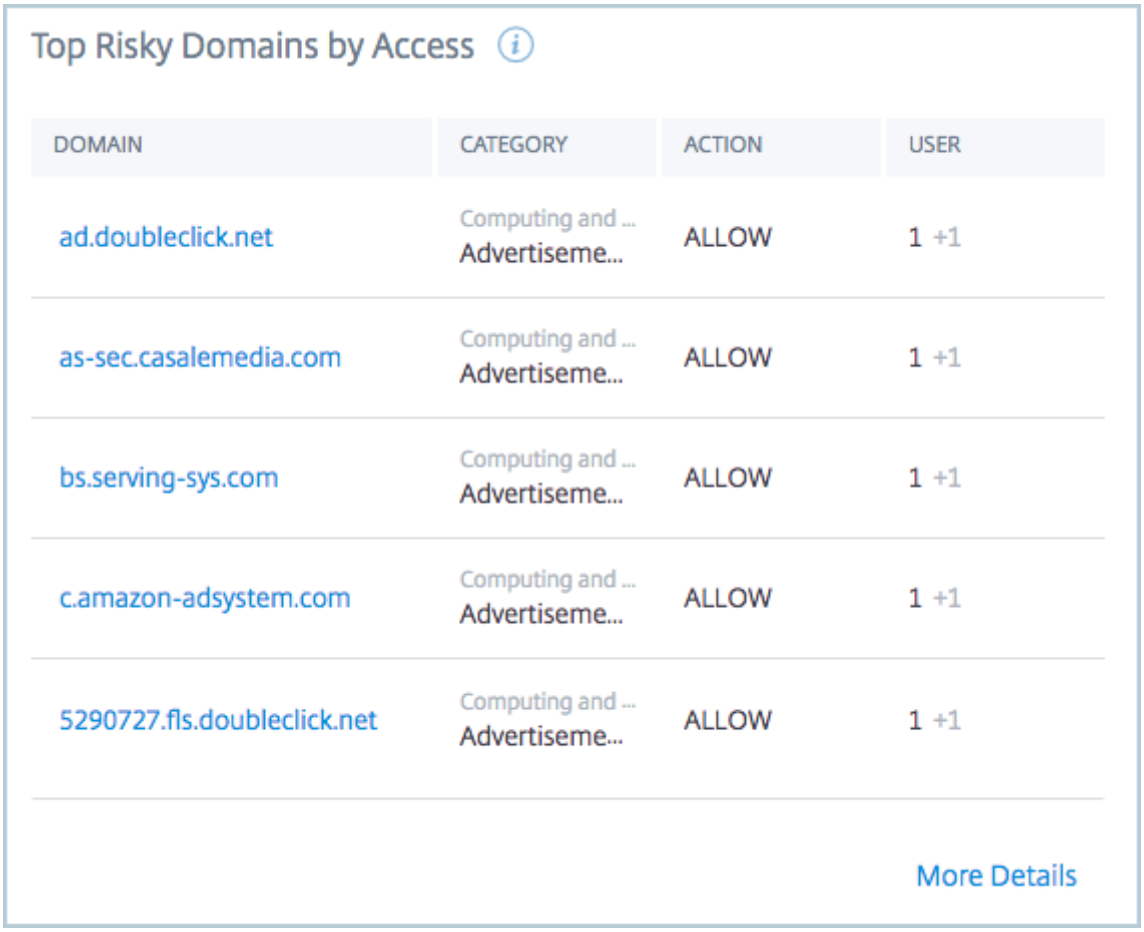
Pour la période sélectionnée, dans la section **App Access Summary**, le tableau debord fournit un aperçu des domaines malveillants, des domaines dangereux, des domaines inconnus et des domaines propres auxquels les utilisateurs de votre réseau ont accédé. Il fournit également le volume de données chargées ou téléchargées depuis des domaines potentiellement dangereux.



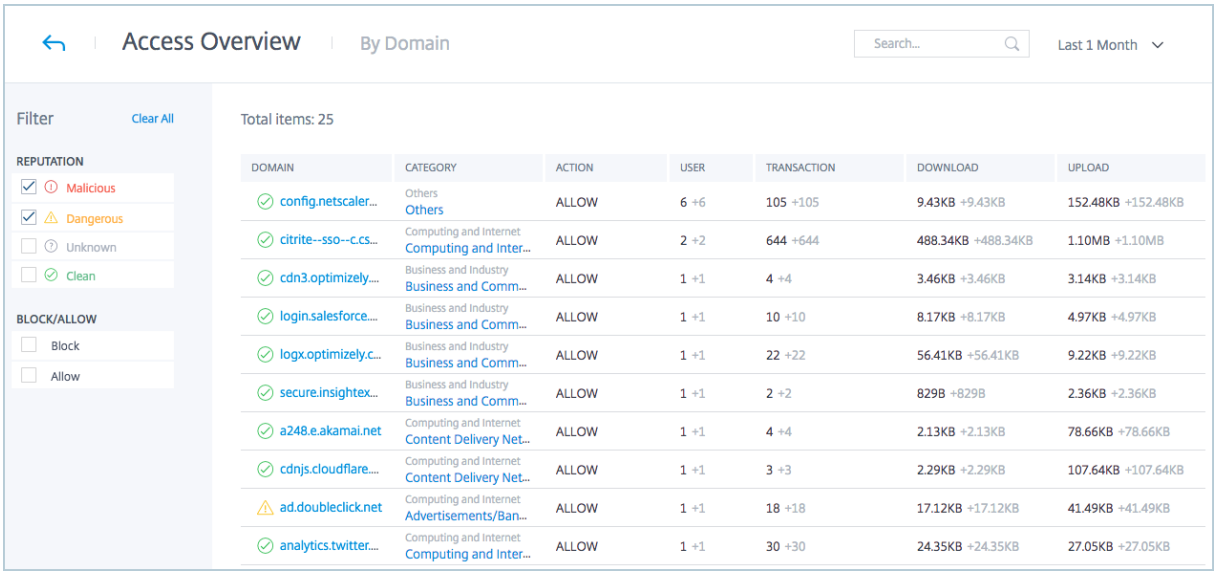
Principaux domaines à risque par accès

La section **Top Risky Domains by Access** fournit des détails sur les domaines malveillants ou dangereux auxquels les utilisateurs de votre réseau ont accédé le plus fréquemment. Elle fournit des détails tels que :

- L'URL du domaine à risque.
- La catégorie dans laquelle le domaine a été classé par Access Control.
- L'action entreprise par le service Contrôle d'accès pour atténuer le risque.
- Le nombre d'utilisateurs ayant accédé à l'URL, avec augmentation de la tendance du nombre d'utilisateurs accédant au domaine à risque pour la période sélectionnée.



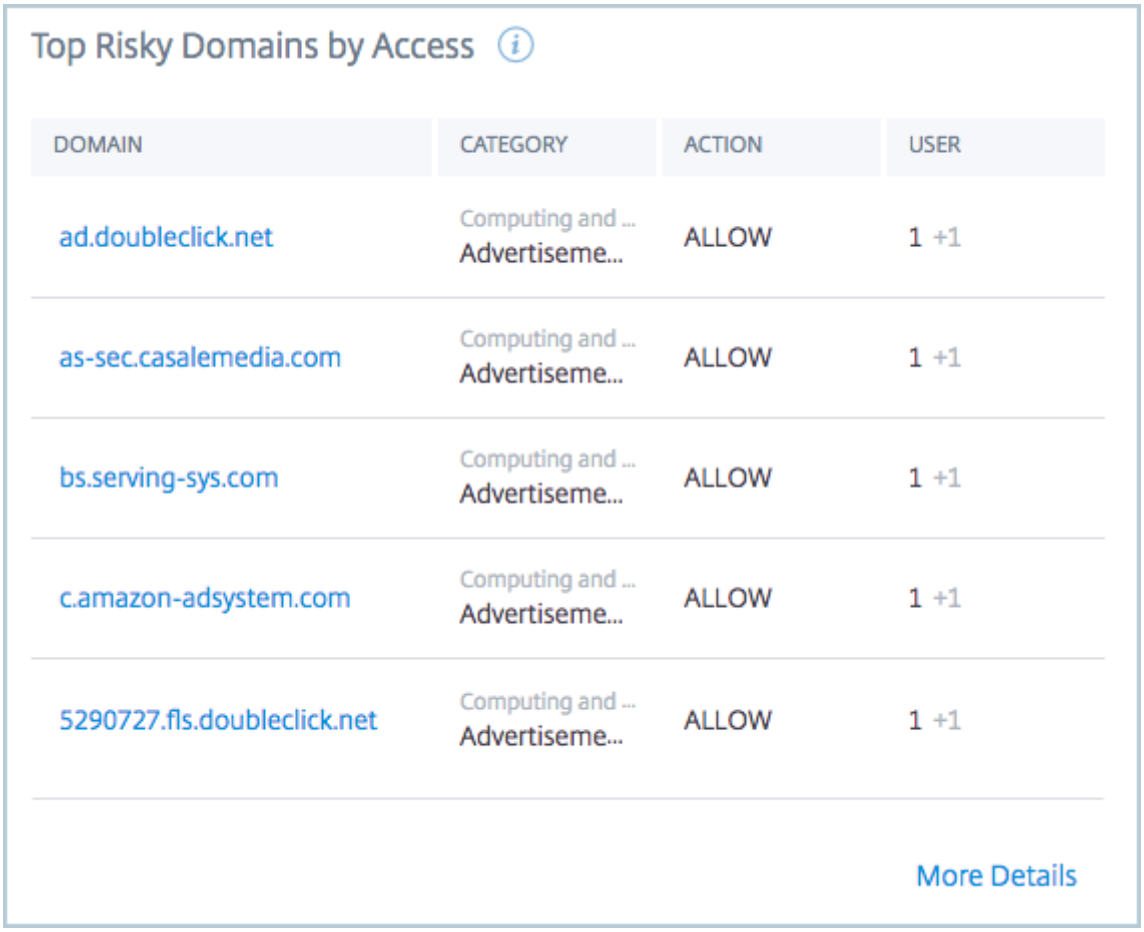
Vous pouvez cliquer sur **More Details** pour afficher la liste complète des domaines malveillants ou dangereux auxquels les utilisateurs de votre réseau ont accédé.



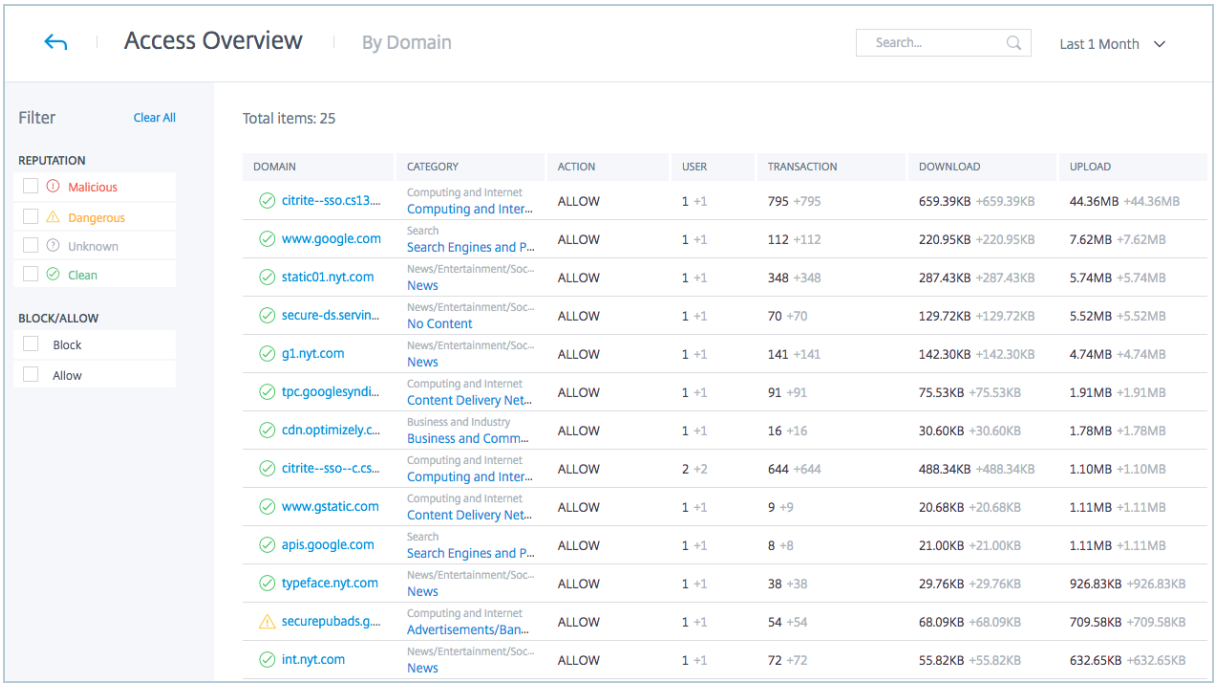
Principaux domaines à risque par volume de données téléchargées

La section **Top Risky Domains by Data Download Volume** fournit des
détails sur les principaux domaines malveillants ou dangereux à partir desquels des données ont été téléchargées
par les utilisateurs. Les détails sont triés par
volume de données du plus élevé au plus bas. Elle fournit des détails tels que :

- L'URL du domaine à risque.
- La catégorie dans laquelle le domaine a été classé par Access Control.
- Le volume de données téléchargées par les utilisateurs du domaine à risque, avec augmentation de la tendance de la quantité de données téléchargées à partir du domaine à risque pour la période sélectionnée.



Vous pouvez cliquer sur **More Details** pour afficher la liste complète des domaines malveillants ou dangereux auxquels les utilisateurs de votre réseau ont accédé.

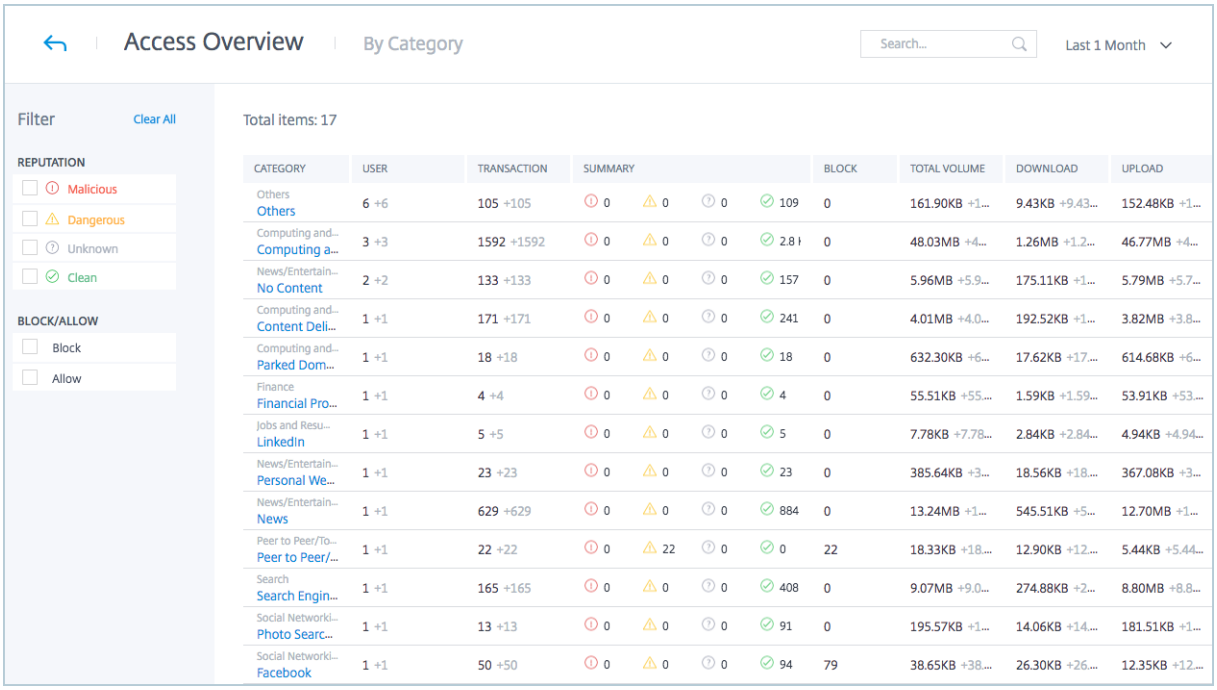


Principales catégories à risque par accès

La section **Top Risky Categories by Access** fournit des détails sur la catégorie des domaines auxquels les utilisateurs de votre réseau ont accédé le plus de fois. Elle fournit des détails tels que :

- La catégorie dans laquelle le domaine a été classé par Access Control.
- Le nombre d'utilisateurs ayant accédé à l'URL, avec augmentation de la tendance du nombre d'utilisateurs accédant au domaine à risque pour la période sélectionnée.
- Le nombre de transactions effectuées par les utilisateurs sur le domaine à risque, avec tendance à la
  hausse du nombre de transactions effectuées par les utilisateurs sur le domaine à risque pour la période sélectionnée.
- Le nombre de transactions bloquées par le service Contrôle d'accès.

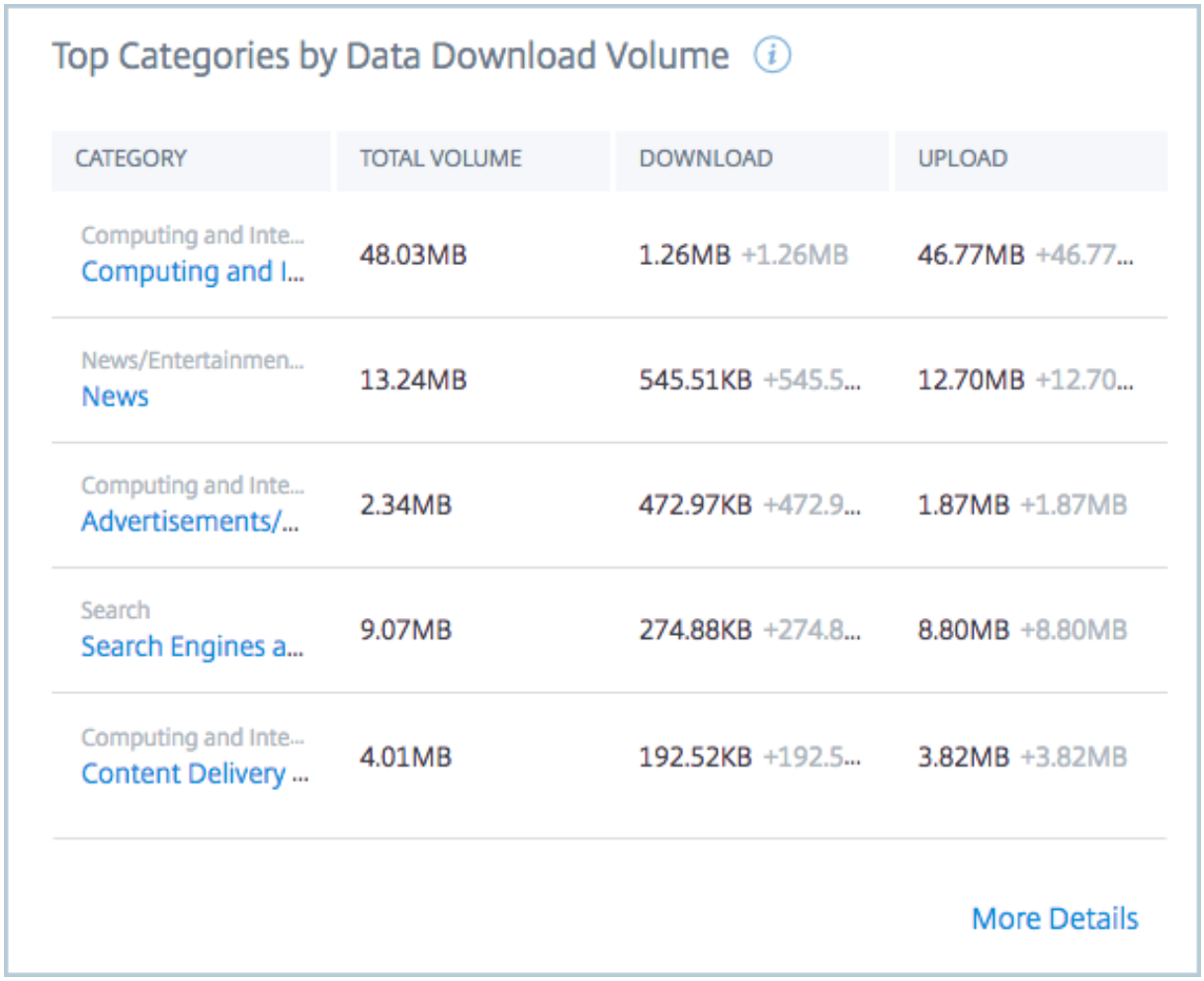
Vous pouvez cliquer sur **More Details** pour afficher la liste complète des domaines malveillants ou dangereux auxquels les utilisateurs de votre réseau ont accédé.



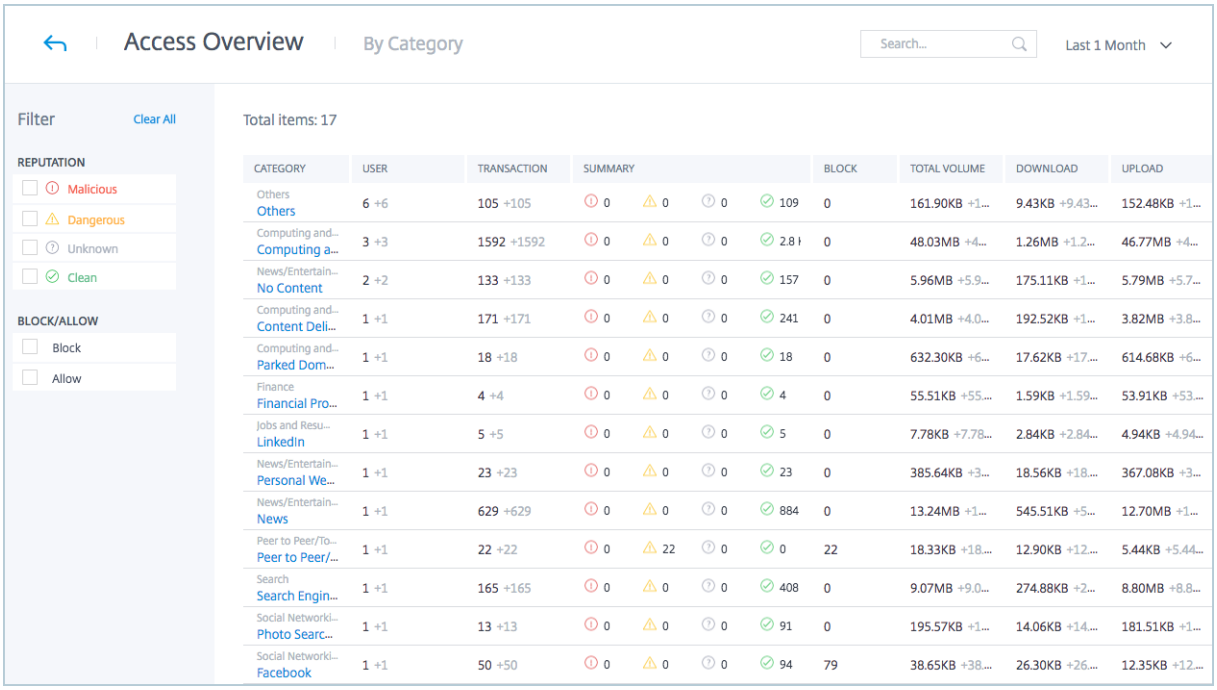
Catégories les plus risquées par volume de données téléchargées

La section **Top Risky Categories by Data Download Volume** fournit des détails sur la catégorie de domaines à partir desquels la plus grande quantité de données a été chargée ou téléchargée par les utilisateurs du réseau. Elle fournit des détails tels que :

- La catégorie dans laquelle le domaine a été classé par Access Control.
- Le volume total des données chargées ou téléchargées depuis le domaine par les utilisateurs de votre réseau.
- Le volume de données téléchargées depuis le domaine par les utilisateurs.
- Le volume de données chargées sur le domaine par les utilisateurs.

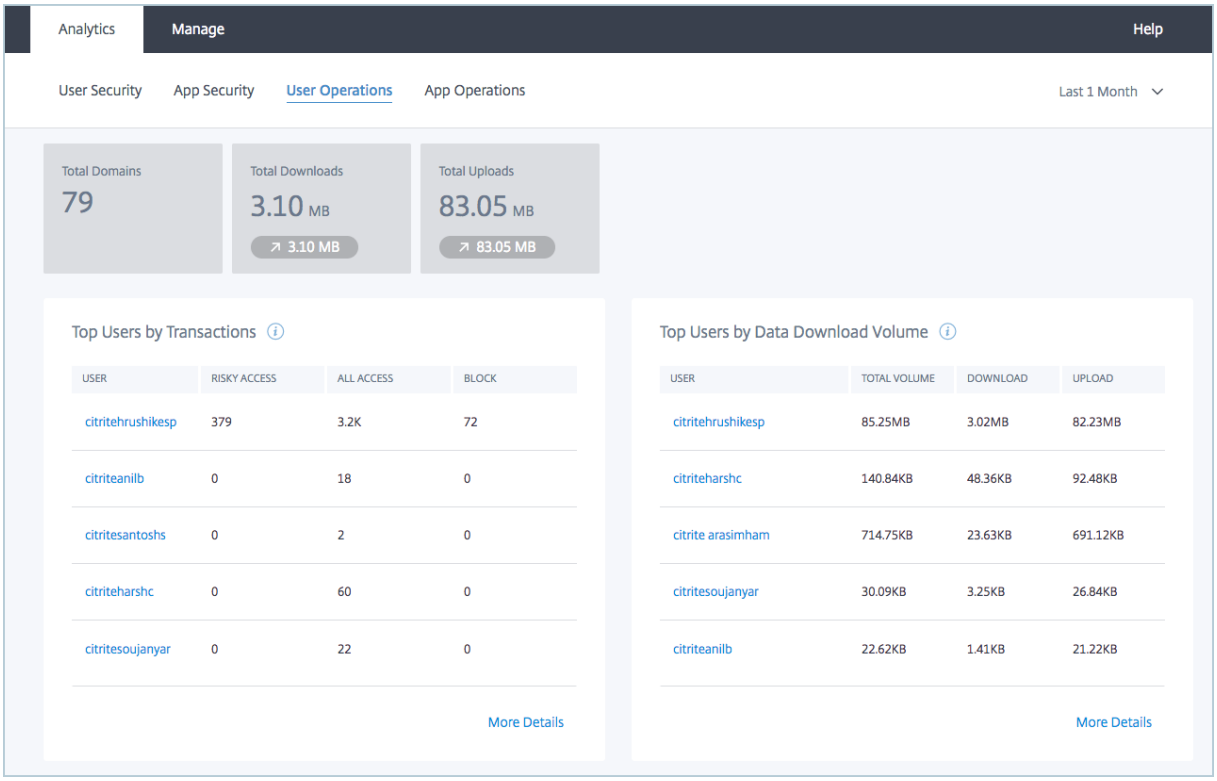


Vous pouvez cliquer sur **More Details** pour afficher la liste complète des données chargées ou téléchargées depuis les domaines par les utilisateurs.



Opérations des utilisateurs

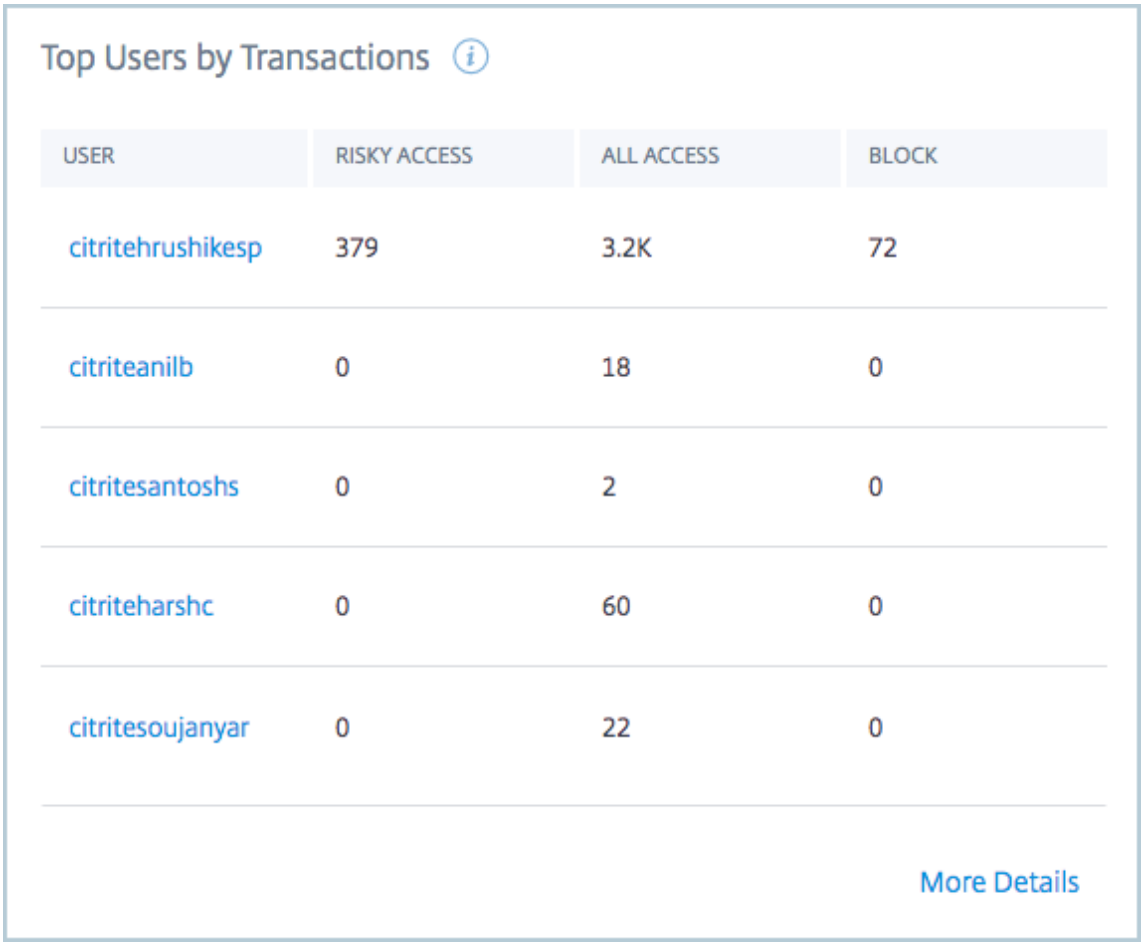
Le tableau de bord **User Operations** fournit un aperçu du nombre total de domaines auxquels les utilisateurs de votre réseau ont accédé. Il fournit également le volume de données chargées ou téléchargées depuis les domaines. Pour accéder au tableau de bord **User Operations**, depuis l'onglet **Analytics**, cliquez sur **User Operations**.



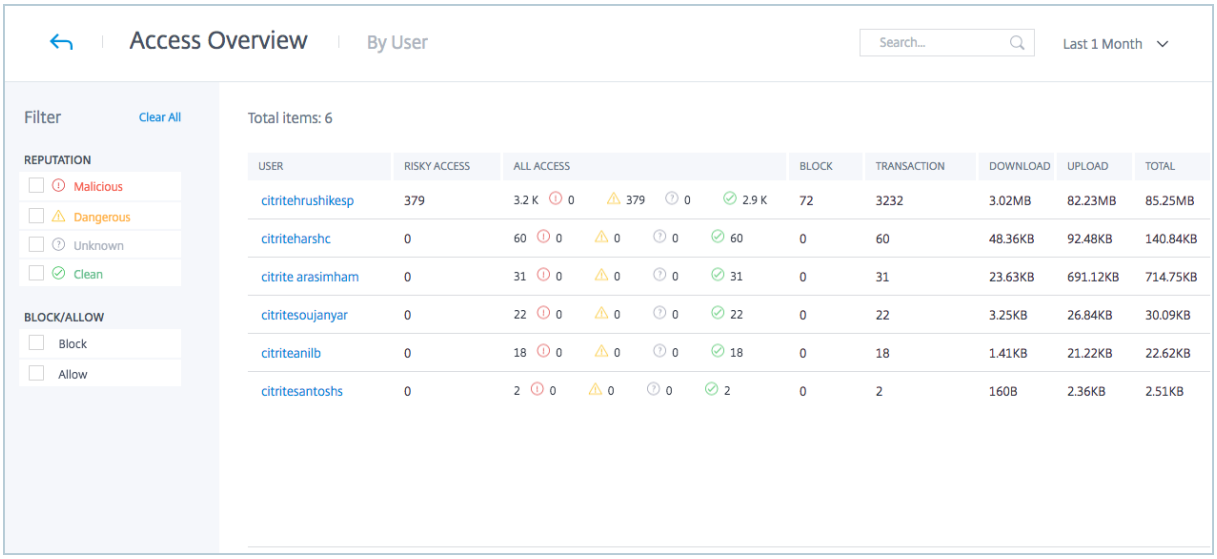
Principaux utilisateurs par transactions

La section **Top Users by Transactions** répertorie les transactions effectuées par un utilisateur lors de l'accès à différentes catégories de domaine et spécifie également le nombre de transactions bloquées pour chaque utilisateur. Elle fournit des détails tels que :

- Le nom de l'utilisateur.
- Le nombre de transactions effectuées par l'utilisateur lors de l'accès à différentes catégories de domaines.
- Le nombre total de domaines auxquels l'utilisateur a accédé.
- Le nombre de transactions bloquées par le service Contrôle d'accès.



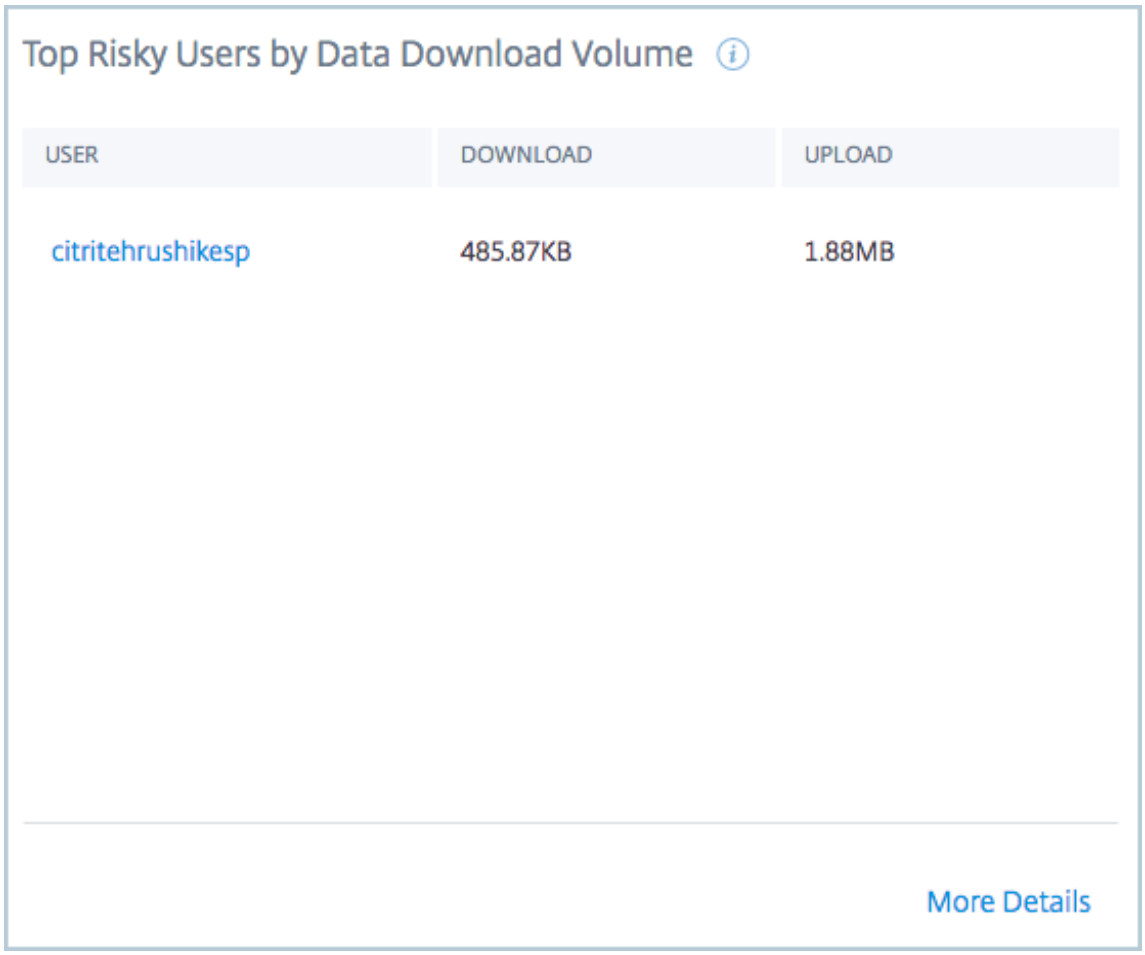
Vous pouvez cliquer sur **More Details** pour afficher des détails complets sur les transactions effectuées par les utilisateurs.



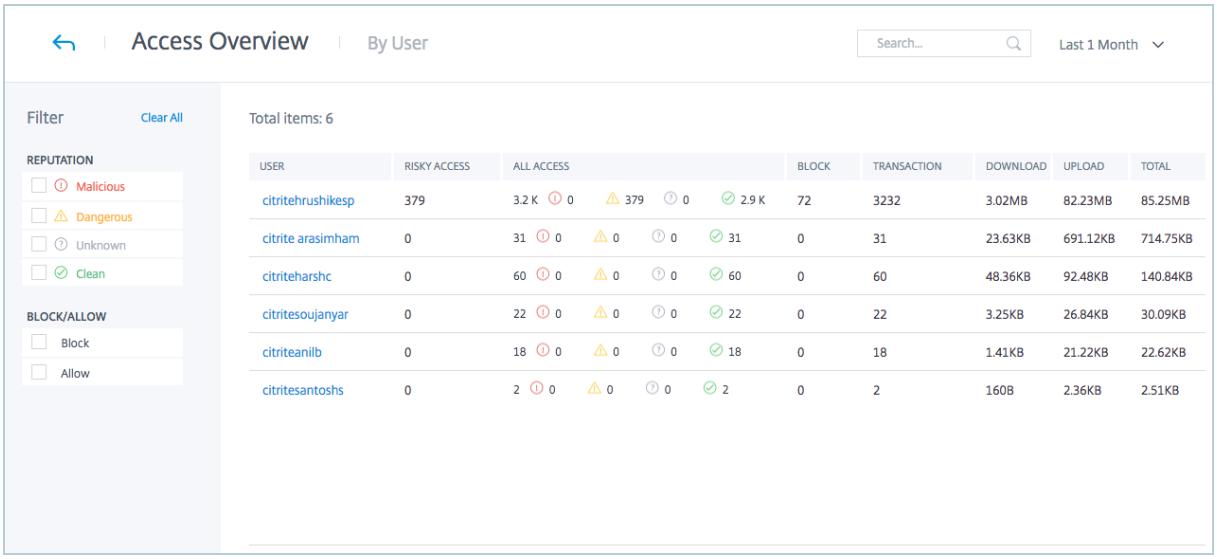
Principaux utilisateurs par volume de données téléchargées

La section **Top Users by Data Download Volume** fournit des informations sur les principaux utilisateurs qui ont chargé ou téléchargé des données depuis les domaines. Elle fournit des détails tels que :

- Le nom de l'utilisateur.
- Le volume total des données chargées ou téléchargées depuis le domaine par l'utilisateur.
- Le volume de données téléchargées depuis le domaine par l'utilisateur.
- Le volume de données chargées sur le domaine par l'utilisateur.

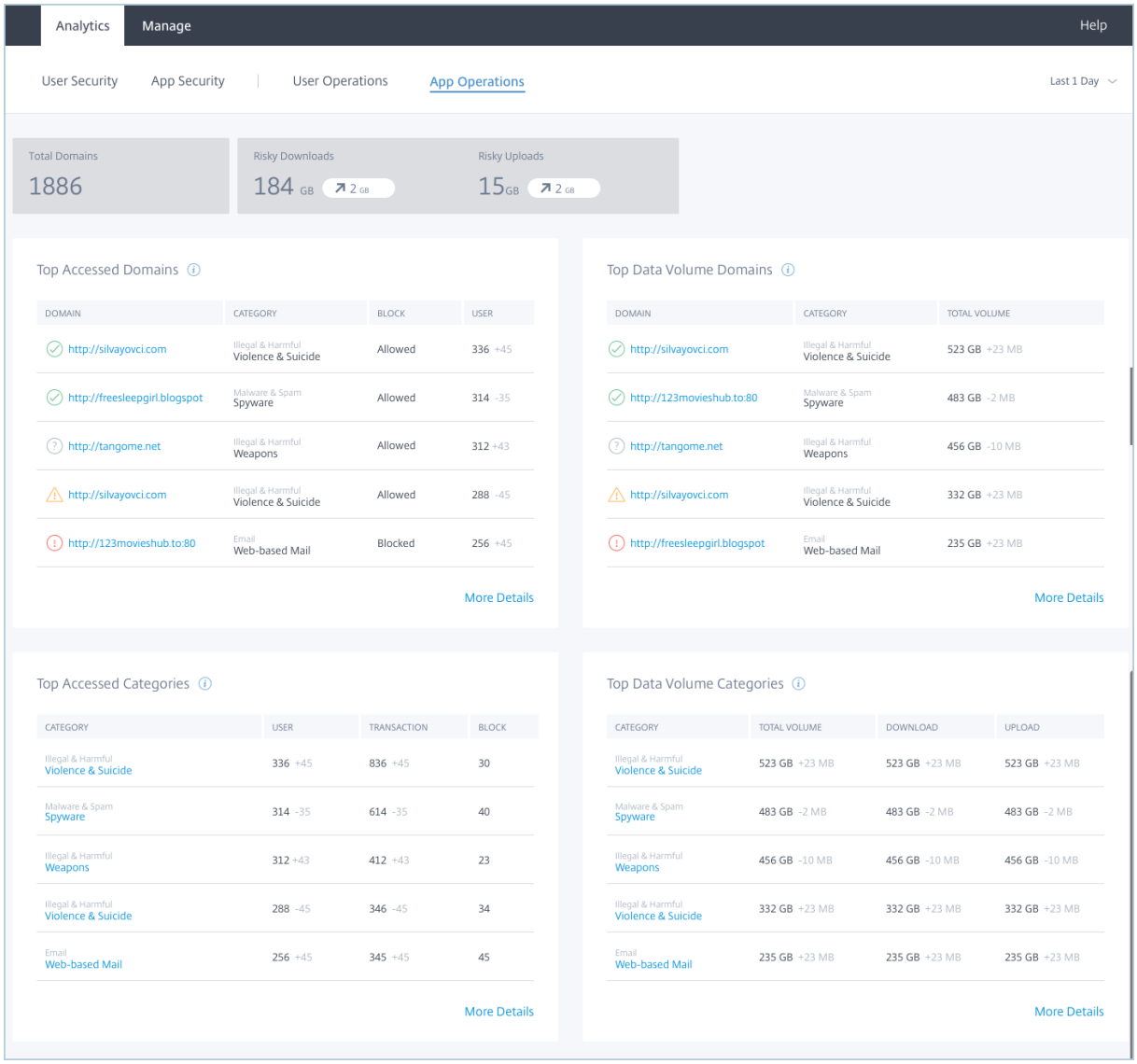


Vous pouvez cliquer sur **More Details** pour afficher des détails complets sur les transactions effectuées par les utilisateurs.

