Citrix Cloud

Contents

Citrix Cloud

July 21, 2021

Citrix Cloud est une plate-forme qui héberge et gère les services Citrix. Il se connecte à vos ressources via des connecteurs sur tout cloud ou toute infrastructure de votre choix (infrastructure locale, cloud public, cloud privé ou cloud hybride). Il vous permet de créer, gérer et déployer des espaces de travail contenant des applications et des données vers vos utilisateurs à partir d'une seule console.

Ressources d'architecture et de déploiement

Citrix Tech Zone contient de nombreuses informations pour vous aider à en savoir plus sur Citrix Cloud et d'autres produits Citrix. Vous trouverez ici des architectures, des diagrammes et des documents techniques qui fournissent des informations sur la conception, la création et le déploiement des technologies Citrix.

- Diagramme conceptuel Citrix Workspace : fournit une vue d'ensemble des domaines clés tels que l'identité, la fonctionnalité Workspace Intelligence et l'authentification unique Single Sign-On.
- Architectures de référence : fournit des guides complets pour la planification de votre mise en œuvre de Citrix Workspace, y compris les cas d'utilisation, les recommandations et les ressources associées.
- Architectures de référence de Virtual Apps and Desktops Service : fournit des conseils détaillés sur le déploiement de Citrix Virtual Apps and Desktops Service, ainsi que des services associés.

Ressources de formation

Le portail Citrix Cloud Learning Series offre des modules éducatifs pour vous permettre de vous familiariser avec Citrix Cloud et ses services. Vous pouvez afficher tous les modules de manière séquentielle, depuis les aperçus jusqu'à la planification et la création de services. Commencez votre parcours cloud avec les cours suivants :

- Fundamentals of Citrix Cloud
- Intro to Citrix Identity and Authentication
- Moving from StoreFront to Workspace

La vidéothèque Citrix Education offre des leçons vidéo en ligne qui vous guider dans les principales tâches de déploiement et de dépannage des composants que vous utilisez avec les services Citrix Cloud. Apprenez-en plus sur les tâches telles que l'installation de Cloud Connector et l'enregistrement de VDA, ainsi que la résolution des problèmes liés à ces composants.

Citrix Cloud Services

Micro-apps

Le service de micro-apps vous aide à envoyer des notifications pertinentes et exploitables à partir de vos applications directement dans les espaces de travail des utilisateurs. Créez des intégrations à partir de vos sources de données applicatives pour extraire des actions dans Workspace. Les micro-apps peuvent écrire sur les systèmes source, de sorte que les utilisateurs peuvent gérer ces actions sans quitter leur espace de travail. Les utilisateurs gagnent du temps et peuvent se concentrer sur leur travail principal car ils n'ont pas besoin de passer à d'autres applications pour interagir avec les principaux systèmes de votre organisation.

Pour de plus amples informations, consultez la documentation du service Micro-apps.

Virtual Apps and Desktops Service

Citrix Virtual Apps and Desktops Service (anciennement XenApp and XenDesktop Service) offre une solution de bureaux et d'applications virtuels, fournie sous la forme d'un service cloud, donnant aux employés la liberté de travailler n'importe où et sur n'importe quel appareil, tout en réduisant les coûts informatiques. Mettez à disposition des applications Windows, Linux, Web et SaaS ou des bureaux virtuels complets à partir de n'importe quel cloud : public, local ou hybride.

Pour en savoir plus sur ce service, consultez la section Citrix Virtual Apps and Desktops Service.

Endpoint Management

Solution de gestion des points de terminaison, Citrix Endpoint Management (anciennement XenMobile Service) offre des fonctionnalités de gestion d'appareils mobiles (MDM) et de gestion d'applications mobiles (MAM). Endpoint Management vous permet de gérer les stratégies d'appareil et d'application, ainsi que de fournir des applications aux utilisateurs.

Pour savoir comment configurer ce service, consultez la section 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 Workspace. Pour plus d'informations, consultez Secure Hub.

Citrix Secure Browser

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. Ce service fournit 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. Pour plus d'informations, consultez Secure Browser Service.

Citrix Gateway

Citrix Gateway (anciennement NetScaler Gateway Service) offre un accès sécurisé et contextuel aux applications et aux données dont vous avez besoin pour travailler efficacement.

Pour en savoir plus sur ce service, consultez la section Citrix Gateway Service.

Citrix Analytics

Citrix Analytics collecte des données sur l'ensemble du portefeuille de produits de Citrix et génère des insights actionnables, ce qui permet aux administrateurs de gérer de manière proactive les menaces de sécurité qui pèsent sur les utilisateurs et les applications, d'améliorer les performances des applications et de garantir la continuité des opérations.

Pour savoir comment configurer ce service, consultez la section Citrix Analytics.

Citrix Application Delivery Management

Citrix Application Delivery Management (anciennement NetScaler Management and Analytics Service) fournit une solution simple et évolutive pour gérer les déploiements de réseau Citrix sur site où sur le cloud à partir d'une console cloud unifiée et centralisée. Il offre toutes les fonctionnalités nécessaires pour configurer, déployer et gérer rapidement la distribution des applications dans les déploiements de réseau Citrix, avec des analyses détaillées de l'intégrité, des performances et de la sécurité des applications.

Pour en savoir plus sur ce service, consultez la section Citrix Application Delivery Management.

Citrix Content Collaboration

Les fonctionnalités avancées d'accès, de collaboration, de flux de travail, de gestion des droits et d'intégration de ShareFile sont désormais disponibles dans le composant Citrix Content Collaboration de Citrix Workspace, notre solution intégrée, contextuelle et sécurisée.

Pour en savoir plus sur ce service, consultez la section Citrix Content Collaboration.

Citrix SD-WAN Orchestrator

Citrix SD-WAN Orchestrator est une offre SaaS de gestion multi-locataire hébergée dans le cloud dont les partenaires Citrix peuvent tirer parti pour offrir des services managés SD-WAN à leurs clients. Cette

solution offre une plate-forme de gestion unique permettant aux partenaires Citrix de gérer de multiples clients de manière centralisée, avec contrôles d'accès basés sur les rôles.

Pour savoir comment configurer ce service, consultez la section Citrix SD-WAN Orchestrator.

Essayer Citrix Cloud

Profitez d'un environnement de production complet (dans le cadre d'une version d'évaluation) comprenant un ou plusieurs services Citrix Cloud. Après vous être inscrit à Citrix Cloud, vous pouvez demander des versions d'évaluation des services directement depuis la console. Une fois la version d'évaluation terminée, vous pouvez la convertir en environnement de production afin de conserver toutes vos configurations. Pour plus d'informations, consultez Évaluations de services Citrix Cloud.

Accord de niveau de service

July 20, 2021

Date d'entrée en vigueur : 30 octobre 2020

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 99.9 % (« 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, 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 (1 000 minimum pour les fournisseurs de services Citrix), selon le modèle de licence applicable au Service, au cours de la période.

Les fournisseurs de services Citrix (FSC) sont éligibles depuis le 1er octobre 2018.

Mesures de disponibilité par service

Service	Mesure par disponibilité mensuelle
Citrix Analytics for Performance	Durée pendant laquelle les utilisateurs peuvent accéder aux performances des applications et des bureaux et les améliorer.
Citrix Analytics for Security	Durée pendant laquelle les utilisateurs peuvent détecter et atténuer les risques liés à l'accès et à l'activité des utilisateurs.
Citrix Application Delivery Management Service	Durée moyenne de disponibilité du Service pour tous les POP.
Citrix Content Collaboration	Durée pendant laquelle les utilisateurs peuvent énumérer les fichiers et dossiers associés à leur compte ou télécharger des fichiers hébergés dans des zones de stockage gérées par Citrix.

Service	Mesure par disponibilité mensuelle
Citrix Endpoint Management	Durée pendant laquelle les utilisateurs peuvent accéder à leurs applications mobiles délivrées par Citrix et aux appareils inscrits via le Service.
Service Citrix Gateway pour proxy HDX	Durée pendant laquelle les utilisateurs peuvent accéder à leur session d'application ou de bureau via le Service.
Citrix 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.
Citrix SD-WAN Orchestrator	Les utilisateurs peuvent accéder à leur compte SD-WAN Orchestrator et gérer leur réseau SD-WAN via le service.
Citrix Secure Workspace Access	Durée pendant laquelle les utilisateurs peuvent accéder à leur application Web interne ou SaaS via le Service.
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.
Citrix Workspace	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 Wrike	Heure à laquelle les utilisateurs peuvent accéder au service et l'utiliser.

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, pendant les mois durant lesquels Citrix a manqué à son Engagement de Service, 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 : < 99.9 %
- Crédit de Service : 10 % pour les mois applicables (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 sera émis par Service, pendant le nombre de mois applicable, avec un maximum d'un seul crédit de service de 10 % pour tous les 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.

Guide de déploiement sécurisé pour la plate-forme Citrix Cloud

July 21, 2021

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 Analytics
- Vue d'ensemble de la sécurité technique de Endpoint Management
- Vue d'ensemble de la sécurité technique de Secure Browser
- Vue d'ensemble de la sécurité technique de ShareFile
- Vue d'ensemble de la sécurité technique de Virtual Apps and Desktops
- Vue d'ensemble de la sécurité technique de Virtual Apps and Desktops Standard pour Azure

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.
- Par défaut, Citrix Cloud met automatiquement fin aux sessions d'administrateur après 60 minutes d'inactivité. Ce délai d'expiration de 60 minutes ne peut pas être modifié. *Inactif* signifie que la session est complètement inactive et que l'administrateur n'interagit en aucune façon avec la console Citrix Cloud. *Activité* fait référence à des actions telles que la navigation dans l'interface graphique, la sélection d'options de configuration, l'enregistrement des modifications apportées à la configuration ou l'attente d'entrée en vigueur d'une modification.

Conformité des mots de passe

Citrix Cloud invite les administrateurs à modifier leurs mots de passe si leur mot de passe actuel date de plus de 60 jours. Les nouveaux mots de passe doivent répondre à tous les critères suivants :

- Au moins 12 caractères
- Inclure au moins une lettre majuscule et une lettre minuscule
- Inclure au moins un chiffre
- Inclure au moins un caractère spécial : ! @ # $ % ^ * ? + = -

Règles de modification des mots de passe :

- Au moins un caractère du mot de passe actuel doit être modifié. Le mot de passe actuel ne peut pas être utilisé comme nouveau mot de passe.
- Les 24 mots de passe précédents ne peuvent pas être réutilisés.

- Le nouveau mot de passe doit être en vigueur pendant au moins un jour avant que Citrix Cloud ne permette sa modification.

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 effectuant un demande explicite 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 et avoir configuré des suites de chiffrement acceptées.

- Si le Cloud Connector est installé sur Windows Server 2016 ou Windows Server 2019, les chiffrements forts suivants sont recommandés : TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- Si le Cloud Connector est installé sur Windows Server 2012 R2, les chiffrements forts ne sont pas disponibles, donc les chiffrements suivants doivent être utilisés : TLS_ECDHE_RSA_WITH_AES_256_CBC_SH TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

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, dans l'Union Européenne et en Australie. 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 Content Collaboration
- Questions fréquemment posées sur la sécurité de ShareFile
- Sécurité et conformité de Citrix ShareFile
- Comment mettre en œuvre des zones de stockage pour le stockage sur site

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.

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.

En outre, Citrix recommande fortement que les machines sur lesquelles le logiciel Cloud Connector est installé se trouvent 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 apporte son assistance aux clients qui utilisent d'autres antivirus standard.

Dans l'Active Directory (AD) du client, Citrix recommande fortement que le compte d'ordinateur du Cloud Connector soit 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 permet aux informations de sécurité sensibles d'être transmises à d'autres composants de plate-forme dans les services Citrix Cloud, mais stocke également les informations sensibles suivantes :

- Clés de service pour communiquer avec Citrix Cloud

- Informations d'identification du service Hypervisor pour la gestion de l'alimentation dans Citrix Virtual Apps and Desktops

Ces informations sensibles sont chiffrées à l'aide de l'API de protection des données (DPAPI) sur le serveur Windows hébergeant le Cloud Connector. Citrix recommande fortement d'autoriser uniquement les administrateurs les plus privilégiés à se connecter aux machines 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 d'autres logiciels 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 des vecteurs d'attaque possibles 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. Citrix recommande fortement que le Cloud Connector ne dispose pas 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 d'autres ports sortants avec accès à Internet. Le Cloud Connector négocie sur une large gamme de ports pour optimiser la bande passante et les performances du réseau si d'autres ports 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.