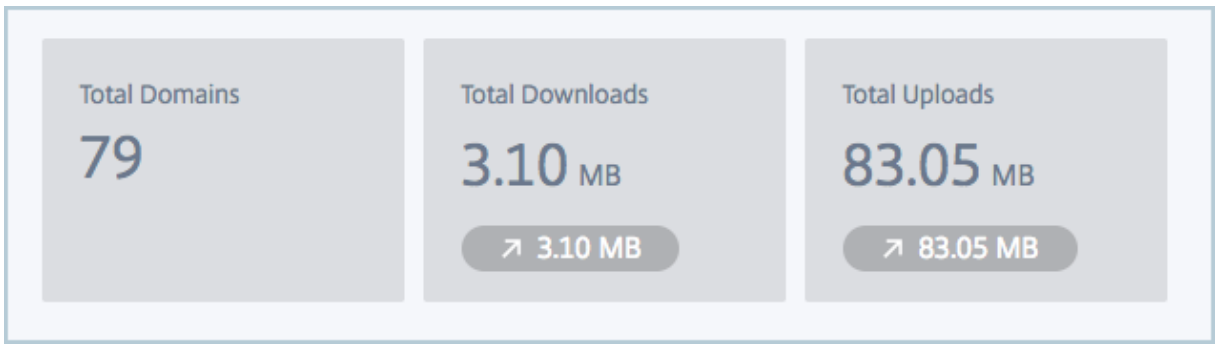


Opérations applicatives

Le tableau de bord **App Operations** fournit un aperçu du nombre total de domaines auxquels les utilisateurs de votre réseau ont accédé. Il fournit également le volume de données chargées ou téléchargées depuis les domaines. Pour accéder au tableau de bord **App Operations**, depuis l'onglet **Analytics**, cliquez sur **App Operations**.



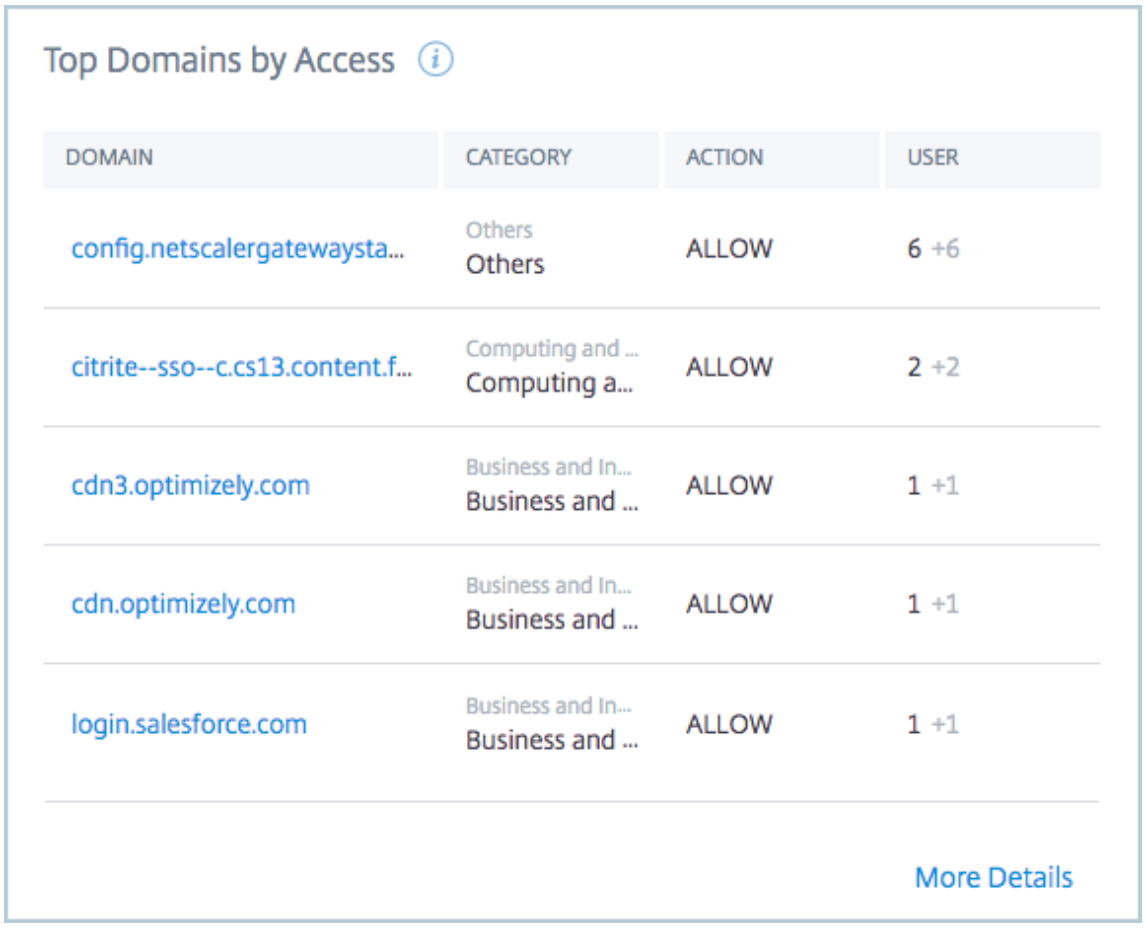
Pour la période sélectionnée, le tableau de bord fournit un aperçu du nombre de domaines auxquels les utilisateurs de votre réseau ont accédé. Il fournit également le volume de données chargées ou téléchargées depuis les domaines.



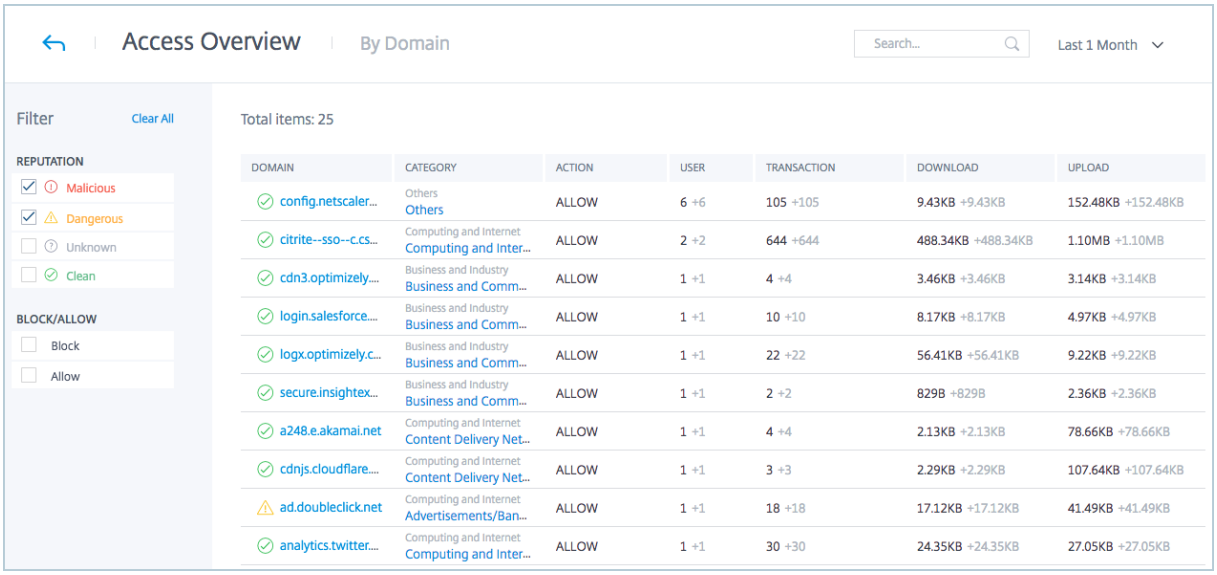
Principaux domaines par accès

La section **Top Domains by Access** fournit des détails sur les
domaines auxquels les utilisateurs de votre réseau ont accédé le plus fréquemment. Elle fournit des détails
tels que :

- L'URL du domaine.
- La catégorie dans laquelle le domaine a été classé par Access Control.
- L'action entreprise par le service Contrôle d'accès pour atténuer le risque.
- Le nombre d'utilisateurs ayant accédé à l'URL, avec la tendance à la hausse du nombre d'utilisateurs accédant au domaine pour la période sélectionnée.



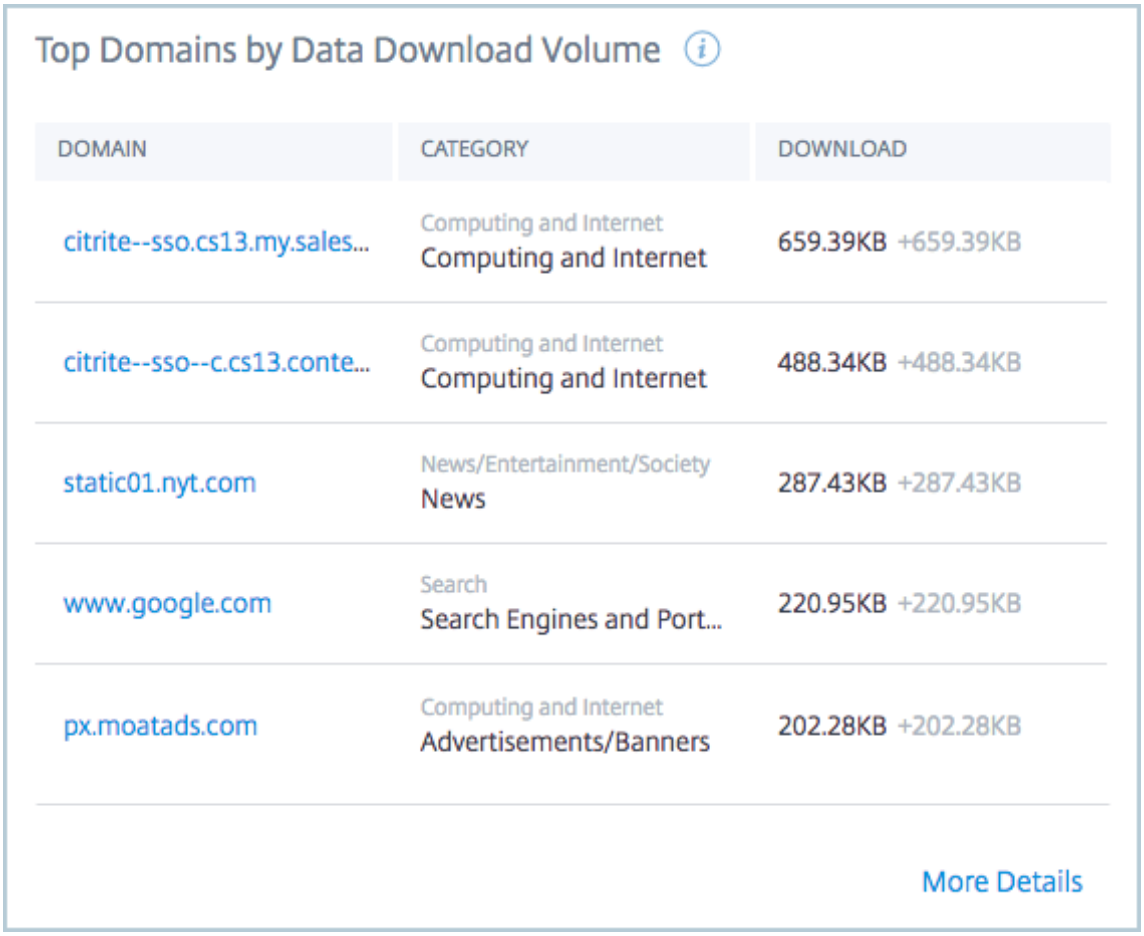
Vous pouvez cliquer sur **More Details** pour afficher la liste complète des domaines auxquels les utilisateurs de votre réseau ont accédé.



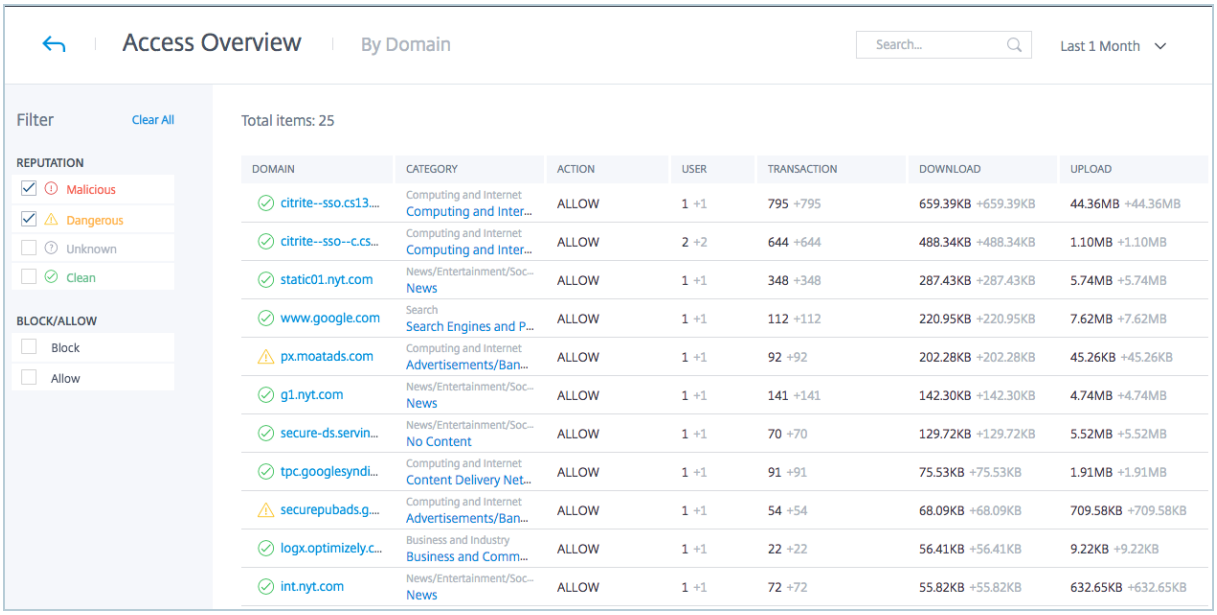
Principaux domaines par volume de données téléchargées

La section **Top Domains by Data Download Volume** fournit des détails sur les principaux domaines à partir desquels des données ont été téléchargées par les utilisateurs.
Les détails sont triés par volume de données du plus élevé au plus bas. Elle fournit des détails tels que :

- L'URL du domaine.
- La catégorie dans laquelle le domaine a été classé par Access Control.
- Le volume de données téléchargées par les utilisateurs du domaine, avec augmentation de la tendance de la quantité de données téléchargées à partir du domaine pour la période sélectionnée.



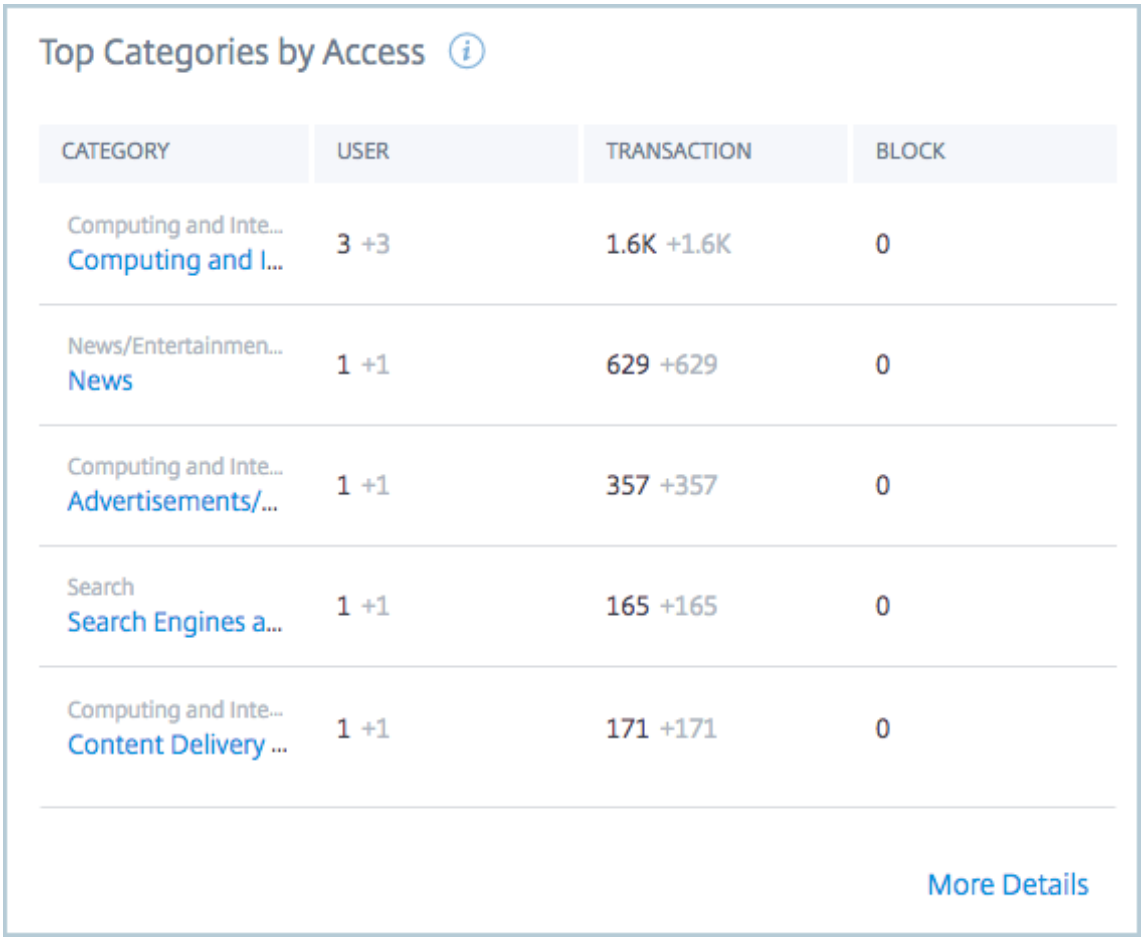
Vous pouvez cliquer sur **More Details** pour afficher la liste complète des domaines auxquels les utilisateurs de votre réseau ont accédé.



Principales catégories par accès

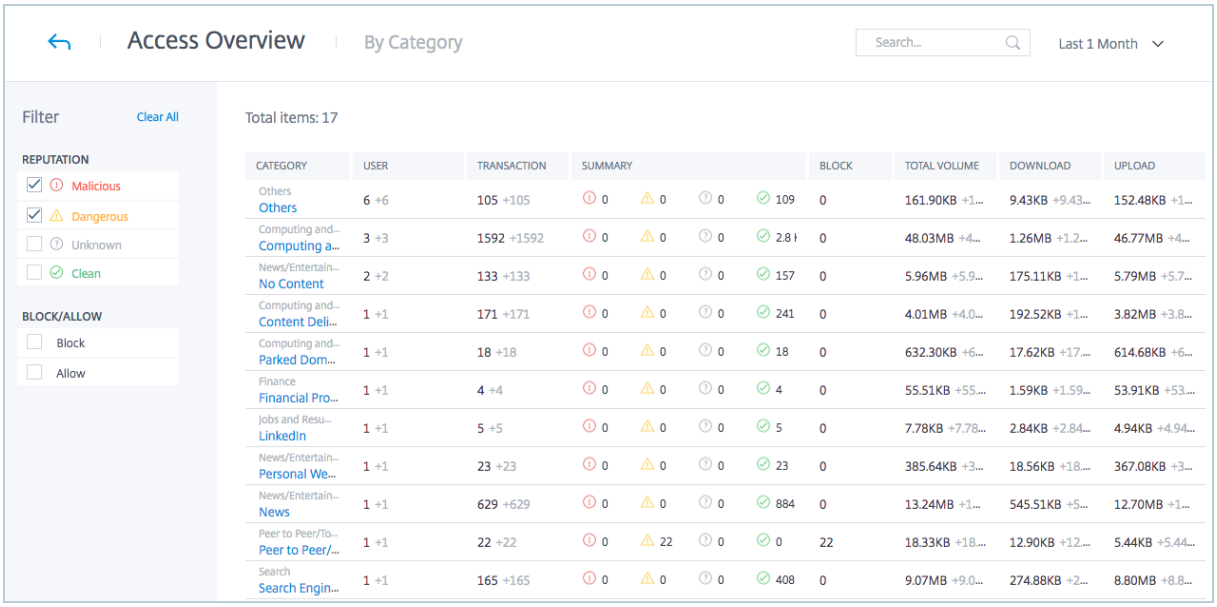
La section **Top Categories by Access** fournit des détails sur la catégorie des domaines auxquels les utilisateurs de votre réseau ont accédé le plus de fois. Elle fournit des détails tels que :

- La catégorie dans laquelle le domaine a été classé par Access Control.
- Le nombre d'utilisateurs ayant accédé à l'URL, avec la tendance à la hausse du nombre d'utilisateurs accédant au domaine pour la période sélectionnée.
- Le nombre de transactions effectuées par les utilisateurs sur le domaine à risque, avec tendance à la hausse du nombre de transactions effectuées par les utilisateurs sur le domaine pour la période sélectionnée.
- Le nombre de transactions bloquées par le service Contrôle d'accès.



Vous pouvez cliquer sur **More Details** pour afficher la liste complète des domaines

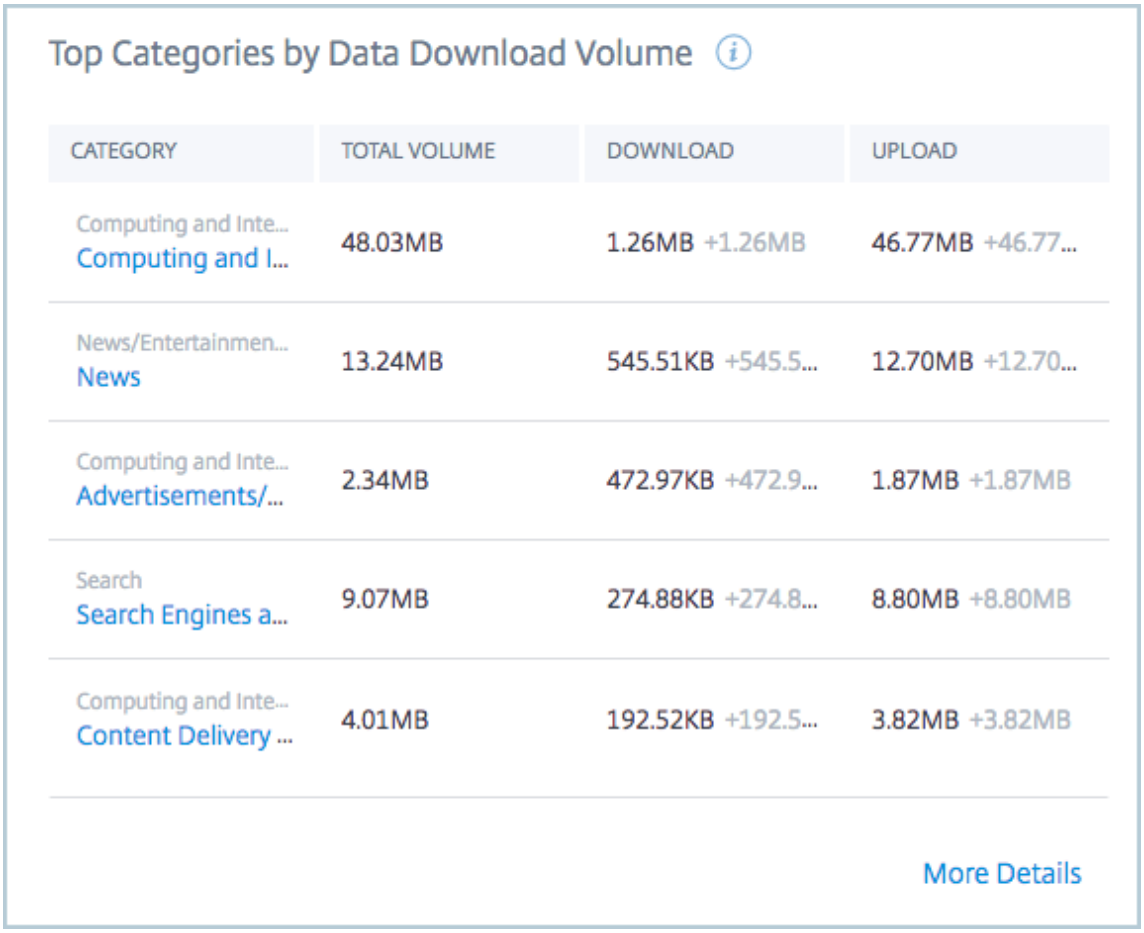
auxquels les utilisateurs de votre réseau ont accédé.



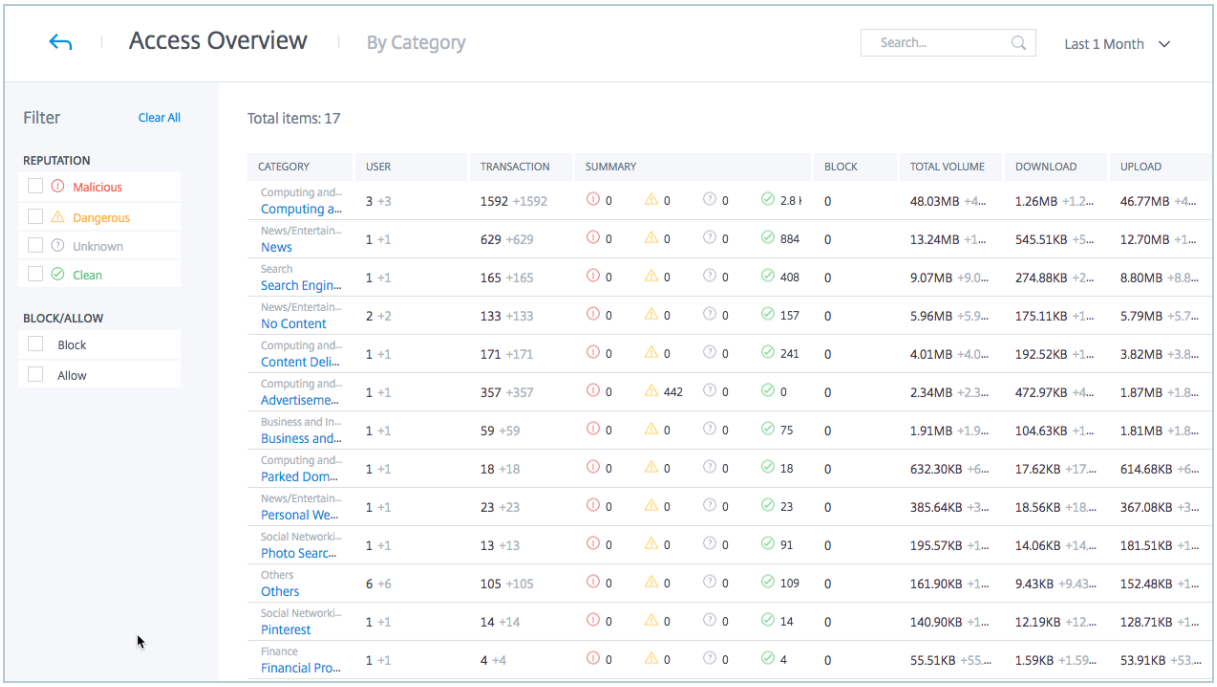
Principales catégories par volume de données téléchargées

La section **Top Risky Categories by Data Download Volume** fournit des détails sur la catégorie de domaines à partir desquels la plus grande quantité de données a été chargée ou téléchargée par les utilisateurs du réseau. Elle fournit des détails tels que :

- La catégorie dans laquelle le domaine a été classé par Access Control.
- Le volume total des données chargées ou téléchargées depuis le domaine par les utilisateurs de votre réseau.
- Le volume de données téléchargées depuis le domaine par les utilisateurs.
- Le volume de données chargées sur le domaine par les utilisateurs.



Vous pouvez cliquer sur **More Details** pour afficher la liste complète des données chargées ou téléchargées depuis les domaines par les utilisateurs.



Content Collaboration

November 7, 2018

Content Collaboration vous permet de synchroniser, partager et sécuriser le contenu du cloud et de vos services de stockage locaux.

Pour plus d'informations sur la création de comptes Content Collaboration dans Citrix Cloud, consultez Créer ou associer un compte Content Collaboration (ShareFile) à Citrix Cloud.

Pour plus d'informations sur les tâches de configuration, consultez Configurer ShareFile.

Pour plus d'informations sur le déploiement de Content Collaboration et l'utilisation de Citrix Files dans Citrix Workspace, consultez Citrix Content Collaboration.

Accord de niveau de service

Content Collaboration a été développé à l'aide des meilleures pratiques de l'industrie afin de garantir la scalabilité du cloud 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.

Créer ou associer un compte Content Collaboration (ShareFile) à Citrix Cloud

November 7, 2018

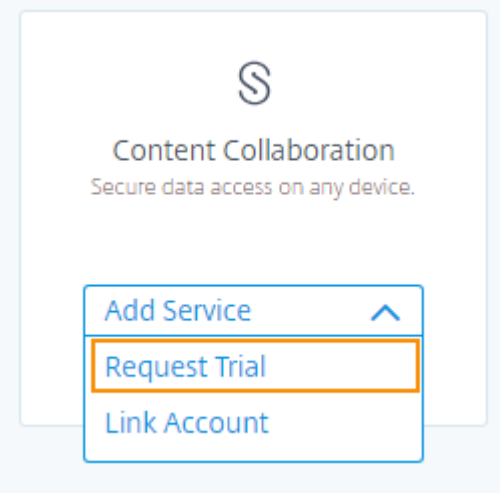
Pour commencer avec Content Collaboration, vous pouvez tirer parti des options suivantes :

- Si vous n'avez jamais utilisé Content Collaboration et que vous souhaitez l'essayer, vous pouvez demander une version évaluation.
- Si vous possédez déjà un compte ShareFile mais que vous n'avez pas acheté de nouveaux droits, vous pouvez connecter votre compte à Citrix Cloud.
- Si vous avez acheté des droits pour ShareFile ou Workspace, vous pouvez créer un nouveau compte dans Citrix Cloud et attribuer vos droits à ce compte.
- Si vous avez acheté des droits à ShareFile ou à Workspace, vous pouvez connecter votre compte ShareFile existant à Citrix Cloud pour attribuer vos nouveaux droits.

Demander une version d'évaluation

Suivez les étapes suivantes si vous ne possédez pas de compte Content Collaboration et que vous souhaitez essayer le service.

1. Connectez-vous à Citrix Cloud avec vos informations d'identification My Citrix
2. Dans la console Citrix Cloud, sous **Services disponibles**, localisez la vignette **Content Collaboration**.
3. Dans **Ajouter un service**, sélectionnez **Demander évaluation**.



   La page Ajouter compte Content Collaboration apparaît avec l'onglet Demander évaluation sélectionné.
4. Dans la section **Emplacement géographique**, sélectionnez la région du service que vous souhaitez utiliser et confirmez que la région ne peut pas être modifiée après avoir demandé

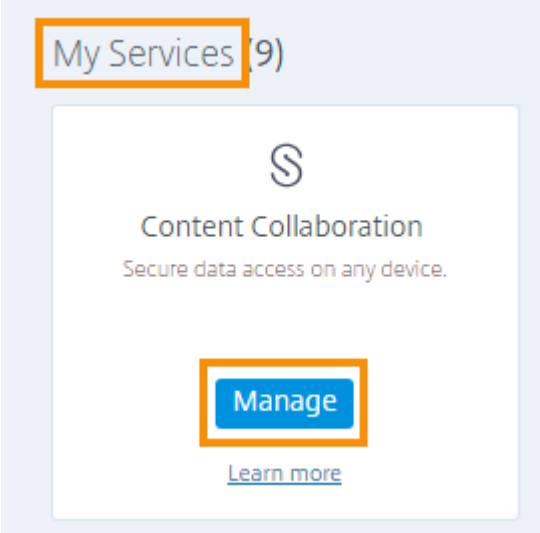
l'évaluation.

5. Dans la section **Sélectionner un sous-domaine**, entrez le sous-domaine unique que vous souhaitez utiliser.
6. Cliquez sur **Demander version d'évaluation**. Citrix Cloud vous envoie un courrier électronique après la création de votre compte Content Collaboration.
7. Sous **Mes services**, cliquez sur **Gérer** dans la vignette Content Collaboration pour passer à la vue d'ensemble de l'administration de Content Collaboration.

Créer un nouveau compte Content Collaboration et attribuer des droits

Procédez comme suit si vous avez acheté des droits d'accès à Content Collaboration et souhaitez créer un nouveau compte et attribuer les droits à ce compte.

1. Connectez-vous à Citrix Cloud avec vos informations d'identification Citrix Cloud.
2. Dans la console Citrix Cloud, sous **Mes services**, localisez la vignette Content Collaboration et cliquez sur **Gérer**.



   La page Attribuer droits de Content Collaboration affiche tous les nouveaux droits liés à Content Collaboration achetés sous votre OrgID Citrix.
3. Cliquez sur **Créer un nouveau compte et attribuer**.
4. Sur la page **Configurer Content Collaboration**, choisissez la région du service, entrez un sous-domaine unique, puis cliquez sur **Créer compte**.

Associer un compte ShareFile existant

Pour associer un compte ShareFile existant à votre compte Citrix Cloud, les conditions suivantes doivent être remplies :

- Vous devez disposer d'autorisations d'administrateur dans Citrix Cloud et ShareFile.

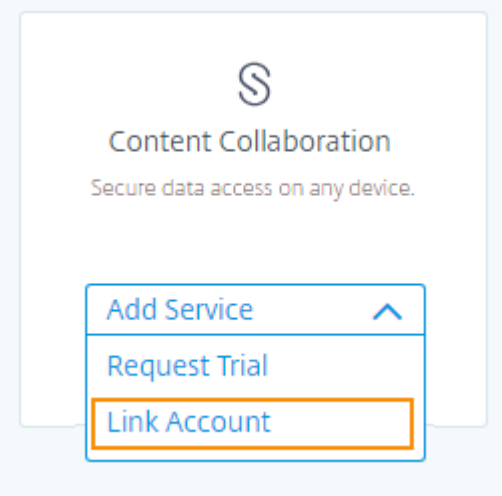
- L'adresse e-mail que vous utilisez pour vous connecter à Citrix Cloud doit correspondre à l'adresse e-mail enregistrée pour ShareFile.

Si l'une de ces conditions n'est pas remplie, Citrix Cloud pourrait ne pas être en mesure de localiser votre compte ShareFile à des fins d'attribution. Si vous avez besoin d'aide avec ces exigences, contactez le support Citrix.

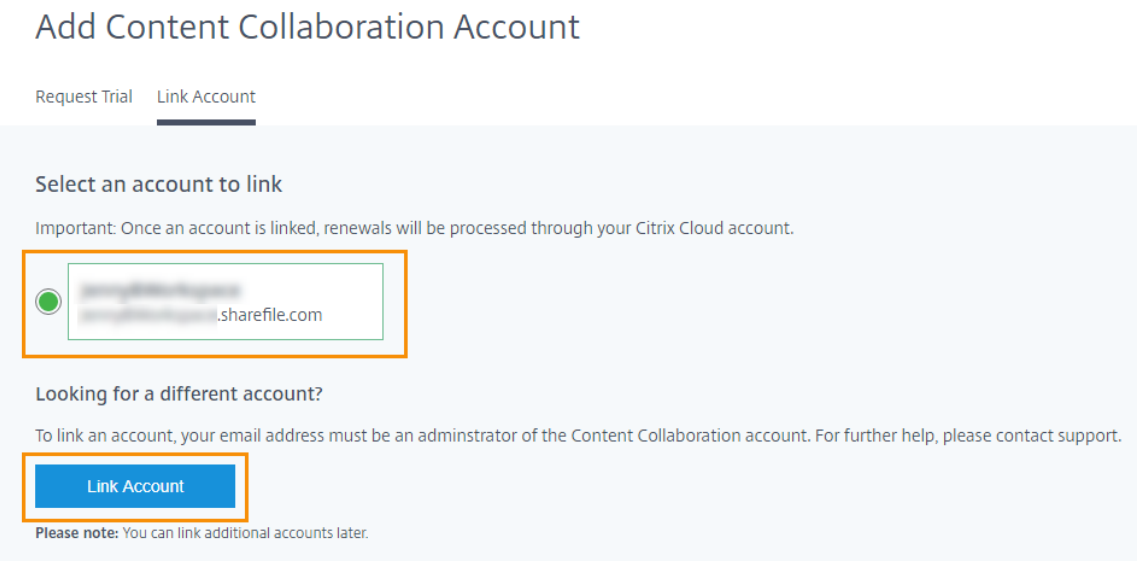
Pour associer votre compte Content Collaboration à Citrix Cloud (pas de nouveaux droits)

Suivez les étapes suivantes si vous n'avez pas acheté de nouveaux droits et souhaitez associer votre compte ShareFile existant à Citrix Cloud.

1. Connectez-vous à Citrix Cloud avec vos informations d'identification My Citrix.
2. Dans la console Citrix Cloud, sous **Services disponibles**, localisez la vignette Content Collaboration.
3. Dans **Ajouter un service**, sélectionnez **Lier compte**. La page Ajouter compte Content Collaboration apparaît avec l'onglet Associer compte sélectionné.



4. Sélectionnez le compte ShareFile que vous souhaitez associer, puis cliquez sur **Associer compte**.

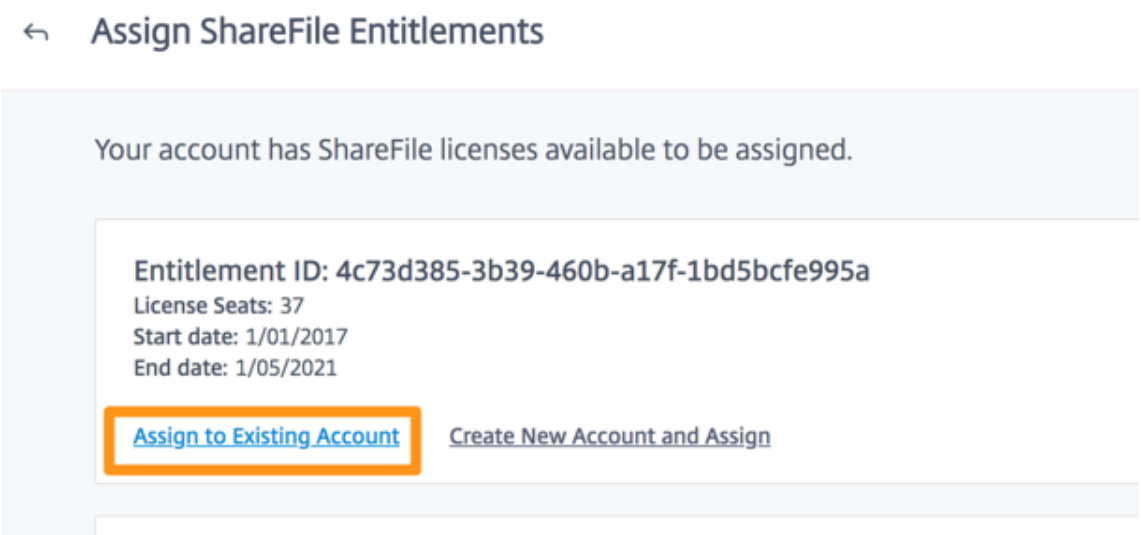


> **Important :** Si aucun compte ne s'affiche, vérifiez que vous êtes administrateur pour ShareFile et que l'adresse e-mail de Citrix Cloud correspond à celle de Content Collaboration. Pour obtenir une assistance supplémentaire, contactez le support Citrix.

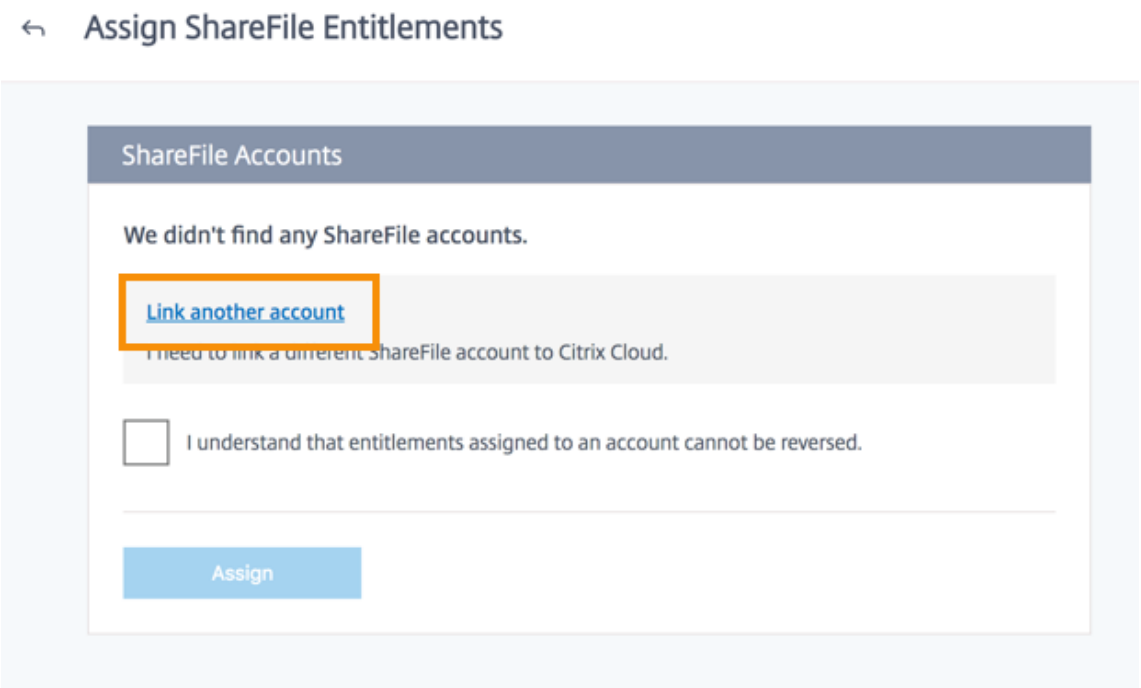
Pour associer votre compte ShareFile et attribuer des droits

Suivez les étapes suivantes si vous avez acheté de nouveaux droits pour ShareFile ou Workspace pour attribuer et gérer vos droits dans Citrix Cloud.

1. Connectez-vous à Citrix Cloud avec vos informations d'identification My Citrix.
2. Dans la console Citrix Cloud, sous **Mes services**, localisez la vignette Content Collaboration et cliquez sur **Gérer**. La page Attribuer droits de Content Collaboration affiche les nouveaux droits que vous avez achetés.
3. Cliquez sur **Attribuer à un compte existant**. La page Comptes ShareFile s'affiche.

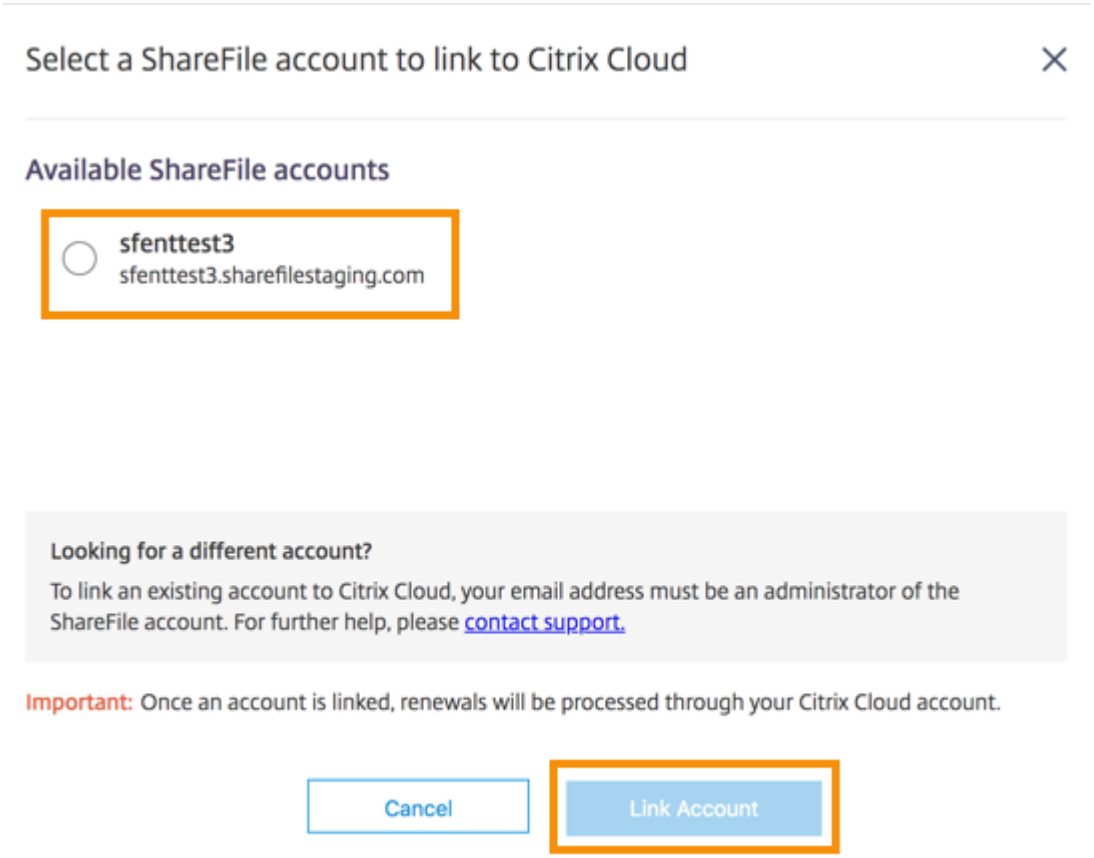


4. Pour associer un compte qui ne s'est jamais connecté à Citrix Cloud, cliquez sur **Associer un autre compte**.



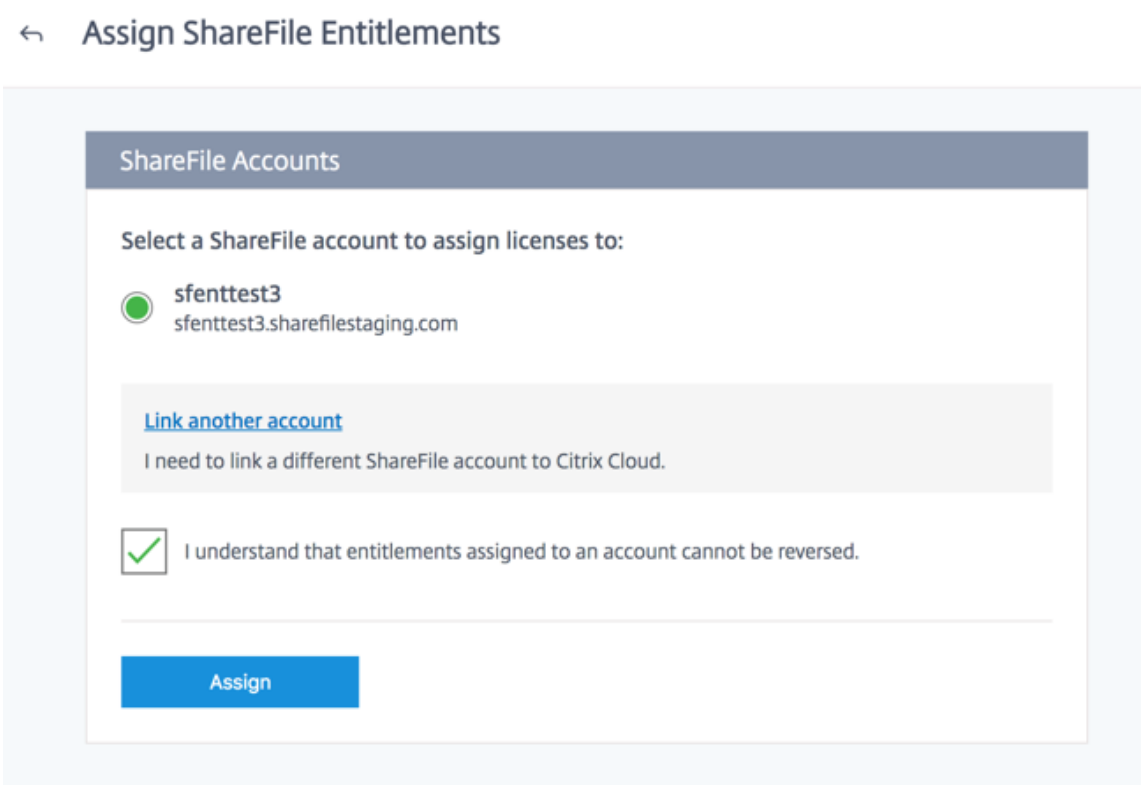
Citrix Cloud affiche les comptes disponibles que vous pouvez associer.

5. Sélectionnez le compte ShareFile que vous souhaitez associer, puis cliquez sur **Associer compte**.

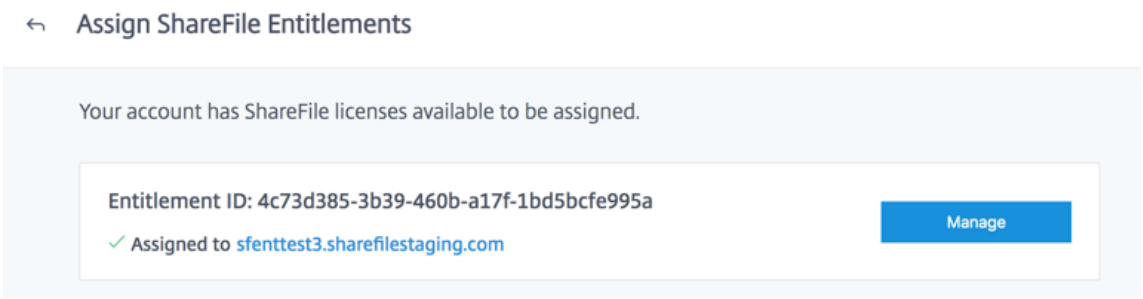


> **Important :** Si aucun compte ne s'affiche, vérifiez que vous êtes administrateur pour Content Collaboration et que l'adresse e-mail de Citrix Cloud correspond à celle de ShareFile. Pour obtenir une assistance supplémentaire, contactez le support Citrix.

6. Sélectionnez **Je comprends que les droits attribués à un compte ne peuvent pas être révoqués**.



7. Cliquez sur **Attribuer**. La page Attribuer droits de Content Collaboration affiche le compte attribué au droit.



8. Cliquez sur **Gérer** pour continuer vers la vue d'ensemble de l'administration de Content Collaboration.

Configurer ShareFile

November 7, 2018

Après avoir créé ou associé votre compte ShareFile, effectuez les tâches suivantes :

1. Provisionner des administrateurs.
2. Provisionner des utilisateurs.

3. Importer des utilisateurs Active Directory dans ShareFile.
4. Configurer l'authentification.

Provisionner des administrateurs

La première chose que vous devez faire est de provisionner des administrateurs. Lors de la création de votre compte, ce dernier a été configuré avec un compte d'administrateur principal. Il s'agit du premier administrateur ajouté à votre compte Citrix Cloud. Vous pouvez provisionner d'autres administrateurs en plus de cet administrateur. Tout administrateur supplémentaire provisionné dans Citrix Cloud sera ajouté à ShareFile avec un accès administrateur.

Provisionner des utilisateurs

Pour commencer à utiliser votre nouveau compte ShareFile, vous devez ajouter des utilisateurs et configurer l'authentification. Vous devez activer l'authentification unique (SSO) entre les différents composants dans l'environnement Citrix Cloud. Afin de fournir une expérience transparente pour vos utilisateurs, vous devez utiliser SAML pour les authentifier auprès de vos comptes utilisateur Active Directory.

Importation d'utilisateurs Active Directory dans ShareFile

L'outil ShareFile User Management Tool (UMT) facilite l'ajout de vos utilisateurs Active Directory dans ShareFile. Vous pouvez utiliser l'outil pour provisionner des comptes utilisateur et créer des groupes de distribution depuis Active Directory (AD).

L'importation d'utilisateurs à partir d'Active Directory peut prendre un certain temps et nécessiter beaucoup de ressources. Pour vous aider, vous pouvez programmer l'outil pour s'exécuter à des heures spécifiques. En plus de l'importation initiale, vous pouvez également utiliser l'outil pour maintenir vos utilisateurs ShareFile synchronisés avec vos utilisateurs AD.

Pour plus d'informations sur l'outil UMT, consultez la section User Management Tool pour l'administration basée sur des stratégies.

Configuration de l'authentification

Après avoir importé vos utilisateurs dans ShareFile, vous devez configurer l'authentification. Lors de l'utilisation de l'environnement Citrix Cloud, vous devez utiliser l'authentification unique (SSO). L'authentification unique est effectuée à l'aide du protocole SAML. Dans cet environnement, vous avez deux options pour configurer SAML : ADFS ou l'autorisation SAML Endpoint Management.

Configuration de l'authentification avec ADFS

Vous pouvez intégrer votre compte ShareFile avec Active Directory (AD) pour activer le Single Sign-On pour les utilisateurs avec des informations d'identification Active Directory. ShareFile prend en charge SAML (Security Assertion Markup Language) pour le Single Sign-On. Vous configurez ShareFile de façon à communiquer avec un outil de fédération SAML exécuté dans votre réseau. Les demandes d'ouverture de session sont ensuite redirigées vers Active Directory. Vous pouvez utiliser le même fournisseur d'identité SAML que celui que vous utilisez pour d'autres applications Web. Pour plus d'informations veuillez consulter Single Sign-On ShareFile.

Configuration de l'authentification à votre Active Directory avec Endpoint Management

Vous pouvez configurer Endpoint Management et Citrix Gateway afin de fonctionner en tant que fournisseur d'identité SAML pour ShareFile. Dans cette configuration, un utilisateur qui se connecte à ShareFile à l'aide d'un navigateur Web ou d'autres clients ShareFile est redirigé vers l'environnement Endpoint Management pour authentifier l'utilisateur. Une fois l'authentification par Endpoint Management réussie, l'utilisateur reçoit un jeton SAML valide pour la connexion à son compte ShareFile. Pour de plus amples informations, consultez la section Single Sign-On pour ShareFile avec Citrix Gateway.

Accès à ShareFile

Maintenant que vous avez configuré vos utilisateurs et l'authentification, vous devez réfléchir à la façon d'accéder à ShareFile. Il existe deux types d'accès à prendre en compte : accès administrateur et accès utilisateur.

Accès administrateur

En tant qu'administrateur, vous serez amené à apporter des modifications à votre configuration ShareFile ou à gérer votre compte.

Accès à l'interface administrateur de Content Collaboration via Citrix Cloud

Vous pouvez accéder à l'interface Web de Content Collaboration directement via le Citrix Cloud. L'accès via le Citrix Cloud fournit une version simplifiée de l'interface utilisateur Web de ShareFile. Elle contient tout ce dont vous avez besoin pour configurer l'accès de vos utilisateurs et votre compte.

Pour accéder à l'interface utilisateur d'administration de Content Collaboration à partir de la console Citrix Cloud, sélectionnez **Mes services > Content Collaboration** dans le menu Citrix Cloud.

Accès direct à l'interface administrateur de ShareFile

Certains paramètres d'administrateur ShareFile peuvent être inaccessibles à l'aide de la version Citrix Cloud de la console. Si vous avez besoin de fonctionnalités supplémentaires, vous pouvez accéder à votre compte ShareFile directement via la page de connexion de ShareFile. Vous pouvez accéder à la page de connexion sur `https://YourSubdomain.sharefile.com`.

Remarque : cette méthode n'est pas recommandée pour accéder à l'interface administrateur de ShareFile dans un environnement Citrix Cloud.

Accès utilisateur

Les utilisateurs peuvent accéder à leurs données ShareFile de trois façons. Ils peuvent accéder aux données directement depuis l'interface Web. Les deux autres options dépendent des autres applications que vous avez activées. Si Citrix Virtual Apps and Desktops ou Endpoint Management est activé, les utilisateurs peuvent accéder à leurs données via l'une de ces applications.

Accès à ShareFile via l'interface Web

Les utilisateurs peuvent accéder à ShareFile directement depuis `http://YourSubdomain.sharefile.com`.

Accès à ShareFile avec Citrix Virtual Apps and Desktops

L'accès à ShareFile avec Citrix Virtual Apps and Desktops se fait à l'aide du client ShareFile Sync. Le client ShareFile Sync permet de synchroniser les documents entre un client local et le cloud ShareFile.

Utilisation de ShareFile Sync pour Windows

Sur Citrix Virtual Apps and Desktops, vous utilisez ShareFile Sync pour Windows. ShareFile Sync pour Windows peut être préinstallé dans votre image de bureau avant le déploiement auprès des utilisateurs. Pour plus d'informations sur l'utilisation de ShareFile Sync, consultez la section Guide utilisateur de ShareFile Sync pour Windows.

Vous devez démarrer en installant ShareFile Sync pour Windows dans votre environnement Citrix Virtual Apps and Desktops. Vous pouvez installer le client une fois et le propager à toutes les sessions Citrix Virtual Apps and Desktops de votre environnement. Pour obtenir des instructions d'installation, consultez la section ShareFile Sync pour Windows dans le centre de connaissances Citrix.

Implémentation de ShareFile On-Demand Sync

ShareFile On-Demand Sync est utilisé lorsque vous souhaitez déployer un volume de données le plus petit possible dans votre environnement Virtual Apps and Desktops. Pour plus d'informations sur l'implémentation de ShareFile On-Demand Sync, consultez la section Configuration de ShareFile On-Demand Sync dans le centre de connaissances Citrix.

Accès à ShareFile avec Endpoint Management

Pour plus d'informations sur l'encapsulation de l'application ShareFile et le déploiement de l'authentification unique entre Endpoint Management et ShareFile, consultez Citrix ShareFile pour Endpoint Management.

Accès à ShareFile avec Endpoint Management

Pour plus d'informations sur l'encapsulation de l'application ShareFile et le déploiement de l'authentification unique entre Endpoint Management et ShareFile, voir Citrix ShareFile pour Endpoint Management.

MDX Service

November 7, 2018

Vous pouvez utiliser MDX Service pour préparer des applications mobiles iOS et Android en encapsulant les applications avec MDX, une technologie de conteneur d'applications. Vous gérez ensuite les applications avec Citrix Endpoint Management. Vous pouvez utiliser MDX Service pour encapsuler les applications créées dans votre organisation.

MDX Service peut utiliser MDX version 10.8.35 ou 10.8.60 pour encapsuler des applications.

Pour plus d'informations sur MDX, le processus d'encapsulation MDX traditionnel à l'aide du MDX Toolkit et une description des ressources de signature requises, consultez :

- À propos du MDX Toolkit
- Encapsulation des applications mobiles iOS
- Encapsulation d'applications mobiles Android

Stratégie de rétention des données

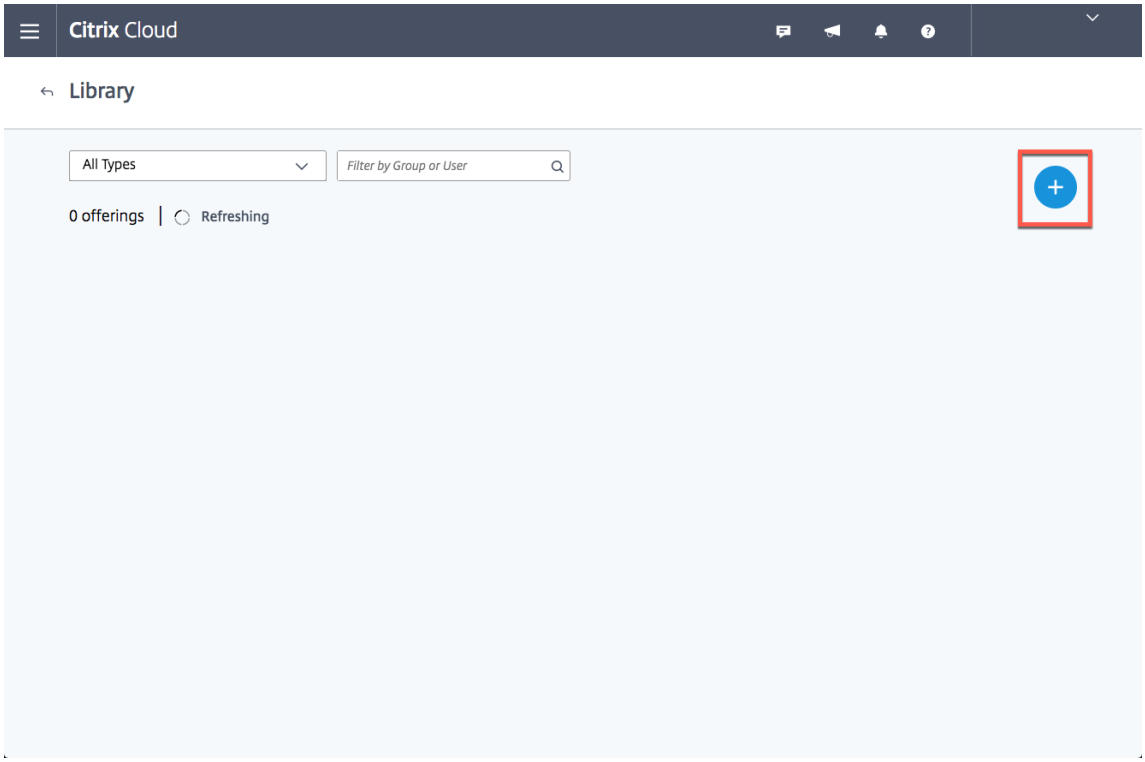
La stratégie de rétention des données pour MDX Service est la suivante :

- **Binaires d'application (fichiers IPA et APK) :** 90 jours.
- **Application encapsulée (fichiers MDX) :** 90 jours (disponible pour les téléchargements).
- **Fichiers de certificat et de keystore :** supprimés immédiatement après l'encapsulation.
- **Profil de provisioning mobile iOS :** supprimé immédiatement après l'encapsulation.

Prise en main du MDX Service

Suivez ces étapes pour commencer à utiliser MDX Service. Pour fournir des commentaires sur votre expérience, utilisez votre ID Citrix pour rejoindre le forum de discussion sur MDX Service.

1. Inscrivez-vous à Citrix Cloud en demandant une version d'évaluation si vous ne disposez pas déjà d'un compte Citrix Cloud. Pour de plus amples informations sur l'inscription, consultez la section Inscription à Citrix Cloud.
2. En haut à droite de cette page se trouve un cercle bleu avec un plus (+). Survolez cette icône avec la souris et cliquez sur **Encapsuler une application mobile**

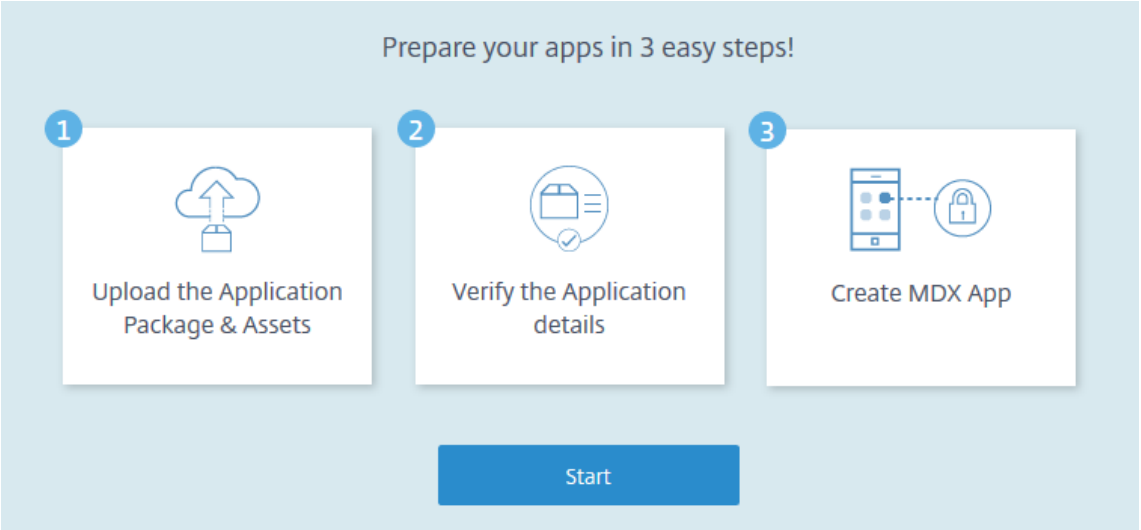


Pour utiliser le MDX Service

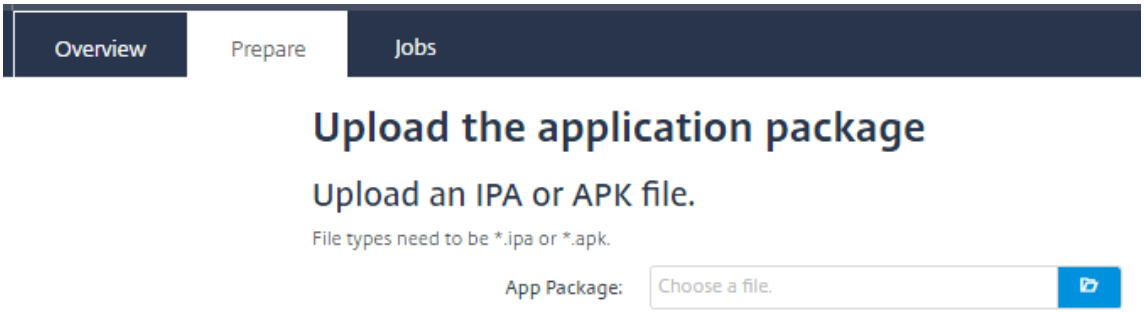
Pour utiliser MDX Service, chargez le fichier binaire du package d'application et les ressources de signature requises. Vérifiez ensuite les détails de l'application et modifiez les attributs, si nécessaire. Vous pouvez ensuite télécharger le package de l'application encapsulée.

Pour encapsuler une application iOS

1. Sur la page Overview de MDX Service, cliquez sur **Start**.



2. Chargez le fichier .ipa pour l'application. Le temps nécessaire au chargement dépend de la taille du fichier.



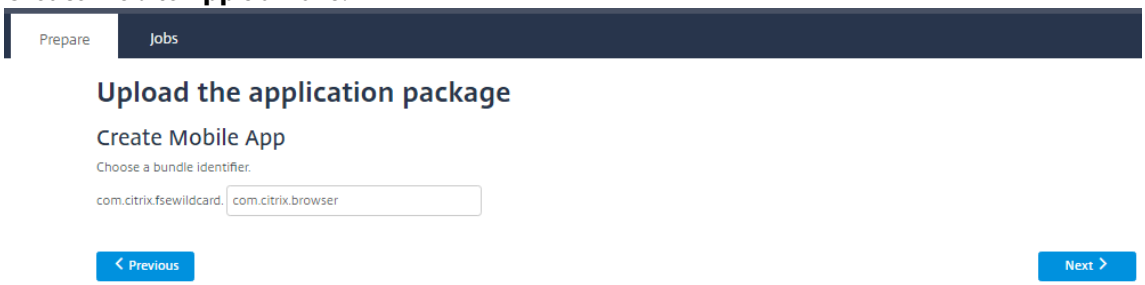
Une fois le fichier .ipa chargé sur MDX Service et traité avec succès, l'écran **Verify App Details** s'affiche.
Page de vérification des détails de l'application

3. Sur l'écran **Verify App Details**, entrez les informations suivantes :
   a) (Facultatif) Modifiez le **nom de l'application**, la **version d'OS minimum** et la **version d'OS maximum**.
   b) Entrez une **description** (obligatoire).
   c) Sélectionnez une version du SDK MDX avec laquelle encapsuler l'application.
   d) Chargez les ressources de signature iOS suivantes :
      - Profil de provisioning
      - Certificat

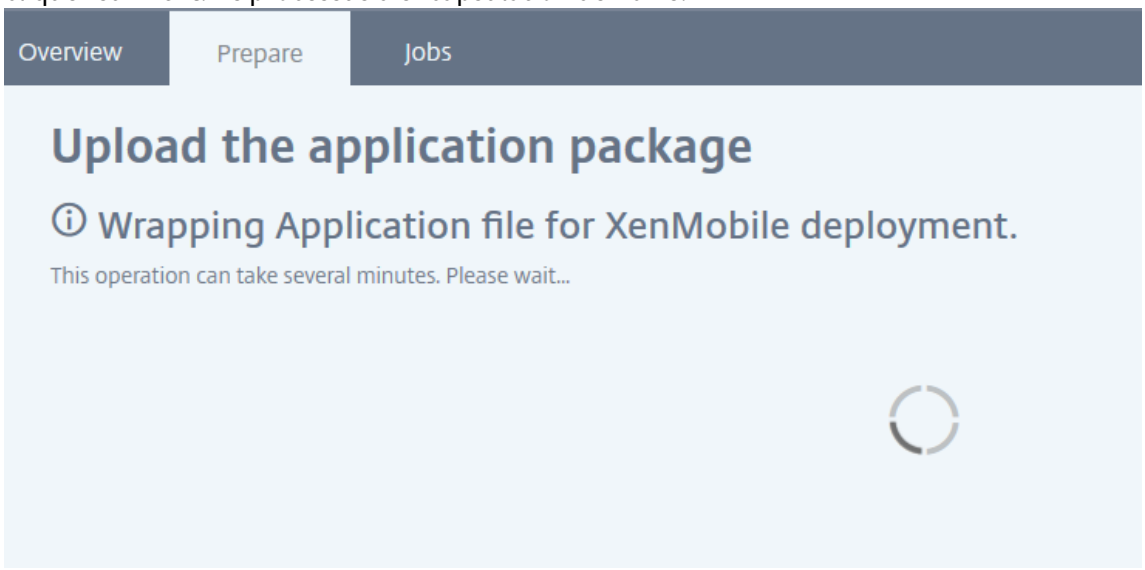
- Mot de passe du certificat

Pour collecter les informations sur le certificat et le profil de provisioning, suivez les étapes de l'article CTX220481.

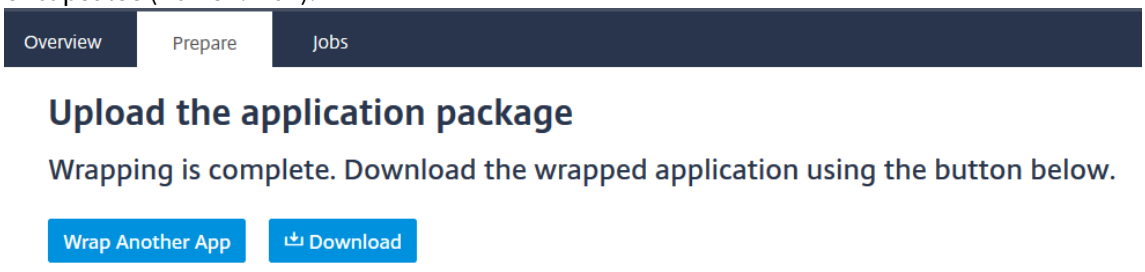
Une fois que MDX Service utilise les ressources de signature pour modifier l'application, l'écran **Create Mobile App** s'affiche.



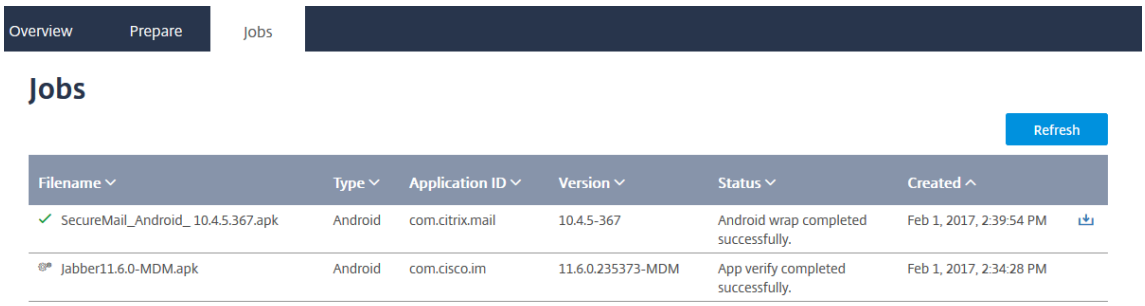
4. (Facultatif) Sur l'écran **Create Mobile App**, modifiez le bundle ID de l'application mobile, puis cliquez sur **Next**. Le processus d'encapsulation démarre.



5. Une fois le processus d'encapsulation terminé, téléchargez le package de l'application MDX encapsulée (fichier .mdx).

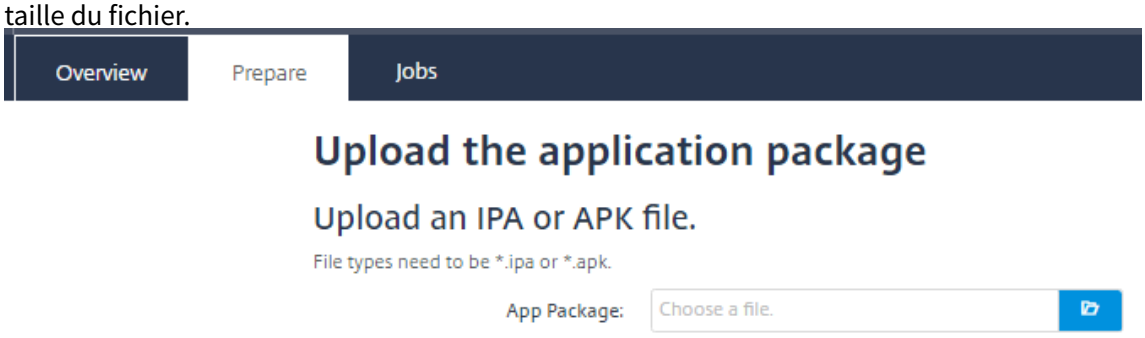


Vous pouvez également télécharger le fichier plus tard à partir de l'onglet **Jobs**.

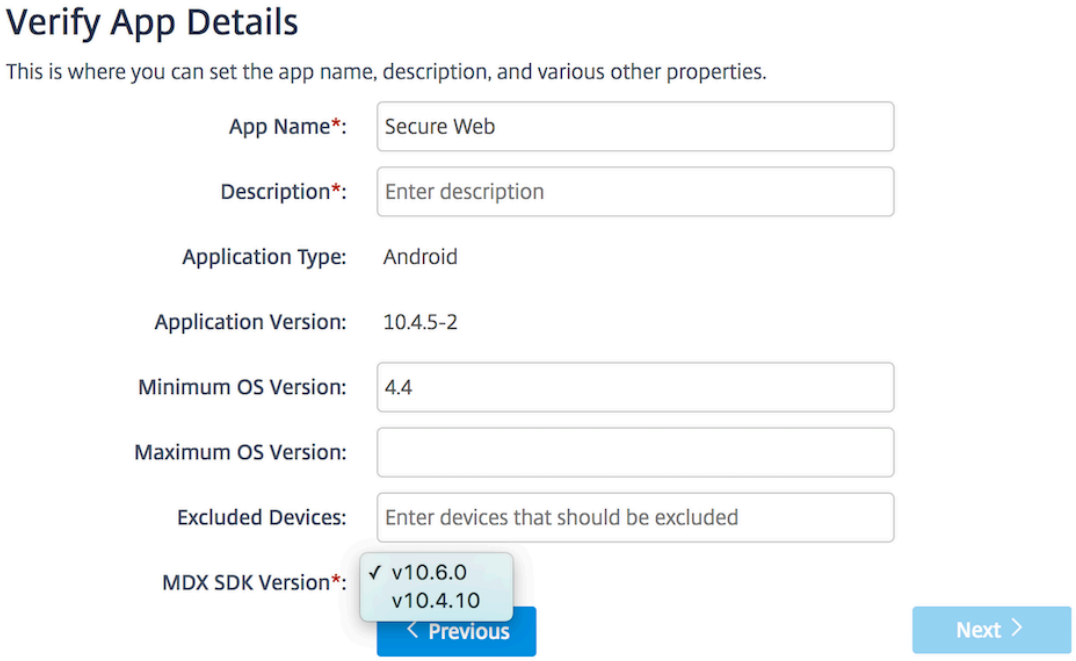


Pour encapsuler une application Android

1. Chargez le fichier .apk pour l'application. Le temps nécessaire au chargement dépend de la taille du fichier.



2. Une fois le fichier .apk chargé sur MDX Service et traité avec succès, l'écran **Verify App Details** s'affiche.

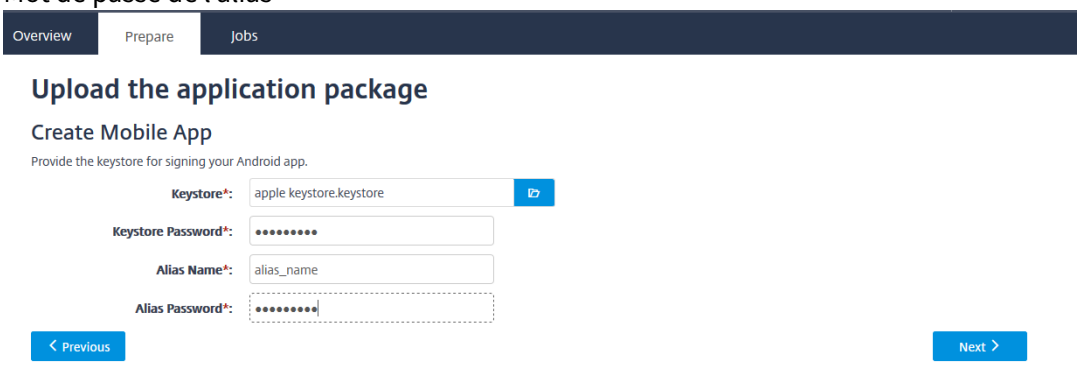


3. Sur l'écran **Verify App Details**, entrez les informations suivantes :

   a) (Facultatif) Modifiez le **nom de l'application**, la **version d'OS minimum** et la **version d'OS maximum**.
   b) Entrez une **description** (obligatoire).
   c) Sélectionnez une version du SDK MDX avec laquelle encapsuler l'application.

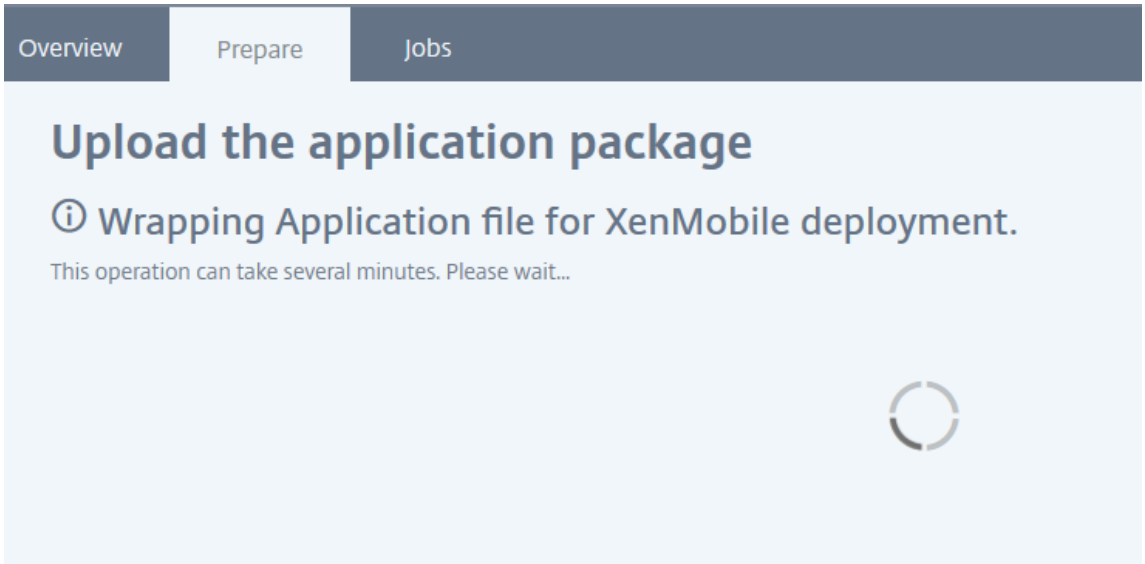
4. Sur l'écran **Create Mobile App**, chargez les ressources de signature Android suivantes :

   - Keystore
   - Mot de passe du KeyStore
   - Nom de l'alias
   - Mot de passe de l'alias

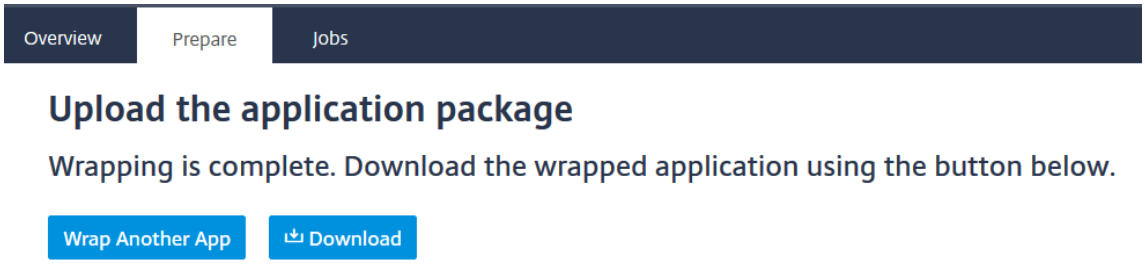


   Pour collecter les informations de keystore et de nom d'alias, suivez les étapes de l'article CTX220480.