Port 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

Port client	Port du serveur	Service
49152 -65535/TCP	49152-65535/TCP	RPC pour LSA, SAM, Netlogon (*)
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 étend 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 termes de connexion Internet pour Citrix Cloud Services
- 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.

En mode de fonctionnement normal, le Cloud Connector communique uniquement avec les contrôleurs de domaine des domaines qui ne sont pas désactivés sur la page **Gestion des identités et des accès** de l'interface utilisateur Citrix Cloud.

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 termes de connexion Internet pour Citrix Cloud Services

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 peuvent changer les certificats et les autorités de certification à l'avenir, mais utilisent 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 section 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.

Appliance Connector Citrix pour les services cloud

Installation de l'appliance Connector

L'appliance Connector est hébergée sur un hyperviseur. Cet hyperviseur doit se trouver à l'intérieur de votre réseau privé et non dans la zone DMZ.

Vérifiez que l'appliance Connector se trouve dans un pare-feu qui bloque l'accès par défaut. Utilisez une liste d'autorisation pour autoriser uniquement le trafic attendu de l'appliance Connector.

Assurez-vous que les hyperviseurs qui hébergent vos appliances Connector sont installés avec des mises à jour de sécurité à jour.

Pour la configuration système et réseau requise et des instructions sur l'installation de l'appliance Connector, consultez la section Appliance Connector pour Cloud Services.

Connexion à l'hyperviseur hébergeant une appliance Connector

L'appliance Connector contient une clé de service permettant de communiquer avec Citrix Cloud. Seuls les administrateurs les plus privilégiés doivent être en mesure de se connecter à un hyperviseur hébergeant l'appliance Connector (par exemple, pour effectuer des opérations de maintenance). En général, il n'est pas nécessaire qu'un administrateur se connecte à ces hyperviseurs pour gérer des produits Citrix. L'appliance Connector est auto-gérée.

Configuration des ports entrants et sortants

L'appliance Connector nécessite que le port sortant 443 soit ouvert avec accès à Internet. Citrix recommande fortement que l'appliance Connector ne dispose pas de ports entrants accessibles depuis Internet.

Vous pouvez placer l'appliance Connector derrière un proxy Web pour surveiller ses communications Internet sortantes. Cependant, le proxy Web doit fonctionner avec une communication cryptée SSL/TLS.

L'appliance Connector peut avoir d'autres ports sortants avec accès à Internet. L'appliance Connector négocie sur une large gamme de ports pour optimiser la bande passante et les performances du réseau si d'autres ports sont disponibles.

L'appliance 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.

Direction de la connexion	Port de l'appliance Connector	Port externe	Service
Entrante	443/TCP	Quelconque	Interface Web locale

Direction de la connexion	Port de l'appliance Connector	Port externe	Service
Sortante	49152-65535/UDP	123/UDP	NTP
Sortante	53, 49152 -65535/TCP/UDP	53/TCP/UDP	DNS
Sortante	67/UDP	68/UDP	DHCP et diffusion

Chacun des services utilisés dans Citrix Cloud étend 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)
- Configuration requise pour le système et la connectivité pour Citrix Cloud Services

Contrôle des communications sortantes

L'appliance Connector communique vers Internet sur le port 443 vers les serveurs Citrix Cloud.

Chaque service dans le Citrix Cloud étend la liste des serveurs et des ressources internes que l'appliance Connector peut contacter au cours de ses opérations normales. En outre, les clients ne peuvent pas contrôler les données que l'appliance 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)
- Configuration requise pour le système et la connectivité pour Citrix Cloud Services

Affichage des journaux de l'appliance Connector

Vous pouvez télécharger un rapport de diagnostic pour votre appliance Connector qui inclut divers fichiers journaux. Pour savoir comment obtenir ce rapport, reportez-vous à la section Appliance Connector pour Cloud Services.

Configuration de SSL/TLS

L'appliance Connector n'a pas besoin de configuration SSL/TLS spéciale.

L'appliance Connector approuve l'autorité de certification utilisée par les certificats SSL/TLS de Citrix Cloud. Citrix peut modifier les certificats et les autorités de certification à l'avenir, mais toujours utiliser les autorités de certification que l'appliance Connector approuve.

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

Conformité aux normes de sécurité

Pour garantir la conformité à la sécurité, l'appliance Connector s'auto-gère et vous ne pouvez pas vous connecter via la console.

Vous n'êtes pas tenu de prendre d'autres mesures pour réagir aux problèmes de sécurité du connecteur. L'appliance Connector applique automatiquement les correctifs de sécurité.

Assurez-vous que les hyperviseurs qui hébergent vos appliances Connector sont installés avec des mises à jour de sécurité à jour.

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 continuent à fonctionner normalement. Les anciens secrets d'autorisation deviennent 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.

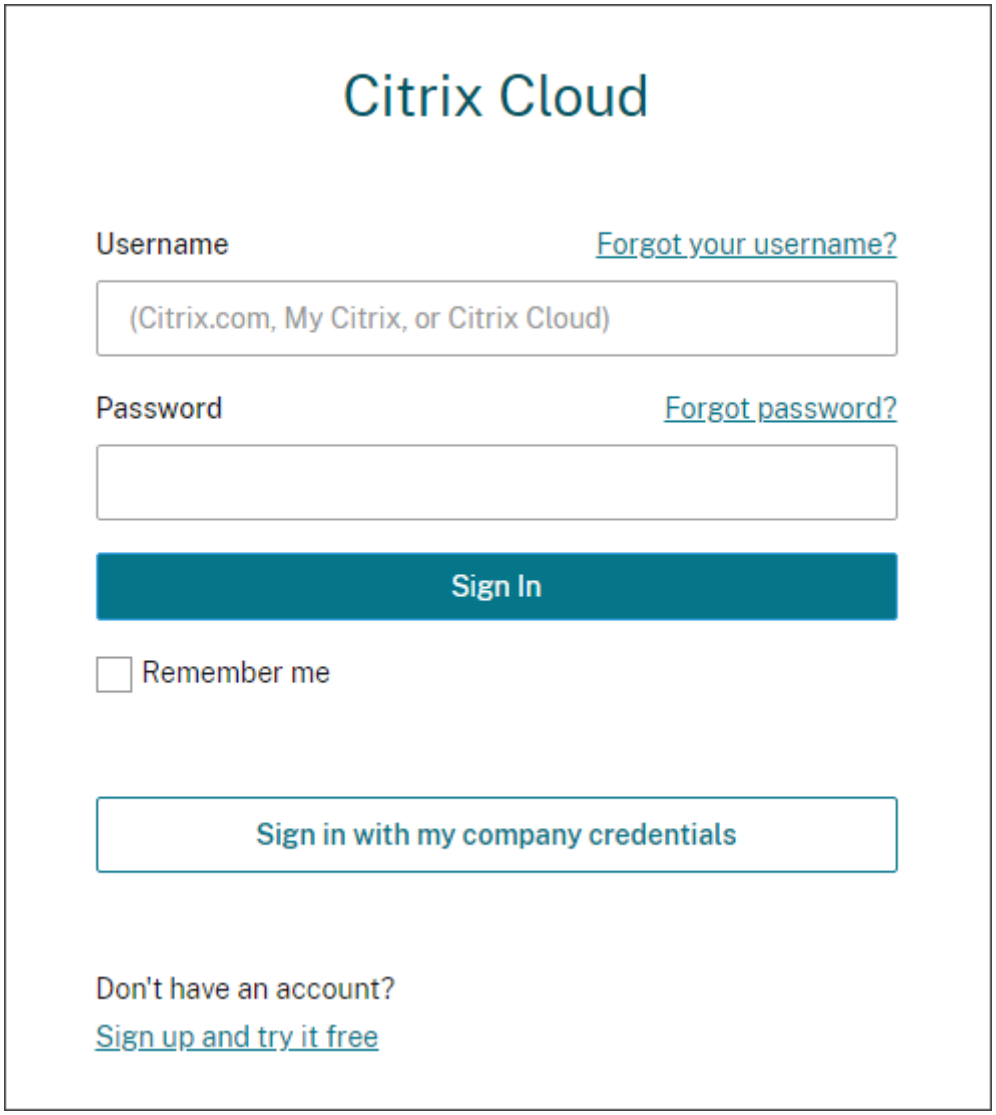
Comment obtenir de l'aide

July 21, 2021

Création d'un compte Citrix Cloud

Si vous rencontrez une erreur lors de votre inscription à un compte Citrix Cloud, contactez le Support technique 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 vous ne vous êtes pas récemment connecté à Citrix Cloud ou si votre mot de passe ne répond pas aux exigences, vous êtes invité à réinitialiser votre mot de passe avant de vous connecter. Pour plus d'informations, consultez la section Modification de votre mot de passe dans cet article.
- Si les utilisateurs accèdent à Citrix Cloud à l'aide des informations d'identification de l'entreprise au lieu d'un compte Citrix, sélectionnez **Se connecter avec les informations d'identification de mon 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.

Modification de votre mot de passe

Si vous avez oublié le mot de passe de votre compte Citrix Cloud, sélectionnez **Nom d'utilisateur ou mot de passe oublié ?** et saisissez l'adresse e-mail de votre compte pour recevoir 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 de Citrix.

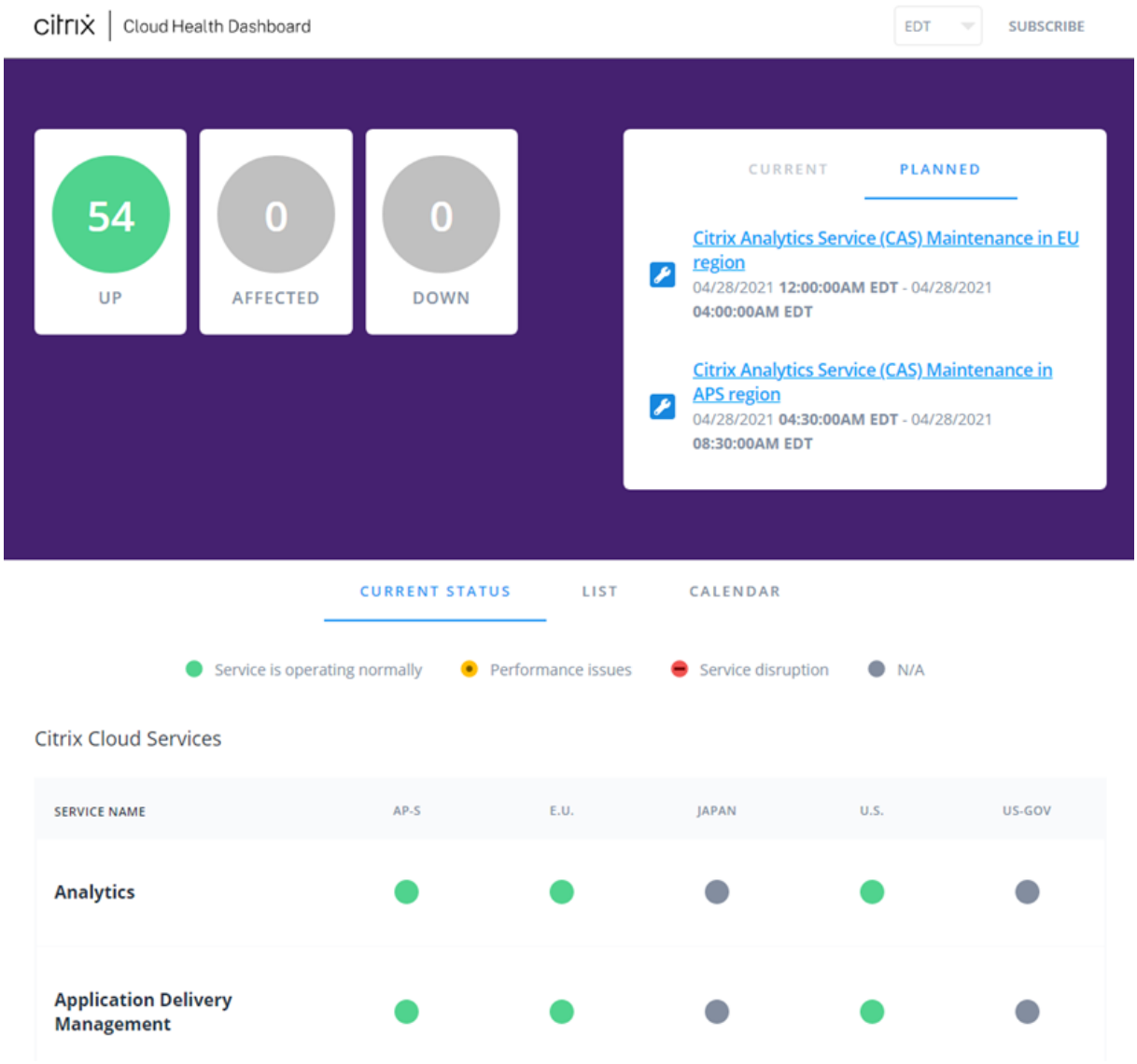
Pour vous aider à préserver la sécurité du mot de passe de votre compte, Citrix Cloud peut vous inviter à réinitialiser votre mot de passe lorsque vous tentez de vous connecter. Cette invite s'affiche si :

- Votre mot de passe ne répond pas aux exigences de complexité de Citrix Cloud. Les mots de passe doivent comporter au moins 8 caractères et comprendre :
  - Au moins un chiffre
  - Au moins une lettre majuscule
  - Au moins un symbole : ! @ # $ % ^ * ? + = -
- Votre mot de passe inclut des mots du dictionnaire.
- Votre mot de passe est répertorié dans une base de données connue de mots de passe compromis.
- Vous ne vous êtes pas connecté à Citrix Cloud au cours des six derniers mois.