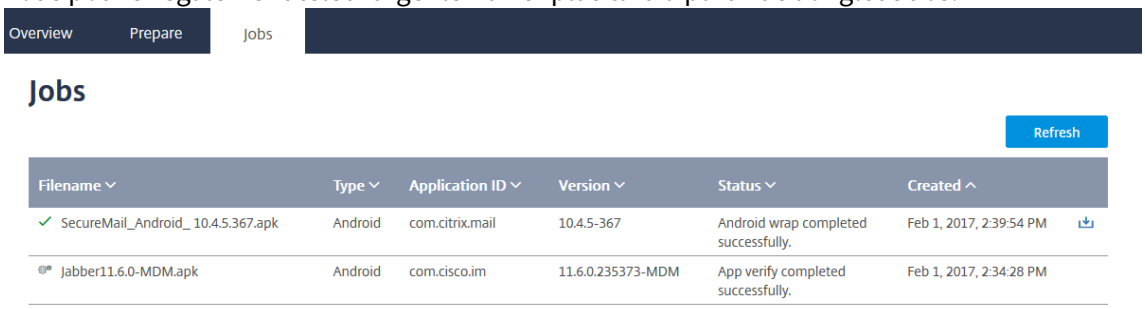
5. Cliquez sur **Next** pour démarrer le processus d'encapsulation.



6. Téléchargez le package de l'application MDX encapsulée (fichier .mdx).



Vous pouvez également télécharger le fichier plus tard à partir de l'onglet **Jobs**.



License Usage Insights Service

November 7, 2018

Le License Usage Insights (LUI) Service de Citrix Cloud est un service de cloud gratuit qui permet aux Citrix Service Providers (CSP) de comprendre et créer des rapports sur l'utilisation des produits.

Le service LUI aide les partenaires CSP à comprendre l'utilisation des produits Citrix et le nombre de licences utilisées. Seuls les partenaires CSP ont accès au service LUI.

Le License Usage Insights Service vous permet de :

- Collecter et agréger automatiquement les informations sur l'utilisation des produits à partir des serveurs de licences Citrix
- Visualiser facilement les utilisateurs qui accèdent à vos déploiements Virtual Apps and Desktops chaque mois
- Créer des ventilations d'utilisation des licences par client
- Optimiser les coûts des licences en identifiant et assurant le suivi d'une liste d'utilisateurs gratuits
- Afficher et comprendre vos activités historiques avec Citrix
- Exporter l'utilisation de Virtual Apps and Desktops et les données d'attribution d'ADC VPX au format CSV

Détails techniques

November 7, 2018

Avant d'utiliser le License Usage Insights (LUI) Service, tenez compte des éléments suivants :

- Seuls les serveurs de licences Windows et VPX sont pris en charge.
- Cela peut prendre jusqu'à 24 heures pour qu'un serveur de licences mis à jour apparaisse dans le service LUI.
- Lorsque les données d'utilisation sont chargées à partir d'un serveur de licences, elles sont traitées et stockées de manière sécurisée afin de permettre au service LUI d'y accéder à une date ultérieure. Ce processus peut prendre jusqu'à 24 heures.
- Par défaut, les noms d'utilisateurs associés aux extractions de licences Virtual Apps and Desktops sont envoyés à Citrix en toute sécurité.
- Les noms d'utilisateurs sont transmis de façon à permettre aux partenaires CSP de tirer parti des fonctionnalités LUI et du programme de licences CSP qui prend en charge les utilisateurs à des fins d'évaluation, de test et d'utilisation administrative des produits.
- Les informations utilisateur sont limitées à une seule entrée utilisateur@domaine ; aucune donnée supplémentaire permettant d'identifier personnellement l'utilisateur n'est transmise. Citrix ne partagera jamais ces informations.
- Pour les partenaires ne souhaitant pas charger les informations de nom d'utilisateur, cette fonctionnalité peut être désactivée sur le serveur de licences Citrix à l'aide de la fonctionnalité d'anonymisation de nom d'utilisateur.

Produits Citrix pris en charge

Le License Usage Insights (LUI) Service fournit des informations d'utilisation pour les produits Citrix suivants :

- Virtual Apps and Desktops
- ADC VPX
- CloudPortal Services Manager (CPSM)

Pour utiliser le service LUI avec CloudPortal Services Manager, CPSM 11.5 Cumulative Update 4 doit être installée dans votre déploiement. Cette mise à jour inclut les fonctionnalités Call Home qui permettent au service LUI d'afficher l'état du déploiement et les informations relatives à l'utilisation des licences. Pour plus d'informations, veuillez consulter l'article CTX220717.

Prise en main du License Usage Insights Service

November 7, 2018

Étape 1 : Mettre à jour le serveur de licences Citrix

Le License Usage Insights Service requiert le serveur de licences Citrix 11.13.1.2 ou une version ultérieure. Avant de commencer à utiliser le service, téléchargez la dernière version du serveur de licences Citrix et mettez à niveau vos serveurs de licences. La mise à niveau sur place est simple et rapide. Pour de plus amples informations sur la dernière version du serveur de licences Citrix, consultez la documentation relative au système de licences Citrix.

Étape 2 : Se connecter à Citrix Cloud avec les informations d'identification My Citrix

Avant de vous connecter, vous devez ouvrir un compte Citrix Cloud. Suivez les étapes décrites dans Ouvrir un compte Citrix Cloud.

Lorsque vous créez votre compte, utilisez les mêmes informations d'identification My Citrix que celles que vous avez utilisées pour allouer et télécharger des licences Citrix depuis citrix.com. Citrix Cloud vous envoie un e-mail à l'adresse associée aux informations d'identification My Citrix pour confirmer le compte.

Lorsque votre compte Citrix Cloud est prêt à être utilisé, connectez-vous à https://citrix.cloud.com à l'aide de votre adresse e-mail et d'un mot de passe.

Étape 3 : Utiliser le License Usage Insights Service

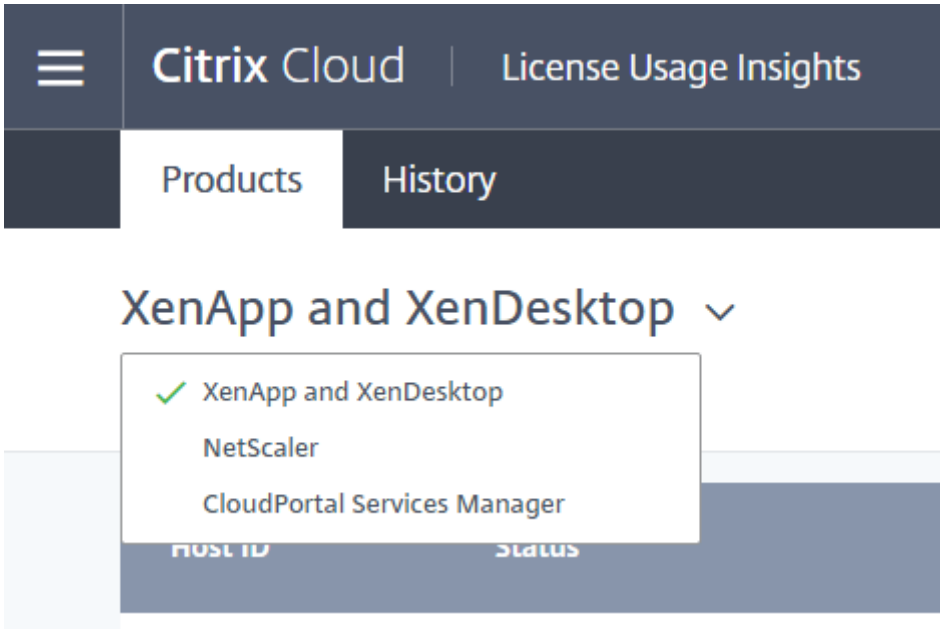
À partir de la console Citrix Cloud, recherchez le License Usage Insights Service et cliquez sur **Gérer**. Pour obtenir un aperçu des fonctionnalités principales du service, consultez la section Utiliser le License Usage Insights Service.

Utiliser le License Usage Insights Service

November 7, 2018

Sélection du produit

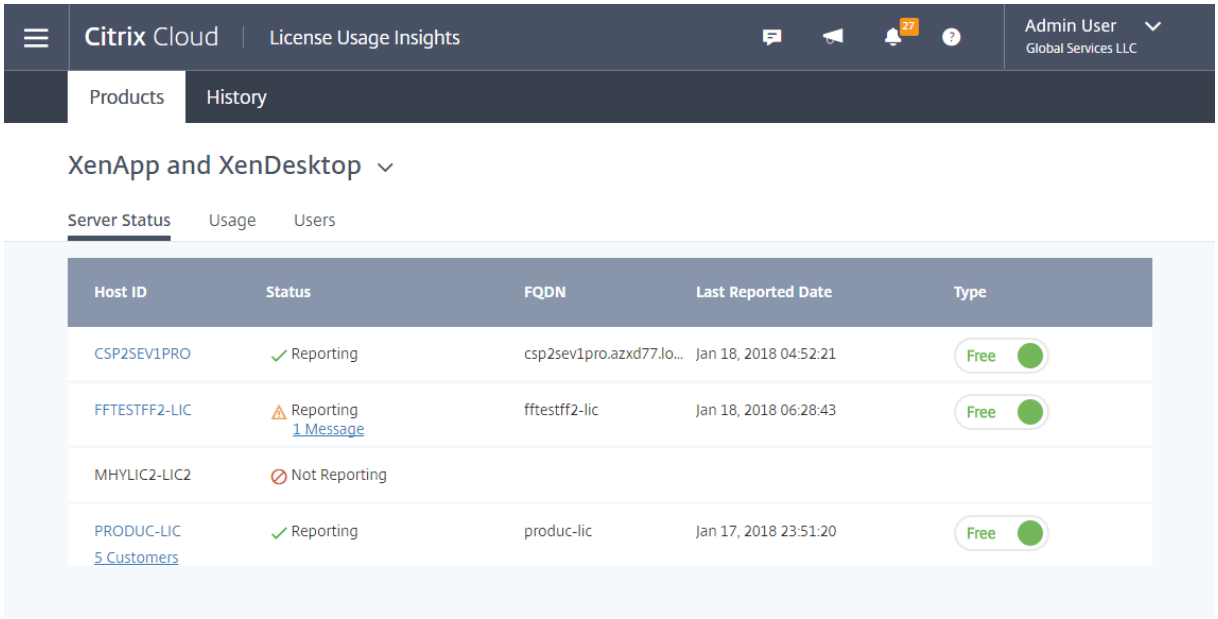
Pour afficher les détails de licence d'un produit différent, cliquez sur la flèche en regard du nom du produit et sélectionnez le produit que vous souhaitez afficher.



État du serveur de licences

Pour être conformes aux recommandations en matière de licences du programme CSP, tous les serveurs de licences actifs doivent être mis à jour et la fonction de reporting doit être opérationnelle. L'état du serveur de licences indique les serveurs de licences dont vous disposez et s'ils sont mis à jour afin de pouvoir être utilisés avec le service LUI.

Le service affiche une liste des serveurs de licences actifs à l'aide des données d'allocation de licences stockées dans le back office de Citrix. Si le serveur de licences est mis à jour et que la fonction de reporting est opérationnelle, le service LUI affiche l'état « reporting » et comprend un horodatage du chargement plus récent.

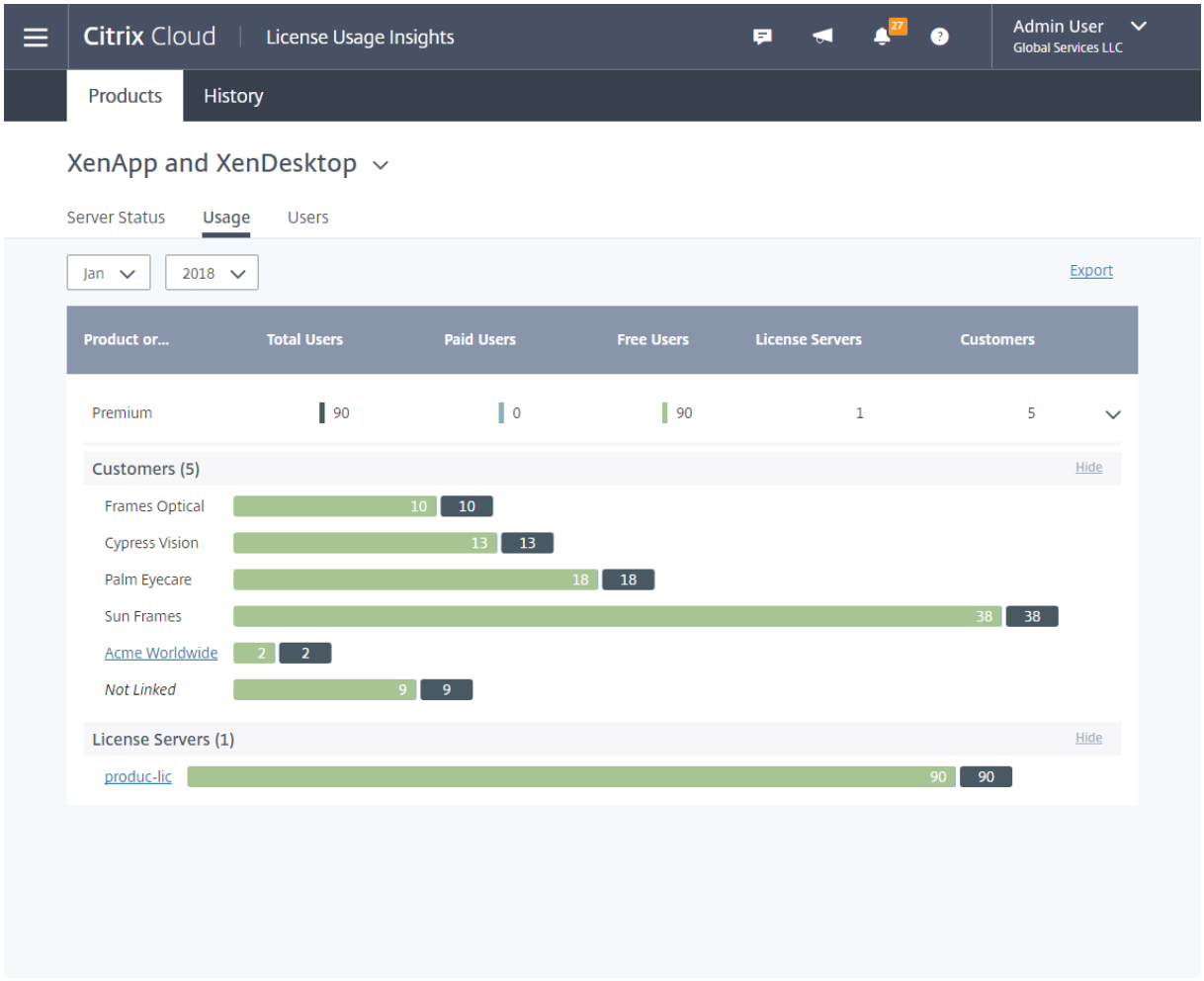


Collecte des données d'utilisation

La collecte des données d'utilisation vous aide à comprendre l'utilisation des produits grâce à la collecte et à l'agrégation automatiques des données. Il n'est pas nécessaire de déployer des outils supplémentaires.

Le service regroupe automatiquement les données d'utilisation des produits sur tous les serveurs de licences Citrix pour fournir une vue complète de l'utilisation sur tous les déploiements. Vous pouvez également créer des ventilations d'utilisation des licences en associant des utilisateurs spécifiques aux clients ou aux locataires à qui ils appartiennent.

Les serveurs de licences collectent et suivent l'utilisation des licences de produit et dressent un rapport qu'ils envoient à Citrix à l'aide d'un canal de transmission sécurisé. Cette approche automatisée vous donne accès à un flux constant de données d'utilisation actualisées, ce qui permet de gagner du temps et d'aider les partenaires à mieux comprendre les tendances d'utilisation au sein de leurs déploiements.



Pour créer une ventilation par client de l'utilisation de Virtual Apps and Desktops

Pour détailler l'utilisation des licences par client, vous devez d'abord associer des utilisateurs aux clients ou aux locataires à qui ils appartiennent. Si aucun client n'est défini dans votre tableau de bord Clients, vous pouvez en ajouter de nouveaux ou vous pouvez vous connecter à des clients Citrix Cloud existants.

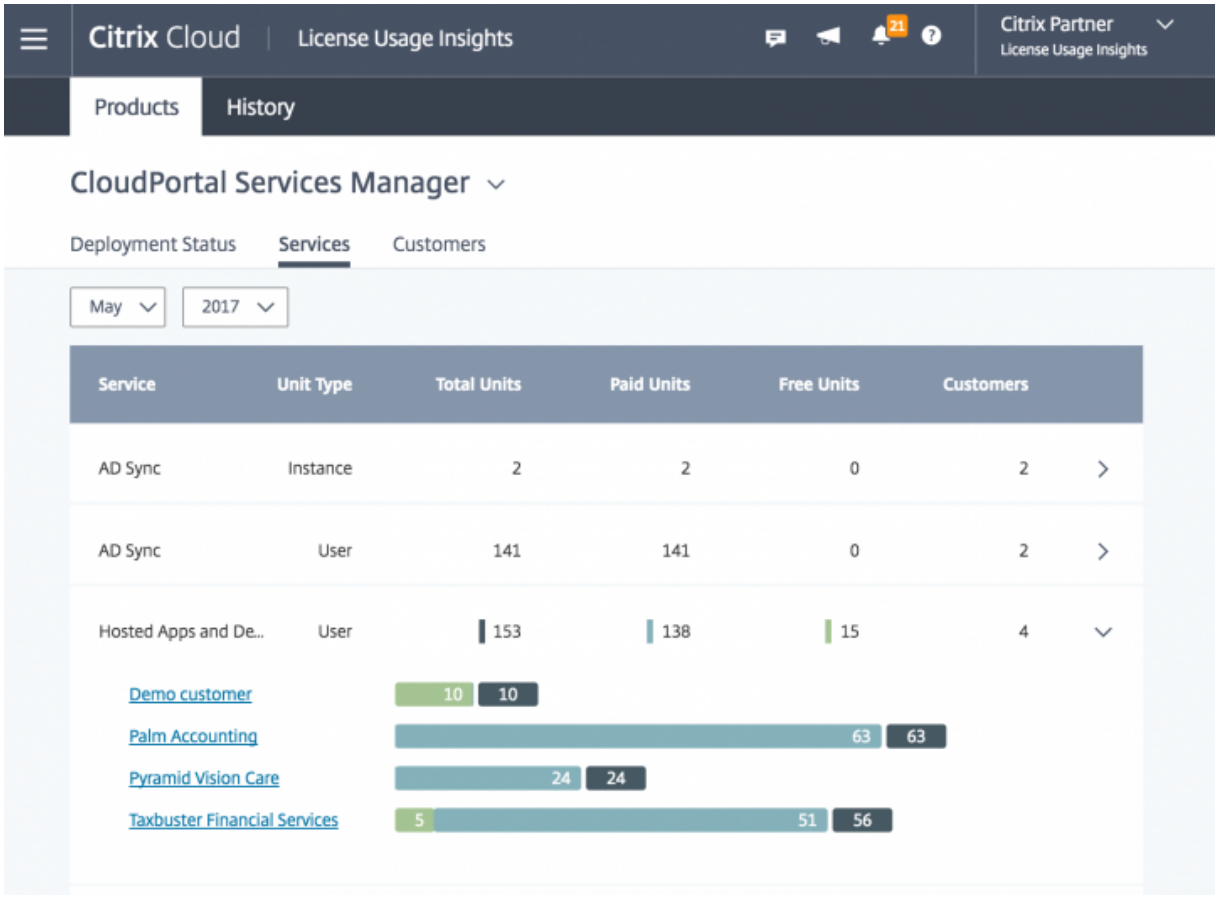
1. Le cas échéant, ajoutez des clients au tableau de bord Clients : dans la page d'accueil de la console de gestion Citrix Cloud, cliquez sur **Clients**, sur **Ajouter ou Inviter**, puis suivez les instructions à l'écran.
2. Cliquez sur le bouton de menu, puis sélectionnez **Mes services > License Usage Insights**.
3. Avec le produit **Virtual Apps and Desktops** sélectionné, cliquez sur **Utilisateurs**.
4. Sélectionnez les utilisateurs que vous souhaitez associer, puis cliquez sur **Actions en bloc > Gérer le lien vers le client**.
5. Dans la liste, sélectionnez le client auquel vous voulez associer les utilisateurs.
6. Cliquez sur **Enregistrer**.

7. Pour afficher la ventilation par client, cliquez sur la vue **Utilisation**.

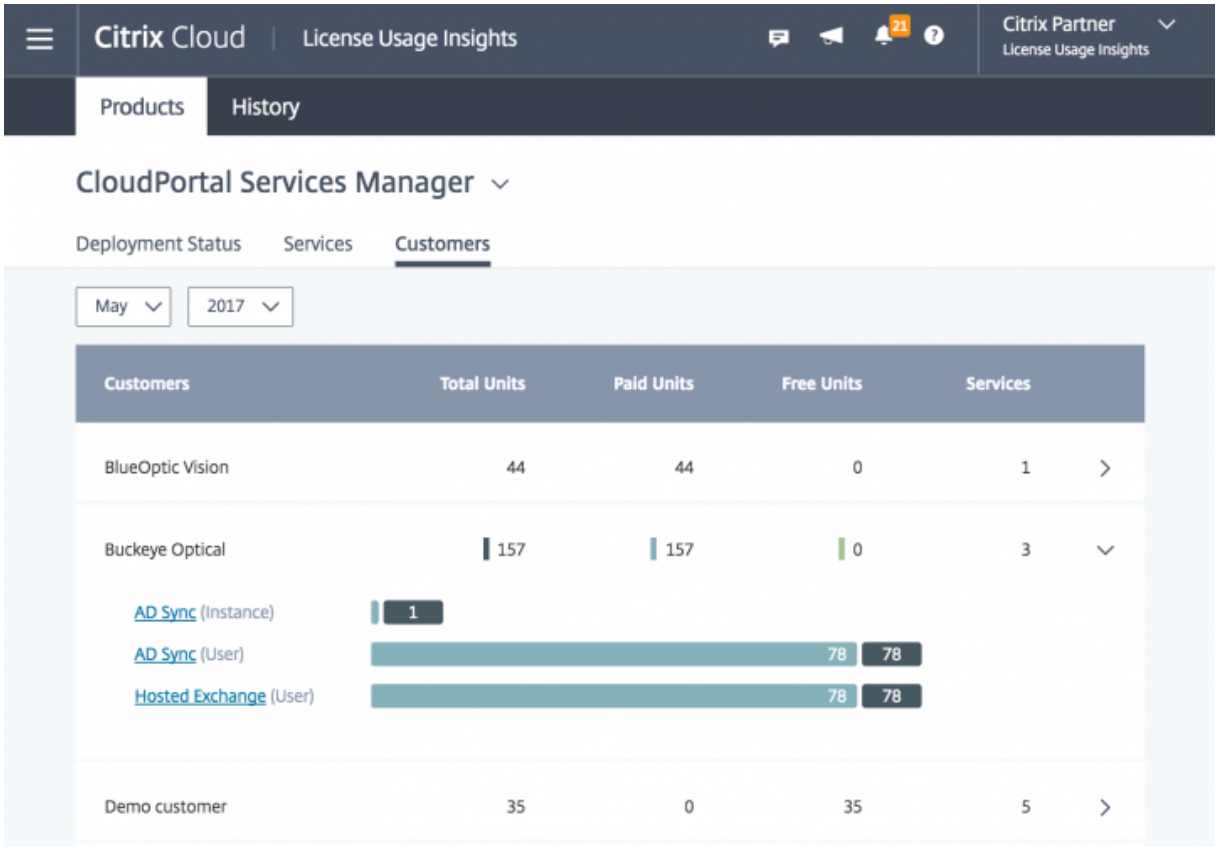
Rapports d'utilisation pour CloudPortal Services Manager

Pour l'utilisation de CloudPortal Services Manager (CPSM), le service LUI inclut les vues Services et Clients.

La vue Services est la vue principale qui permet de comprendre l'utilisation totale des licences CPSM par tous vos clients. Les données d'utilisation des licences sont regroupées par service, en les mappant directement avec la manière dont vous rapportez l'utilisation des licences CPSM. Lorsque vous explorez un service spécifique, l'utilisation totale est ventilée pour indiquer clairement quels clients contribuent à cette utilisation.

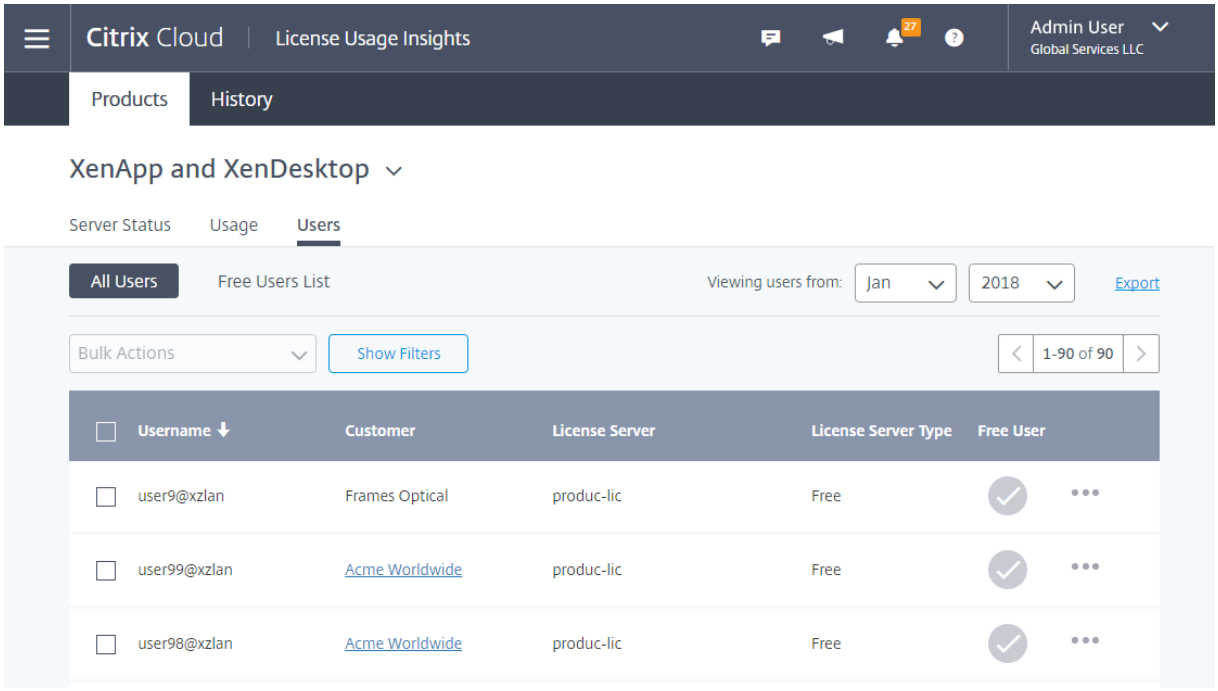


La vue Clients présente des données similaires à la vue Services, mais dans un format différent. Cette vue vous aide à comprendre les services qu'un client spécifique utilise ou consomme. Lorsque vous sélectionnez un client spécifique, vous pouvez explorer plus en détail les services CPSM que ce client utilise.



Gestion des utilisateurs

Le service LUI fournit une vue complète de l'utilisation des produits sur les déploiements tout en vous permettant de profiter pleinement du programme de licences CSP qui prend en charge les utilisateurs à des fins d'évaluation, de test et d'utilisation administrative.

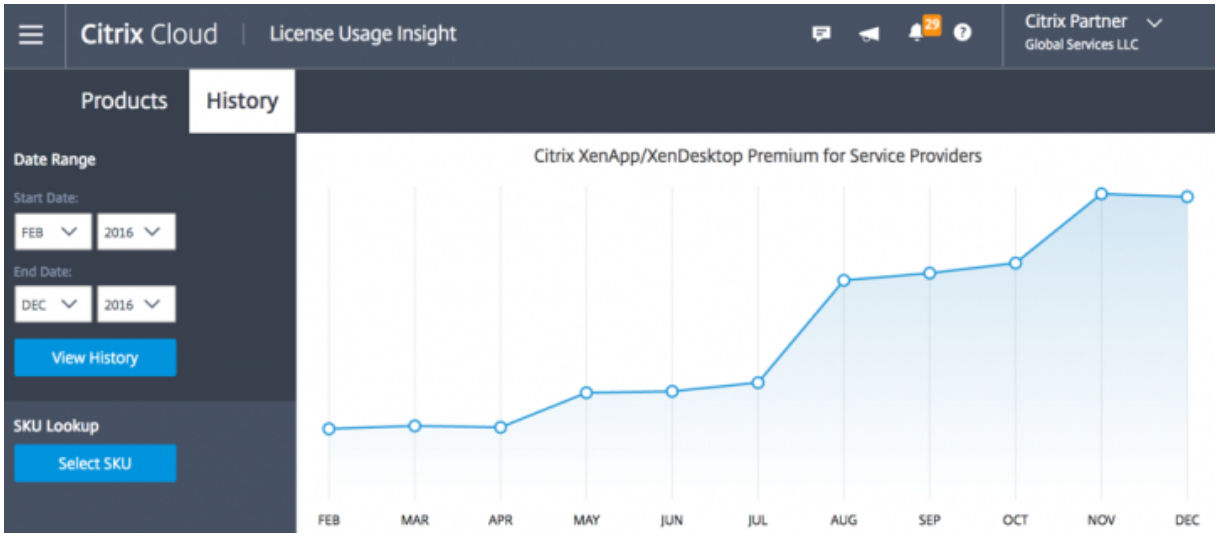


Remarque : les utilisateurs gratuits de CloudPortal Services Manager (CPSM) ne sont visibles que dans le service LUI. La gestion des utilisateurs CPSM gratuits se produit dans la console CPSM.

Tendances historiques

Vous pouvez afficher un rapport historique complet de toutes vos activités antérieures avec Citrix. Vérifiez l'utilisation déclarée le mois dernier, l'année dernière, ou sur une période de temps configurable.

Les vues historiques offrent des informations précieuses sur les activités de l'entreprise. En tant que CSP, vous pouvez rapidement évaluer la manière dont votre activité avec Citrix se développe et découvrir les produits qui enregistrent la plus forte croissance auprès de vos clients et abonnés.



Exporter les données d'utilisation et d'allocation

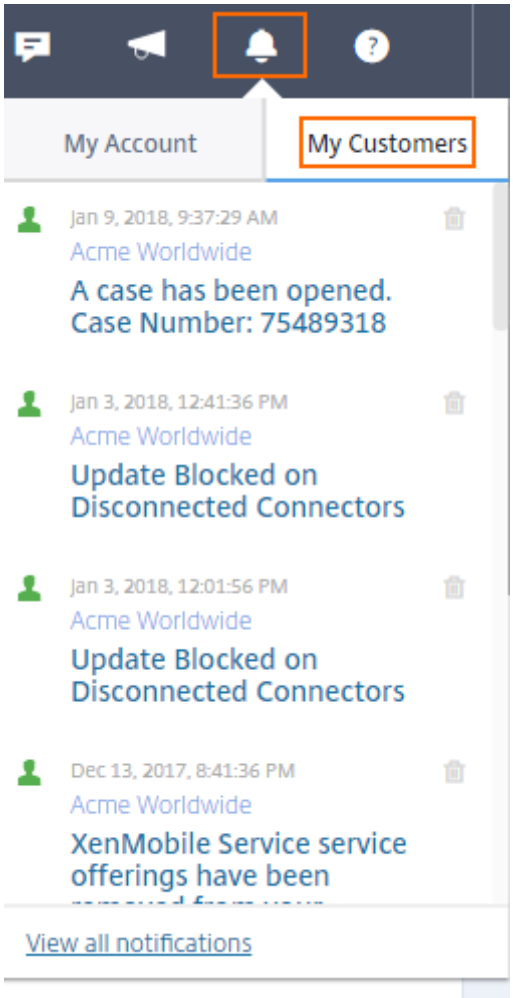
Vous pouvez exporter les types de données suivants en tant que fichier CSV à partir du service LUI :

- Utilisation des produits Virtual Apps and Desktops et liste des utilisateurs pour un mois donné
- Détails actuels de l'allocation ADC VPX

1. Sélectionnez **Virtual Apps and Desktops** ou **Réseau** dans la liste des produits.
2. Le cas échéant, sélectionnez la vue que vous souhaitez exporter. Par exemple, pour exporter les détails d'utilisation de Virtual Apps and Desktops, cliquez sur la vue **Utilisation**.
3. Le cas échéant, sélectionnez le mois et l'année que vous souhaitez exporter.
4. Sur le côté gauche de l'écran, cliquez sur **Exporter**.

Afficher les notifications des clients

Citrix Cloud vous permet de surveiller l'intégrité de la solution de plusieurs clients sans avoir à visiter chaque déploiement individuellement. La zone Notifications dans Citrix Cloud regroupe les notifications des clients sur votre tableau de bord afin que vous puissiez vous assurer que les alertes sont traitées et que les services continuent à fonctionner.



1. Dans la console de gestion Citrix Cloud, cliquez sur l'icône **Notifications**, puis sur **Mes clients**. Une liste des notifications les plus récentes apparaît.
2. Pour afficher la liste complète des notifications des clients, cliquez sur **Afficher toutes les notifications**.

Mettre à jour et configurer le serveur de licences Citrix

November 7, 2018

Le serveur de licences Citrix est un composant essentiel du License Usage Insights (LUI) Service. Pour utiliser le service LUI, vos serveurs de licences Citrix doivent être mis à jour vers la version 11.13.1.2 ou une version ultérieure.

À propos du serveur de licences Citrix

Le serveur de licences Citrix 11.13.1.2 et versions ultérieures contient les fonctionnalités principales dont les partenaires CSP ont besoin.

- Collecte de l'utilisation optimisée : le serveur de licences contient une nouvelle fonctionnalité qui optimise le comportement et le suivi des licences afin d'offrir un meilleur soutien aux CSP.
- Call Home : le serveur de licences comprend les fonctionnalités de Call Home qui permettent d'automatiser la collecte de données sur l'utilisation des produits pour les partenaires CSP. Ces fonctionnalités sont exclusives aux partenaires CSP et sont uniquement activées lorsqu'une licence CSP est détectée sur le serveur de licences.

Mettre à niveau vos serveurs de licences Citrix pour utiliser le License Usage Insights Service

Effectuez les tâches suivantes :

1. Téléchargez la dernière version du serveur de licences.
2. Mettez à niveau votre serveur de licences actuel.
3. Répétez le processus de mise à niveau pour chacun de vos serveurs de licences.
4. Commencez à utiliser le service LUI.

Anonymiser les noms d'utilisateurs via le serveur de licences

Par défaut, les noms d'utilisateurs associés aux extractions de licences Virtual Apps and Desktops sont envoyés à Citrix en toute sécurité.

Les noms d'utilisateurs sont transmis de façon à permettre aux partenaires CSP de tirer parti des fonctionnalités LUI et du programme de licences CSP qui prend en charge les utilisateurs à des fins d'évaluation, de test et d'utilisation administrative des produits.

Les informations utilisateur sont limitées à une seule entrée utilisateur@domaine ; aucune donnée supplémentaire permettant d'identifier personnellement l'utilisateur n'est transmise. Citrix ne partage pas ces informations.

Pour les partenaires ne souhaitant pas charger les informations de nom d'utilisateur, l'anonymisation peut être activée. Lorsqu'elle est activée, l'anonymisation du nom d'utilisateur convertit les noms d'utilisateurs lisibles en chaînes uniques à l'aide d'un algorithme sécurisé et irréversible avant le chargement.

Le service LUI utilise ces identificateurs uniques pour suivre l'utilisation des produits au lieu des noms d'utilisateurs. Cette approche permet aux fournisseurs de services de bénéficier d'analyses mensuelles sans avoir accès aux noms d'utilisateurs dans l'interface utilisateur du service de cloud.

Pour configurer l'anonymisation des noms d'utilisateurs

1. Sur le serveur de licences, ouvrez le fichier de configuration dans un éditeur de texte. Le fichier de configuration se trouve généralement sous C:\Program Files\Citrix\Licensing\WebServicesForLicensing\S
2. Dans la section **Configurations**, localisez le paramètre **UsageBasedBillingScramble**.
3. Modifiez la valeur actuelle sur **1** et enregistrez le fichier.

Informations sur le serveur de licences incluses dans les chargements

Lorsque CSP Home est activé sur un serveur de licences Citrix, il charge les informations suivantes quotidiennement :

- Informations sur le serveur de licences : version du serveur de licences
- Informations sur les licences du serveur de licences :
  - Fichiers de licences installés sur le serveur
  - Dates d'expiration du fichier de licences
  - Informations sur les droits associés à l'édition et les fonctionnalités du produit
  - Nombre de licences
- Informations sur l'utilisation des licences :
  - Licences utilisées dans le mois calendaire en cours
  - Noms d'utilisateurs associés aux licences extraites
  - Fonctionnalités des produits et éditions activées

Afficher le chargement d'un serveur de licences

Les partenaires CSP peuvent examiner la dernière charge utile chargée sur leur serveur de licences afin de comprendre tous les détails que le serveur de licences envoie à Citrix. Une copie de cette charge utile est stockée dans un fichier .zip sur le serveur de licences. Par défaut, cet emplacement est C:\Program Files (x86)\Citrix\Licensing\LS\resource\usage\upload_1456166761.zip.

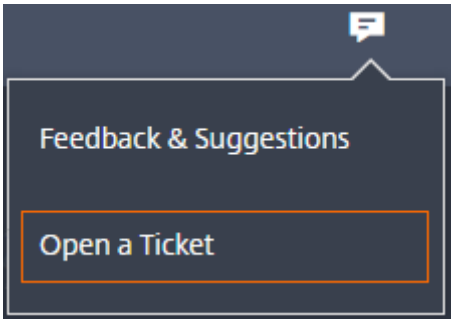
Remarque

Les chargements réussis sont supprimés à l'exception du dernier. Les chargements ayant échoué sont conservés sur le disque jusqu'à ce qu'un chargement réussisse. Lorsque cela se produit, tous les chargement sont supprimés à l'exception du dernier.

Questions fréquemment posées

November 7, 2018

- **Quelles informations sont-elles envoyées ? Puis-je consulter les informations que mes serveurs de licences envoient à Citrix ?** Oui, vous pouvez afficher une copie des informations envoyées à Citrix. Pour de plus amples informations, consultez la section Utilisation du License Usage Insights Service.
- **Le service LUI est-il disponible auprès des clients ou partenaires Citrix qui ne sont pas membres du programme Citrix Service Provider (CSP) ?** Non. Le service LUI est uniquement disponible auprès des partenaires CSP qui ont rejoint ce programme de partenariat.
- **Puis-je désactiver la fonction Phone Home sur le serveur de licences ?** Non. Conformément au contrat de licence Citrix Service Provider, tous les serveurs de licences Citrix sont tenus de transmettre les données d'utilisation des produits. Les partenaires souhaitant ne pas utiliser la fonction Phone Home peuvent utiliser la fonction d'anonymisation du nom d'utilisateur. Pour de plus amples informations, consultez la section Anonymiser les noms d'utilisateurs via le serveur de licences.
- **Serais-je facturé en fonction de l'utilisation du produit indiquée dans le service LUI ?** Non. Le service LUI aide les partenaires à comprendre leur utilisation des produits afin de pouvoir en faire état rapidement et précisément à leur distributeur Citrix. Les partenaires CSP continueront d'être facturés en fonction de l'utilisation des produits qu'ils présentent à leur distributeur Citrix. Les distributeurs Citrix continueront à entretenir la relation de facturation avec les partenaires CSP.
- **Quels produits Citrix le service LUI prend-il en charge ?** Le service LUI prend actuellement en charge les produits Citrix suivants :
  - Utilisation du produit Virtual Apps and Desktops.
  - Attributions de Citrix ADC VPX.
  - CloudPortal Services Manager Call Home. CPSM 11.5 Cumulative Update 4 est requise pour utiliser le service LUI avec votre déploiement CPSM. Pour plus d'informations, veuillez consulter l'article CTX220717.
- **Combien coûte le License Usage Insights service ?** Le service LUI est fourni gratuitement avec Citrix Cloud.
- **Comment obtenir de l'aide avec le License Usage Insights Service ?** Ouvrez un ticket de support à partir de Citrix Cloud :
  1. Connectez-vous à Citrix Cloud.
  2. Cliquez sur l'icône **Commentaires/support** en haut à droite de l'écran.
  3. Sélectionnez **Ouvrir un ticket** et remplissez le formulaire.



Un membre du support technique Citrix donnera suite à votre demande.

- **Comment fournir des commentaires sur le License Usage Insights services ?** Pour fournir des commentaires sur le service LUI :

1. Connectez-vous à Citrix Cloud.
2. Cliquez sur l'icône **Commentaires/support** en haut à droite de l'écran.
3. Sélectionnez **Commentaires et suggestions**. La page de suggestions de Citrix Cloud s'ouvre dans une fenêtre ou un onglet de navigateur séparé.
4. Dans **Tell us about your suggestion** (Faites-nous part de vos suggestions), commencez à taper un titre pour vos commentaires. Au fur et à mesure que vous tapez, des champs supplémentaires apparaissent de manière à ce que vous puissiez fournir plus de détails.
5. Cliquez sur **Post idea** (Poster idée). Vos commentaires s'affichent sur la page de suggestions de Citrix Cloud. Ils sont ensuite soumis aux votes et commentaires d'autres utilisateurs, y compris l'équipe Citrix Cloud.