Lorsque vous y êtes invité, sélectionnez **Réinitialiser mot de passe** pour créer un nouveau mot de passe fort pour votre compte.

Cloud Health Dashboard

Citrix Cloud Health Dashboard (https://status.cloud.com) fournit une vue d'ensemble de la disponibilité en temps réel de la plate-forme et des services Citrix Cloud dans chaque région géographique. Si vous rencontrez des problèmes avec Citrix Cloud, consultez Cloud Health Dashboard pour vérifier si Citrix Cloud ou des services spécifiques fonctionnent normalement.

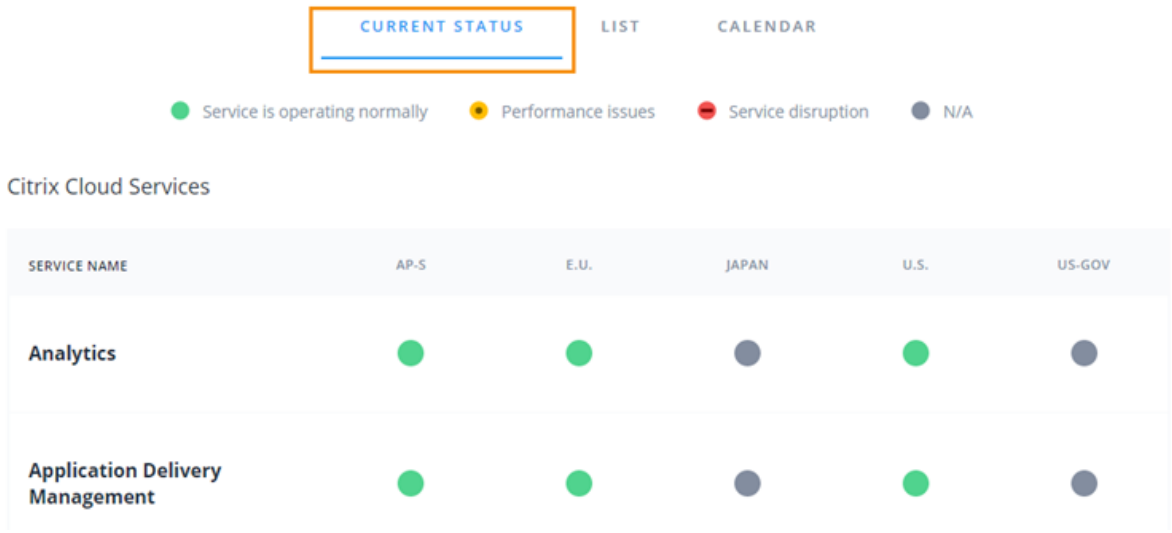


Utilisez le tableau de bord pour en savoir plus sur les conditions suivantes :

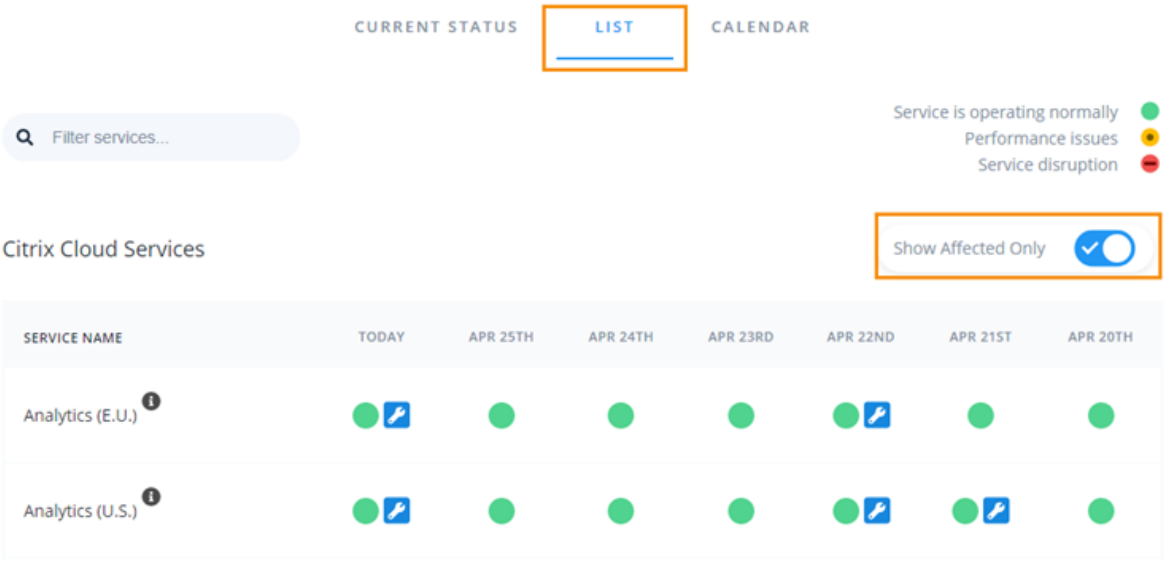
- État de santé actuel de tous les services Citrix Cloud, regroupés par région géographique
- Historique de santé de chaque service au cours des sept derniers jours
- Fenêtres de maintenance pour des services spécifiques

Afficher l'état de santé et de maintenance

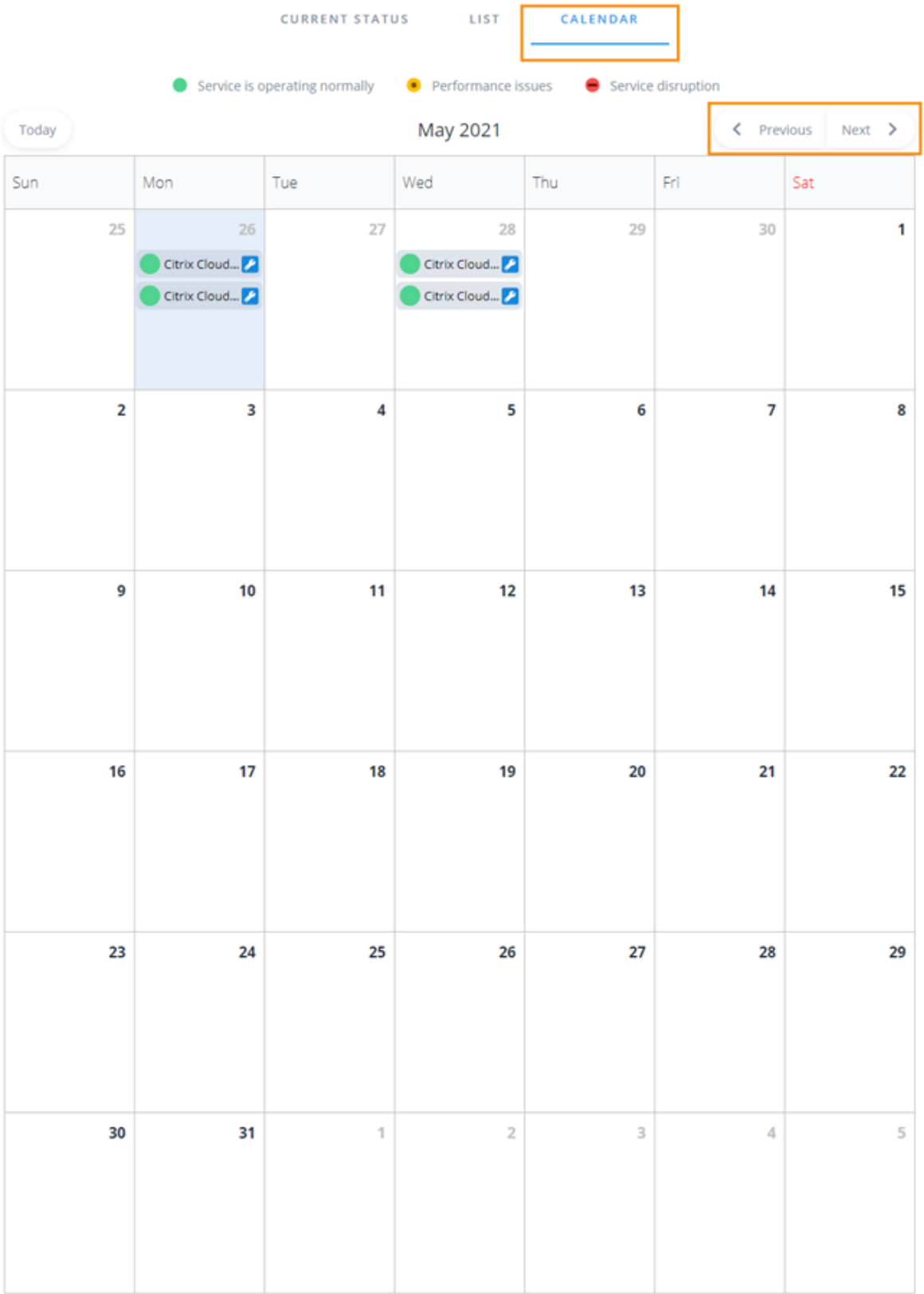
Sélectionnez **Current Status** pour afficher l'état de santé actuel de tous les services et composants de plate-forme Citrix Cloud dans chaque région géographique.



Sélectionnez **List** pour afficher l'état de santé de tous les services et composants de plate-forme Citrix Cloud au cours des sept derniers jours. Sélectionnez **Show Affected Only** pour afficher uniquement les services ayant subi des événements de maintenance ou de santé au cours des sept derniers jours.