Secure Browser Service

November 7, 2018

Le Citrix Secure Browser Service protège le réseau d'entreprise contre les attaques basées sur les navigateurs en isolant les activités de navigation sur le Web. Il délivre un accès distant sécurisé et cohérent aux applications Web hébergées sur Internet sans configuration du terminal. Les administrateurs peuvent déployer des navigateurs sécurisés rapidement, ce qui offre un retour sur investissement instantané. En isolant la navigation Internet, les administrateurs informatiques peuvent offrir aux utilisateurs un accès Internet sécurisé sans compromettre la sécurité.

Les utilisateurs se connectent via Citrix Workspace (ou Citrix Receiver) et peuvent ouvrir des applications Web dans le navigateur Web configuré. Le site Web ne transfère pas directement les données de navigation vers ou depuis l'appareil utilisateur, ce qui garantit une expérience sécurisée.

Le Secure Browser Service peut publier des navigateurs sécurisés à utiliser avec :

- Des applications Web externes non authentifiées. Bien que cela ne soit généralement pas recommandé, des applications Web externes non authentifiées peuvent être utilisées pour une

preuve de concept simple.
- Des applications Web externes authentifiées. La publication d'applications Web externes authentifiées nécessite un emplacement de ressources contenant au moins un Cloud Connector (deux ou plus sont recommandés). Pour plus de détails, voir Citrix Cloud Connector.

Le service propose également :

- Intégration d'applications publiées avec Citrix Workspace
- Intégration d'applications publiées avec StoreFront local
- Liste blanche d'adresses URL simples pour garantir la sécurité
- Surveillance de l'utilisation
- Commandes d'utilisation du presse-papiers, de l'impression et du mode kiosque

Nouveautés

Novembre 2018 :

- Vous pouvez configurer un navigateur sécurisé pour vous connecter automatiquement à la région la plus proche en fonction de votre géolocalisation. Cette fonctionnalité est disponible uniquement pour les lancements sur launch.cloud.com.

Octobre 2018 :

- Secure Browser est disponible dans cinq langues. Pour obtenir davantage d'informations sur la globalisation, veuillez consulter l'article CTX119253.
- Prise en charge d'une région supplémentaire : Secure Browser prend en charge la région Est de l'Australie.

Septembre 2018 :

- Vous pouvez maintenant télécharger une icône personnalisée pour votre navigateur publié.

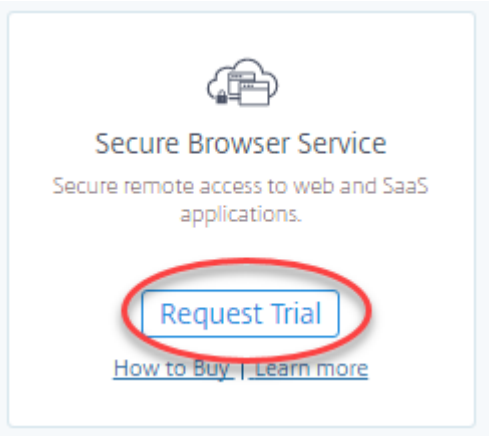
Août 2018 :

- Citrix Secure Browser Service est désormais intégré à Citrix Workspace. Pour plus de détails, voir Intégration avec Citrix Workspace.
- Prise en charge de régions supplémentaires : lorsque vous publiez un navigateur sécurisé, vous pouvez choisir les régions suivantes : Est des États-Unis, Ouest des États-Unis, Europe de l'Ouest et Asie du Sud-Est.

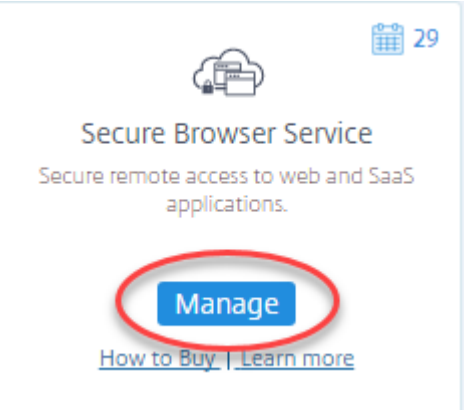
Mise en route

Pour commencer, vous pouvez demander une version d'évaluation de Citrix Secure Browser Service de 30 jours.

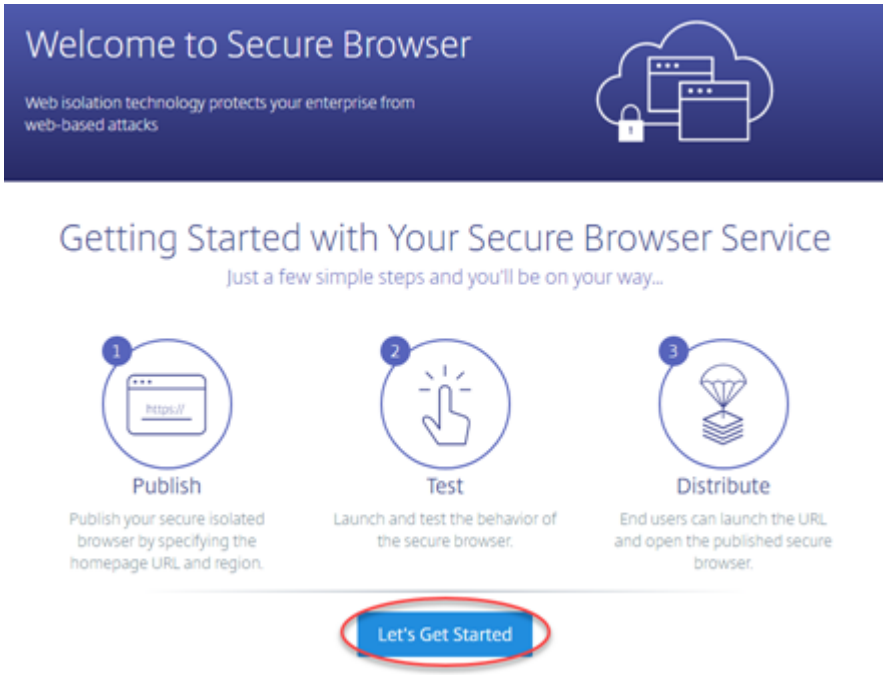
1. Connectez-vous à Citrix Cloud. Si vous n'avez pas de compte, consultez Ouvrir un compte Citrix Cloud.
2. Dans la vignette **Secure Browser Service**, cliquez sur **Demander évaluation**.



3. Vous allez recevoir un e-mail dans quelques instants (l'e-mail associé à votre compte Citrix Cloud). Cliquez sur le lien **Connexion** de l'e-mail.
4. De retour dans Citrix Cloud, cliquez sur **Gérer** dans la vignette de **Secure Browser Service**.



5. Sur la page **Bienvenue sur Secure Browser**, cliquez sur **Commençons**. Vous apprendrez comment publier votre premier navigateur sécurisé.



Pour plus d'informations sur l'achat de Citrix Secure Browser Service, cliquez sur **Comment acheter** sur la page d'accueil de Citrix Cloud.

Intégration avec Citrix Workspace

Secure Browser peut être intégré à Citrix Workspace. Pour s'assurer qu'il est intégré :

1. Connectez-vous à Citrix Cloud.
2. Dans le menu en haut à gauche, sélectionnez **Configuration de l'espace de travail**.
3. Sélectionnez l'onglet **Intégrations de services**.
4. L'entrée de Secure Browser doit indiquer **Activée**. Si ce n'est pas le cas, cliquez sur le menu des points de suspension et sélectionnez **Activer**.

Par défaut, toutes les applications non authentifiées sont disponibles pour tous les utilisateurs de Workspace sans attribution d'utilisateur. Pour les applications authentifiées, vous devez explicitement ajouter des utilisateurs avec la bibliothèque Citrix Cloud.

Vous pouvez vous authentifier à l'aide d'Active Directory ou d'Azure Active Directory. Si vous choisissez Azure Active Directory, le domaine local contenant vos contrôleurs de domaine Active Directory doit contenir un (de préférence deux) Cloud Connector. Pour plus d'informations, consultez :

- Modifier l'authentification aux espaces de travail
- Connecter Azure Active Directory à Citrix Cloud

Intégration avec votre magasin StoreFront local

Les clients Citrix Virtual Apps and Desktops disposant d'un StoreFront local peuvent facilement s'intégrer à Secure Browser Service pour offrir les avantages suivants :

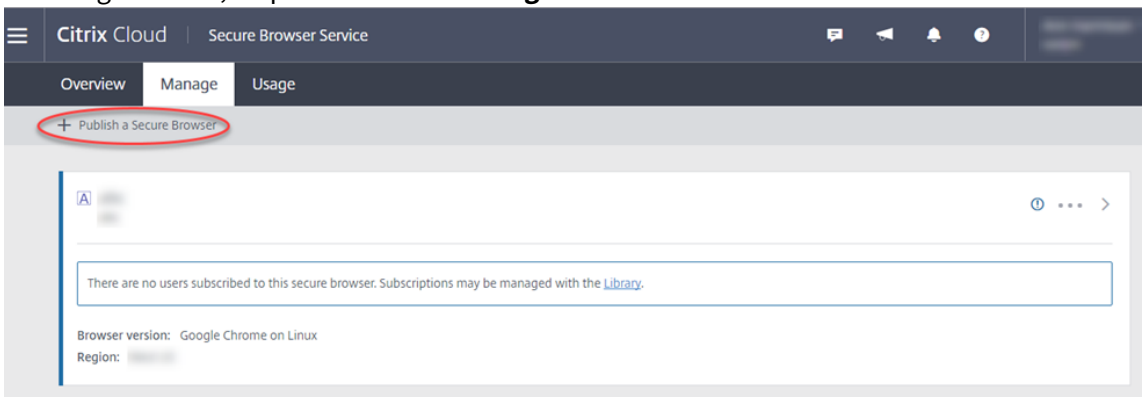
- Regroupez vos navigateurs sécurisés publiés avec vos applications Citrix Virtual Apps and Desktops existantes pour une expérience de magasin unifiée.
- Utilisez des Citrix Receiver natifs pour une expérience utilisateur optimisée.
- Renforcez la sécurité des lancements de Secure Browser en utilisant votre solution d'authentification multifacteur existante intégrée à votre StoreFront.

Pour plus de détails, voir l'article CTX230272 et la documentation sur la configuration de StoreFront.

Publier un navigateur sécurisé

Si vous n'avez pas encore publié de navigateur sécurisé, commencez par l'étape 3.

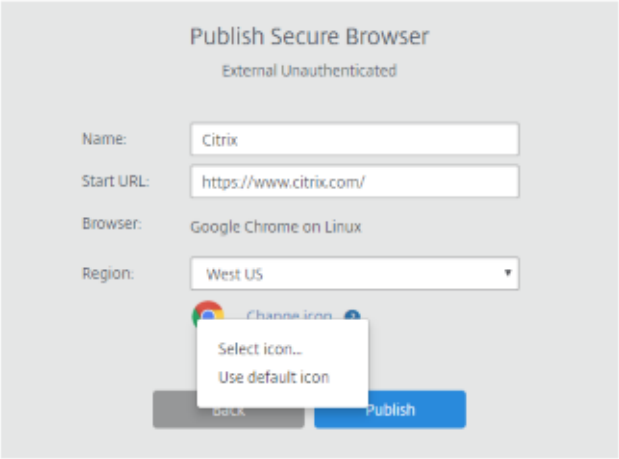
1. Si vous n'êtes pas déjà dans Citrix Cloud, connectez-vous. Dans la vignette **Secure Browser Service**, cliquez sur **Gérer**.
2. Sur l'onglet **Gérer**, cliquez sur **Publier navigateur sécurisé**.



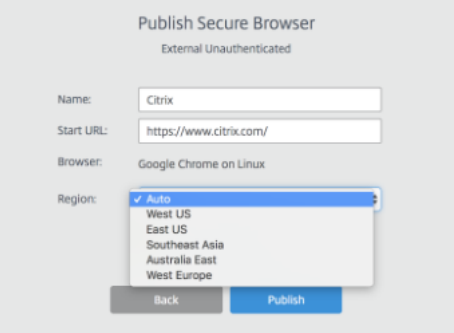
3. Sélectionnez le type de navigateur sécurisé à publier : externe non authentifié (par défaut) ou externe authentifié. Puis cliquez sur **Continuer**.

4. Entrez le nom, l'URL de démarrage et sélectionnez la région. Par défaut, l'icône de l'exécutable de Google Chrome est utilisée lorsque vous publiez un navigateur sécurisé. Vous pouvez maintenant charger votre propre icône pour représenter un navigateur publié.

   - Cliquez sur **Changer icône > Sélectionner une icône** pour charger l'icône de votre choix ou choisissez **Utiliser icône par défaut** pour utiliser l'icône Google Chrome existante.

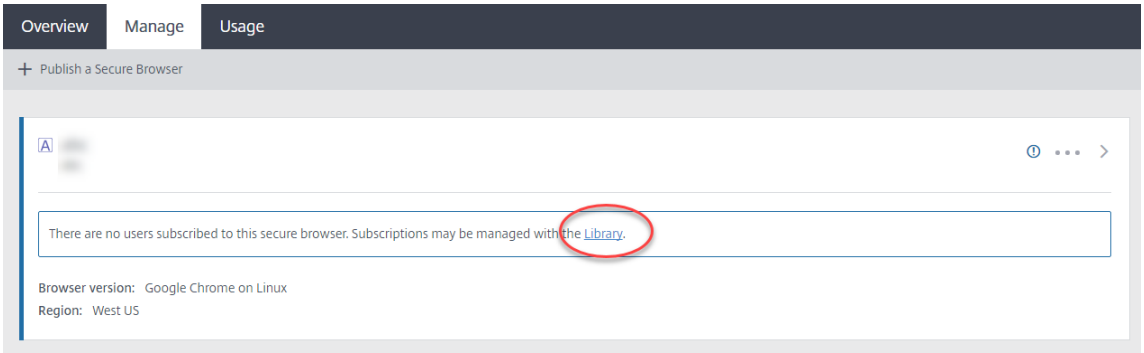


   - Choisissez parmi les régions suivantes : Est des États-Unis, Ouest des États-Unis, Europe de l'Ouest, Asie du Sud-Est et Est de l'Australie.
   - Si vous sélectionnez **Auto**, votre Secure Browser se connecte à la région la plus proche en fonction de votre géolocalisation. Cette fonctionnalité est prise en charge uniquement pour les lancements sur launch.cloud.com.



- Une fois terminé, cliquez sur **Publier**. Lorsque la publication est terminée, l'onglet **Gérer** répertorie le navigateur que vous avez publié.

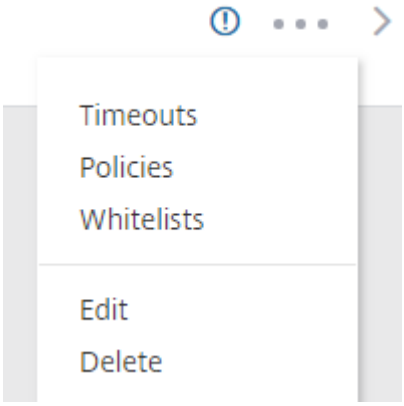
5. Utilisez la bibliothèque Citrix Cloud pour ajouter des abonnés (utilisateurs) au navigateur sécurisé que vous avez créé. Cliquez sur la flèche droite à la fin de la ligne pour développer un volet d'informations contenant un lien vers la bibliothèque.



6. Lorsque vous cliquez sur ce lien, vous êtes dirigé vers l'écran Bibliothèque qui contient votre navigateur sécurisé. Cliquez sur les points de suspension de la vignette contenant le navigateur sécurisé et cliquez sur **Gérer les abonnés**. Pour plus d'informations sur l'ajout d'abonnés, voir Attribuer des utilisateurs et des groupes à des offres de services à l'aide de la bibliothèque.

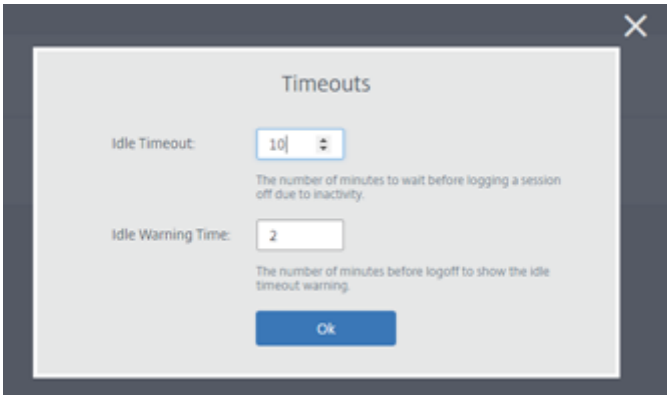
Gérer les navigateurs sécurisés publiés

L'onglet **Gérer** répertorie les navigateurs sécurisés publiés. Pour accéder aux tâches de gestion, cliquez sur les points de suspension à la fin de la ligne d'une entrée, puis sélectionnez la tâche.



Si vous sélectionnez une entrée de menu, puis décidez de ne rien changer, annulez la sélection en cliquant sur le bouton **X** en dehors de la boîte de dialogue.

Délais d'expiration



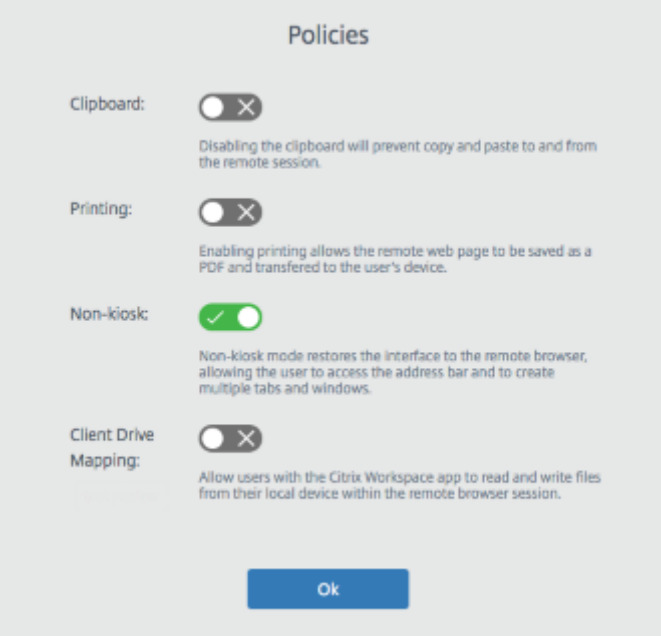
Les paramètres de délai d'expiration incluent :

- Délai d'inactivité : nombre de minutes pendant lesquelles une session peut rester inactive avant d'être fermée pour cause d'inactivité.
- Délai d'avertissement d'inactivité : nombre de minutes après lesquelles un message d'avertissement est envoyé à l'utilisateur avant fermeture de la session.

Par exemple, si vous définissez un délai d'inactivité de 20 et un délai d'avertissement d'inactivité de 5, un message sera envoyé à l'utilisateur si aucune activité n'est détectée dans la session pendant 15 minutes (20 moins 5). Si l'utilisateur ne répond pas, la session se termine cinq minutes plus tard.

Lorsque vous avez terminé, cliquez sur **OK**.

Stratégies

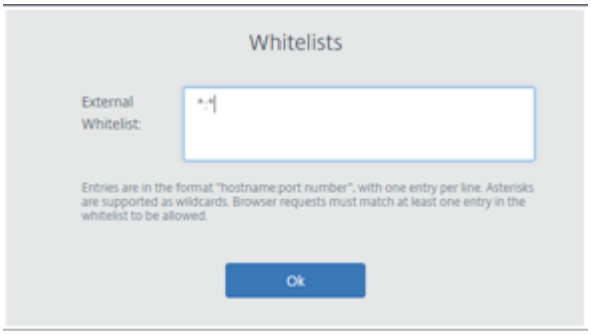


Les paramètres de la page des stratégies contrôlent ce qui suit :

- **Presse-papiers :** La désactivation du Presse-papiers empêche les opérations de copier-coller vers et depuis la session distante. (Le bouton Presse-papiers est supprimé de la barre d'outils de l'application Citrix Workspace.) Par défaut, ce paramètre est désactivé.
- **Impression :** Lorsque vous activez l'impression, la page Web distante peut être enregistrée au format PDF et transférée sur l'appareil de l'utilisateur. L'utilisateur peut ensuite appuyer sur Ctrl-P et sélectionner l'imprimante Citrix PDF. Par défaut, ce paramètre est désactivé.
- **Kiosque :** L'activation du mode non-kiosque restaure l'interface sur le navigateur distant. L'utilisateur peut alors accéder à la barre d'adresses et créer plusieurs onglets et fenêtres. (La désactivation du mode non-kiosque supprime les contrôles de navigation et la barre d'adresses du navigateur distant.) Par défaut, ce paramètre est activé (le mode non-kiosque est activé).

Lorsque vous avez terminé, cliquez sur **OK**.

Listes blanches



Utilisez la tâche **Listes blanches** pour limiter l'accès des utilisateurs uniquement aux URL présentes sur les listes blanches dans leur session Secure Browser publiée. Cette fonctionnalité est disponible pour les applications Web authentifiées externes.

Saisissez les entrées de liste blanche au format nom d'hôte:numéro de port. Spécifiez chaque entrée sur une nouvelle ligne. Les astérisques sont pris en charge en tant que caractères génériques. Les demandes de navigateur doivent correspondre à au moins une entrée dans la liste blanche.

Par exemple, pour définir `https://example.com` comme une URL sur liste blanche :

- `example.com:*` permet de se connecter à cette URL depuis n'importe quel port.
- `example.com:80` permet de se connecter à cette URL uniquement à partir du port 80.
- `*:*` permet d'accéder à cette URL depuis n'importe quel port et depuis n'importe quel lien vers d'autres URL et ports. Le format `.` permet d'accéder à toutes les applications Web externes à partir de l'application publiée. Ce format est le paramètre par défaut pour le champ de liste blanche d'URL d'applications Web externes.

Lorsque vous avez terminé, cliquez sur **OK**.

Des fonctionnalités avancées de filtrage Web sont disponibles via l'intégration au service Contrôle d'accès. En savoir plus sur Use case: Selective access to apps.

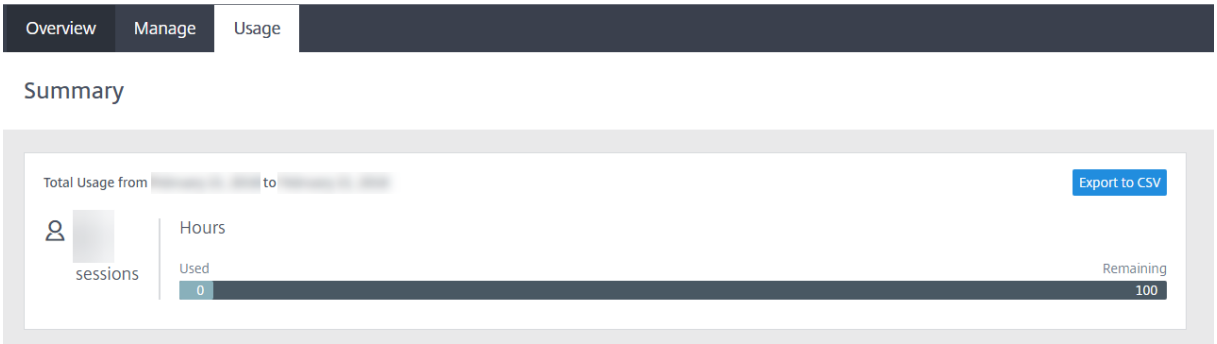
Modifier

Utilisez la tâche **Modifier** pour modifier le nom, l'URL de démarrage où la région d'un navigateur publié. Une fois terminé, cliquez sur **Publier**.

Supprimer

Utilisez la tâche **Supprimer** pour supprimer un navigateur sécurisé publié. Lorsque vous sélectionnez cette tâche, vous êtes invité à confirmer la suppression.

Surveiller l'utilisation



L'onglet **Utilisation** affiche le :

- Nombre de sessions initiées
- Nombre d'heures utilisées

Pour créer une feuille de calcul contenant des détails d'utilisation, cliquez sur **Exporter au format CSV** et sélectionnez une période.

Vue d'ensemble de la sécurité technique

Secure Browser Service est un produit SaaS administré et exploité par Citrix. Il permet d'accéder aux applications Web via un navigateur Web intermédiaire hébergé dans le cloud.

Service de cloud

Le Citrix Secure Browser Service se compose de navigateurs Web exécutés sur des VDA (Virtual Delivery Agents) et de la console de gestion qui est utilisée pour gérer et connecter les utilisateurs à ces VDA. Citrix Cloud gère le fonctionnement de ces composants, y compris la sécurité et l'application de correctifs aux systèmes d'exploitation, navigateurs Web et composants Citrix.

Lors de l'utilisation de Secure Browser Service, les navigateurs Web hébergés peuvent suivre l'historique de navigation de l'utilisateur et effectuer la mise en cache des requêtes HTTP. Citrix utilise des profils obligatoires et garantit que ces données sont supprimées à la fin de la session de navigation.

Secure Browser Service est accessible avec un navigateur Web compatible HTML5. Le service ne fournit aucun client téléchargeable. Tout le trafic entre le navigateur utilisé et le service cloud est crypté à l'aide du cryptage TLS standard. Secure Browser prend en charge TLS 1.0, 1.1 et 1.2.

Applications Web

Citrix Secure Browser Service est utilisé pour fournir des applications Web appartenant au client ou à un tiers. Le propriétaire de l'application Web est responsable de sa sécurité, y compris de l'application de correctifs au serveur Web et à l'application afin de les protéger contre toute vulnérabilité.

La sécurité du trafic entre Secure Browser et l'application Web dépend des paramètres de cryptage du serveur Web. Pour protéger ce trafic pendant son transit sur Internet, les administrateurs doivent publier des URL HTTPS.

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
- Documentation Citrix Cloud : Guide de déploiement sécurisé pour la plate-forme Citrix Cloud

Ressources supplémentaires

Pour les développeurs : Preview API for Secure Browser Service

Citrix Virtual Apps Essentials

November 7, 2018

Citrix Virtual Apps Essentials vous permet de distribuer des applications Windows et des bureaux hébergés partagés à partir de Microsoft Azure à tout utilisateur, sur n'importe quel périphérique. Ce service associe le service Citrix Virtual Apps, leader du marché, à la puissance et à la flexibilité de Microsoft Azure. Vous pouvez également utiliser Virtual Apps Essentials pour publier des bureaux Windows Server.

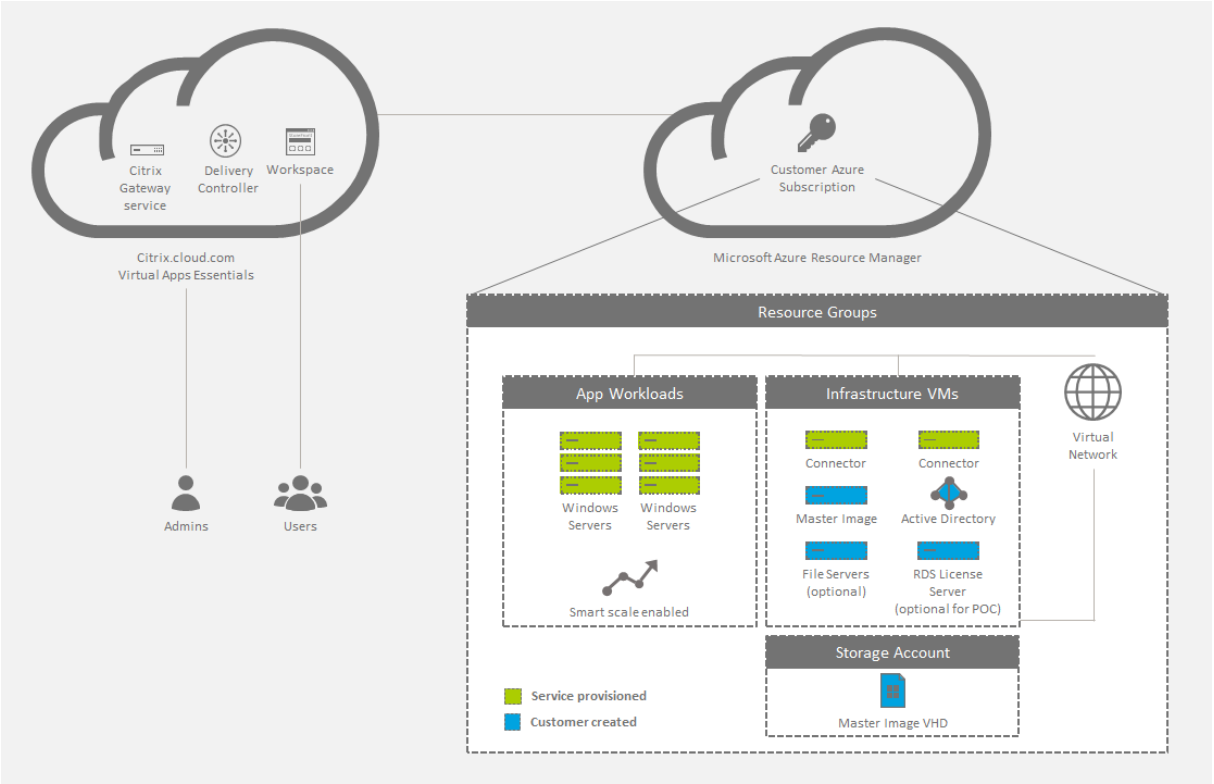
Les machines équipées d'un système d'exploitation serveur exécutent plusieurs sessions à partir d'une seule machine pour mettre à disposition plusieurs applications et bureaux vers de multiples utilisateurs connectés simultanément. Chaque utilisateur requiert une seule session depuis laquelle il peut exécuter toutes ses applications hébergées.

Le service est fourni via Citrix Cloud et vous aide à déployer facilement vos charges applicatives au sein de votre abonnement Azure. Lorsque les utilisateurs ouvrent des applications à partir de l'expérience d'espace de travail, l'application semble s'exécuter localement sur l'ordinateur de l'utilisateur. Les utilisateurs peuvent accéder à leurs applications en toute sécurité depuis n'importe quel appareil, n'importe où.

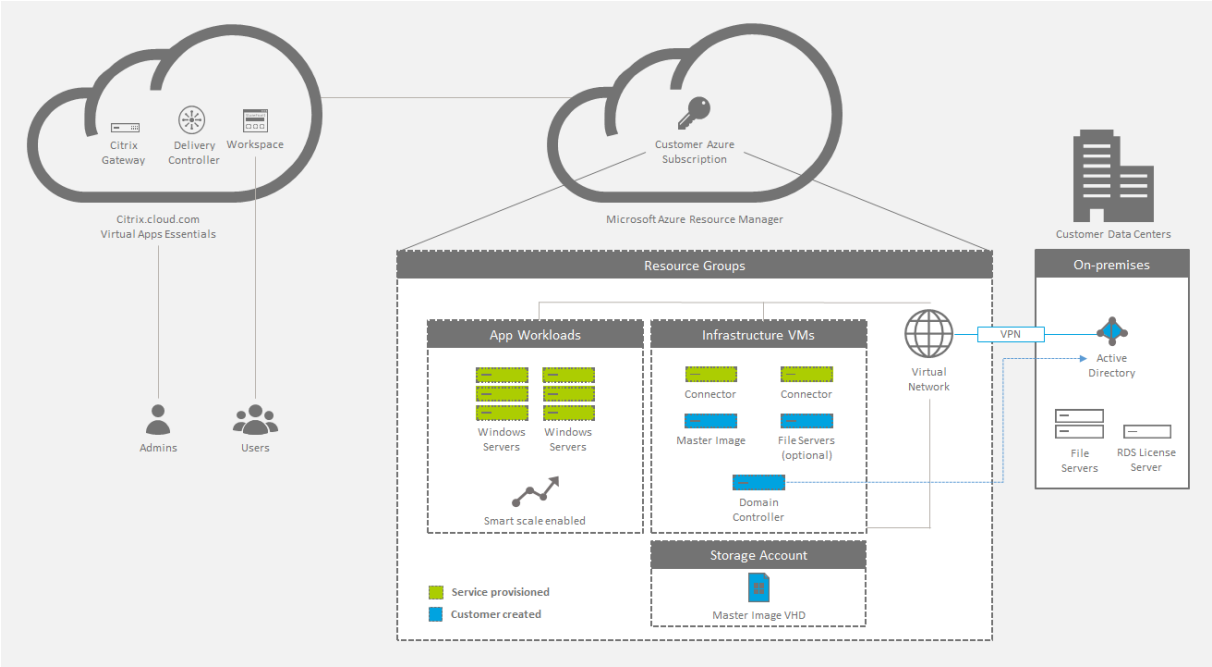
Virtual Apps Essentials inclut l'expérience d'espace de travail et le service Citrix Gateway, en plus de ses services de gestion de base. Vos charges de travail applicatives s'exécutent dans votre abonnement Azure.

Architecture de déploiement

Le diagramme suivant présente une vue d'ensemble de l'architecture d'un déploiement cloud de base de Virtual Apps Essentials :



Vous pouvez également permettre aux utilisateurs de se connecter à votre centre de données sur site. Les connexions entre le cloud Azure et votre centre de données sur site se font via une connexion VPN. Les utilisateurs se connectent via Virtual Apps Essentials à votre serveur de licences, vos serveurs de fichiers ou Active Directory via la connexion VPN.



Récapitulatif du déploiement

Suivez ces étapes pour déployer Citrix Virtual Apps Essentials :

- Achetez Citrix Virtual Apps Essentials sur Azure Marketplace.
- Préparez et associez votre abonnement Azure.
- Créez et chargez votre image principale.
- Déployez un catalogue, publiez des applications et des bureaux et affectez des abonnés.

Pour des instructions de déploiement détaillées, voir le Guide de déploiement de XenApp Essentials.

Nouveautés

- 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. Cet article utilise les noms suivants.

  - **Citrix Virtual Apps Essentials :** XenApp fait partie de notre stratégie espace de travail, qui consiste à regrouper de nombreux types d'applications à l'endroit choisi pour donner accès aux outils de travail. Composant d'un espace de travail sécurisé, unifié et contextuel, XenApp Essentials s'appelle désormais Citrix Virtual Apps Essentials.

  - **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.
  - **Citrix Gateway :** NetScaler Unified Gateway, qui permet un accès sécurisé et contextuel aux applications et aux données dont vous avez besoin pour travailler efficacement, s'appelle désormais Citrix Gateway.

  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, d'autres ressources (telles que des vidéos et des articles de blog) et d'autres sites (tels que Azure Marketplace) peuvent toujours contenir d'anciens noms. 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/.

- Mai 2018 : **Création d'images supplémentaires à partir de l'interface Virtual Apps Essentials**

  Après avoir créé une image de production à partir de l'interface Azure Resource Manager, vous pouvez créer des images supplémentaires via Azure, si nécessaire. Désormais, comme alternative à la création d'images supplémentaires via l'interface Azure, vous pouvez créer une nouvelle image principale à partir de l'interface Virtual Apps Essentials. Pour plus de détails, voir Préparer et télécharger une image principale.

- Mai 2018 : **Améliorations de l'écran Surveiller**

  L'écran Surveiller inclut désormais des informations sur l'utilisation des applications et des principaux utilisateurs. Pour de plus amples informations, consultez Surveiller le service.

Configuration système requise

Microsoft Azure

Citrix Virtual Apps Essentials prend en charge la configuration des machines uniquement via Azure Resource Manager.

Utilisez Azure Resource Manager pour :

- Déployer des ressources telles que des machines virtuelles, des comptes de stockage et un réseau virtuel.

- Créer et gérer le groupe de ressources (un conteneur pour les ressources que vous souhaitez gérer en tant que groupe).

Pour provisionner et déployer des ressources dans Microsoft Azure, vous avez besoin des éléments suivants :

- Un compte Azure.
- Un abonnement Azure Resource Manager.
- Un compte d'administrateur global Azure Active Directory dans l'annuaire associé à votre abonnement. Le compte d'utilisateur doit disposer de l'autorisation Propriétaire pour que l'abonnement Azure l'utilise pour le provisionnement des ressources. Pour plus d'informations sur la configuration d'un client Azure Active Directory, voir Comment obtenir un locataire Azure Active Directory.

Citrix Cloud

Virtual Apps Essentials est fourni via Citrix Cloud et nécessite un compte Citrix Cloud pour mener à bien le processus d'intégration. Vous pouvez créer un compte Citrix Cloud sur la page d'inscription à Citrix Cloud avant d'accéder à Azure Marketplace pour finaliser la transaction.

Le compte Citrix Cloud que vous utilisez ne peut pas être affilié à un service Citrix Virtual Apps and Desktops existant ou à un compte de service Citrix Virtual Desktops Essentials.

Console Virtual Apps Essentials

Vous pouvez ouvrir la console d'administration Virtual Apps Essentials dans les navigateurs Web suivants :

- Google Chrome
- Internet Explorer

Problèmes connus

Virtual Apps Essentials présente les problèmes connus suivants :

- 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.
- Lorsque vous configurez des utilisateurs pour un catalogue et sélectionnez un domaine, vous pouvez voir et choisir les utilisateurs du groupe Builtin\users.

- La création du catalogue échoue si la taille de machine virtuelle n'est pas disponible pour la région sélectionnée. Pour vérifier les machines virtuelles disponibles dans votre région, consultez le tableau Produits disponibles par région sur le site Web de Microsoft.
- Vous ne pouvez pas créer et publier simultanément plusieurs instances de la même application à partir du menu Démarrer. Par exemple, dans le menu Démarrer, vous publiez Internet Explorer. Ensuite, vous souhaitez publier une seconde instance d'Internet Explorer qui ouvre un site Web spécifique au démarrage. Pour ce faire, publiez la deuxième application en utilisant le chemin de l'application au lieu du menu Démarrer.
- Virtual Apps Essentials prend en charge l'association d'un abonnement utilisant un compte d'utilisateur Azure Active Directory. Virtual Apps Essentials ne prend pas en charge les comptes authentifiés Live.com.
- Les utilisateurs ne peuvent pas démarrer une application s'il existe une session RDP (Remote Desktop Protocol) sur le VDA. Ce comportement ne se produit que si la session RDP démarre sans qu'aucun autre utilisateur ne soit connecté au VDA.
- Vous ne pouvez pas entrer une adresse de serveur de licences plus longue que serveur.domaine.sousdomaine
- Si vous effectuez plusieurs mises à jour séquentielles de la gestion de la capacité, il est possible que les paramètres mis à jour ne se propagent pas correctement vers les VDA.
- Si vous utilisez une version autre que la version anglaise d'un navigateur Web, le texte affiché combine l'anglais et la langue du navigateur.

Comment acheter le service

> **Remarque :**
>
> Les informations contenues dans cette section sont également disponibles au format PDF. Ce contenu utilise les anciens noms de produits.

Achetez Citrix Virtual Apps Essentials directement auprès de Azure Marketplace, en utilisant votre compte Microsoft Azure. Citrix Virtual Apps Essentials requiert au moins 25 utilisateurs.

Le service est fourni via Citrix Cloud et nécessite un compte Citrix Cloud pour mener à bien le processus d'intégration. Voir Configuration requise > Citrix Cloud pour plus de détails.

Lorsque vous achetez Citrix Virtual Apps Essentials, veillez à entrer les informations correctes pour tous les détails, y compris les champs d'adresse, afin de garantir le traitement rapide de votre commande. Avant de configurer Virtual Apps Essentials, assurez-vous de bien procéder comme suit dans Azure Marketplace :

- Fournissez les informations de contact et les détails de votre entreprise.
- Fournissez vos informations de facturation.
- Créez votre abonnement.

Pour configurer le client et la tarification :

1. Dans **Sélectionnez un client**, sélectionnez le nom du client.
2. Sous **Tarifs**, dans **Nombre d'utilisateurs**, tapez le nombre d'utilisateurs ayant accès à Virtual Apps Essentials.
3. Sous **Prix par mois**, cochez la case d'approbation puis cliquez sur **Créer**.

La page récapitulative apparaît et affiche les détails de la ressource.

Une fois votre compte provisionné, cliquez sur **Gérer via Citrix Cloud**.

> **Important :**
>
> Attendez que Microsoft Azure provisionne votre service. Ne cliquez pas sur le lien **Gérer via Citrix Cloud** tant que le provisionnement n'est pas terminé. Ce processus peut prendre jusqu'à quatre heures.

Lorsque vous cliquez sur le lien, Citrix Cloud s'ouvre dans le navigateur Web et vous pouvez commencer le processus de configuration décrit ci-dessous.

Préparer votre abonnement Azure

Choisissez votre abonnement Azure comme connexion hôte pour vos VDA et les ressources associées. Ces ressources peuvent entraîner des frais en fonction de votre consommation.

> **Remarque :**
>
> Ce service nécessite que vous vous connectiez avec un compte Azure Active Directory. Virtual Apps Essentials ne prend pas en charge les autres types de compte, tels que live.com.