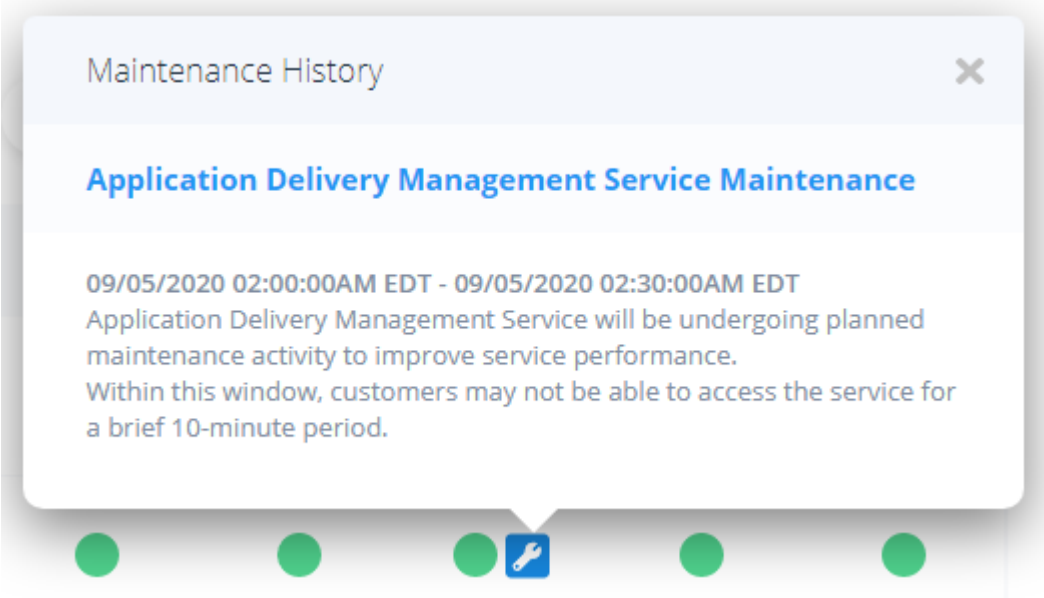
Sélectionnez **Calendar** pour afficher une vue du calendrier des fenêtres de maintenance du service. Sélectionnez **Next** ou **Previous** pour faire défiler les événements de maintenance planifiés pour chaque mois.



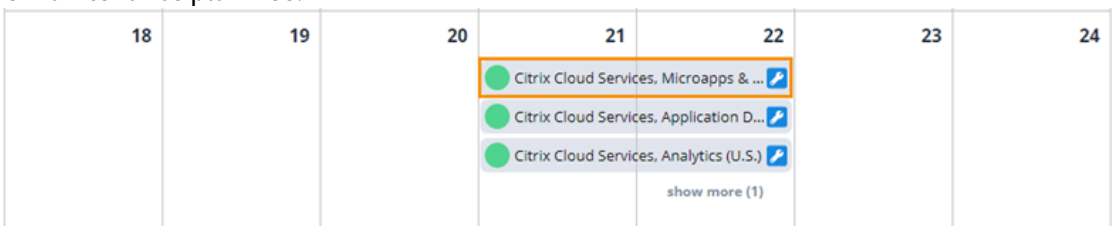
Afficher les détails des incidents d'un service

Pour afficher des informations plus détaillées sur l'incident de santé d'un service concerné :

- Dans la vue List, cliquez sur l'icône en regard de l'indicateur de service pour afficher des informations plus détaillées sur l'incident.



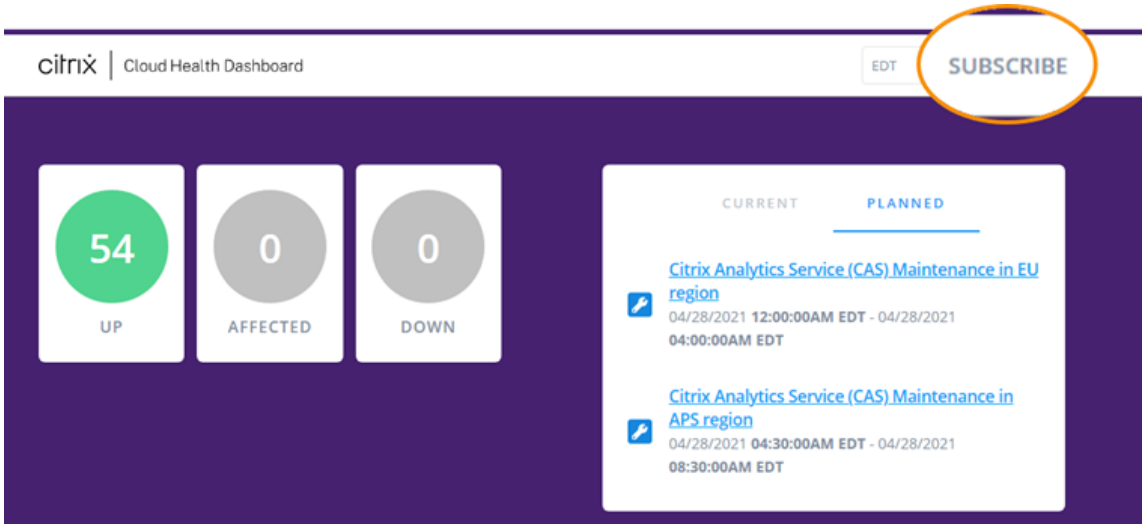
- Dans la vue Calendar, cliquez sur l'entrée de service pour afficher la page d'état de la fenêtre de maintenance planifiée.



S'abonner aux notifications

Vous pouvez recevoir des notifications sur les événements de santé du service à l'aide des méthodes suivantes :

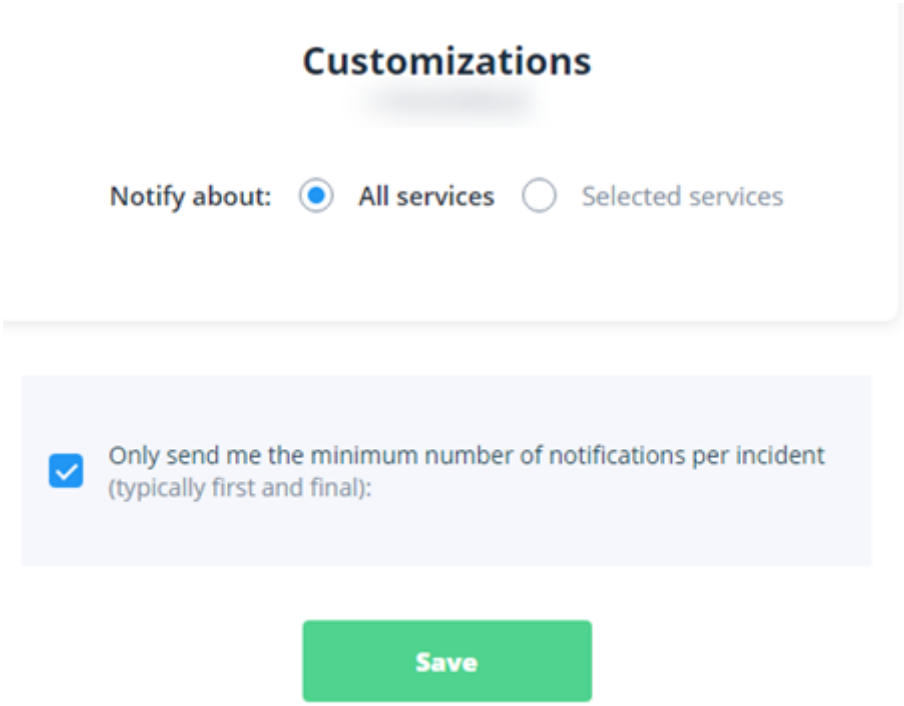
- Sélectionnez **Subscribe** en haut à droite du tableau de bord et sélectionnez la méthode de notification que vous souhaitez utiliser. Vous pouvez choisir parmi plusieurs méthodes, y compris l'e-mail et le téléphone.



- Entrez les URL suivantes dans votre lecteur RSS pour vous abonner au flux RSS Citrix Cloud Health :
  - Pour recevoir des notifications d'incident de service et de maintenance dans un seul flux, abonnez-vous à `https://status.cloud.com/?format=atom`.
  - Pour recevoir uniquement les notifications d'incident de service, abonnez-vous à `https://status.cloud.com/atom/incidents`.
  - Pour recevoir uniquement les notifications de maintenance, abonnez-vous à `https://status.cloud.com/atom/maintenances`.

Pour vous abonner à toutes les notifications de service dans toutes les régions géographiques :

1. Sélectionnez **Subscribe** en haut à droite du tableau de bord et sélectionnez la méthode de notification que vous souhaitez utiliser.
2. Entrez les coordonnées ou l'URL de la méthode d'abonnement choisie. Sélectionnez **Next**.
3. Dans la page **Customizations**, sélectionnez **All services** pour recevoir des notifications pour tous les services dans toutes les régions géographiques.
4. Pour ne recevoir que les première et dernière notifications pour chaque incident, sélectionnez **Only send me the minimum number of notifications per incident**.
5. Cliquez sur **Enregistrer**.



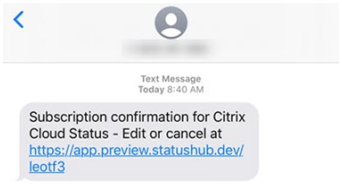
Pour vous abonner aux notifications pour des services ou régions spécifiques :

1. Sélectionnez **Subscribe** en haut à droite du tableau de bord et sélectionnez la méthode de notification que vous souhaitez utiliser.
2. Entrez les coordonnées ou l'URL de la méthode d'abonnement choisie. Sélectionnez **Next**.
3. Dans la page **Customizations**, sélectionnez **Selected services**. Une liste de plusieurs pages affiche tous les services dans chaque région prise en charge.
4. Sélectionnez les services dans les régions géographiques pour lesquelles vous souhaitez être averti. Pour être informé de tous les services d'une région géographique, sélectionnez **Aggregate by groups**, puis sélectionnez la région.
5. Pour ne recevoir que les première et dernière notifications pour chaque incident, sélectionnez **Only send me the minimum number of notifications per incident**.
6. Cliquez sur **Enregistrer**.

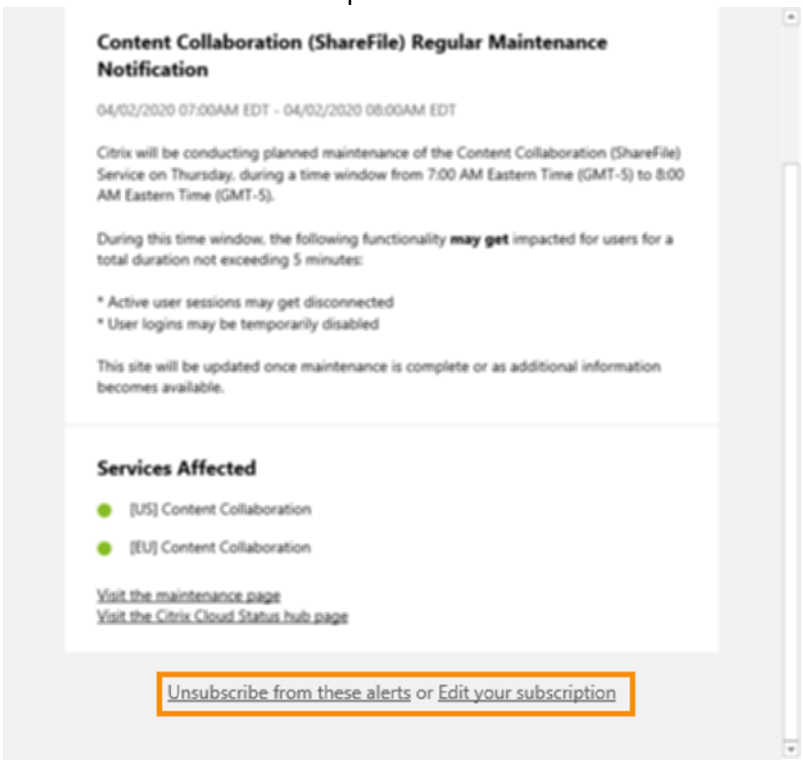
Se désabonner des notifications

Selon le mode d'abonnement, des liens pour vous désabonner ou modifier votre abonnement sont inclus dans le message de confirmation que vous recevez (par exemple, lors de l'abonnement à des notifications téléphoniques) ou dans chaque message de notification (par exemple, lorsque vous vous abonnez à des notifications par e-mail). Par exemple :

- Notification téléphonique avec options d'abonnement :



- E-mail de notification avec options d'abonnement



Pour vous désabonner de toutes les notifications et supprimer toutes les méthodes d'abonnement :

1. Localisez votre message de confirmation d'abonnement ou une notification existante et sélectionnez le lien pour vous désabonner. Certaines méthodes d'abonnement peuvent fournir un lien unique pour modifier ou annuler votre abonnement.
2. Selon votre méthode d'abonnement, utilisez l'une des options suivantes sur la page **Edit Subscriptions** :
   - Sélectionnez **Remove all subscriptions**.
   - Sélectionnez **Unsubscribe**. Dans la page **Unsubscribe methods**, sélectionnez **Remove all subscriptions**.