Pour préparer votre abonnement Azure, configurez les éléments suivants dans Azure Resource Manager :

1. Créez un groupe de ressources et fournissez les informations suivantes :
   - Nom du groupe de ressources
   - Nom de l'abonnement
   - Emplacement
2. Dans Azure Resource Manager, créez un réseau virtuel dans le groupe de ressources et attribuez un nom au réseau. Vous pouvez utiliser tous les autres paramètres par défaut. Vous créez un compte de stockage lorsque vous créez l'image principale.
3. Utilisez un contrôleur de domaine existant ou créez-en un. Si vous créez un contrôleur de domaine :
   a) Utilisez la machine virtuelle A3 Standard ou toute autre machine virtuelle Windows Server 2012 R2 de taille différente dans le groupe de ressources et le réseau virtuel. Cette machine virtuelle devient le contrôleur de domaine. Si vous envisagez de créer plusieurs con-

trôleurs de domaine, créez un groupe à haute disponibilité et placez tous les contrôleurs de domaine dans ce groupe.

b) Attribuez une adresse IP statique privée à la carte réseau de la machine virtuelle. Vous pouvez attribuer l'adresse dans le portail Azure. Pour plus d'informations, voir Configurer des adresses IP privées pour une machine virtuelle à l'aide du portail Azure sur le site Web de la documentation Microsoft.

c) [Facultatif] Associez un nouveau disque de données à la machine virtuelle pour stocker les utilisateurs et les groupes Active Directory, ainsi que tous les journaux Active Directory. Pour plus d'informations, voir Attachement d'un disque de données géré à une machine virtuelle Windows dans le portail Azure. Lorsque vous connectez le disque, sélectionnez toutes les options par défaut pour les paramètres.

d) Ajoutez l'adresse IP privée de la machine virtuelle du contrôleur de domaine au serveur DNS du réseau virtuel. Pour plus d'informations, voir Configurer un réseau virtuel (Classic) à l'aide d'un fichier config réseau.

e) Ajoutez un serveur DNS public en plus du serveur Microsoft DNS. Utilisez l'adresse IP 168.63.129.16 pour le deuxième serveur DNS.

f) Ajoutez le rôle Services de domaine Active Directory à la machine virtuelle du contrôleur de domaine. Une fois cette étape terminée, vous devez promouvoir la machine virtuelle du contrôleur de domaine en contrôleur de domaine et DNS.

g) Créez une forêt et ajoutez des utilisateurs Active Directory. Pour plus d'informations, voir Installer une nouvelle forêt Active Directory sur un réseau virtuel Azure.

Si vous préférez utiliser les services de domaine Azure Active Directory au lieu d'un contrôleur de domaine, Citrix vous recommande de consulter la documentation Azure Active Directory Domain Services for Beginners sur le site de Microsoft.

Lier votre abonnement Azure

Dans Citrix Cloud, liez Citrix Virtual Apps Essentials à votre abonnement Azure.

1. Connectez-vous à Citrix Cloud. Dans le menu en haut à gauche, sélectionnez **Mes services > Virtual Apps and Desktops**.
2. Sur l'onglet **Gérer**, cliquez sur **Abonnements Azure**.
3. Cliquez sur **Ajouter un abonnement**. Le portail Azure s'ouvre.
4. Connectez-vous à votre abonnement Azure avec vos informations d'identification Azure d'administrateur global.
5. Cliquez sur **Accepter** pour permettre à Virtual Apps Essentials d'accéder à votre compte Azure. Les abonnements disponibles sur votre compte sont répertoriés.
6. Sélectionnez l'abonnement que vous souhaitez utiliser, puis cliquez sur **Lien**.
7. Revenez à la console Virtual Apps Essentials pour voir l'abonnement à l'état lié.

Après avoir lié votre abonnement Azure à Virtual Apps Essentials, téléchargez votre image principale.

Préparer et télécharger une image principale

La création de catalogue utilise une image principale pour déployer des machines virtuelles contenant des applications et des bureaux. Cela peut être une image principale que vous préparez (avec applications et VDA installés) ou une image préparée par Citrix. Pour les déploiements en production, Citrix vous recommande de préparer et d'utiliser votre propre image principale. Les images préparées par Citrix sont uniquement destinées à des déploiements pilotes ou de tests.

La première image de production doit être préparée à partir de l'interface Azure Resource Manager. Plus tard, vous pourrez créer des images supplémentaires via Azure, si nécessaire.

Comme alternative à la création d'images supplémentaires via l'interface Azure, vous pouvez créer une nouvelle image principale à partir de l'interface Virtual Apps Essentials.

- Cette méthode utilise une image principale créée précédemment. Vous pouvez obtenir les paramètres réseau d'un catalogue existant ou les spécifier manuellement.
- Après avoir utilisé une image principale existante pour créer une nouvelle image, vous vous connectez à la nouvelle image et la personnalisez, en ajoutant ou en supprimant les applications copiées à partir du modèle. Le VDA est déjà installé, vous n'avez donc pas à le refaire.
- Cette méthode vous permet de rester avec le service Essentials. Vous n'avez pas besoin d'accéder à Azure pour créer la nouvelle image, puis de revenir au service Essentials pour importer l'image.

Par exemple, supposons que vous disposiez d'un catalogue nommé RH qui utilise une image principale contenant plusieurs applications RH. Récemment, une nouvelle application que vous souhaitez mettre à la disposition des utilisateurs du catalogue des ressources humaines vient de paraître. À l'aide de la fonctionnalité de création d'une image dans Virtual Apps Essentials, vous sélectionnez l'image principale actuelle en tant que modèle pour créer une nouvelle image principale. Vous sélectionnez également le catalogue RH afin que la nouvelle image principale utilise les mêmes paramètres de connexion réseau. Après la configuration initiale de l'image, installez la nouvelle application sur la nouvelle image. Après avoir effectué un test, mettez à jour le catalogue RH avec la nouvelle image principale, ce qui la met à la disposition des utilisateurs de ce catalogue. L'image principale RH d'origine est conservée dans la liste Mes images, au cas où elle serait requise ultérieurement.

Les sections suivantes décrivent comment préparer et télécharger une image principale via l'interface Azure. Pour plus d'informations sur la création d'une image à partir de Virtual Apps Essentials, voir Préparer une image principale dans Virtual Apps Essentials.

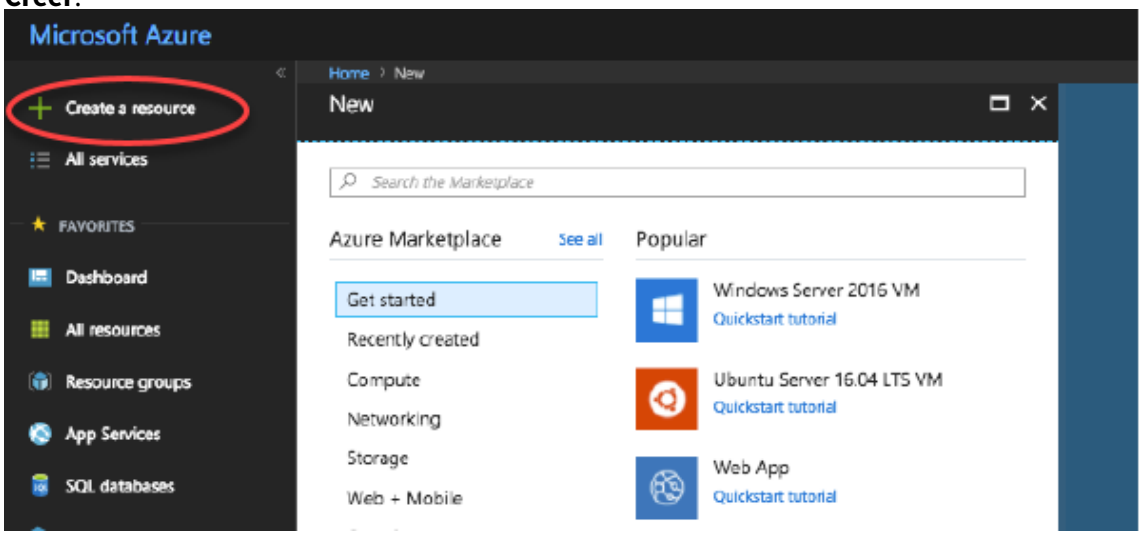
Résumé de la procédure

1. Préparez une VM image principale dans Azure ou Virtual Apps Essentials.
2. Installez les applications sur l'image principale.
3. Installez un VDA Citrix sur l'image principale.
4. Téléchargez l'image principale d'Azure Resource Manager vers Virtual Apps Essentials (si nécessaire).

Citrix recommande d'installer la dernière version actuelle (CR) du VDA serveur ou la dernière mise à jour cumulative (CU) de la version LTSR du VDA serveur 7.15 sur des machines Windows Server 2016 ou Windows Server 2012 R2. Si vous utilisez un ordinateur Windows Server 2008 R2, vous devez installer le VDA serveur 7.15 LTSR (dernière version CU recommandée) également disponible sur la page de téléchargement. Voir Stratégie de cycle de vie du service Citrix Cloud Virtual Apps and Desktops pour en savoir plus sur la stratégie de cycle de vie des VDA CR et LTSR.

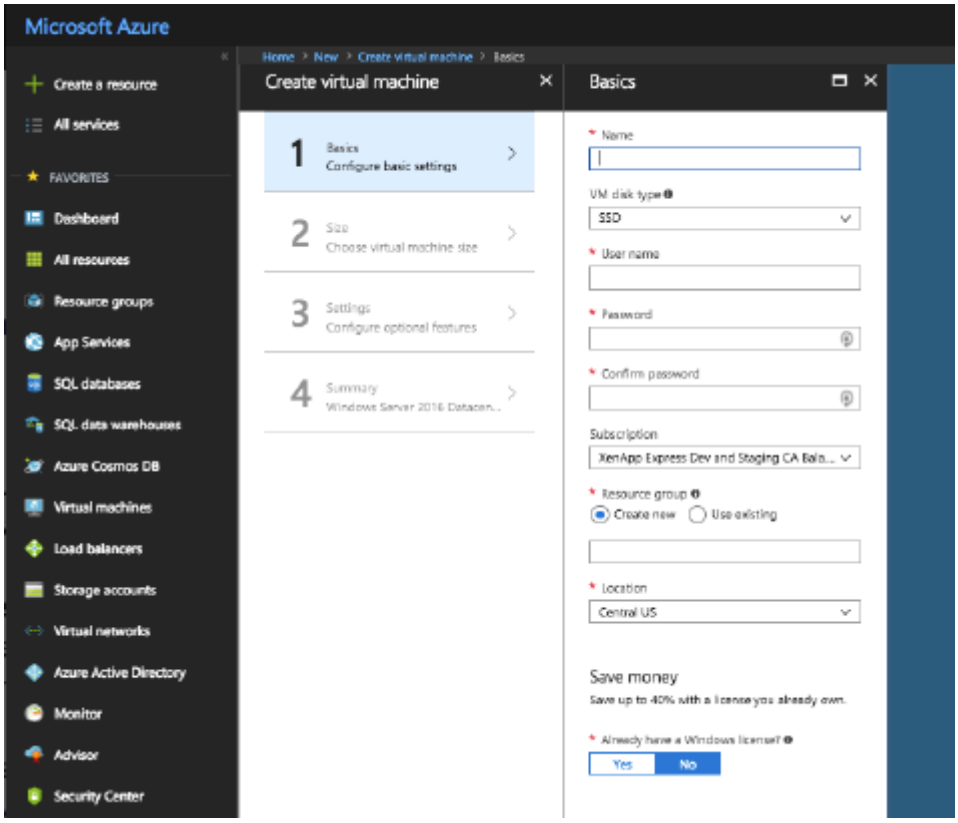
Créer une VM image principale dans Azure

1. Connectez-vous au portail Azure.
2. Cliquez sur **Créer une ressource** dans le volet de navigation. Sélectionnez ou recherchez une entrée Windows Server 2008 R2, Windows Server 2012 R2 ou Windows Server 2016. Cliquez sur **Créer**.



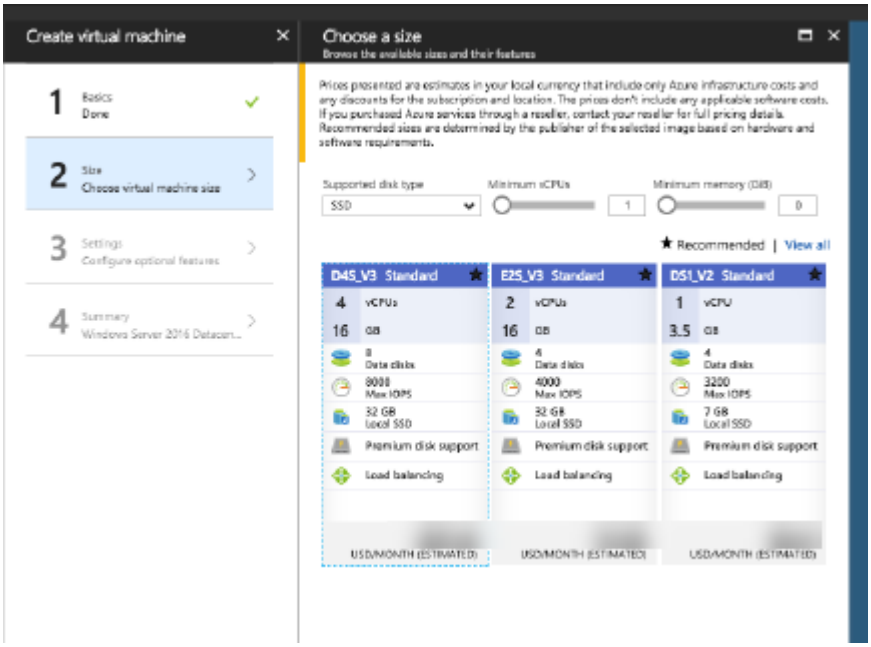
3. Sur la page **Créer une machine virtuelle**, dans le volet 1 De base :
   a) Entrez un nom pour la VM.
   b) Sélectionnez un type de disque de machine virtuelle (facultatif). Créez un disque standard. Les disques gérés ne sont pas pris en charge dans Virtual Apps Essentials.
   c) Entrez le nom d'utilisateur et le mot de passe locaux et confirmez le mot de passe.
   d) Sélectionnez votre abonnement.

e) Créez un nouveau groupe de ressources ou sélectionnez un groupe de ressources existant.
f) Sélectionnez l'emplacement.
g) Sélectionnez le groupe de ressources et l'emplacement.
h) Indiquez si vous utiliserez une licence Windows que vous possédez déjà.
i) Cliquez sur **OK**.



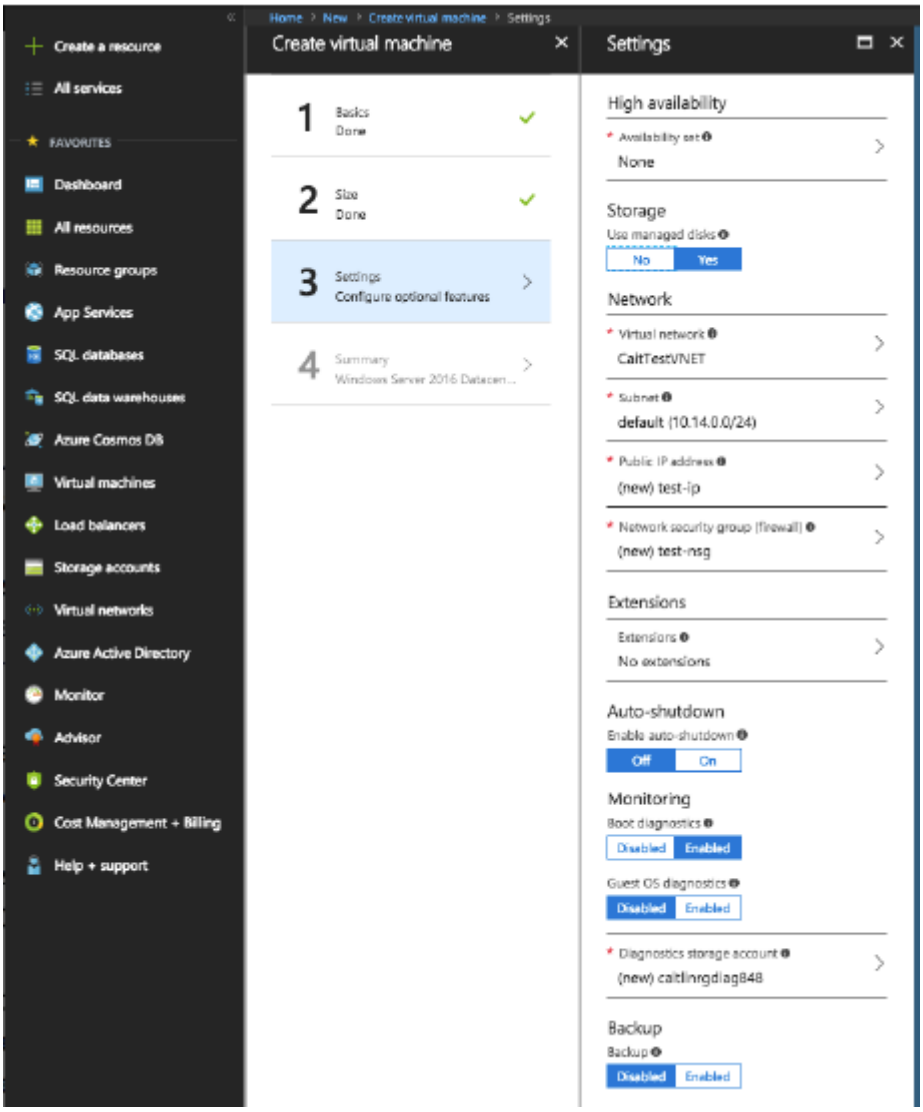
4. Sur la page **Créer une machine virtuelle**, dans le volet 2 Taille, choisissez la taille de la machine virtuelle :

a) Sélectionnez un type de machine virtuelle, puis indiquez le nombre minimal de vCPU et la mémoire minimale. Les choix recommandés sont affichés. Vous pouvez également afficher tous les choix.
b) Choisissez une taille, puis cliquez sur **Sélectionner**.



5. Sur la page **Créer une machine virtuelle**, dans le volet 3 Paramètres :

   a) Indiquez si vous souhaitez utiliser la haute disponibilité.
   b) Les disques gérés ne sont pas pris en charge avec ce service.
   c) Indiquez le nom du réseau virtuel, le sous-réseau, l'adresse IP publique et la sécurité du réseau.
   d) Vous pouvez aussi sélectionner les extensions.
   e) Activez ou désactivez l'arrêt automatique, la surveillance (diagnostics de démarrage, diagnostics de système d'exploitation invité, compte de stockage des diagnostics).
   f) Activez ou désactivez la sauvegarde.
   g) Cliquez sur **OK**.



6. Dans le volet 4 Résumé, cliquez sur **OK** pour commencer la création de la VM.

N'effectuez pas de Sysprep de l'image.

Installer des applications sur l'image principale

Sur la VM image principale que vous venez de créer, ajoutez les applications qui seront disponibles pour les utilisateurs lorsqu'ils se connecteront avec l'URL de l'espace de travail. (Plus tard, après avoir créé le catalogue qui utilise cette image principale, vous spécifierez exactement quelles applications seront disponibles pour les utilisateurs que vous spécifiez.)

1. Connectez-vous à la VM image principale après l'avoir créée et pendant son exécution.
2. Installez des applications.

Installer un VDA sur l'image principale

1. Connectez-vous à la VM image principale (si vous n'êtes pas déjà connecté).
2. Vous pouvez télécharger un VDA pour OS de serveur à l'aide du lien **Téléchargements** sur la barre de navigation de Citrix Cloud. Ou utilisez un navigateur pour accéder à la page de téléchargement du service Citrix Virtual Apps and Desktops. Téléchargez un VDA pour OS de serveur sur la VM. (Voir les instructions ci-dessus pour obtenir des informations sur la version de VDA.)
3. Lancez le programme d'installation de VDA en double-cliquant sur le fichier téléchargé. L'assistant d'installation démarre.
4. Sur la page **Environnement**, sélectionnez **Créer une image MCS principale**, puis cliquez sur **Suivant**.
5. Sur la page **Composants principaux**, cliquez sur **Suivant**.
6. Sur la page **Delivery Controller**, sélectionnez **Laisser Machine Creation Services effectuer ceci automatiquement**, puis cliquez sur **Suivant**.
7. Laissez les paramètres par défaut sur les pages **Composants supplémentaires**, **Fonctionnalités** et **Pare-feu**, sauf avis contraire de Citrix. Cliquez sur **Suivant** sur chaque page.
8. Sur la page **Résumé**, cliquez sur **Installer**. Les composants prérequis commencent à s'installer. Lorsque vous êtes invité à redémarrer, acceptez.
9. L'installation du VDA reprend automatiquement. L'installation des composants prérequis est terminée, puis les composants et les fonctionnalités sont installés. Sur la page **Call Home**, laissez le paramètre par défaut (sauf indication contraire de Citrix), puis cliquez sur **Suivant**.
10. Cliquez sur **Terminer**. La machine redémarre automatiquement.
11. Pour vous assurer que la configuration est correcte, lancez une ou plusieurs des applications que vous avez installées.
12. Arrêtez la VM. N'effectuez pas de Sysprep de l'image.

Télécharger l'image principale

Dans cette procédure, vous téléchargez l'image principale d'Azure Resource Manager vers Virtual Apps Essentials.

1. Si vous n'êtes pas déjà dans Citrix Cloud, connectez-vous. Dans le menu en haut à gauche, sélectionnez **Mes services > Virtual Apps and Desktops**.
2. Sur l'écran **Gérer**, cliquez sur **Images principales**.
3. Cliquez sur **Ajouter image principale**.
4. Sur la page **Ajouter une image**, spécifiez l'emplacement de l'image en sélectionnant l'abonnement, le groupe de ressources, le compte de stockage, le disque dur virtuel et la région.
5. Entrez un nom pour l'image principale.

6. Cliquez sur **Enregistrer**.

Le service vérifie l'image principale. Après vérification, l'image téléchargée apparaît sous **Images principales > Mes images**.

Conseil : au lieu de télécharger l'image principale avant la création du catalogue, vous pouvez importer une image principale à partir d'Azure Resource Manager lors de la création du catalogue.

Préparer une image principale dans Virtual Apps Essentials

Cette méthode utilise une image principale existante en tant que modèle (et éventuellement les détails de connexion d'un catalogue existant) pour créer une autre image principale. Vous pouvez ensuite personnaliser la nouvelle image principale. Cette procédure est entièrement réalisée via l'interface Virtual Apps Essentials.

1. Connectez-vous à Citrix Cloud si vous ne l'avez pas déjà fait. Dans le menu en haut à gauche, sélectionnez **Mes services > Virtual Apps and Desktops**.
2. Cliquez sur **Gérer**, puis sélectionnez l'onglet **Images principales**.
3. Cliquez sur **Créer image**.
4. Sur la page **Créer image**, dans le volet **Sélectionner une image**, sélectionnez une image principale. Spécifiez un nom pour votre nouvelle image. Cliquez sur **Suivant**.
5. Dans le volet **Spécifier les paramètres de la connectivité réseau**, vous pouvez utiliser les paramètres d'un catalogue existant ou les spécifier. Les paramètres sont les suivants : abonnement, réseau virtuel, région, sous-réseau, domaine et type d'instance de VM. (Si vous n'avez pas de catalogue, vous devez entrer les paramètres.)

   Si vous sélectionnez **Copier les paramètres d'un catalogue**, sélectionnez le catalogue. Les paramètres de connexion réseau s'affichent pour vous permettre de vérifier visuellement que vous souhaitez les utiliser avec votre nouvelle image principale. Entrez le nom d'utilisateur et le mot de passe de votre compte de service pour rejoindre le domaine. Cliquez sur **Enregistrer**.

   Si vous sélectionnez **Entrer de nouveaux paramètres**, sélectionnez des valeurs dans les champs de paramètres appropriés. Entrez le nom d'utilisateur et le mot de passe de votre compte de service pour rejoindre le domaine. Cliquez sur **Enregistrer**.
6. Cliquez sur **Démarrer provisioning**.
7. Lorsque la nouvelle image a été créée, elle apparaît dans la liste **Gérer > Images principales** avec l'état **Entrée obligatoire**. Cliquez sur **Connecter à la VM**. Un client RDP est téléchargé. Utilisez RDP pour vous connecter à la VM nouvellement créée. Personnalisez la nouvelle image en ajoutant ou en supprimant des applications et d'autres logiciels. Comme pour toutes les images principales, n'effectuez pas de Sysprep de l'image.

8. Lorsque vous avez fini de personnaliser votre nouvelle image, retournez à la page **Gérer > Images principales** et cliquez sur **Terminer** pour votre nouvelle image principale. La nouvelle image est ensuite envoyée au processus de vérification.
9. Une fois le processus de vérification terminé, la nouvelle image apparaît dans la liste **Mes images** avec l'état **Prêt**.

Plus tard, lorsque vous créez un catalogue et sélectionnez **Lier une image existante** sur la page **Choisir image principale**, la nouvelle image apparaît sous **Nom de l'image**.

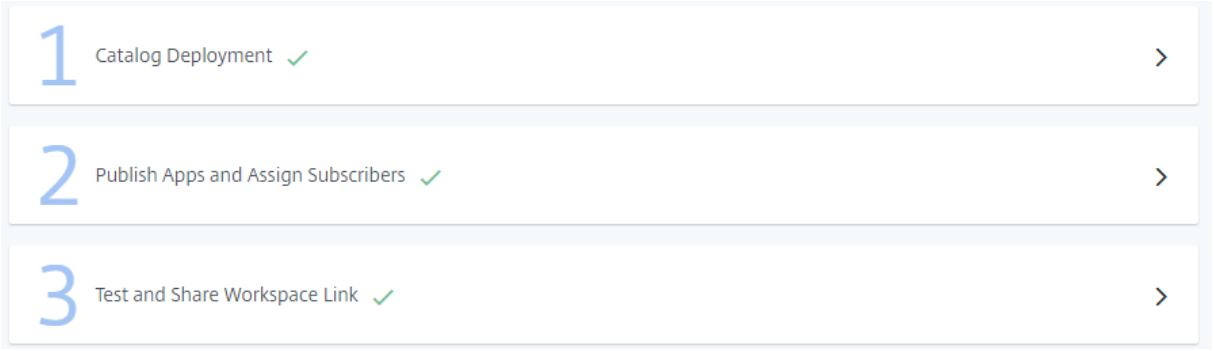
Déployer un catalogue, publier des applications et des bureaux et affecter des abonnés

Un catalogue répertorie les applications et les bureaux que vous choisissez de partager avec les utilisateurs sélectionnés.

Si vous avez déjà travaillé avec des produits de mise à disposition d'applications et de bureaux Citrix, un catalogue de ce service revient à associer un catalogue de machines et un groupe de mise à disposition. Toutefois, les flux de travail de création de catalogue de machines et de groupes de mise à disposition dans d'autres services ne sont pas disponibles dans ce service.

Le déploiement d'un catalogue et le partage d'applications avec des abonnés est un processus en plusieurs étapes.

- Créer un catalogue
- Publier des applications et affecter des abonnés à ce catalogue
- Tester et partager le lien d'espace de travail que vos abonnés utiliseront



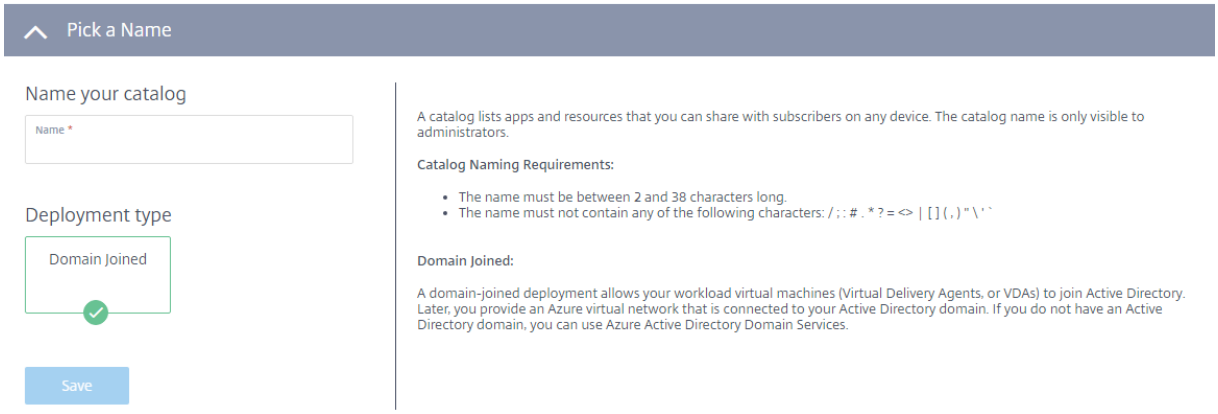
Créer un catalogue

Lors de la création d'un catalogue, veillez à disposer des informations d'identification du compte Azure Active Directory et du nom de votre abonnement.

1. Si vous n'êtes pas déjà dans Citrix Cloud, connectez-vous. Dans le menu en haut à gauche, sélectionnez **Mes services > Virtual Apps and Desktops**.

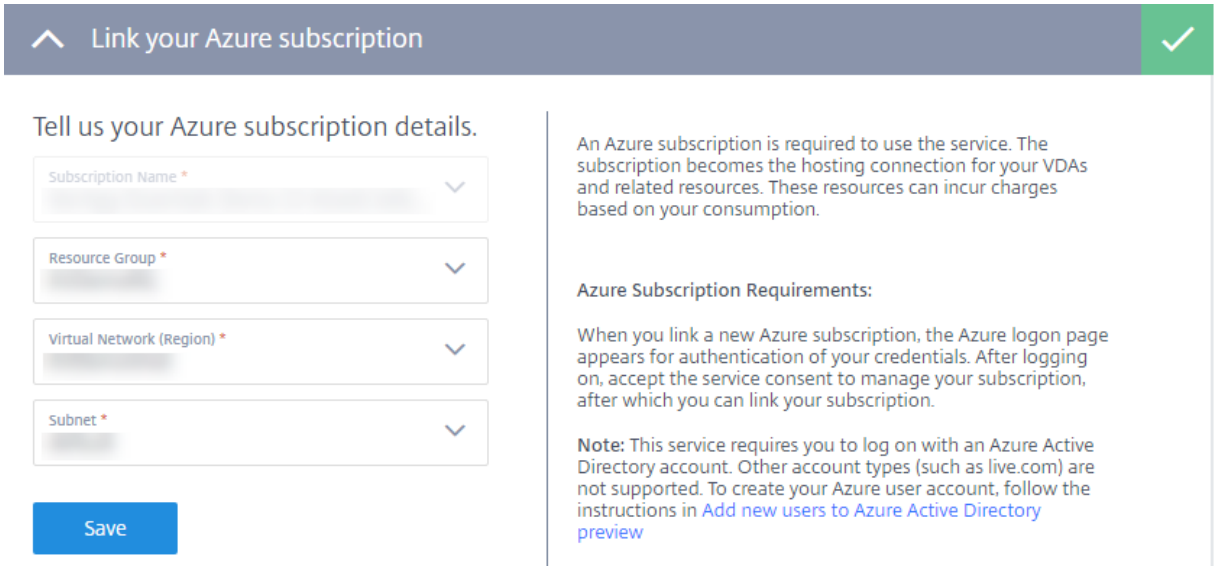
2. Sur l'onglet **Gérer**, cliquez sur **Catalogues** et sur **Ajouter un catalogue**.
3. Fournissez des informations dans les volets suivants. Cliquez sur **Enregistrer** quand vous avez fini avec chaque volet. Un signe d'avertissement apparaît dans l'en-tête du volet si des informations requises sont manquantes ou invalides. Une coche indique que l'information est complète.

Choisir un nom



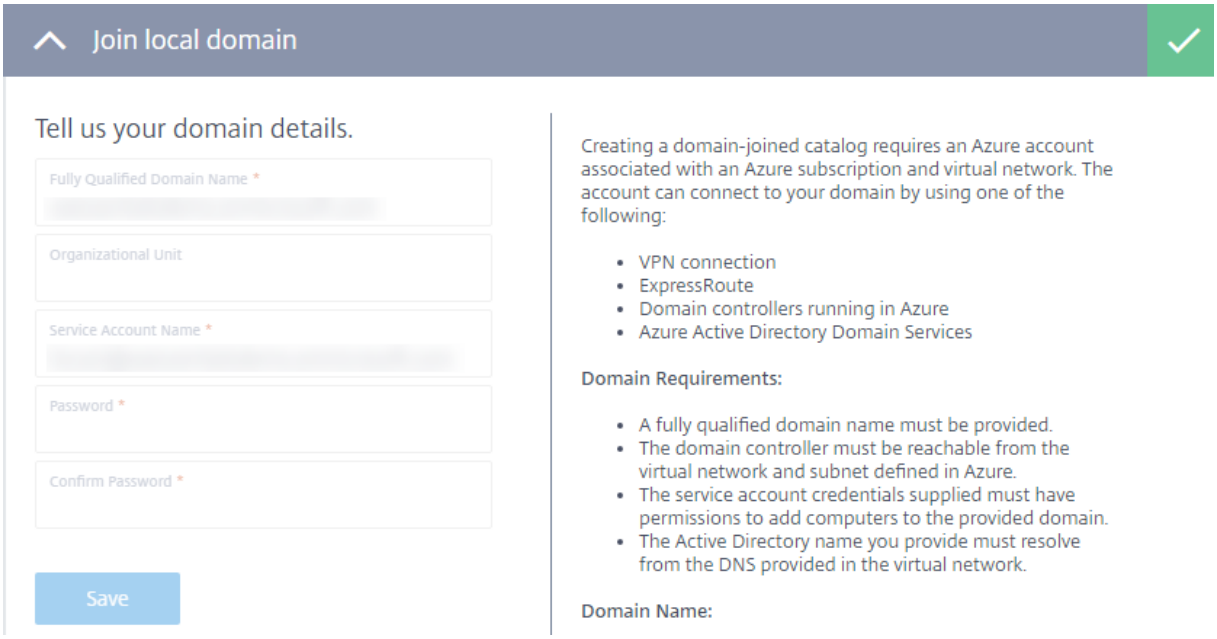
1. Tapez un nom de 2 à 38 caractères pour le catalogue. (Lettres et chiffres uniquement, pas de caractères spéciaux.) Ce nom n'est visible que pour les administrateurs.
2. Sélectionnez **Joint au domaine** si ce n'est pas déjà sélectionné. Un déploiement joint à un domaine permet aux VDA de rejoindre Active Directory. Par la suite, vous fournissez un réseau virtuel Azure connecté à votre domaine. Si vous ne disposez pas de domaine, vous pouvez utiliser les services de domaine Azure Active Directory.
3. Cliquez sur **Enregistrer**.

Lier votre abonnement Azure



1. Sélectionnez votre abonnement Azure. Lorsque vous liez un nouvel abonnement Azure, la page de connexion Azure apparaît pour l'authentification de vos informations d'identification Azure. Une fois connecté, acceptez le consentement du service pour gérer votre abonnement. Ensuite, vous pouvez lier un abonnement. Virtual Apps Essentials nécessite que vous vous connectiez avec un compte Azure Active Directory. Les autres types de compte (tels que live.com) ne sont pas pris en charge. Pour créer votre compte d'utilisateur Azure, voir Ajouter de nouveaux utilisateurs à Azure Active Directory.
2. Sélectionnez votre groupe de ressources, votre réseau virtuel (VNET) et votre sous-réseau. Le réseau virtuel détermine la région Azure où vos ressources sont déployées. Le sous-réseau doit pouvoir atteindre votre contrôleur de domaine.
3. Cliquez sur **Enregistrer**.

Rejoindre un domaine local



1. Entrez les informations du domaine :
   - **Nom de domaine complet :** entrez le nom de domaine. Le nom doit être résolu à partir du DNS fourni dans le réseau virtuel.
   - **Unité d'organisation :** (facultatif) assurez-vous qu'Active Directory contient l'unité d'organisation spécifiée. Si vous laissez ce champ vide, les machines sont placées dans le conteneur Ordinateurs par défaut.
   - **Nom du compte de service**, **Mot de passe** et **Confirmer le mot de passe** : entrez le nom d'utilisateur principal (UPN) du compte disposant des autorisations pour ajouter des machines au domaine. Ensuite, entrez et confirmez le mot de passe pour ce compte.
2. Cliquez sur **Enregistrer**.

Vous pouvez tester la connectivité via le réseau virtuel en créant une VM dans votre abonnement Azure. La VM doit appartenir au même groupe de ressources, au même réseau virtuel et au même sous-réseau que ceux utilisés pour déployer le catalogue. Assurez-vous que la VM peut se connecter à Internet. Assurez-vous également que vous pouvez accéder au domaine en joignant la VM au domaine. Vous pouvez effectuer un test en utilisant les mêmes informations d'identification que celles utilisées pour déployer ce catalogue.

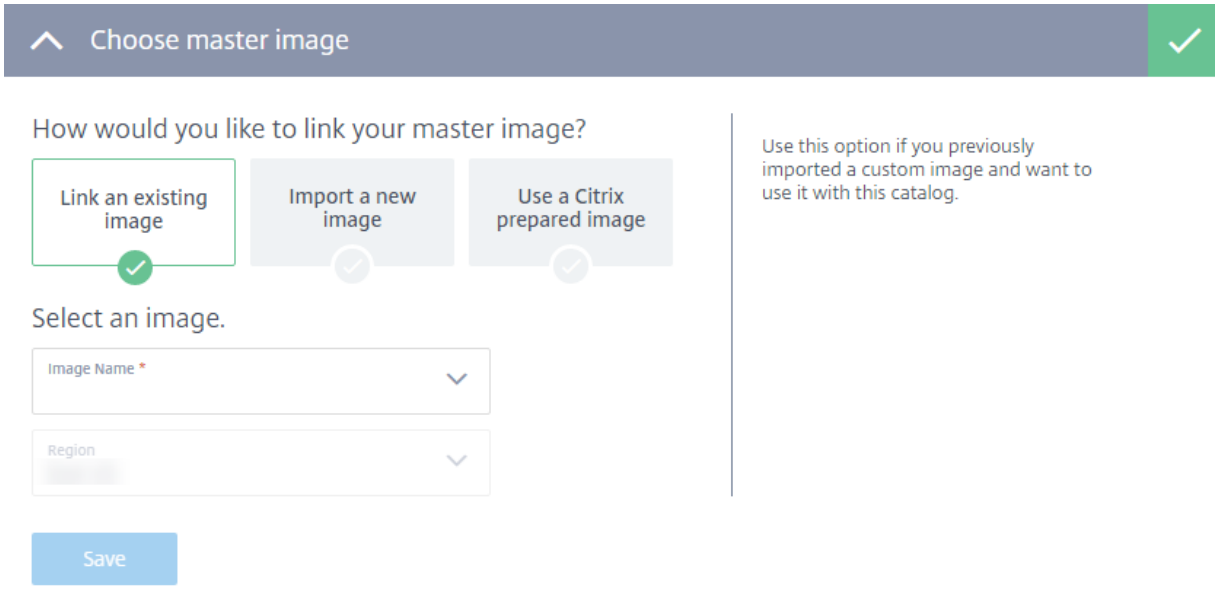
Se connecter à un emplacement de ressources

Chaque emplacement de ressources doit avoir au moins deux Cloud Connector qui communiquent avec Citrix Cloud. Le service gère automatiquement le déploiement de Cloud Connector lorsqu'un catalogue est déployé. Les deux VM Windows Server sont créés dans Azure Resource Manager, puis un Cloud Connector est installé automatiquement sur chaque serveur.

Si l'emplacement de ressources sélectionné est disponible, la connexion est établie automatiquement. Cliquez simplement sur **Enregistrer**.
Pour créer un emplacement de ressources, entrez un nom pour celui-ci.

- Pour créer des Cloud Connector dans un groupe de ressources Azure spécifique, cliquez sur **Modifier** à côté de **Groupe de ressources Azure** pour changer l'emplacement de ressources. Sinon, le service utilise le groupe de ressources que vous avez spécifié lorsque vous avez lié votre abonnement Azure.
- Pour placer les Cloud Connector dans une unité d'organisation distincte, cliquez sur **Modifier** à côté de **Unité d'organisation** pour changer l'unité. Sinon, Virtual Apps Essentials utilise le groupe de ressources que vous avez spécifié lorsque vous avez lié votre abonnement Azure.

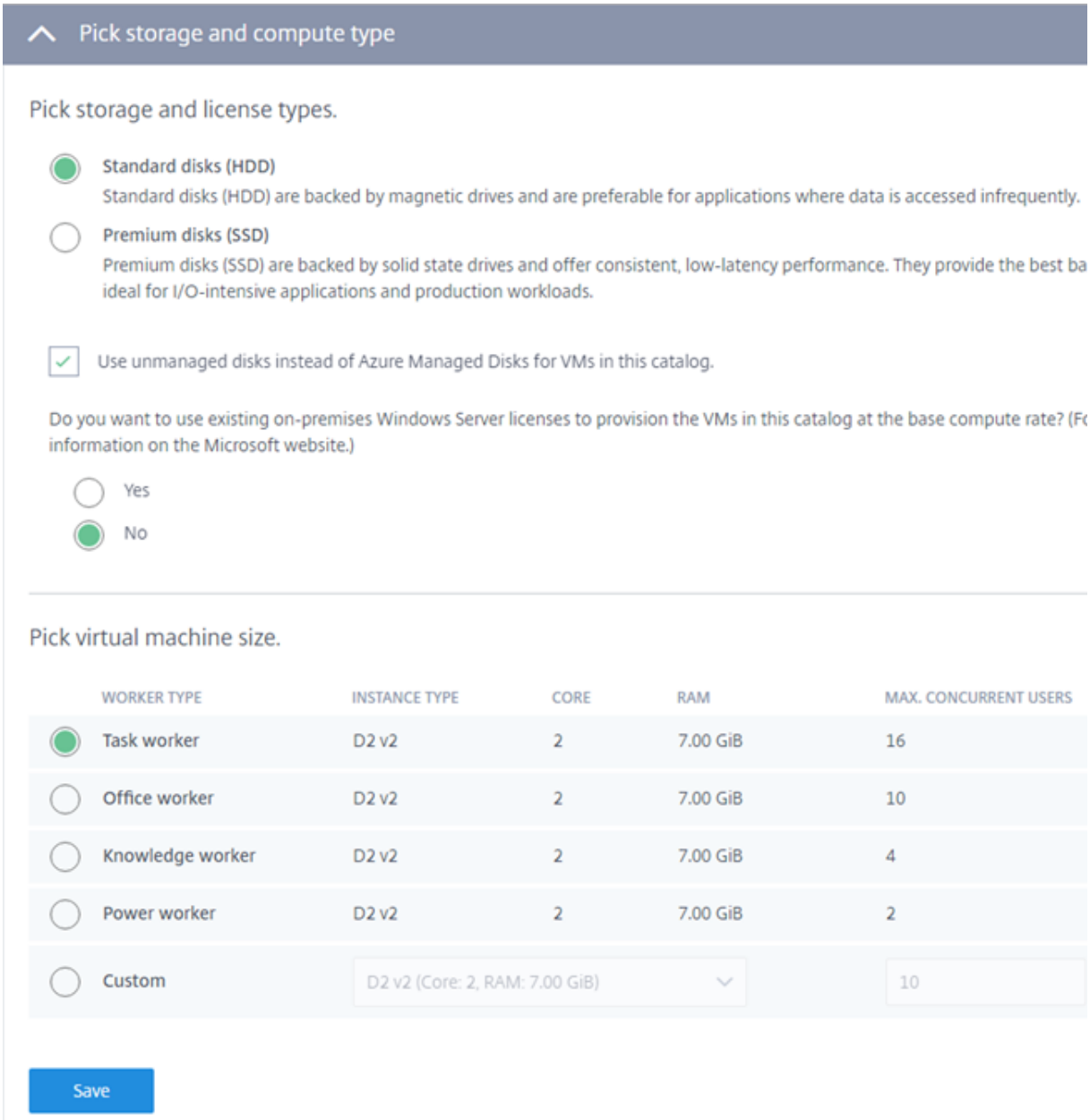
Choisir une image principale



1. Sélectionnez l'une des options suivantes :
    - **Lier une image existante :** utilisez cette option si vous avez importé précédemment une image personnalisée et souhaitez l'utiliser avec ce catalogue. Sélectionnez l'image et éventuellement une région.
    - **Importer une nouvelle image :** utilisez cette option si vous souhaitez utiliser une image personnalisée avec ce catalogue, mais que vous ne l'avez pas encore importée. Sélectionnez l'abonnement, le groupe de ressources, le compte de stockage et le disque dur virtuel. Entrez un nom convivial pour l'image.
    - **Utiliser une image préparée par Citrix :** utilisez cette option pour tester le service sans utiliser votre propre image personnalisée. Ces images ne conviennent qu'aux environnements de démonstration et ne sont pas recommandées pour la production. Sélectionnez une image préparée.

2. Cliquez sur **Enregistrer**.

Choisir le type de stockage et de calcul



1. Configurez les éléments suivants :
   - **Disques standard ou premium :** les disques standard (HDD) reposent sur des disques magnétiques. Ils sont préférables pour les applications où l'accès aux données est peu fréquent. Les disques Premium (SDD) reposent sur des disques SSD. Ils sont recommandés pour les applications intensives en E/S.
   - **Utiliser Azure Managed Disks ou des disques non gérés :** par défaut la case à cocher

Utiliser des disques non gérés plutôt que Azure Managed Disks pour les VM de ce catalogue est sélectionnée en raison de problèmes connus intermittents. Décochez la case si vous souhaitez utiliser Azure Managed Disks pour vos machines VDA. Vous trouverez des informations sur les disques gérés Azure à l'adresse https://docs.microsoft.com/fr-fr/azure/virtual-machines/windows/managed-disks-overview.

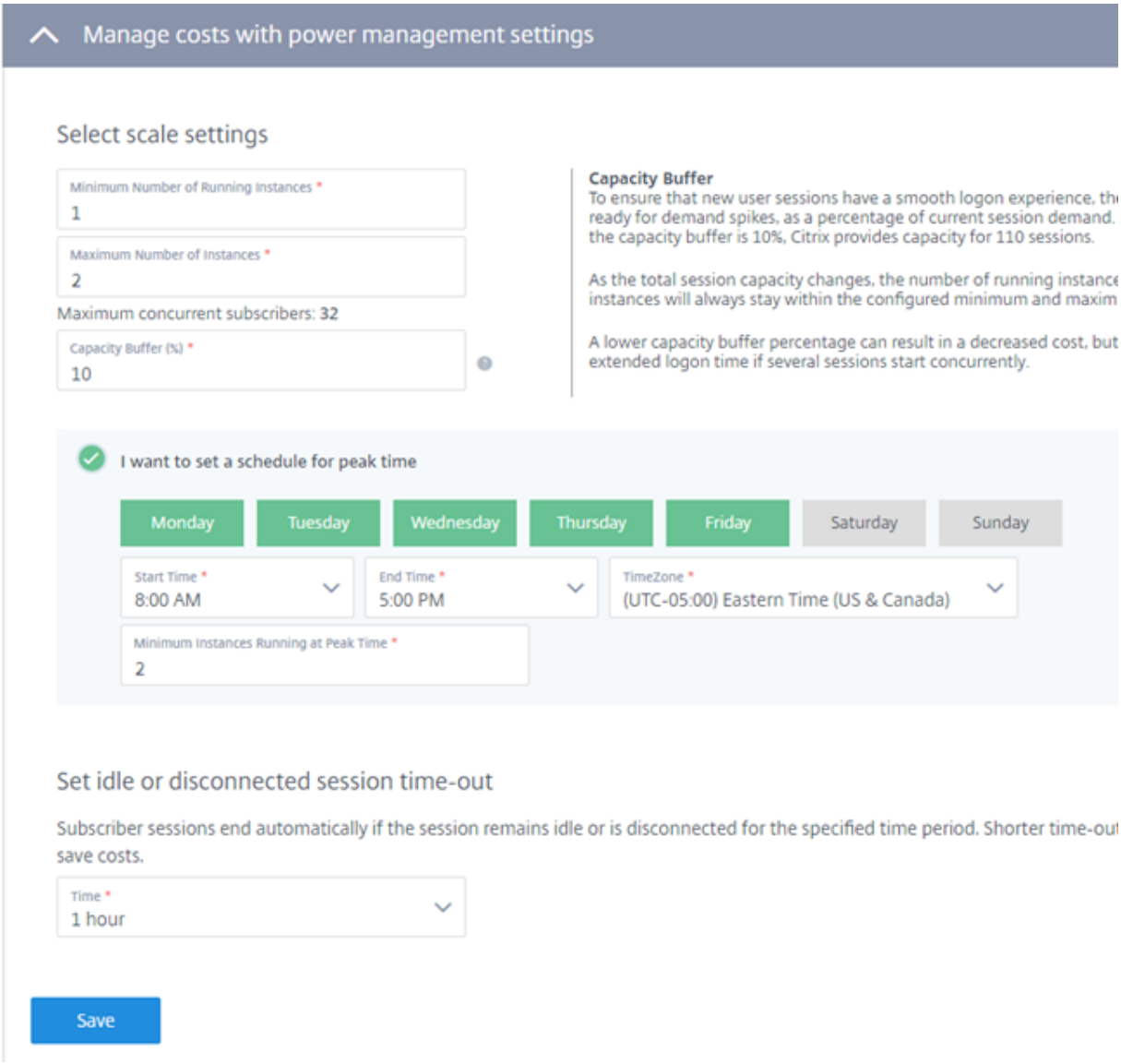
- **Azure Hybrid Use Benefit :** indiquez si vous souhaitez utiliser des licences Windows Server locales existantes. Si cette fonction est activée et que vous utilisez les images Windows Server locales existantes, Azure Hybrid Use Benefits (HUB) est utilisé. Plus de détails sont disponibles sur https://azure.microsoft.com/pricing/hybrid-use-benefit/.

  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. Voir le blog de Microsoft How can I use the Hybrid Use Benefit in Azure.

- **Choisissez la taille de la machine virtuelle :** sélectionnez un rôle de travailleur (par exemple, tâche, bureau, savoir, avancé). Le rôle de travailleur définit les ressources utilisées. Lorsque vous spécifiez un rôle de travailleur, le service détermine le chargement par instance approprié. Vous pouvez sélectionner une option ou créer votre propre option personnalisée.

2. Cliquez sur **Enregistrer**.

Gérer les coûts avec les paramètres de gestion de l'alimentation



1. Entrez les informations suivantes :
    - **Paramètres d'échelle :**
        - **Nombre minimal d'instances exécutées :** le service garantit que ce nombre de VM sont sous tension en permanence.
        - **Nombre maximal d'instances exécutées :** le service ne dépasse pas ce nombre de VM.
        - **Nombre maximal d'utilisateurs simultanés :** le service n'autorise pas les utilisateurs simultanés au-delà de cette limite.
        - **Mémoire tampon de capacité :** permet à des sessions supplémentaires d'être prêtes pour les pics de demande, en pourcentage de la demande de session actuelle. Par exemple, si 100 sessions sont actives et que la mémoire tampon de capacité est de 10

%, le service fournit une capacité de 110 sessions.

À mesure que la capacité totale de la session change, le nombre d'instances en cours d'exécution pour ce catalogue augmente ou diminue. Le nombre d'instances en cours d'exécution reste toujours dans les valeurs minimale et maximale configurées. Un pourcentage de mémoire tampon de capacité plus faible peut permettre de réduire les coûts. Toutefois, ds ce cas, certaines sessions peuvent également avoir une durée de connexion étendue si plusieurs sessions démarrent simultanément.

- **Horaire pour les heures de pointe :** sélectionnez cette option si vous souhaitez qu'un nombre différent de VM s'exécutent pendant les heures de pointe et pendant les heures creuses. Sélectionnez les jours de la semaine pour les heures de pointe, les heures de début et de fin et le fuseau horaire. Spécifiez le nombre minimal d'instances exécutées pendant les heures de pointe.
- **Délai d'inactivité ou de déconnexion de la session :** définissez le délai de déconnexion de la session. Les sessions utilisateur se terminent automatiquement si la session reste inactive ou est déconnectée pendant la période spécifiée. Des valeurs de délai plus courtes permettent aux VDA non utilisés de s'éteindre, réalisant ainsi des économies.

2. Cliquez sur **Enregistrer**.

Déployer le catalogue

Une fois la configuration terminée, cliquez sur Démarrer le déploiement pour lancer la création du catalogue. La création d'un catalogue peut prendre 1 à 2 heures (ou plus, si vous avez spécifié un grand nombre de VM).

Lors de la création d'un catalogue :

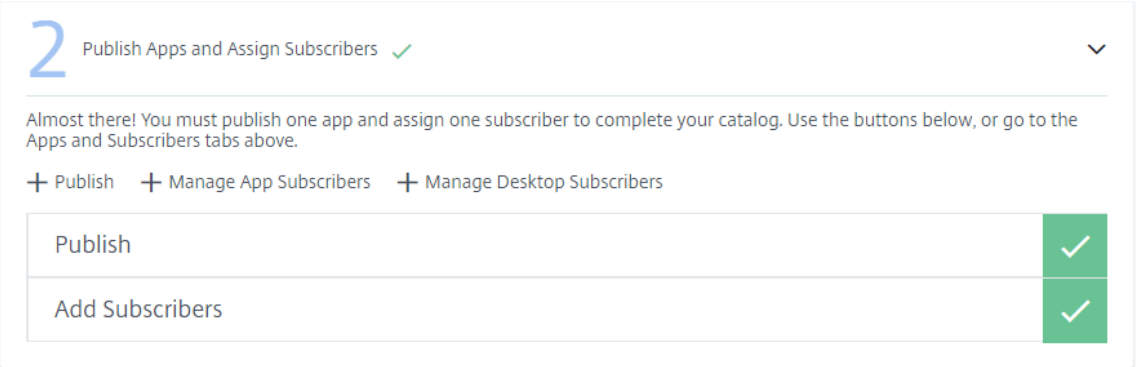
- Un groupe de ressources et un compte de stockage dans ce groupe de ressources pour les machines de charge de travail sont créés automatiquement dans Azure.
- Les VM sont nommées Xenappxx-xx-yyy, où xx est dérivé d'un facteur environnemental et yy est un nombre ordinal.

Publier des applications et affecter des abonnés à un catalogue

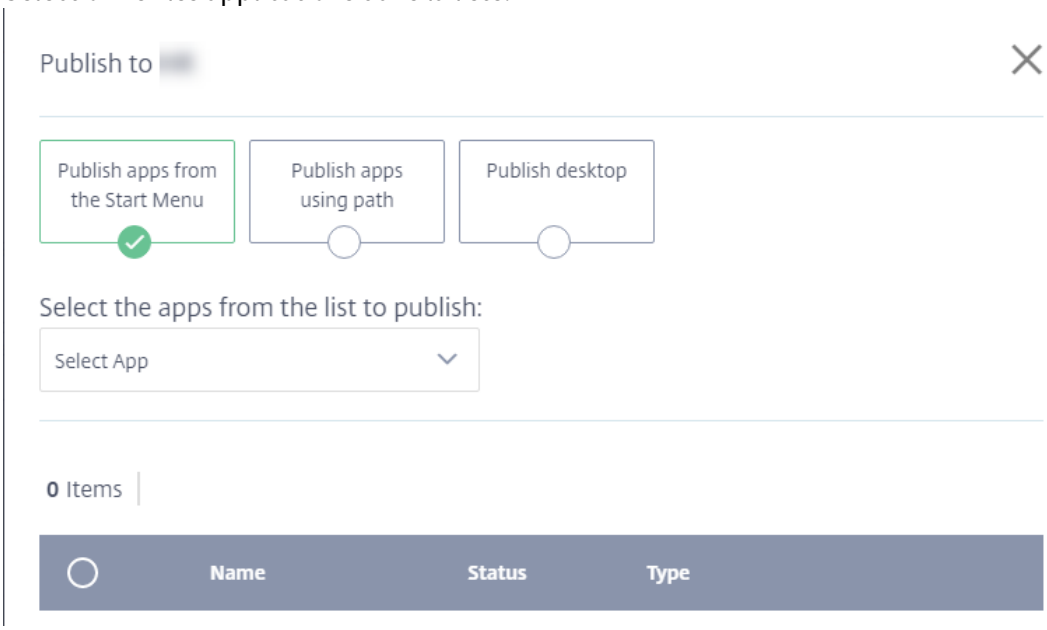
Pour finaliser le catalogue après son déploiement, vous devez publier une application ou un bureau et attribuer au moins un abonné.

L'image que vous avez utilisée pour créer le catalogue inclut les applications (ou le bureau) que vous pouvez publier. Vous pouvez sélectionner des applications dans le menu Démarrer ou spécifier un chemin de répertoire sur la machine.

1. Si vous n'êtes pas déjà dans Citrix Cloud, connectez-vous. Dans le menu en haut à gauche, sélectionnez **Mes services > Virtual Apps and Desktops**.
2. Sur l'onglet **Gérer**, cliquez sur **Catalogues**.
3. Dans le menu de points de suspension (…) du catalogue créé, sélectionnez **Gérer le catalogue**.
4. Sélectionnez **Publier des applications et affecter des abonnés**. La page suivante s'affiche.

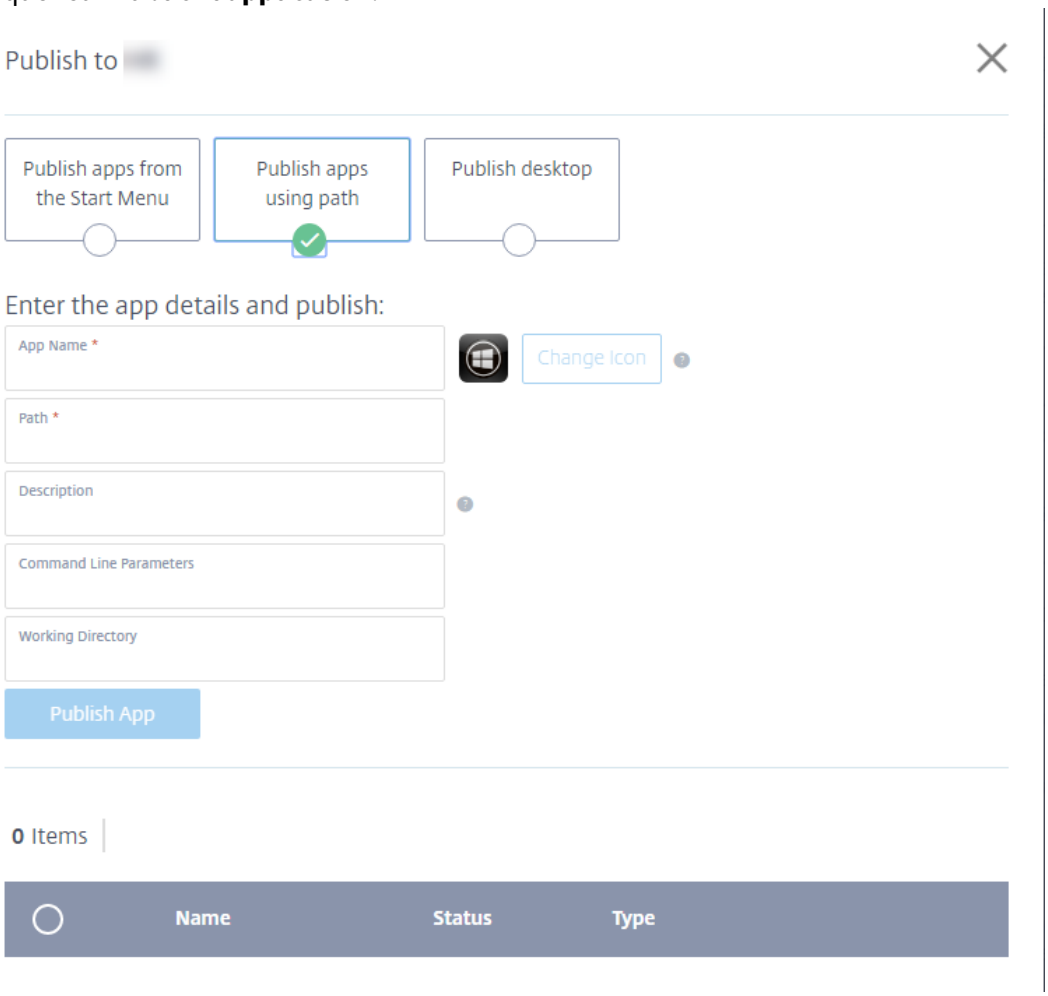


5. Dans la boîte de dialogue **Publier des applications et attribuer des abonnés**, cliquez sur **Publier**. La page Publier dans nom-catalogue contient trois choix. Sélectionnez-en au moins un. Vous pouvez éventuellement en choisir un autre (par exemple, pour publier à la fois des applications et des bureaux à l'aide de ce catalogue).
6. Pour publier des applications situées dans le menu Démarrer :
   a) Sélectionnez **Publier applications depuis le menu Démarrer**.
   b) Sélectionnez les applications dans la liste.



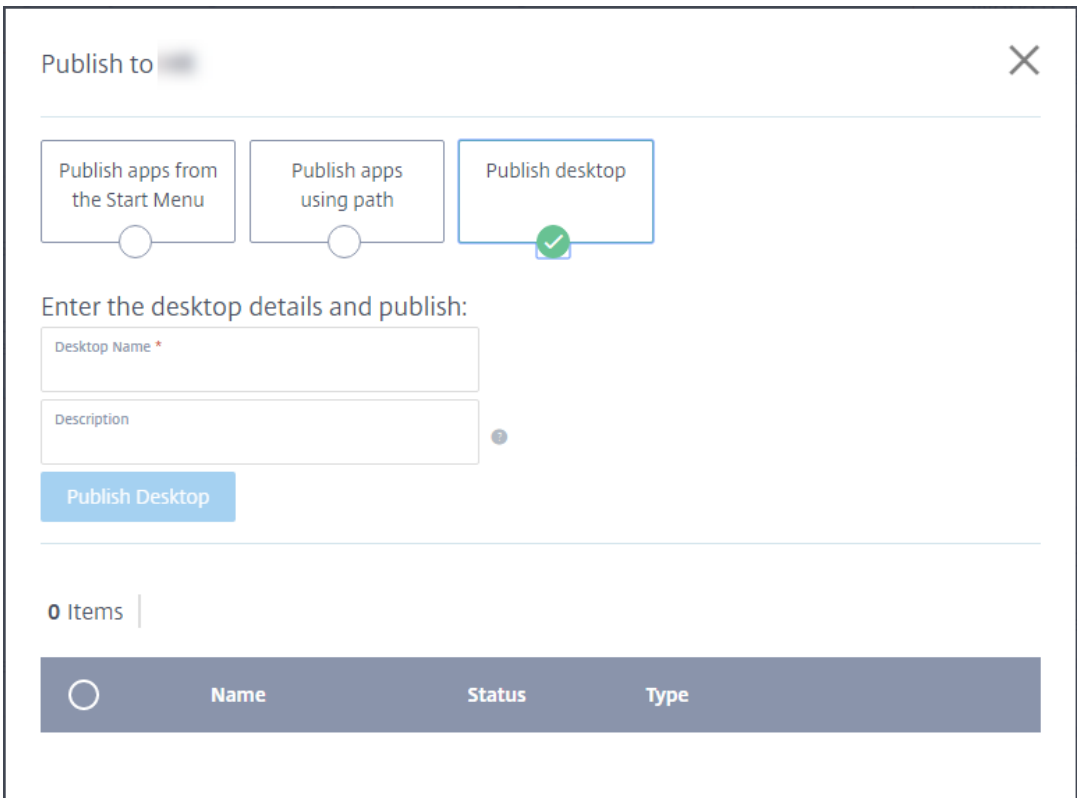
7. Pour publier des applications en spécifiant leur emplacement et d'autres informations :
   a) Sélectionnez **Publier applications à l'aide du chemin**.

b) Entrez le nom et le chemin de chaque application (par exemple, c:\Windows\system1\app.exe).
c) Entrez éventuellement une description qui apparaîtra dans l'espace de travail de l'utilisateur, les paramètres de ligne de commande et le répertoire de travail.
d) Pour changer l'icône qui représente l'application publiée, cliquez sur **Changer d'icône**, puis naviguez jusqu'à l'emplacement de l'icône. Un message apparaît si l'icône sélectionnée ne peut pas être extraite. Dans ce cas, vous pouvez réessayer ou continuer à utiliser l'icône existante.
e) Cliquez sur **Publier l'application**.



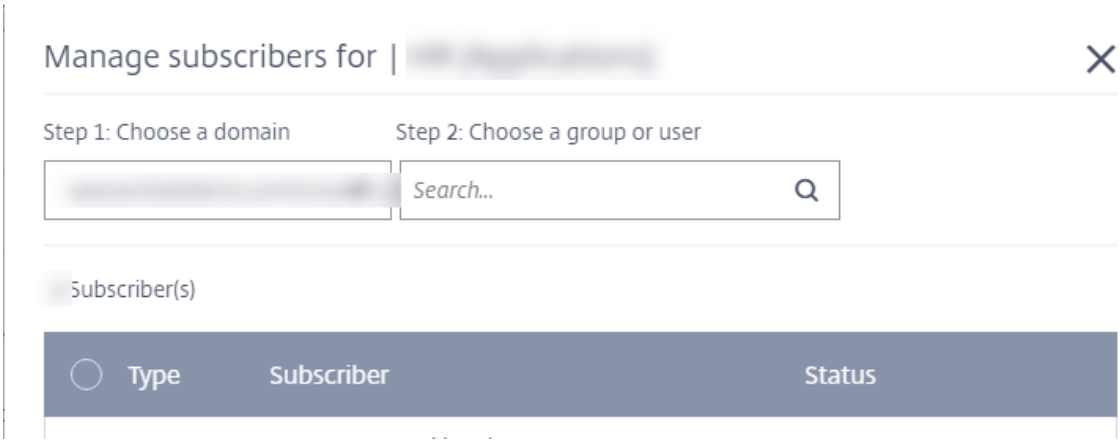
8. Pour publier un bureau :

a) Sélectionnez **Publier le bureau**.
b) Entrez le nom du bureau.
c) Entrez éventuellement une description qui apparaîtra dans l'espace de travail de l'utilisateur.
d) Cliquez sur **Publier le bureau**.



Une fois les applications ou les bureaux ajoutés, ils apparaissent dans la liste sous les sélecteurs. Pour supprimer une application ou un bureau que vous avez ajouté, sélectionnez le bouton situé à gauche de l'entrée (ou cliquez sur l'icône de la corbeille en regard de l'entrée), puis cliquez sur **Supprimer**. Plus tard, si vous souhaitez annuler la publication d'une application ou d'un bureau, sélectionnez le bouton situé à gauche de l'entrée, puis cliquez sur **Annuler la publication**.

9. Dans la boîte de dialogue **Publier des applications et attribuer des abonnés**, cliquez soit sur **Gérer les abonnés aux applications** soit sur **Gérer les abonnés aux bureaux**.



10. Sélectionnez un domaine, puis recherchez un utilisateur ou un groupe d'utilisateurs.

11. Les affectations d'utilisateurs pour les applications et les bureaux sont séparées. Pour attribuer à un utilisateur un accès aux applications et aux bureaux, attribuez à cet utilisateur **Gérer les abonnés aux applications** et avec **Gérer les abonnés aux bureaux**.

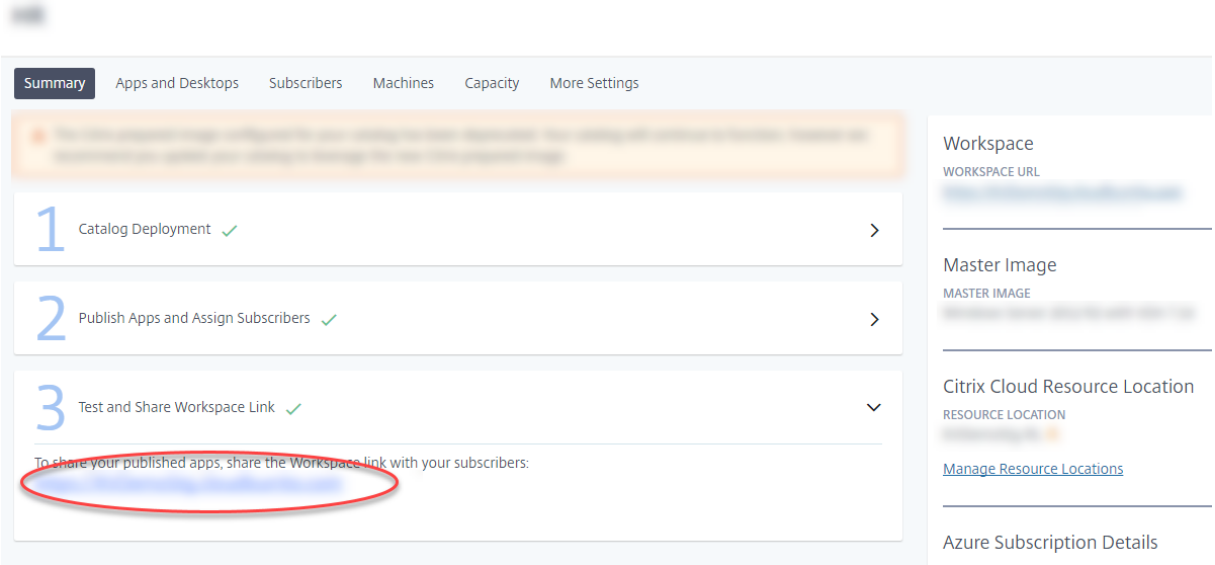
    Une fois que vous avez ajouté un utilisateur ou un groupe, il apparaît dans la liste sous les sélecteurs. Pour supprimer un utilisateur ou un groupe sélectionné, cliquez sur l'icône de la corbeille en regard de l'entrée, puis cliquez sur **Supprimer**. Plus tard, si vous souhaitez supprimer des utilisateurs, sélectionnez le bouton situé à gauche de l'entrée, puis cliquez sur **Supprimer la sélection**.

Tester et partager le lien de l'espace de travail

Une fois que vous avez déployé un catalogue, publié des applications et affecté des abonnés, vous recevez le lien que vos abonnés utilisent pour accéder aux applications et aux bureaux que vous avez publiés pour eux.

1. Si vous n'êtes pas déjà dans Citrix Cloud, connectez-vous. Dans le menu en haut à gauche, sélectionnez **Mes services > Virtual Apps and Desktops**.
2. Sur l'onglet **Gérer**, cliquez sur **Catalogues**.
3. Dans le menu de points de suspension (…) du catalogue, sélectionnez **Gérer le catalogue**.
4. Sélectionnez **Tester et partager le lien de l'espace de travail**.

Dans le graphique suivant, le lien de l'espace de travail apparaît dans la zone entourée. Partagez ce lien avec vos abonnés. La partie droite de la page répertorie l'URL de l'espace de travail, ainsi que des informations sur l'image principale du catalogue, l'emplacement de ressources, l'abonnement Azure et le domaine.



Voir Expérience d'espace de travail pour plus d'informations.

Mettre à jour les images principales et les catalogues

Pour mettre à jour ou ajouter des applications, mettez à jour la machine virtuelle sur laquelle vous avez créé l'image principale du catalogue.

Mettre à jour l'image principale

1. Mettez la VM de l'image principale sous tension. La mise sous tension de la machine n'affecte pas l'image principale installée dans Azure Resource Manager.
2. Installez les mises à jour ou les applications sur la VM.
3. Arrêtez la VM.
4. Dans la console Virtual Apps Essentials, ajoutez la nouvelle image qui inclut le chemin d'accès à l'image VHD de la VM.

Mettre à jour un catalogue avec une nouvelle image

1. Si vous n'êtes pas déjà dans Citrix Cloud, connectez-vous. Dans le menu en haut à gauche, sélectionnez **Mes services > Virtual Apps and Desktops**.
2. Sur l'onglet **Gérer**, cliquez sur **Catalogues**.
3. Cliquez sur le menu de points de suspension pour le catalogue, puis cliquez sur **Mettre à jour l'image du catalogue**.
4. Sélectionnez soit **Lier une image existante** soit **Importer une nouvelle image**. Entrez les informations appropriées pour votre choix.
5. Dans **Temps jusqu'à déconnexion automatique**, choisissez le délai avant la fin de la session.
6. Cliquez sur **Mettre à jour**.

Lorsque vous démarrez la mise à jour du catalogue, les utilisateurs peuvent continuer à travailler jusqu'à la fin du traitement initial. Ensuite, les utilisateurs reçoivent un message d'avertissement les invitant à enregistrer leur travail et à fermer les applications. Après la fermeture de toutes les sessions actives sur le VDA, la mise à jour se termine sur ce VDA. Si les utilisateurs ne se déconnectent pas dans le délai imparti, la session se ferme automatiquement.

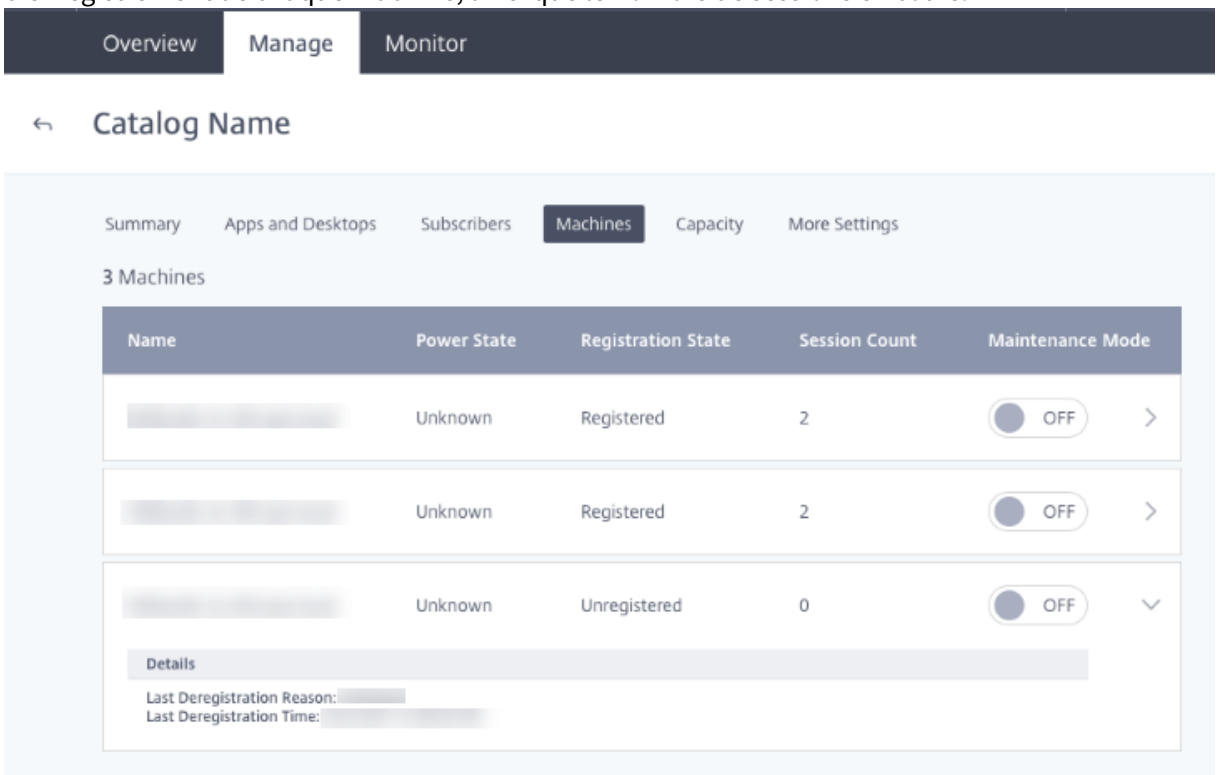
Mettre à jour le nombre de VDA dans un catalogue

1. Si vous n'êtes pas déjà dans Citrix Cloud, connectez-vous. Dans le menu en haut à gauche, sélectionnez **Mes services > Virtual Apps and Desktops**.
2. Cliquez sur l'onglet **Gérer**.
3. Sur l'onglet **Catalogues**, sélectionnez un catalogue.
4. Sur l'onglet **Capacité**, sous **Sélectionnez les paramètres d'échelle**, cliquez sur **Modifier**.

5. Changez la valeur **Nombre maximal d'instances exécutées** sur le nombre de VDA souhaité pour le catalogue.
6. Cliquez sur **Enregistrer**.

Surveiller les états de la machine

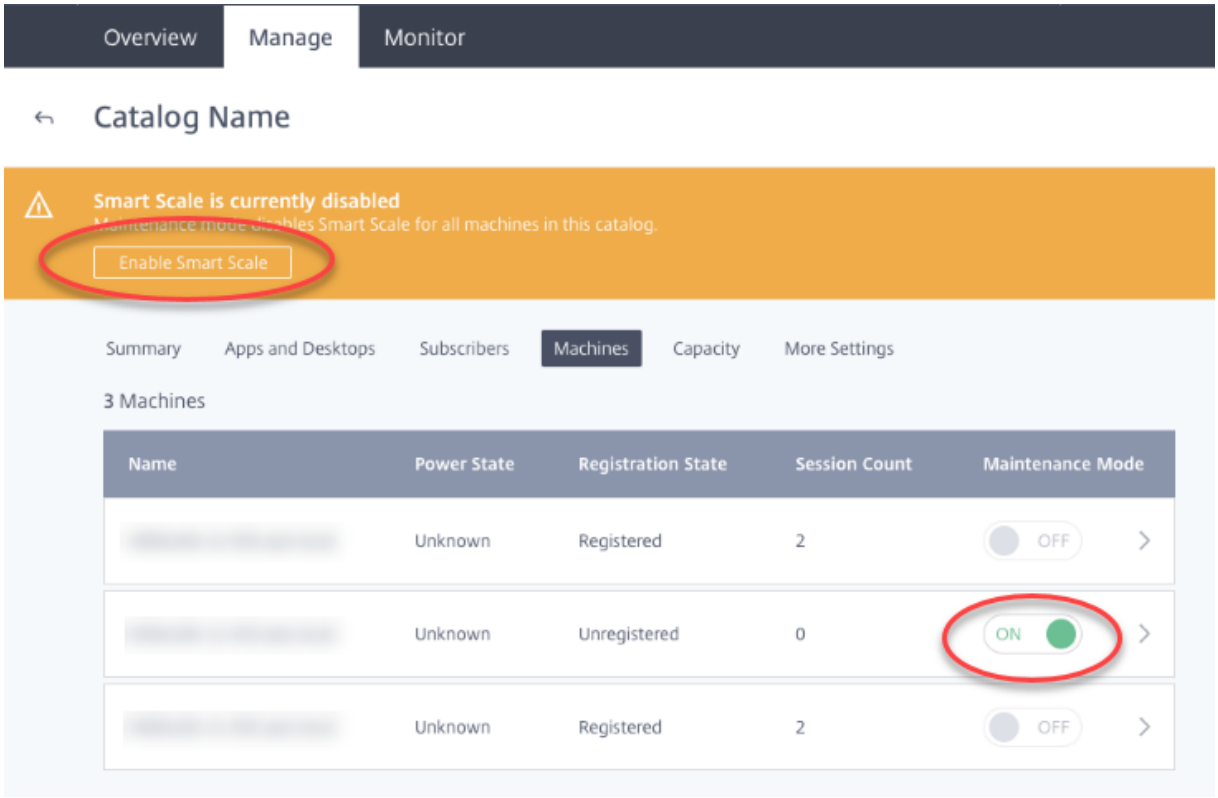
Lorsque vous sélectionnez un catalogue, l'onglet Machines de la page de synthèse du catalogue répertorie toutes les machines de ce catalogue. L'affichage inclut les états d'alimentation et d'enregistrement de chaque machine, ainsi que le nombre de sessions en cours.



Vous pouvez activer ou désactiver le mode de maintenance pour une machine. L'activation du mode de maintenance empêche toute nouvelle connexion à la machine. Les utilisateurs peuvent se connecter à des sessions existantes, mais ils ne peuvent pas démarrer de nouvelles sessions. Il peut être utile de placer une machine en mode de maintenance avant d'appliquer les correctifs.

Si vous activez le mode de maintenance pour une ou plusieurs machines, Smart Scale est temporairement désactivé pour toutes les machines de ce catalogue. L'une ou l'autre des actions suivantes activera à nouveau Smart Scale :

- Cliquez sur **Activer Smart Scale** dans l'avertissement en haut de l'écran. Cette action désactive automatiquement le mode de maintenance pour toutes les machines du catalogue pour lesquelles le mode de maintenance est activé.
- Désactivez explicitement le mode de maintenance pour chaque machine sur laquelle le mode de maintenance est actuellement activé.



Surveiller le service

1. Si vous n'êtes pas déjà dans Citrix Cloud, connectez-vous. Dans le menu en haut à gauche, sélectionnez **Mes services > Virtual Apps and Desktops**.
2. Cliquez sur l'onglet **Surveiller**.

Informations de session

Pour surveiller les performances globales de Citrix Virtual Apps Essentials :

1. Sélectionnez le catalogue que vous souhaitez surveiller. Vous pouvez afficher des informations sur les sessions, la durée de connexion et d'autres informations.
2. Choisissez une session puis :
   - Déconnectez la session
   - Déconnectez-vous de la session
   - Envoyez un message
3. Cliquez sur chaque session pour afficher des détails supplémentaires sur la session, tels que les processus, les applications en cours d'exécution, etc.

Informations d'utilisation

Les informations d'utilisation affichent des données agrégées pour tous les catalogues (plutôt qu'un catalogue spécifique).

- **Vue d'ensemble de l'utilisation** affiche le nombre total de lancements d'applications et le nombre d'utilisateurs uniques qui ont lancé des applications au cours des six dernières semaines.
- **Top des applications** répertorie les applications les plus fréquemment utilisées pour le mois en cours et les mois précédents. Le survol d'une entrée affiche le nombre de fois que cette application a été lancée.
- **Utilisateurs principaux** répertorie les dix principaux utilisateurs des mois en cours et des mois précédents, avec le nombre de fois où ils ont lancé des applications.

Les intervalles de données hebdomadaires commencent le lundi (UTC 00:00) et se terminent à l'heure de la requête. Les intervalles de données mensuels commencent le premier jour du mois (UTC 00:00) et se terminent à l'heure de la requête.

Profile Management

Profile Management veille à ce que les paramètres personnels soient appliqués à leurs applications virtuelles, indépendamment de l'emplacement de la machine utilisateur.

La configuration de Profile Management est facultative.

Vous pouvez activer Profile Management avec le service d'optimisation de profil. Ce service constitue un moyen fiable de gérer ces paramètres sous Windows. La gestion des profils assure une expérience cohérente grâce à un profil unique qui suit l'utilisateur. Il se consolide automatiquement et optimise les profils utilisateur afin de minimiser les besoins en gestion et en stockage. Le service d'optimisation de profil ne nécessite pas beaucoup d'administration, de support et d'infrastructure. En outre, l'optimisation des profils offre aux utilisateurs une meilleure expérience en termes de connexion et de déconnexion.

Le service d'optimisation des profils nécessite un partage de fichiers dans lequel tous les paramètres personnels sont conservés. Vous devez spécifier le partage de fichiers en tant que chemin UNC. Le chemin peut contenir des variables d'environnement système, des attributs d'utilisateur Active Directory ou des variables Profile Management. Pour en savoir plus sur le format de la chaîne de texte UNC, voir Pour spécifier le chemin d'accès au magasin de l'utilisateur.

Profile Management est configuré dans Citrix Cloud.

Pour configurer Profile Management

1. Si vous n'êtes pas déjà dans Citrix Cloud, connectez-vous. Dans le menu en haut à gauche, sélectionnez **Mes services > Virtual Apps and Desktops**.

2. Sur l'onglet **Gérer**, cliquez sur **Catalogues**.
3. Cliquez sur le nom du catalogue.
4. Cliquez sur **Plus de paramètres**.
5. Dans **Configurer la gestion des profils dans l'abonnement Azure**, entrez le chemin d'accès au partage de profil. Par exemple, \fileserver\share#sAMAccountName#
6. Cliquez sur **Enregistrer**.