Pour se désabonner de toutes les notifications pour une méthode d'abonnement spécifique :

1. Localisez votre message de confirmation d'abonnement ou une notification existante et sélectionnez le lien pour vous désabonner. Certaines méthodes d'abonnement peuvent fournir un lien unique pour modifier ou annuler votre abonnement.
2. Selon votre méthode d'abonnement, utilisez l'une des options suivantes sur la page **Edit Subscriptions** :

- Sélectionnez la méthode d'abonnement que vous souhaitez supprimer. Votre abonnement est immédiatement supprimé.
- Sélectionnez **Unsubscribe**. Dans la page **Unsubscribe methods**, sélectionnez la méthode d'abonnement à supprimer. Votre abonnement est immédiatement supprimé.

Modifier les notifications de service

1. Localisez votre message de confirmation d'abonnement ou une notification existante et sélectionnez le lien pour modifier votre abonnement. Certaines méthodes d'abonnement peuvent fournir un lien unique pour modifier ou annuler votre abonnement.
2. Sur la page **Edit Subscriptions**, sélectionnez la méthode d'abonnement à gérer.
3. Sur la page **Customizations**, sélectionnez les services pour lesquels vous souhaitez recevoir des notifications ou désactivez les services pour lesquels vous ne souhaitez plus recevoir de notifications, le cas échéant.
4. Sélectionnez **Enregistrer**.

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 articles du forum. Cependant, vous devez vous connecter pour publier un article ou y 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 compte Citrix, accédez à la page Create or request an account (Créer ou demander un compte).

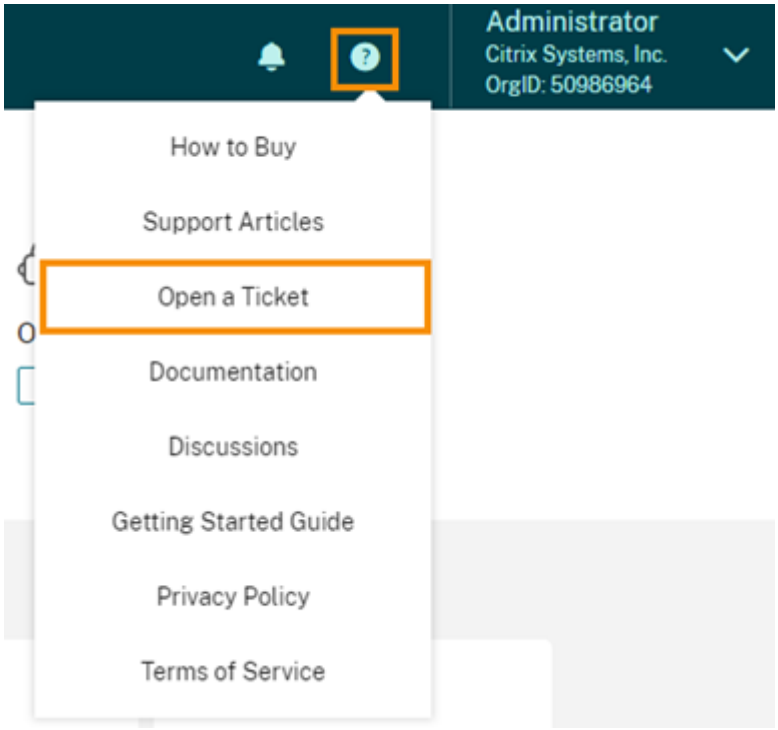
Support technique

Si vous rencontrez un problème nécessitant une aide technique, vous pouvez accéder au Centre de connaissances du support Citrix pour ouvrir un ticket de support ou discuter avec un représentant du support technique Citrix.

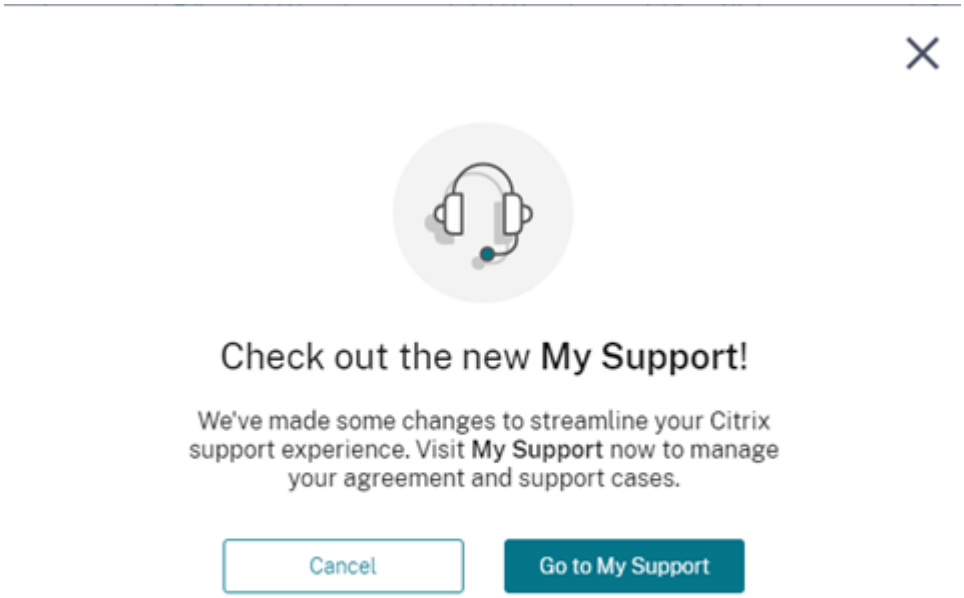
Pour accéder au Centre de connaissances du support, accédez à https://support.citrix.com/case/manage.

Vous pouvez également procéder comme suit dans Citrix Cloud :

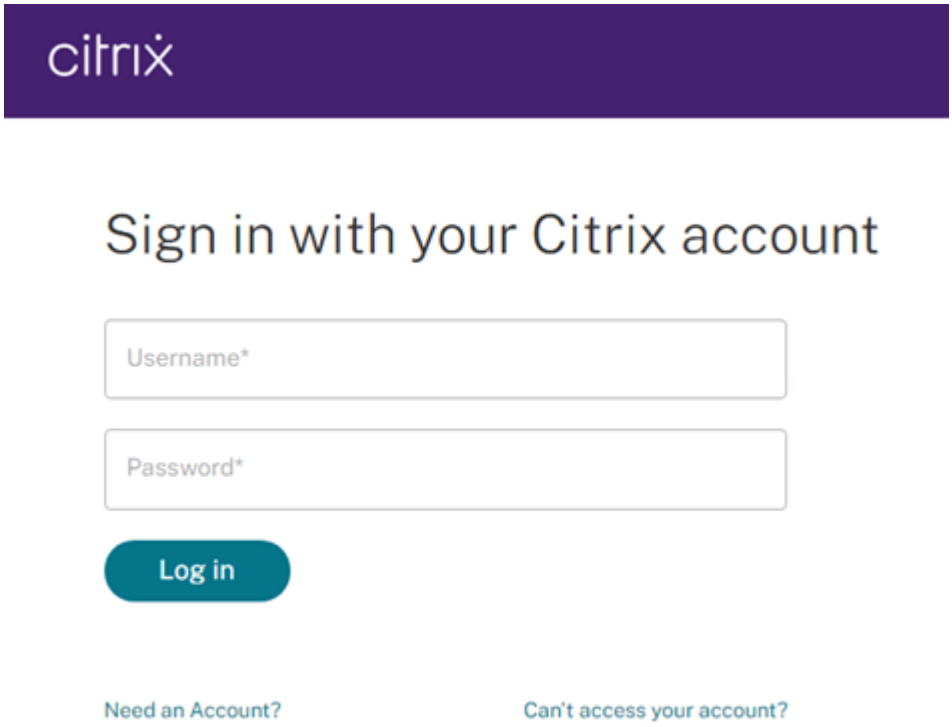
1. Sélectionnez l'icône **Aide** en haut à droite de l'écran.



2. Sélectionnez **Ouvrir un ticket > Accéder à My support**.

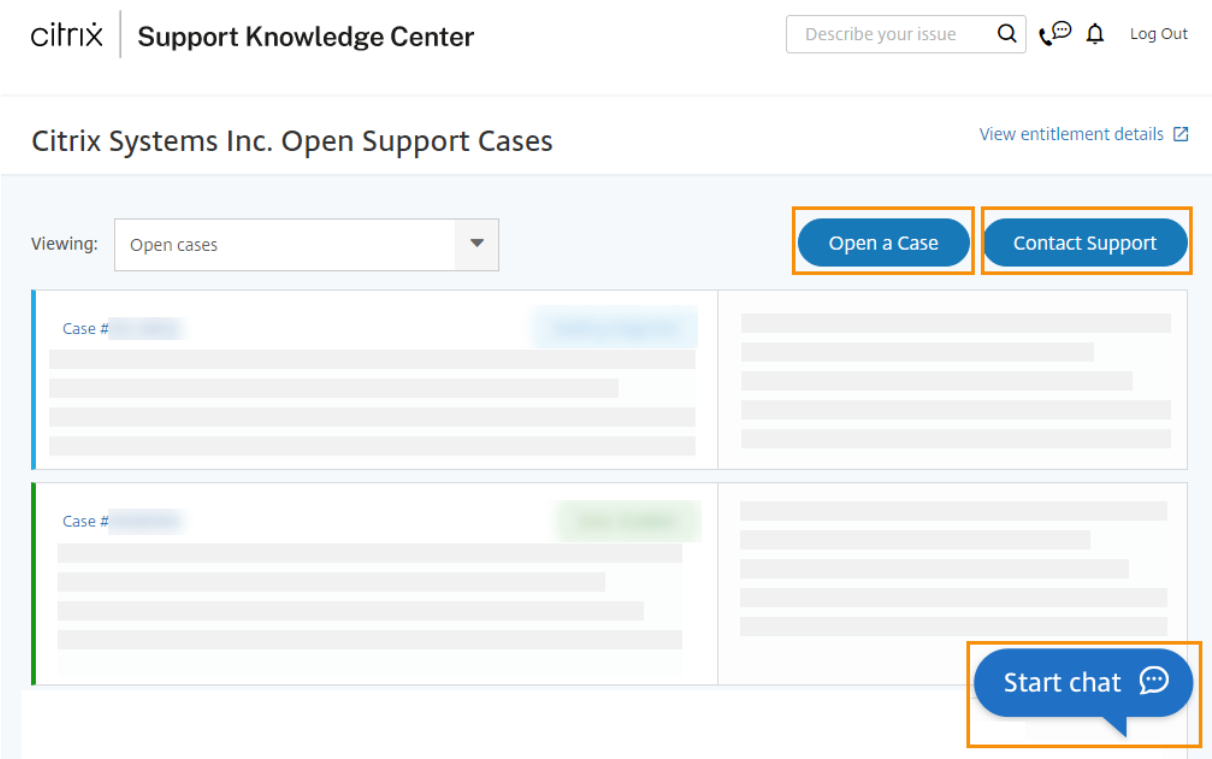


3. Connectez-vous avec votre compte Citrix.



Après vous être connecté, contactez le support technique Citrix en utilisant l'une des méthodes suivantes :

- Ouverture d'un ticket de support : sélectionnez **Open a Case**, puis fournissez les détails du problème que vous rencontrez.
- Par téléphone : sélectionnez **Contact Support** pour afficher la liste des numéros de téléphone locaux que vous pouvez utiliser pour appeler le support technique Citrix.
- Chat en direct : sélectionnez **Start chat** dans le coin inférieur droit de la page pour discuter avec un représentant du support technique Citrix.



Articles de support et documentation

Citrix propose un grand nombre d'articles de support et de documentation produit pour vous aider à tirer le meilleur parti de Citrix Cloud et à résoudre les problèmes que vous pourriez rencontrer avec les produits Citrix.

Ressources de formation

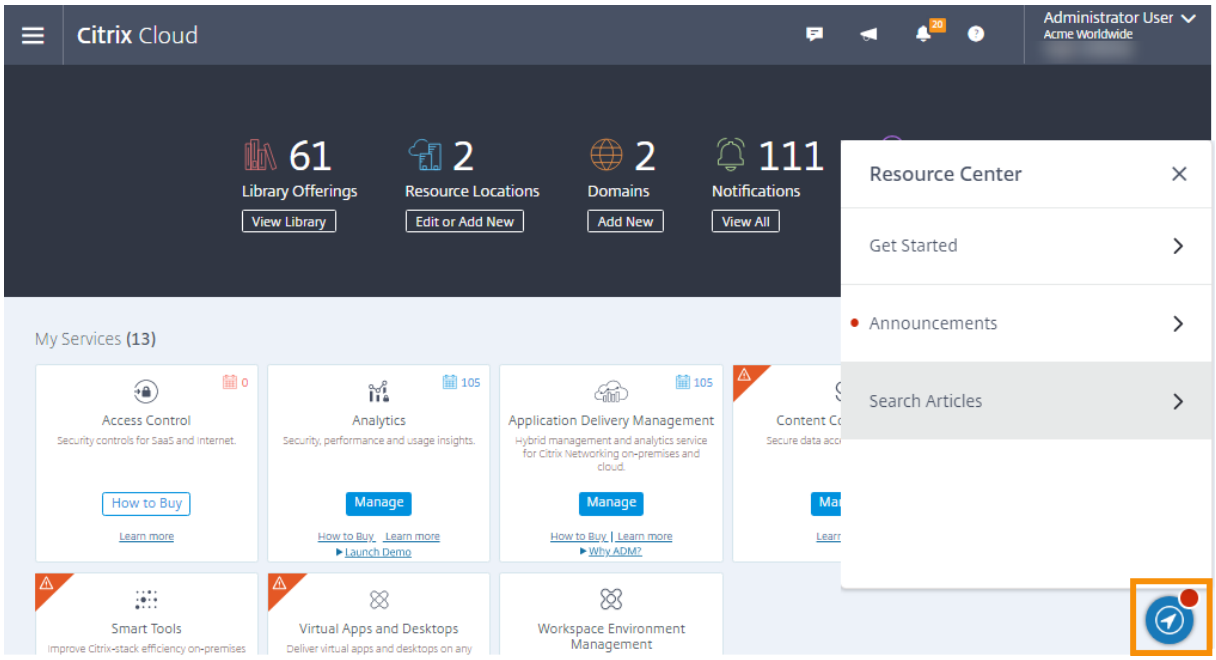
Le portail Citrix Cloud Learning Series offre des modules éducatifs pour vous permettre de vous familiariser avec Citrix Cloud et ses services. Vous pouvez afficher tous les modules de manière séquentielle, depuis les aperçus jusqu'à la planification et la création de services. Commencez votre parcours cloud avec les cours suivants :

- Fundamentals of Citrix Cloud
- Intro to Citrix Identity and Authentication
- Moving from StoreFront to Workspace

La vidéothèque Citrix Education offre des leçons vidéo en ligne qui vous guider dans les principales tâches de déploiement et de dépannage des composants que vous utilisez avec les services Citrix Cloud. Apprenez-en plus sur les tâches telles que l'installation de Cloud Connector et l'enregistrement de VDA, ainsi que la résolution des problèmes liés à ces composants.

Centre de ressources Citrix Cloud

Le centre de ressources Citrix Cloud peut vous aider à faire vos premiers pas avec Citrix Cloud, à en savoir plus sur les fonctionnalités et à effectuer des recherches pour résoudre les problèmes. Cliquez sur l'icône de la boussole bleue en bas à droite de la page. Cette fonctionnalité est disponible pour la plate-forme Citrix Cloud, Virtual Apps and Desktops et les services Application Delivery Management.



- **Mise en route** : fournit une brève présentation guidée des tâches clés spécifiques au service avec lequel vous travaillez actuellement. Vous pouvez également trouver des liens vers des ressources de formation et d'intégration pour vous aider à en savoir plus sur les fonctionnalités de service et à configurer vos utilisateurs.
- **Annonces** : fournit des notifications sur les fonctionnalités nouvellement publiées et des liens vers les communications Citrix importantes. Sélectionnez une notification de fonctionnalité pour obtenir une courte présentation guidée de la fonctionnalité.
- **Rechercher des articles** : fournit une liste des documents produit et des articles du Centre de connaissances pour les tâches courantes et vous aide à trouver d'autres articles, sans quitter Citrix Cloud. Entrez une requête de recherche dans le champ **Comment...** pour obtenir une liste d'articles filtrée en fonction du service avec lequel vous travaillez. En général, les articles de support apparaissent en premier dans la liste, suivis des articles de documentation produit.

Citrix Tech Zone

Citrix Tech Zone contient de nombreuses informations pour vous aider à en savoir plus sur Citrix Cloud et d'autres produits Citrix. Vous trouverez ici des architectures, des diagrammes, des vidéos et des documents techniques qui fournissent des informations sur la conception, la création et le dé-

ploiement des technologies Citrix.

Avis de tiers

June 10, 2021

- Citrix Cloud - Avis de tiers (PDF)
- Citrix Analytics Service - Avis de tiers (PDF)
- Virtual Apps and Desktops - Avis de tiers (PDF)
- Virtual Apps and Desktops Standard pour Azure - Avis de tiers (PDF)
- Citrix ShareFile Sync pour Mac - Avis de tiers (PDF)
- Citrix ShareFile Sync pour Windows - Avis de tiers (PDF)
- Secure Browser Service (PDF)
- Citrix Endpoint Management - Avis de tiers (PDF)
- Citrix Cloud Linux VDA Image Service - Avis de tiers (PDF)
- Appliance Connector pour Cloud Services – Avis de tiers (PDF)
- Avis tiers du service Citrix Microapps (PDF)

Ouvrir un compte sur Citrix Cloud

July 21, 2021

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.

> **Conseil :**
>
> Le module de formation « Getting Started with Citrix Cloud », inclus dans le cours Fundamentals of Citrix Cloud, fournit de courtes vidéos qui vous expliquant les tâches décrites dans cet article. Le cours complet vous fournit également une base solide pour comprendre Citrix Cloud, ses avantages pour votre organisation et les principaux cas d'utilisation utilisés par les services Citrix Cloud.

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 support client Citrix à l'adresse https://www.citrix.com/contact/support.html.

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

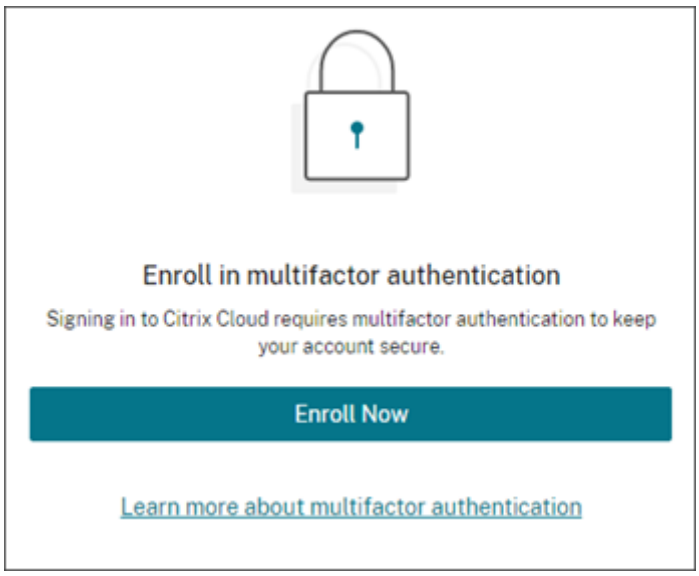
Un compte Citrix Cloud vous permet d'utiliser un ou plusieurs services Citrix Cloud de façon à pouvoir distribuer vos applications et vos données en toute sécurité. Un compte Citrix Cloud est également identifié de manière unique par un OrgID, tout comme votre compte Citrix. Il est important d'utiliser 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.

Exigences liées à l'authentification multifacteur

Pour garantir la sécurité de votre compte Citrix Cloud, Citrix Cloud exige que tous les clients s'inscrivent à l'authentification multifacteur. Pour vous inscrire, vous n'avez besoin que d'un appareil, tel qu'un ordinateur ou un appareil mobile, ainsi qu'une application d'authentification installée, telle que Citrix SSO.

Si vous êtes un client Citrix existant, Citrix Cloud vous invite à vous inscrire lorsque vous accédez à la page d'inscription et entrez les informations d'identification associées à votre compte Citrix.com. Si vous débutez avec Citrix, Citrix Cloud vous invite à vous inscrire après avoir créé un compte Citrix au cours du processus d'inscription.

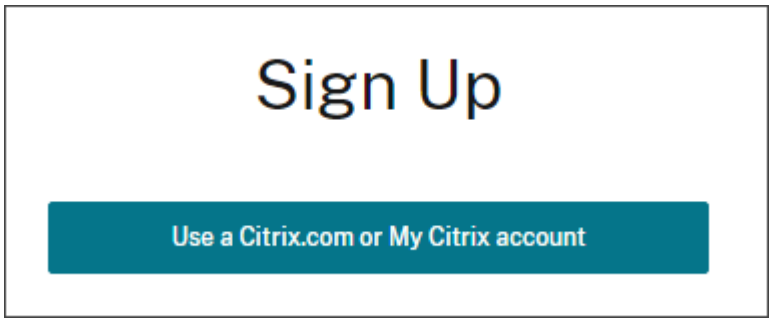


Étape 1 : Accéder à la page d'inscription

À l'aide d'un navigateur Web, accédez à https://onboarding.cloud.com.

Si vous êtes un client Citrix existant ou disposez d'un compte Citrix.com ou My Citrix

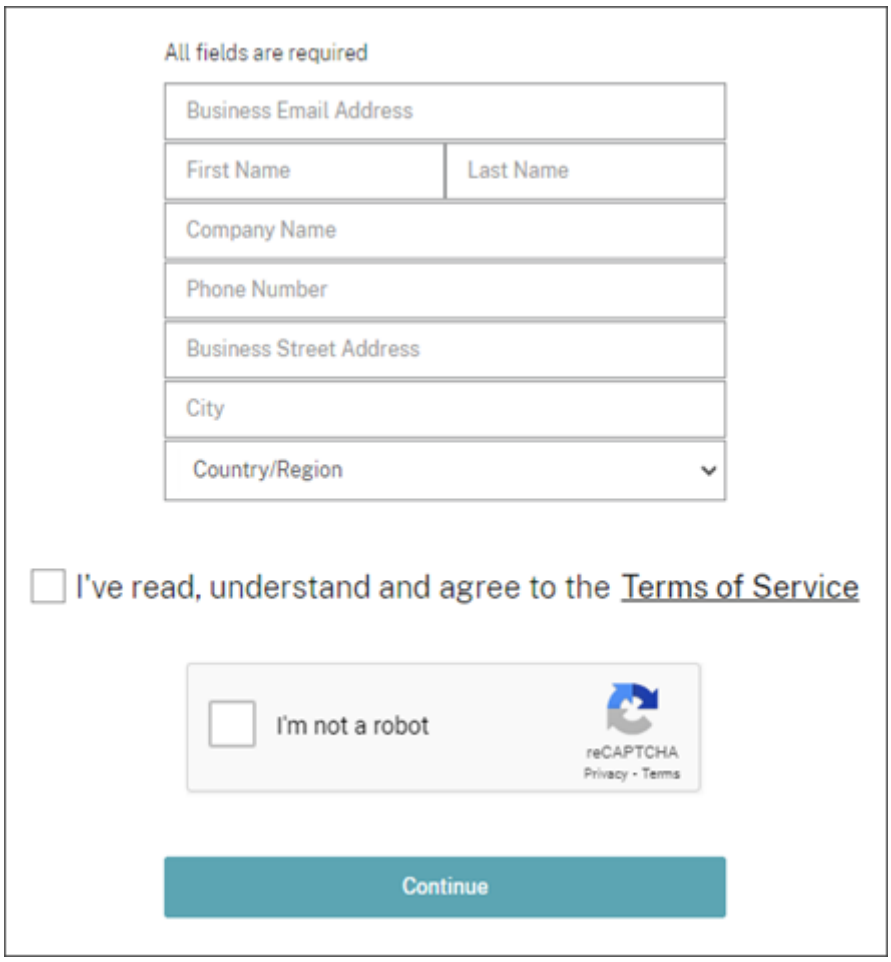
1. Sélectionnez **Utiliser un compte Citrix.com ou My Citrix**.