Lorsque vous activez Profile Management, vous pouvez envisager d'optimiser davantage le profil de l'utilisateur en configurant la redirection de dossiers afin de minimiser les effets de la taille de ce dernier. L'application de la redirection de dossiers vient compléter la solution Profile Management. Pour plus d'informations, voir Redirection de dossiers Microsoft.

Configurer le serveur de licences Microsoft RDS

Citrix Virtual Apps Essentials accède aux fonctionnalités de session distante Windows Server qui nécessitent généralement une licence d'accès client Remote Desktop Services (RDS CAL). Le VDA doit pouvoir contacter un serveur de licences RDS pour demander des licences RDS CAL. Installez et activez le serveur de licences. Pour plus d'informations, voir Activer le serveur de licences Remote Desktop Services. Pour les environnements de validation technique, vous pouvez utiliser le délai de grâce fourni par Microsoft.

Avec cette méthode, vous pouvez faire en sorte que Virtual Apps Essentials applique les paramètres du serveur de licences. Vous pouvez configurer le serveur de licences et le mode par utilisateur dans la console RDS sur l'image principale. Vous pouvez également configurer le serveur de licences à l'aide des paramètres de stratégie de groupe Microsoft. Pour plus d'informations, voir Attribuer une licence à votre déploiement RDS avec des licences d'accès client (CAL).

Pour configurer le serveur de licences RDS à l'aide des paramètres de stratégie de groupe

1. Installez un serveur de licences Services Bureau à distance sur l'une des VM disponibles. La VM doit toujours être disponible. Les charges de travail du service Citrix doivent pouvoir atteindre ce serveur de licences.
2. Spécifiez l'adresse du serveur de licences et le mode de licence par utilisateur à l'aide de la stratégie de groupe Microsoft. Pour plus de détails, voir Spécifier le mode de licence Bureau à distance pour un serveur hôte de session Bureau à distance.
3. Si vous avez acheté des licences CAL auprès de Microsoft Remote Access, vous n'avez pas besoin d'installer les licences. Vous pouvez acheter des licences auprès de Microsoft Remote Access sur Azure Marketplace, ainsi que Virtual Apps Essentials.

Pour configurer le serveur de licences RDS

1. Si vous n'êtes pas déjà dans Citrix Cloud, connectez-vous. Dans le menu en haut à gauche, sélectionnez **Mes services > Virtual Apps and Desktops**.
2. Sur l'onglet **Gérer**, cliquez sur **Catalogues**.
3. Sélectionnez le catalogue puis sélectionnez **Plus de paramètres**.
4. Dans Entrez le nom de domaine complet du serveur de licences, tapez le nom de domaine complet du serveur de licences.
5. Cliquez sur **Enregistrer**.

Connecter les utilisateurs

Expérience d'espace de travail

Virtual Apps Essentials dans Citrix Cloud active l'expérience d'espace de travail pour chaque client. Après avoir créé le premier catalogue, Virtual Apps Essentials configure automatiquement l'URL de l'espace de travail. L'URL est celle à partir de laquelle les utilisateurs peuvent accéder à leurs applications et à leurs bureaux. L'URL de l'espace de travail apparaît dans le panneau de détails du catalogue sous l'onglet Résumé. La nouvelle URL de l'espace de travail remplace StoreFront hébergé dans le cloud. Virtual Apps Essentials ne prend pas en charge les déploiements sur site de StoreFront.

Après avoir créé un catalogue, vous pouvez utiliser Configuration de l'espace de travail pour personnaliser l'URL de l'espace de travail et l'apparence des espaces de travail. Vous pouvez également activer la version de prévisualisation de l'authentification fédérée à l'aide d'Azure Active Directory.

L'activation de l'authentification fédérée à l'aide d'Azure Active Directory comprend les tâches suivantes :

- Définissez Azure AD en tant que fournisseur d'identité. Pour de plus amples informations, consultez la section Connecter Azure Active Directory à Citrix Cloud.
- Activez Azure AD pour l'authentification auprès de l'expérience Citrix Workspace.

Pour plus d'informations, consultez la section Configuration de l'espace de travail.

Service Citrix Gateway

Pour permettre aux utilisateurs d'accéder de manière sécurisée à leurs applications publiées, Virtual Apps Essentials utilise le service Citrix Gateway. Ce service ne nécessite aucune configuration de votre part. Chaque utilisateur est limité à 1 Go de transfert de données sortantes par mois. Vous pouvez acheter un supplément de 25 Go sur Azure Marketplace. Les frais pour le supplément sont mensuels.

Annuler Virtual Apps Essentials

Vous pouvez imputer des frais Azure liés à Virtual Apps Essentials en raison des éléments suivants :

- Abonnement Virtual Apps Essentials
- Ressource Azure créée par Virtual Apps Essentials

Les frais Microsoft Azure pour le service Virtual Apps Essentials sont mensuels. Lorsque vous achetez Virtual Apps Essentials, vous êtes facturé pour le mois en cours. Si vous annulez votre commande, votre service ne sera pas renouvelé pour le mois suivant. Vous continuez d'avoir accès à Virtual Apps Essentials jusqu'à la fin du mois en cours en utilisant Citrix Cloud.

Votre facture Azure peut contenir plusieurs éléments pour Virtual Apps Essentials, notamment :

- Abonnement au service Virtual Apps Essentials
- Supplément du service Citrix Gateway, si acheté
- Frais Microsoft Remote Access
- Ressource Azure créée lors de l'utilisation de Virtual Apps Essentials

Annuler Virtual Apps Essentials dans Azure

Pour annuler votre abonnement Virtual Apps Essentials, supprimez la ressource de commande dans le portail Azure.

1. Connectez-vous au portail Azure.
2. Cliquez sur **Toutes les ressources**.
3. Dans la colonne **Type**, double-cliquez pour ouvrir Citrix Virtual Apps Essentials.
4. Cliquez sur l'icône de la corbeille. Le processus de suppression commence.

Supprimer les ressources Azure créées par Virtual Apps Essentials

Dans Citrix Cloud, supprimez les catalogues et les images associés à votre compte. Supprimez également les liens d'abonnement et assurez-vous que les VM Cloud Connector sont supprimées de Cloud Citrix.

Si vous n'êtes pas déjà dans Citrix Cloud, connectez-vous. Dans le menu en haut à gauche, sélectionnez **Mes services > Virtual Apps and Desktops**.

Pour supprimer des catalogues

1. Sur l'onglet **Gérer**, cliquez sur **Catalogues**.
2. Dans le menu de points de suspension (…) en regard du catalogue que vous souhaitez supprimer, sélectionnez **Supprimer le catalogue**.
3. Répétez l'étape précédente pour chaque catalogue à supprimer.

Pour supprimer des images principales

1. Sur l'écran **Gérer**, cliquez sur **Images principales**.
2. Sélectionnez une image et cliquez sur **Supprimer**.
3. Répétez l'étape précédente pour chaque image principale à supprimer.

Pour supprimer des liens vers des abonnements Azure

1. Sur l'onglet **Gérer**, cliquez sur **Abonnements**.
2. Cliquez sur l'icône de la corbeille en regard de l'abonnement. Le portail Azure s'ouvre.
3. Connectez-vous à votre abonnement Azure avec vos informations d'identification Azure d'administrateur global.
4. Cliquez sur **Accepter** pour permettre à Virtual Apps Essentials d'accéder à votre compte Azure.
5. Cliquez sur **Supprimer** pour dissocier l'abonnement.
6. Répétez les étapes précédentes pour les autres abonnements Azure liés.

Pour assurer la suppression des VM Citrix Cloud Connector

1. Dans le menu en haut à gauche, sélectionnez **Emplacements des ressources**.
2. Identifiez les VM Cloud Connector.
3. Connectez-vous au portail Azure.
4. Supprimez les VM de la page **Ressource** dans Azure.

Ressources partenaires

Ce service est maintenant disponible via le canal Fournisseur de solutions Microsoft Cloud. Pour plus de détails, voir Activation de Microsoft CSP pour Citrix Essentials.

Obtenir de l'aide

Si vous rencontrez des problèmes avec Virtual Apps Essentials, ouvrez un ticket en suivant les instructions de la section Comment obtenir de l'aide.

Plus d'informations

Pour plus d'informations sur l'utilisation des stratégies Citrix dans un environnement Virtual Apps Essentials, voir l'article CTX220345.

Citrix Virtual Desktops Essentials

November 7, 2018

Citrix Virtual Desktops Essentials permet la gestion et la distribution de bureaux virtuels Windows 10 à partir de Microsoft Azure.

Virtual Desktops Essentials est conçu spécifiquement pour Azure Marketplace. Citrix et Microsoft se sont associés pour offrir une expérience intégrée à Virtual Desktops Essentials et Azure IaaS. Ce partenariat vous offre une interface unique pour fournir un espace de travail numérique Windows 10 complet à partir d'Azure.

Avec Virtual Desktops Essentials, vous pouvez :

- Déployer et sécuriser des bureaux virtuels Windows 10 sur Azure
- Offrir une expérience utilisateur de premier ordre en utilisant les fonctionnalités Citrix HDX
- Fournir un accès sécurisé sur n'importe quel périphérique à l'aide de l'application Citrix Workspace.
- Gérer et administrer le déploiement à partir de Microsoft Azure et Citrix Cloud

Citrix Virtual Desktops Essentials simplifie le déploiement de Windows 10. Vous pouvez déployer des bureaux rapidement, gérer à l'échelle et offrir une expérience d'accès utilisateur avancée à partir d'un seul plan de gestion.

Vous gérez les bureaux Windows 10 à l'aide de Studio et surveillez les sessions à l'aide de Director. Les utilisateurs se connectent à leurs bureaux virtuels Windows 10 en se connectant avec l'application Citrix Workspace.

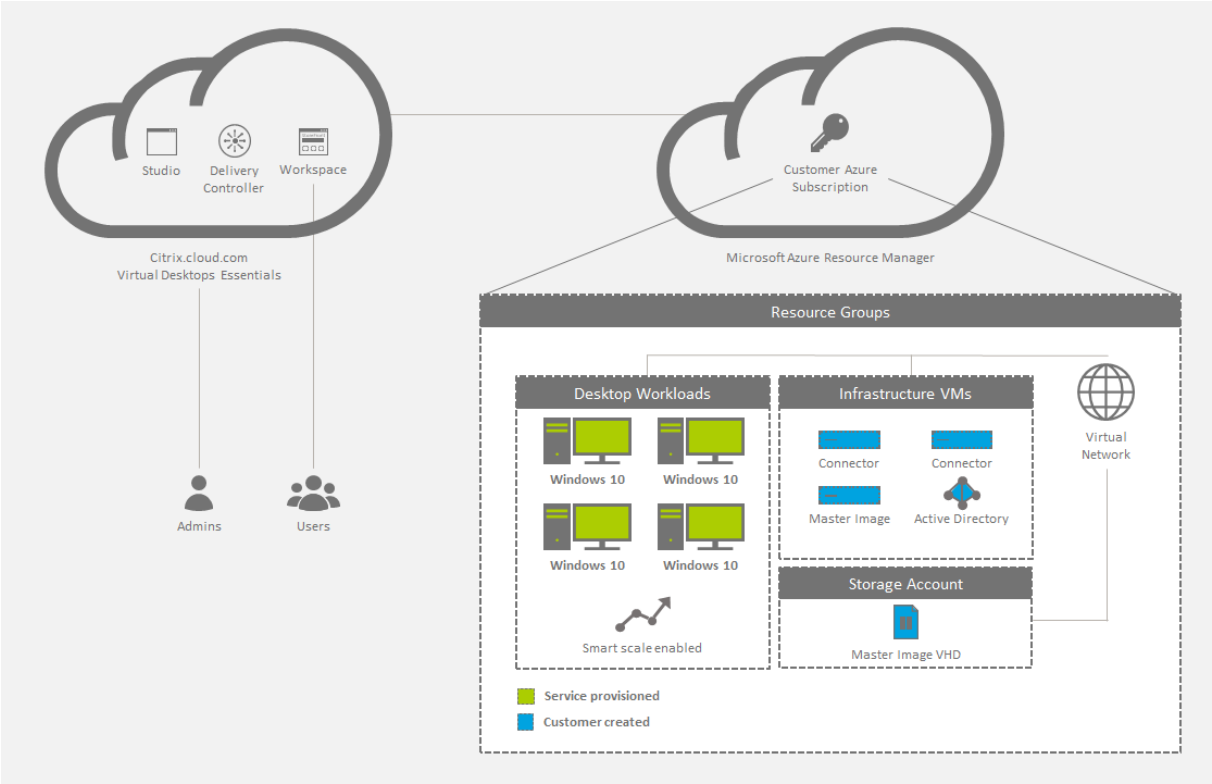
Après avoir configuré Citrix Virtual Desktops Essentials, vous fournissez à vos utilisateurs une URL vers un espace de travail Citrix ou StoreFront. Les utilisateurs se connectent à leurs bureaux via l'application Citrix Workspace sur leurs périphériques, avec l'URL fournie. Lorsque les utilisateurs se connectent à l'application Citrix Workspace, l'icône du bureau Windows 10 apparaît dans la fenêtre de l'espace de travail ou de StoreFront.

> **Important :**
>
> Pour les nouveaux clients depuis décembre 2017, Virtual Desktops Essentials inclut une URL Citrix Workspace, généralement au format `https://<yourcompanyname>.cloud.com`. Une fois que vous avez configuré Virtual Desktops Essentials, testez et partagez le lien de l'URL de l'espace de travail avec vos abonnés pour leur donner accès à leurs bureaux.

Pour plus d'informations sur l'espace de travail, voir Configuration de l'espace de travail.

Des mises à jour ultérieures suivront pour les clients ayant acheté Virtual Desktops Essentials (anciennement XenDesktop Essentials) avant décembre 2017. Actuellement, ces clients continuent à utiliser StoreFront hébergé sur le cloud, comme indiqué dans cet article. Virtual Desktops Essentials ne prend pas en charge StoreFront sur site.

Le diagramme présente une vue d'ensemble de l'architecture d'un déploiement de Virtual Desktops Essentials.



Nouveautés

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. Cet article utilise les noms suivants.

- **Citrix Virtual Desktops Essentials :** la technologie qui a fait de XenDesktop le leader du secteur s'appelle désormais Citrix Virtual Desktops. Elle introduit VDI dans une application moderne, contextuelle et sécurisée, qui offre le meilleur moyen d'accéder de manière sécurisée à toutes vos applications professionnelles. XenDesktop Essentials s'appelle désormais Citrix Virtual Desktops Essentials.
- **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.

- **Citrix Gateway :** NetScaler Unified Gateway, qui permet un accès sécurisé et contextuel aux applications et aux données dont vous avez besoin pour travailler efficacement, s'appelle désormais Citrix Gateway.

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. 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/.

Comment acheter Virtual Desktops Essentials

Pour plus d'informations sur l'achat ou l'annulation de Virtual Desktops Essentials, téléchargez Comment acheter ou annuler le service Virtual Desktops Essentials.

Configuration système requise, conditions préalables et compatibilité

Virtual Desktops Essentials nécessite certains produits et composants complémentaires ainsi que des autorisations de compte spécifiques pour son installation, sa configuration et son fonctionnement.

Microsoft Azure

Virtual Desktops Essentials est conçu pour une prise en charge exclusive de Microsoft Azure. Votre environnement Azure doit répondre à certaines exigences minimales pour prendre en charge Virtual Desktops Essentials :

- Un abonnement Azure avec un contrat d'entreprise ou un abonnement Microsoft CSP Azure.
- Service de domaine Windows Server Active Directory ou Azure Active Directory.
- Un locataire Azure Active Directory.

> **Important :**
>
> Microsoft requiert le locataire Azure Active Directory de l'abonnement Azure pour déployer des bureaux Windows 10. Vous pouvez utiliser le locataire Azure Active Directory ou un

> autre annuaire actif pour identifier les utilisateurs autorisés.

- Un contrôleur de domaine Active Directory.
- Un réseau virtuel et un sous-réseau Azure Resource Manager (ARM) dans la région de votre choix. Configurez le réseau virtuel avec une entrée de serveur de nom de domaine (DNS) personnalisée pointant vers le contrôleur de domaine. Le réseau virtuel doit avoir un sous-réseau suffisamment grand pour contenir les bureaux.

  Utilisez le même réseau virtuel pour l'entrée DNS et le sous-réseau du bureau.
- Un utilisateur Azure Active Directory avec des autorisations de contributeur (au minimum) dans l'abonnement.
- Une machine virtuelle sur laquelle Microsoft Windows 10 est installé, y compris les personnalisations et applications requises.

Citrix Cloud Connector

Citrix Cloud Connector authentifie et crypte les communications entre Citrix Cloud et vos emplacements de ressources. Avec Virtual Desktops Essentials, vos ressources sont situées dans Microsoft Azure. Citrix Cloud nécessite l'installation de Citrix Cloud Connector sur deux VM de serveur Windows pour garantir la disponibilité continue de vos emplacements de ressources.

Pour plus d'informations sur les Cloud Connector, voir Citrix Cloud Connector.

Citrix Cloud

- Un compte Citrix Cloud.
- Un accès au service Citrix Virtual Apps and Desktops dans Citrix Cloud, activé lors de l'achat de Virtual Desktops Essentials.
- (Facultatif) Un Citrix ADC VPX configuré en mode proxy ICA pour un accès depuis l'extérieur du réseau d'entreprise.
  - Le proxy ICA permet un accès sécurisé aux applications et aux bureaux proposés à vos utilisateurs.
  - Pour plus d'informations sur la configuration du Citrix ADC VPX, voir Déploiement de Citrix NetScaler VPX sur Microsoft Azure.

Problèmes connus

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 Ser-

vices. 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.

Étape 1 : Connecter votre abonnement Azure à Virtual Desktops Essentials

1. Connectez-vous au portail Azure.
2. Dans Azure, ouvrez une machine virtuelle Windows Server jointe à un domaine, puis ouvrez un navigateur Web.
3. Dans le navigateur Web de la machine virtuelle, connectez-vous à Citrix Cloud. Le service Virtual Apps and Desktops s'ouvre.
4. Dans le menu en haut à gauche, sélectionnez **Emplacements des ressources**.
5. Sur la page **Emplacements des ressources**, cliquez sur **Télécharger**. Le fichier `cwcconnector.exe` est téléchargé.
6. Double-cliquez sur le programme téléchargé pour lancer le programme d'installation.
7. Lorsque vous y êtes invité, entrez vos informations d'identification Citrix Cloud. Suivez les instructions à l'écran pour installer et configurer le Citrix Cloud Connector.
8. Répétez les étapes 4 à 7 sur au moins une machine virtuelle de serveur pour installer un autre Cloud Connector.

Lors de l'installation, le Cloud Connector accède à Citrix Cloud pour s'authentifier, valider les autorisations du programme d'installation, puis télécharger et configurer les services fournis par le Cloud Connector. L'installation utilise les privilèges de l'utilisateur qui lance l'installation.

Après l'installation, Citrix Cloud enregistre votre domaine dans **Gestion des identités et des accès**. Pour de plus amples informations, consultez la section Gestion des identités et des accès.

Étape 2 : Créer une connexion hôte

Avant de commencer, assurez-vous que vos informations d'identification Azure Active Directory et votre ID d'abonnement sont disponibles. L'utilisateur Azure AD qui crée la connexion à l'hôte doit être un utilisateur de cloud natif dans Azure AD ou synchronisé pour le domaine d'entreprise. Le compte d'utilisateur ne peut pas être un compte Microsoft invité ou délégué.

1. Connectez-vous à Citrix Cloud.
2. Dans le menu en haut à gauche, sélectionnez **Mes services > Virtual Apps and Desktops**.
3. Cliquez sur **Gérer**. La console de gestion Studio s'ouvre.
4. Sélectionnez **Configuration > Hébergement** dans le volet de navigation de Studio.
5. Sélectionnez **Ajouter une connexion et des ressources** dans le volet Actions.
6. Dans la page **Ajouter une connexion et des ressources** :
   a) Dans **Type de connexion**, sélectionnez **Microsoft Azure**.
   b) Dans l'environnement Azure, sélectionnez **Azure Global** puis cliquez sur **Suivant**.

7. Dans **Détails de la connexion** :
    a) Dans **ID d'abonnement**, tapez l'ID d'abonnement Azure.
    b) Dans **Nom de la connexion**, tapez un nom pour la connexion, puis effectuez une de ces procédures :
        i. Cliquez sur **Créer** puis suivez la procédure Option 1 : Créer une connexion.
        ii. Cliquez sur **Utiliser existant** et continuez la configuration des paramètres. Suivez la procédure Option 2 : Utiliser une connexion hôte existante.

Option 1 : Créer une connexion

1. Connectez-vous à Azure avec le compte contributeur (au minimum) de l'abonnement.
2. Azure crée automatiquement la connexion hôte. Dans Studio, une coche verte avec le mot **Connecté** apparaît sur la page **Ajouter une connexion et des ressources**.
3. Cliquez sur **Suivant**.
4. Sur la page **Région**, sélectionnez la région où réside votre réseau virtuel, puis cliquez sur **Suivant**.
5. Sur la page **Réseau** :
    a) Tapez un nom pour les ressources.
    b) Sélectionnez le réseau virtuel pour le groupe de ressources.
    c) Sélectionnez le sous-réseau qui s'applique au groupe de ressources, puis cliquez sur **Suivant**.
6. Dans la page **Résumé**, cliquez sur **Terminer**. La connexion de l'hôte à Microsoft Azure Resource Manager est terminée.

Option 2 : Utiliser une connexion hôte existante

Une fois que vous avez cliqué sur **Utiliser existant**, la page **Détails du principal de service existant** apparaît :

1. Dans **ID d'abonnement**, tapez l'ID d'abonnement Microsoft Azure.
2. Dans **Nom de l'abonnement**, tapez le nom de l'abonnement Azure.
3. Cliquez sur **OK**.
4. Sur la page **Connexion** :
    a) Cliquez sur **Créer une nouvelle connexion**, tapez votre identifiant d'abonnement Microsoft Azure et un nom de connexion (facultatif), puis cliquez sur **Créer**. La boîte de dialogue d'authentification Microsoft apparaît.

        Si vous souhaitez utiliser une connexion que vous avez créée à un autre moment, choisissez **Utiliser une connexion existante**. Ensuite, sélectionnez la connexion.

b) Tapez le nom d'utilisateur et le mot de passe de l'utilisateur Microsoft Azure Active Directory. Citrix Cloud crée un principal de service avec les droits de création et de gestion des machines pour cet abonnement.

5. Sur la page **Région**, sélectionnez la région Azure dans laquelle se trouve votre groupe de ressources Microsoft Azure.
6. Sur la page **Réseau** :

   a) Tapez un nom pour les ressources. Si vous avez saisi un nom de connexion, utilisez-le pour le nom des ressources.
   b) Choisissez le réseau virtuel pour votre groupe de ressources Microsoft Azure.
   c) Sélectionnez les sous-réseaux à utiliser pour cette connexion. Si un seul sous-réseau existe, il est sélectionné par défaut.

Étape 3 : Créer un pool de bureaux Windows 10

Pour préparer l'hébergement des bureaux, installez le logiciel VDA (Citrix Virtual Delivery Agent) sur la machine virtuelle Windows 10. Le VDA :

- Permet à la machine de s'inscrire auprès de Virtual Desktops Essentials.
- Établit et gère la connexion entre la machine et l'appareil de l'utilisateur.
- Vérifie qu'une licence Citrix est disponible pour l'utilisateur ou la session.
- Applique toutes les stratégies configurées pour la session.
- Communique les informations de session à Virtual Desktops Essentials.

Pour installer le VDA sur l'image de base

1. Démarrez l'image de Windows 10.
2. Accédez à https://www.citrix.com/downloads/citrix-cloud/product-software/xenapp-and-xendesktop-service.html et téléchargez un VDA pour OS de bureau.
3. Démarrez l'installation du VDA.
4. Sur la page **Environnement**, cliquez sur **Créer une image MCS principale**.
5. Sur la page **Composants additionnels**, sélectionnez tous les composants sauf **Activer Citrix App-V**.
6. Sur la page **Delivery Controller**, entrez les emplacements de vos machines virtuelles Cloud Connector. Cliquez sur **Suivant** et confirmez tous les messages d'avertissement.
7. Sur la page **Fonctionnalités**, conservez les paramètres par défaut et cliquez sur **Suivant**.
8. Cliquez sur **Suivant** pour accepter les paramètres par défaut sur les pages restantes.
9. Sur la page **Résumé**, cliquez sur **Installer**.
10. Redémarrez la machine virtuelle et reconnectez-vous.
11. Confirmez que les paramètres ont été appliqués.

12. Arrêtez la machine virtuelle. L'arrêt de la machine virtuelle est requis pour l'enregistrement de VDA.

Créer un compte de stockage

Dans Microsoft Azure, vous avez besoin d'un compte de stockage pour héberger le disque dur virtuel de l'image de base. Vous pouvez héberger le lecteur dans un compte de stockage existant ou créer un compte de stockage.

> **Important :**
>
> Téléchargez l'image principale de Windows 10 sur le compte de stockage de destination dans Azure avant de créer le catalogue de machines.

Pour créer un compte de stockage pour les images

1. Dans le volet de navigation Microsoft Azure, cliquez sur **Comptes de stockage**.
2. Sur la page **Comptes de stockage**, cliquez **Ajouter**.
3. Dans **Nom**, spécifiez un nom.
4. Dans **Modèle de déploiement**, sélectionnez **Resource Manager**.
5. Dans **Performance**, sélectionnez **Standard**.
6. Pour **Réplication**, **Storage service encryption** et **Abonnement**, gardez les paramètres par défaut.
7. Dans **Groupe de ressources**, cliquez sur l'un des éléments suivants :
   a) Cliquez sur **Créer** pour créer un groupe de ressources. Tapez le nom du groupe.
   b) Cliquez sur **Utiliser existant** pour utiliser un groupe de ressources existant. Sélectionnez un groupe.
8. Pour que le compte de stockage apparaisse sur le tableau de bord, cliquez sur **Épingler au tableau de bord**.
9. Cliquez sur **Créer**.

Après avoir créé un compte de stockage, créez un conteneur d'objets blob, puis nommez-le pour refléter le disque dur virtuel, tel que "VHD".

Pour créer un conteneur d'objets blob pour les disques durs virtuels d'image

1. Dans le volet de navigation Microsoft Azure, cliquez sur **Comptes de stockage** et accédez au compte de stockage que vous avez créé précédemment.
2. Dans le volet de navigation central, sous **SERVICE BLOB**, cliquez sur **Conteneurs**.
3. Dans le volet de détails, cliquez sur **Conteneur**.
4. Dans le volet **Nouveau conteneur**, donnez un nom au conteneur.

5. Dans **Type d'accès**, sélectionnez **Blob**, puis cliquez sur **Créer**. Le nouveau conteneur d'objets blob apparaît dans le volet.
6. Copiez l'URL blob et enregistrez-la dans un fichier texte. L'URL est utilisée ultérieurement pour télécharger le disque dur virtuel converti.

Créer un catalogue de machines pour Citrix Virtual Desktops Essentials

Les catalogues de machines sont des collections de bureaux virtuels que vous gérez comme une seul entité. Ces bureaux virtuels sont les ressources que vous mettez à la disposition de vos utilisateurs. Toutes les machines d'un catalogue ont le même système d'exploitation et VDA installé.

En général, vous pouvez créer une image principale et l'utiliser pour créer les mêmes machines virtuelles dans le catalogue.

1. Connectez-vous à Citrix Cloud. Dans le menu en haut à gauche, sélectionnez **Mes services > Virtual Apps and Desktops**.
2. Sélectionnez l'onglet **Gérer**.
3. Cliquez sur **Catalogues de machines** dans le volet de navigation Studio.
4. Sélectionnez **Créer un catalogue de machines** dans le volet Actions.
5. Sur la page **Système d'exploitation**, OS de bureau devrait être la seule option disponible. Sélectionnez-le puis cliquez sur **Suivant**.
6. Sur la page **Expérience de bureau** :
    a) Sélectionnez **Je veux que les utilisateurs se connectent au même bureau (statique) chaque fois qu'ils ouvrent une session**.
    b) Sélectionnez **Oui, créer une machine virtuelle dédiée et enregistrer les modifications sur le disque local**.
7. Sur la page **Image principale** :
    a) Naviguez jusqu'au disque dur virtuel que vous avez créé précédemment et sélectionnez-le. La structure de l'arborescence de navigation s'aligne sur la hiérarchie Azure :
        - Groupe de ressources
        - Comptes de stockage
        - Conteneurs
        - Disques durs virtuels (VHD)
        - Noms d'image
    b) Conservez la sélection par défaut dans **Sélectionnez le niveau fonctionnel minimum pour ce catalogue**.
8. Sur la page **Types de stockage et de licence**, sélectionnez le type de stockage de destination et votre préférence pour la licence.
9. Sur la page **Machines virtuelles**, sélectionnez le nombre de machines virtuelles et la taille de la machine virtuelle Azure.

10. Sur la page **Cartes d'interface réseau**, sélectionnez une carte réseau à associer au nom de sous-réseau Azure pour vos machines Citrix. Vous pouvez aussi cliquer sur **Ajouter une carte** pour ajouter une autre carte réseau.
11. Sur la page **Comptes d'ordinateurs** :
    a) Cliquez sur **Créer des nouveaux comptes Active Directory**.
    b) Choisissez le domaine pour les comptes d'ordinateurs.
    c) Accédez à l'unité d'organisation pour les nouvelles machines.
    d) Tapez un schéma d'affectation de nom de compte pour les nouvelles machines. Incluez deux signes numériques (##) pour incrémenter les numéros automatiquement. Sélectionnez un nombre ou des lettres. Les signes dièse traduisent le schéma d'affectation de nom. Par exemple, mymachcatalog## devient mymachcatalog01 ou mymachcatalogAB.
12. Sur la page **Informations d'identification du domaine**, cliquez sur **Entrer informations d'identification**, puis dans la boîte de dialogue **Sécurité Windows**, tapez votre nom d'utilisateur et votre mot de passe. Ce compte est utilisé pour créer les comptes d'ordinateurs.
13. Sur la page **Résumé**, tapez un nom pour le catalogue et une description pour les administrateurs.
14. Cliquez sur **Terminer**.

Les machines virtuelles sont créées et un nouveau compte de stockage apparaît dans le tableau de bord Microsoft Azure. Pendant que les services de catalogue de machines déploient les machines virtuelles, une machine virtuelle de préparation avec un VHS est créée temporairement dans Azure.

Pour identifier le nom de l'image dans Microsoft Azure

1. Connectez-vous au portail Azure.
2. Dans le volet de navigation du tableau de bord, cliquez sur **Toutes les ressources**. Une liste d'abonnements apparaît.
3. Choisissez l'abonnement.
4. Cliquez sur **Tous les paramètres**.
5. Cliquez sur **Groupes de ressources**.
6. Sélectionnez le groupe de ressources.
7. Sélectionnez la machine virtuelle Windows 10 contenant le VDA Citrix.
8. Cliquez sur **Tous les paramètres**.
9. Cliquez sur **Disques**.
10. Sélectionnez le disque du système d'exploitation. La première zone de texte de la fenêtre du disque du système d'exploitation contient l'URL de l'image, structurée comme dans l'exemple suivant. Vous pouvez obtenir le nom du compte de stockage et le nom de l'image à partir de l'URL. Par exemple : `https://<storage account name>.blob.core.window.net/vhds/<image name>`.
11. Sur la page **Machines**, les modèles répertoriés sont directement extraits de votre abonnement

Azure.

Étape 4 : Attribuer des bureaux Windows 10 à vos utilisateurs

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 spécifie quels utilisateurs peuvent utiliser ces machines.

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation Studio, puis sélectionnez **Créer un groupe de mise à disposition** dans le volet Actions.
2. Spécifiez le nombre de machines que vous souhaitez mettre à la disposition pour le groupe. Le nombre que vous spécifiez ne peut pas dépasser le nombre de machines disponibles dans votre catalogue de machines.
3. Sur la page **Type de mise à disposition**, choisissez **Bureaux**.
4. Sur la page **Utilisateurs**, choisissez l'option permettant de laisser la gestion des utilisateurs à Citrix Cloud. La sélection de cette option vous permet d'utiliser Citrix Cloud pour déterminer qui peut accéder aux machines du groupe de mise à disposition (vous pouvez également ajouter des utilisateurs via Studio.)
5. Sur la page **Résumé**, indiquez un nom et (éventuellement) une description du groupe de mise à disposition.

Une fois ces étapes terminées, éditez le groupe de mise à disposition pour configurer l'accès des utilisateurs. Vous pouvez ajouter ou supprimer des utilisateurs et modifier leurs paramètres.

Ajouter ou supprimer des utilisateurs dans un groupe de mise à disposition via Studio

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe, puis sélectionnez **Modifier le groupe de mise à disposition** dans le volet Actions.
3. Sur la page **Utilisateurs**, pour ajouter des utilisateurs, cliquez sur **Ajouter**, puis spécifiez les utilisateurs que vous souhaitez ajouter. Pour supprimer des utilisateurs, sélectionnez un ou plusieurs utilisateurs, puis cliquez sur **Supprimer**. Vous pouvez également sélectionner ou désactiver la case à cocher qui permet d'activer ou de désactiver l'accès par des utilisateurs non authentifiés.
4. Cliquez sur **OK**.

Modifier les paramètres utilisateur dans un groupe de mise à disposition via Studio

Le nom de cette page peut apparaître sous **Paramètres utilisateur** ou **Paramètres de base**.

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.

2. Sélectionnez un groupe, puis sélectionnez **Modifier le groupe de mise à disposition** dans le volet Actions.
3. Sur la page **Paramètres utilisateur** (ou **Paramètres de base**) :
   a) Dans **Description**, tapez le texte que l'espace de travail ou StoreFront affiche pour les utilisateurs.
   b) Définissez le fuseau horaire sur le fuseau horaire Azure.
   c) Sélectionnez **Activer le groupe de mise à disposition**.
   d) Définissez le nombre maximum de bureaux par utilisateur.
4. Cliquez sur **OK** pour enregistrer les paramètres.

Ajouter un accès utilisateur via Citrix Cloud

1. Connectez-vous à Citrix Cloud, puis cliquez sur **Afficher bibliothèque**.
2. Sur la vignette des bureaux, cliquez sur le bouton de points de suspension (…) dans le coin droit.
3. Recherchez les groupes d'utilisateurs autorisés à accéder au groupe de mise à disposition et ajoutez-les à la liste.
4. Lorsque vous avez terminé, cliquez sur le bouton **X** pour fermer la fenêtre.

Vos bureaux virtuels Windows 10 sont affectés aux groupes ajoutés à la liste des abonnés.

Étape 5 : Configurer Citrix ADC VPX dans Azure (facultatif)

Le boîtier virtuel Citrix ADC VPX est disponible en tant qu'image dans Microsoft Azure Marketplace. Lorsque vous déployez Citrix ADC VPX sur Microsoft Azure Resource Manager, vous pouvez utiliser les fonctionnalités de cloud computing Azure. Vous pouvez utiliser les fonctionnalités d'équilibrage de charge et de gestion du trafic de Citrix Gateway pour répondre aux besoins de votre entreprise.

Vous pouvez déployer des instances Citrix ADC VPX sur Azure Resource Manager de deux manières :

- Une instance autonome.
- Une paire à haute disponibilité en mode actif-actif ou actif-veille.

Si des utilisateurs se connectent depuis un emplacement distant, configurez Citrix ADC VPX dans Azure pour créer des connexions sécurisées entre l'application Citrix Workspace et les bureaux Windows 10.

Une fois le déploiement terminé, utilisez le protocole RDP (Remote Desktop Protocol) pour vous connecter à l'une des machines Cloud Connector. Lorsque vous vous connectez, passez à la configuration de Citrix ADC VPX à partir de la console d'administration Citrix Gateway.

Pour des informations complètes sur la configuration, voir Déploiement de l'instance Citrix ADC VPX sur Microsoft Azure.

Après avoir configuré Citrix ADC VPX dans Azure, activez Citrix Gateway dans Citrix Cloud.

Pour configurer les paramètres de Citrix Gateway pour un accès sécurisé

1. Connectez-vous à la console de gestion à l'aide des informations d'identification de l'administrateur Citrix Gateway. Vous n'avez pas besoin de configurer plus d'adresses IP. Cliquez sur **Ignorer**.
2. Dans **Nom d'hôte**, **Adresse IP DNS** et **Fuseau horaire**, utilisez l'adresse IP et les paramètres DNS du réseau virtuel. Les paramètres sont sur votre contrôleur de domaine Active Directory.
3. Cliquez sur **Terminé**. Vous n'avez pas besoin de redémarrer Citrix ADC VPX maintenant.
4. Cliquez sur **Licences** sous l'onglet Configuration et téléchargez les licences nécessaires pour configurer Citrix Gateway.
5. Une fois les licences téléchargées, redémarrez le boîtier.
6. Lorsque la machine virtuelle redémarre, connectez-vous à nouveau à l'aide des informations d'identification Citrix Gateway.

Configurer les paramètres Citrix Virtual Desktops Essentials dans Citrix Gateway

Après avoir configuré les paramètres précédents, exécutez l'Assistant de configuration rapide dans Citrix Gateway. Pour plus d'informations, voir Configuration des paramètres avec l'assistant de configuration rapide.

Configurer Citrix Gateway pour la haute disponibilité et l'équilibrage de charge

Dans un déploiement Microsoft Azure, une configuration haute disponibilité de deux machines virtuelles Citrix Gateway est obtenue à l'aide de l'équilibrage de charge Azure. L'équilibrage de charge répartit le trafic client sur les serveurs virtuels configurés sur les deux instances de Citrix Gateway.

Si le trafic client provient d'Internet, déployez un équilibrage de charge externe entre Internet et les instances de Citrix Gateway pour répartir le trafic client. Pour plus d'informations sur cette configuration, voir Configurer une configuration haute disponibilité avec une seule adresse IP et une seule carte réseau.

Vous pouvez également ajouter le port entrant 80 au groupe de sécurité réseau Citrix Gateway pour configurer Citrix Gateway à l'aide de son adresse IP publique. Une fois la configuration terminée, vous pouvez supprimer la règle du port entrant 80 pour sécuriser l'accès à la console de gestion.

Étape 6 : Connecter les utilisateurs

Citrix Workspace ou StoreFront hébergé dans le cloud fournit le service aux appareils des utilisateurs. Dans la console Citrix Cloud :

- Si le menu en haut à gauche inclut la configuration de l'espace de travail, vous utilisez l'espace de travail. Elle est visible si vous avez acheté Citrix Virtual Desktops Essentials à partir de décembre 2017.
- Si le menu en haut à gauche n'inclut pas la configuration de l'espace de travail, vous utilisez StoreFront hébergé dans le cloud.

Distribution de services via Citrix Workspace

Après avoir créé le premier catalogue, Virtual Desktops Essentials configure automatiquement l'URL de l'espace de travail. Cette URL apparaît sous les détails du catalogue. Vous pouvez personnaliser l'URL de l'espace de travail et l'apparence des espaces de travail. Vous pouvez également activer la version de prévisualisation de l'authentification fédérée à l'aide d'Azure Active Directory. Pour plus d'informations, voir Configuration de l'espace de travail.

1. Dans la console Citrix Cloud, sélectionnez **Configuration de l'espace de travail** dans le menu supérieur gauche. Sélectionnez l'onglet **Intégrations de services**. Le service est répertorié.
2. Testez votre connexion en vous connectant à l'URL de l'espace de travail avec vos informations d'identification de domaine et en démarrant un bureau.
3. Fournissez à vos utilisateurs l'URL, qu'ils peuvent copier. Les utilisateurs peuvent taper ou coller cette URL dans la barre d'adresse de leur navigateur ou dans l'application Citrix Workspace pour accéder aux bureaux.

Mise à disposition de services via StoreFront hébergé sur le cloud

1. Dans la console Citrix Cloud, cliquez sur **Gérer**, puis sur **Mise à disposition du service**.
2. Assurez-vous que StoreFront hébergé sur cloud est activé. Il est activé par défaut si vous avez acheté Virtual Desktops Essentials avant décembre 2017.
3. Testez votre connexion en vous connectant à l'URL de StoreFront avec vos informations d'identification de domaine et en démarrant un bureau.
4. Fournissez à vos utilisateurs l'URL, qu'ils peuvent copier. Les utilisateurs peuvent taper ou coller cette URL dans la barre d'adresse de leur navigateur ou dans l'application Citrix Workspace pour accéder aux bureaux.

Accès à distance à l'aide de Citrix ADC VPX

1. Dans la console Citrix Cloud, cliquez sur **Gérer**, puis sur **Mise à disposition du service**.
2. Activez **Citrix Gateway**.
3. Sélectionnez **Utiliser votre propre Citrix Gateway** dans l'emplacement des ressources.
4. Tapez l'adresse Citrix Gateway dans le champ de texte. N'incluez pas de protocole. Vous pouvez inclure un numéro de port.

5. Activez la fiabilité de session, le cas échéant.
6. Enregistrez.
7. Testez votre connexion en vous connectant à l'URL de StoreFront ou de l'espace de travail avec vos informations d'identification de domaine et en démarrant un bureau.
8. Fournissez à vos utilisateurs l'URL, qu'ils peuvent copier. Les utilisateurs peuvent taper ou coller cette URL dans la barre d'adresse de leur navigateur ou dans l'application Citrix Workspace pour accéder aux bureaux.

Ressources partenaires

Ce service est aussi disponible via le canal Fournisseur de solutions Microsoft Cloud. Pour plus de détails, voir Activation de Microsoft CSP pour Citrix Essentials.

Concepts avancés

November 7, 2018

- Considérations sur le dimensionnement et la scalabilité des Cloud Connector
- Considérations sur le dimensionnement et la scalabilité du cache d'hôte local

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