2. Entrez votre nom d'utilisateur et votre mot de passe (votre connexion web) ou l'adresse e-mail et le mot de passe associés à votre compte Citrix.com.
3. Lorsque vous êtes invité à vous inscrire à l'authentification multifacteur, sélectionnez **S'inscrire maintenant**.
4. Terminez le processus d'inscription comme décrit à la section Étape 5 : S'inscrire à l'authentification multifacteur de cet article.

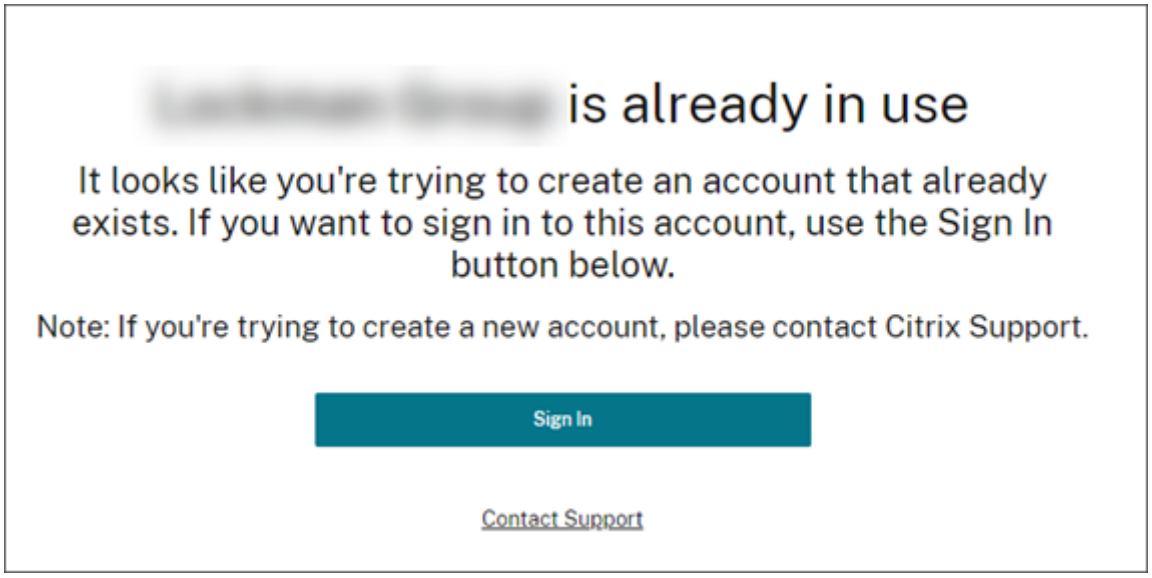
Si vous débutez avec Citrix et Citrix Cloud

Renseignez les champs du formulaire et sélectionnez **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.

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

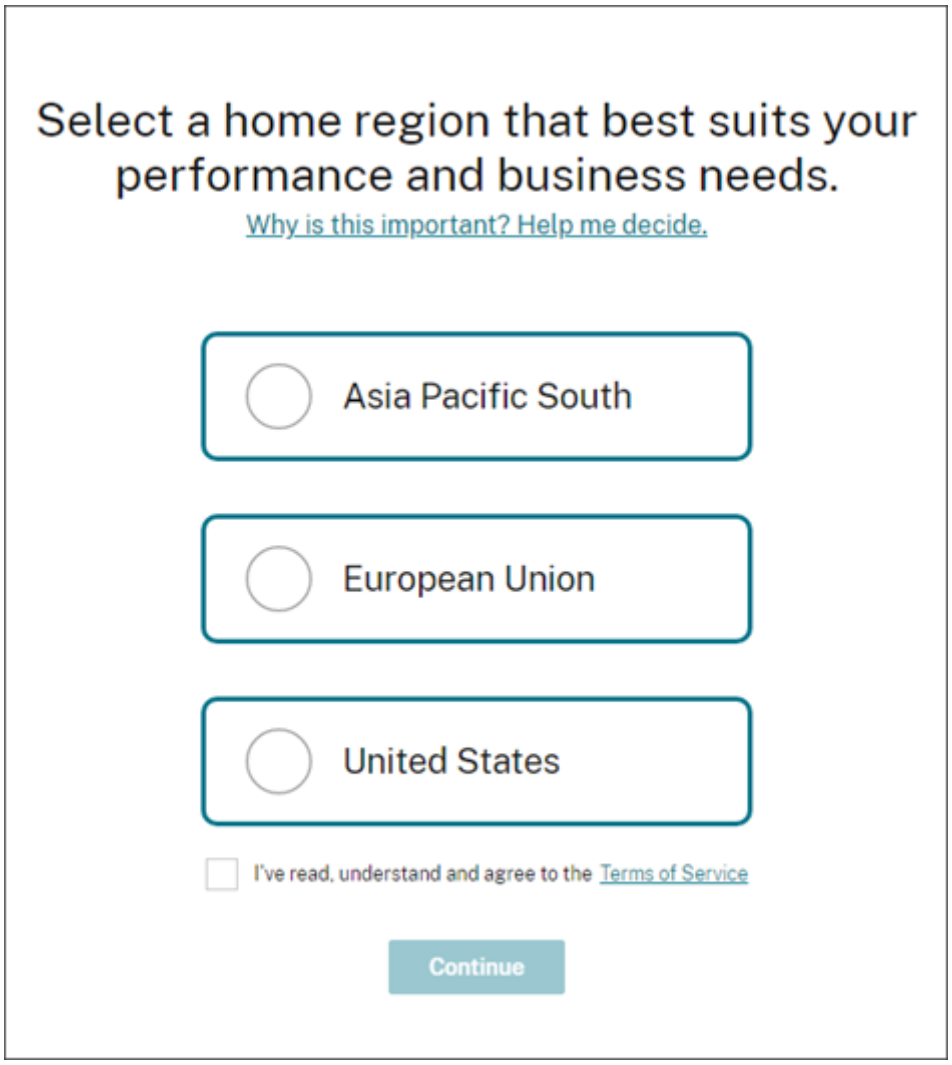


Si vous voyez ce message, cela signifie qu'un autre administrateur de votre compte Citrix a déjà créé le compte Citrix Cloud.

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.

Si vous sélectionnez **Demander approbation**, tous les administrateurs existants du compte sont informés de votre demande. Si les administrateurs existants ne font plus partie de votre organisation, contactez le support Citrix.

Étape 2 : Choisir votre région Citrix Cloud

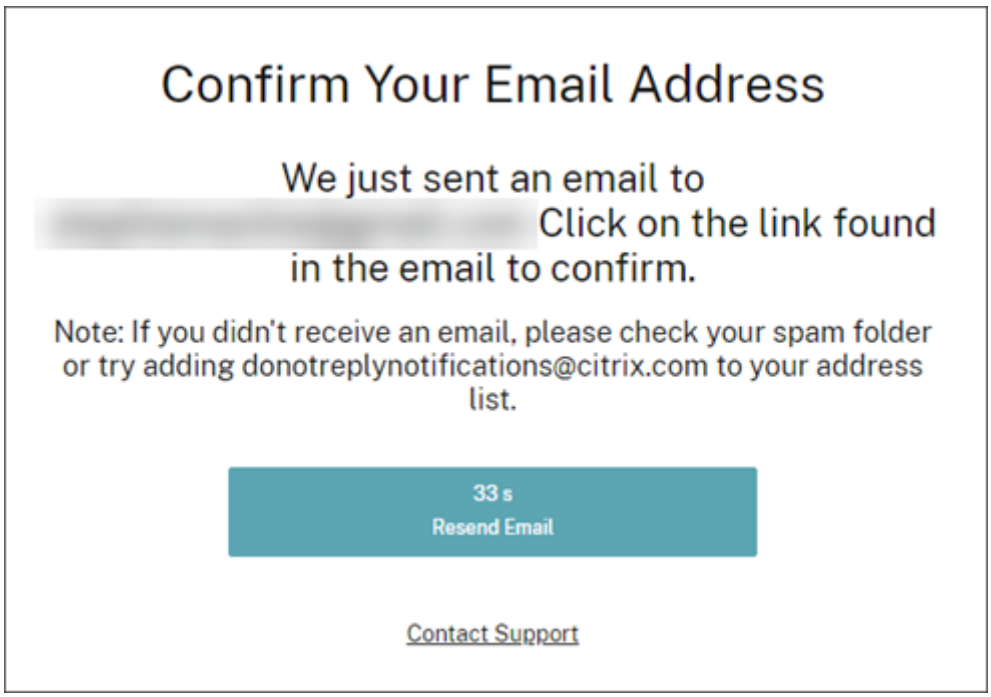


Une région Citrix Cloud est une limite géographique dans laquelle Citrix exploite, stocke et réplique des services et des données dans le but de mettre à disposition des services Citrix Cloud. Citrix peut utiliser plusieurs clouds publics ou privés situés dans un ou plusieurs pays de la région, y compris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

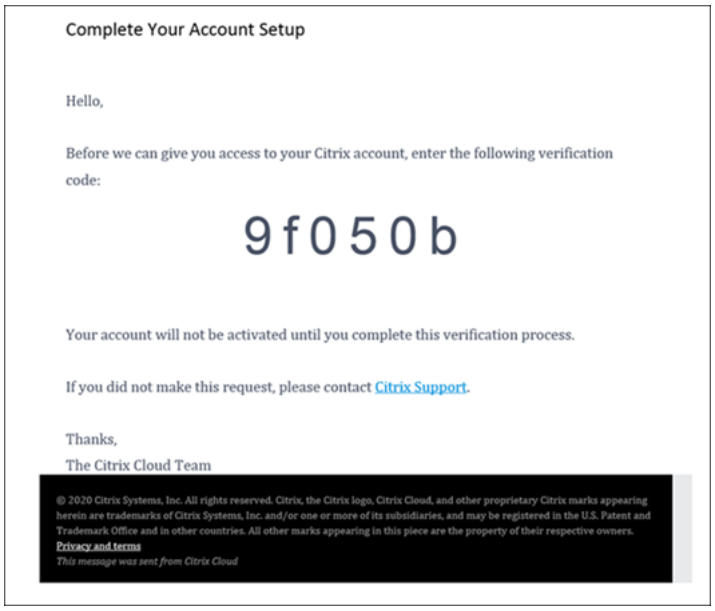
> **Important :**
>
> Une fois que vous avez sélectionné une région, votre sélection ne peut pas être annulée ou modifiée.

Étape 3 : Vérifier votre adresse e-mail

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



Citrix Cloud vous envoie ensuite un e-mail de vérification. Voici un exemple du message que vous recevrez :

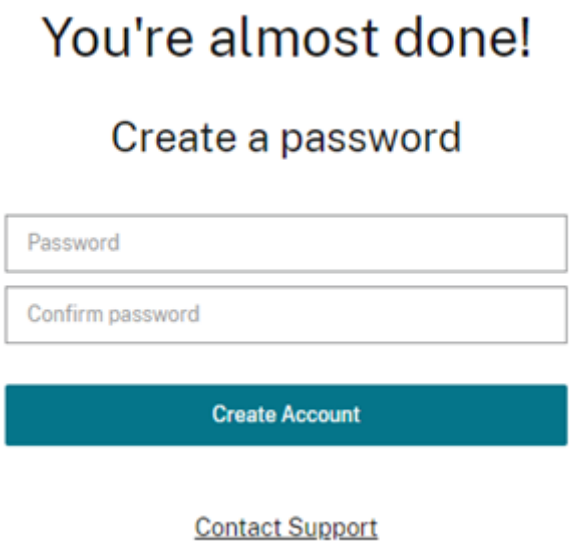


Après avoir reçu l'e-mail de vérification et confirmé votre adresse e-mail, votre compte Citrix Cloud est actif.

Étape 4 : Choisir un mot de passe

> **Remarque :**
>
> Citrix Cloud vous invite à choisir un mot de passe uniquement si vous créez un compte Citrix pour la première fois.

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

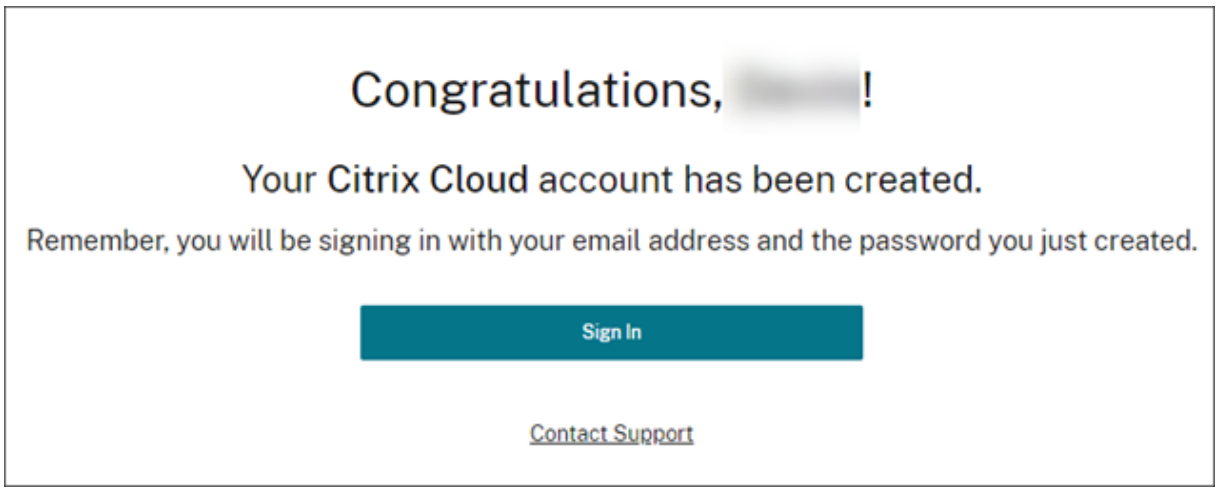


Le mot de passe que vous sélectionnez respecte la casse et doit répondre à tous les critères suivants :

- Au moins 8 caractères
- Au moins une lettre majuscule
- Au moins un chiffre
- Un symbole : ! @ # $ % ^ * ? + = -

Les mots de passe valides ne peuvent pas inclure de mots du dictionnaire. Si, après avoir choisi votre mot de passe, Citrix détermine que votre mot de passe n'est pas suffisamment complexe ou est répertorié dans une base de données connue de mots de passe compromis, Citrix Cloud peut vous inviter à le modifier lors de votre prochaine connexion à Citrix Cloud. Pour plus d'informations, consultez Modification de votre mot de passe.

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



Étape 5 : S'inscrire à l'authentification multifacteur

Pour garantir la sécurité de votre compte administrateur, Citrix Cloud exige que vous utilisiez l'authentification multifacteur lorsque vous vous connectez. L'inscription à l'authentification multifacteur empêche l'accès non autorisé à votre compte d'administrateur et nécessite uniquement un appareil, tel qu'un ordinateur ou un appareil mobile, sur lequel est installée une application d'authentification conforme à la norme TOTP (mot de passe à usage unique temporaire), telle que Citrix SSO.

Si vous ne vous êtes pas inscrit à l'authentification multifacteur, Citrix Cloud vous invite à vous inscrire lorsque vous vous connectez.

Lors de l'inscription, Citrix Cloud présente un code QR et une clé. Selon votre application d'authentification, vous pouvez scanner le code QR ou entrer la clé pour enregistrer votre appareil. Pour faciliter le processus d'inscription, Citrix recommande de télécharger et d'installer cette application sur votre appareil au préalable. Citrix Cloud génère également des codes de sauvegarde à usage unique que vous pouvez utiliser pour accéder à votre compte en cas de perte de votre appareil ou si vous ne pouvez pas utiliser votre application d'authentification.

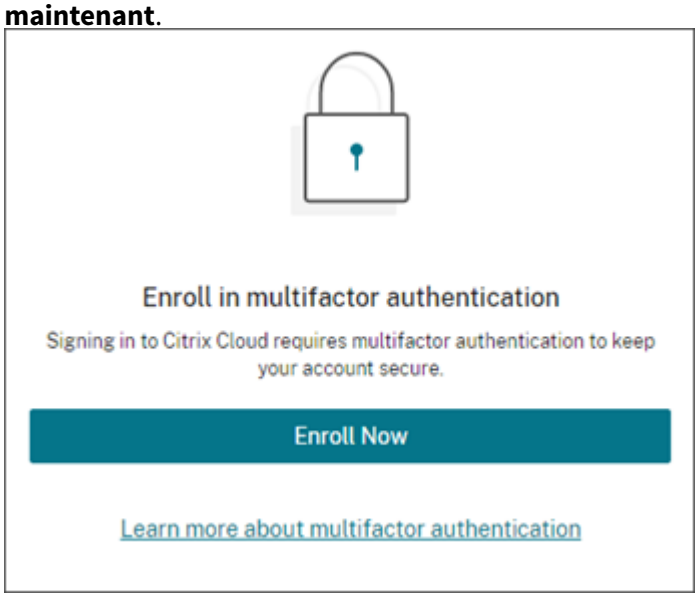
> **Remarques :**
>
> - Lorsque vous vous connectez à Citrix Cloud, vérifiez que vous utilisez bien la page de connexion Citrix Cloud à l'adresse https://accounts.cloud.com. Si vous vous connectez à Citrix Cloud à l'aide d'une autre URL (telle que `https://accounts-internal.cloud.com`), l'inscription à l'authentification multifacteur échoue.
> - Seuls les administrateurs sous le fournisseur d'identité Citrix peuvent s'inscrire à l'authentification multifacteur via Citrix Cloud. Si vous utilisez Azure AD pour gérer les administrateurs Citrix Cloud, vous pouvez configurer l'authentification multifacteur à l'aide du portail Azure. Pour plus d'informations, consultez la page Configurer les paramètres

d'authentification multifacteur Azure sur le site Microsoft.

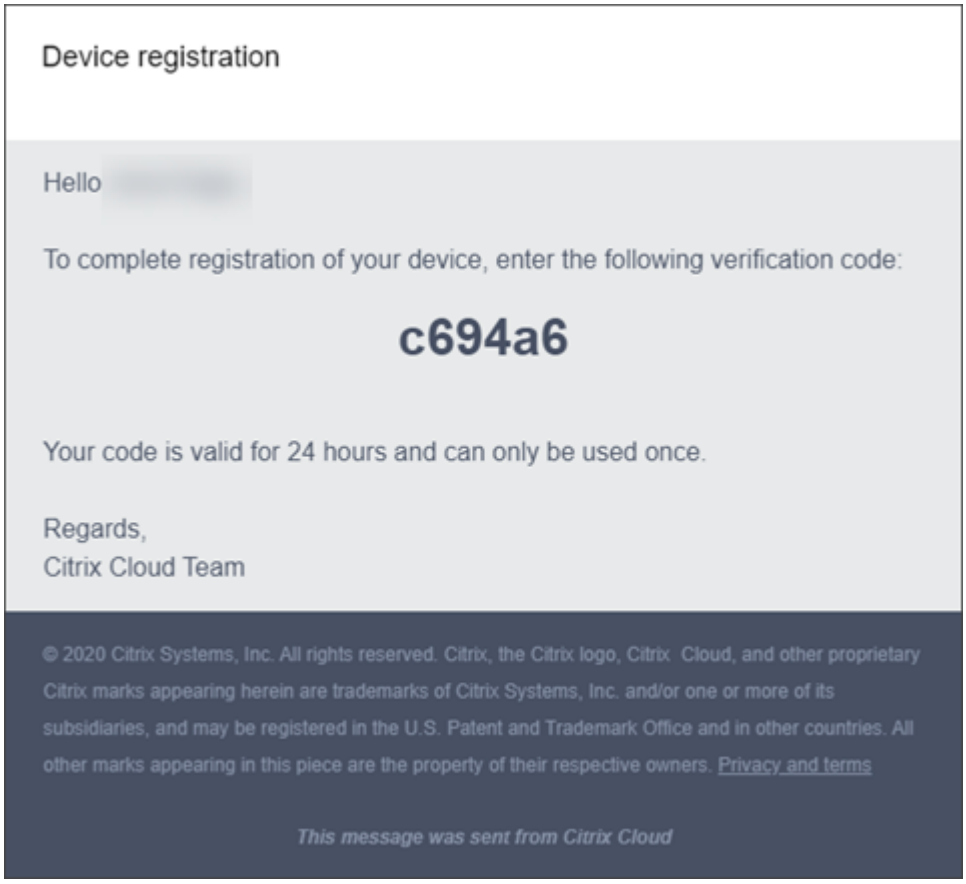
- Après votre inscription, l'authentification multifacteur est utilisée pour toutes les organisations clients auxquelles vous appartenez dans Citrix Cloud. Vous ne pouvez pas désactiver l'authentification multifacteur après avoir effectué le processus d'inscription.
- Vous ne pouvez inscrire qu'un seul appareil. Si vous inscrivez un autre appareil ultérieurement, Citrix Cloud supprime l'inscription de l'appareil actuel et le remplace par le nouvel appareil. Pour plus d'informations, consultez Changer d'appareil pour l'authentification multifacteur.

Inscrire votre appareil à l'authentification multifacteur

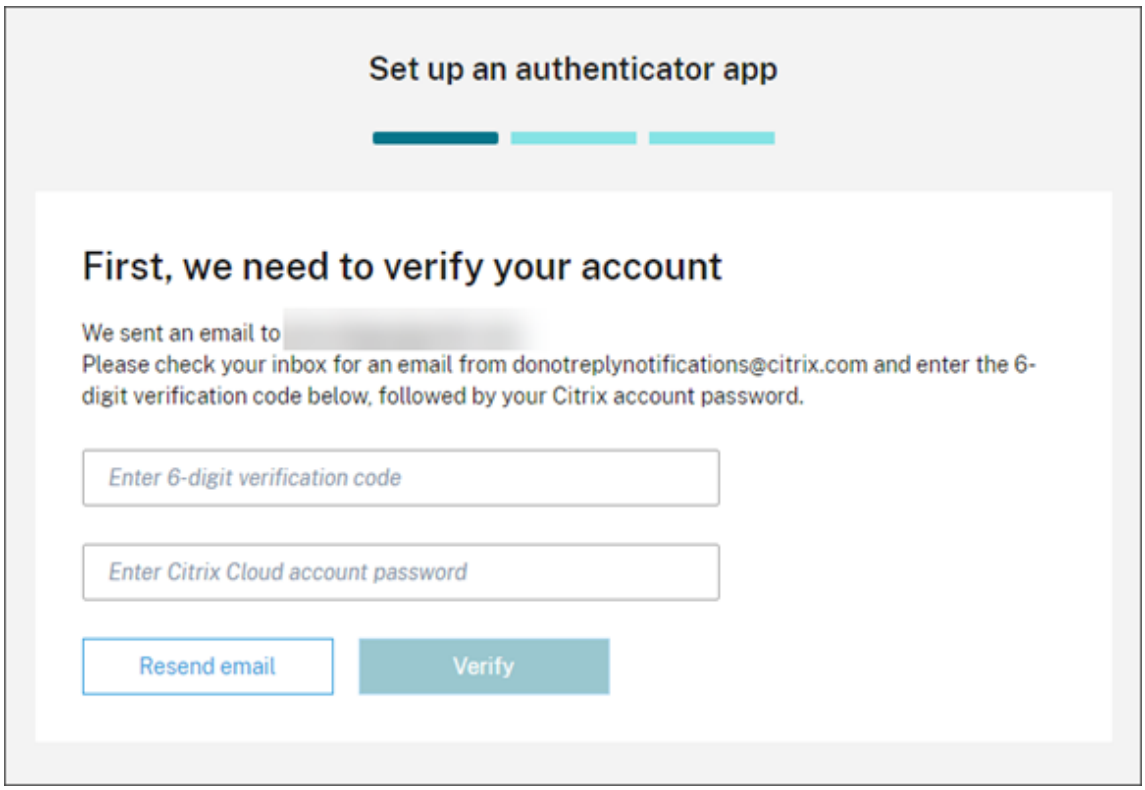
1. Accédez à https://citrix.cloud.com et vérifiez que l'URL redirige vers https://accounts.cloud.com. Connectez-vous avec vos informations d'identification Citrix Cloud.
2. Lorsque vous êtes invité à vous inscrire à l'authentification multifacteur, sélectionnez **S'inscrire maintenant**.



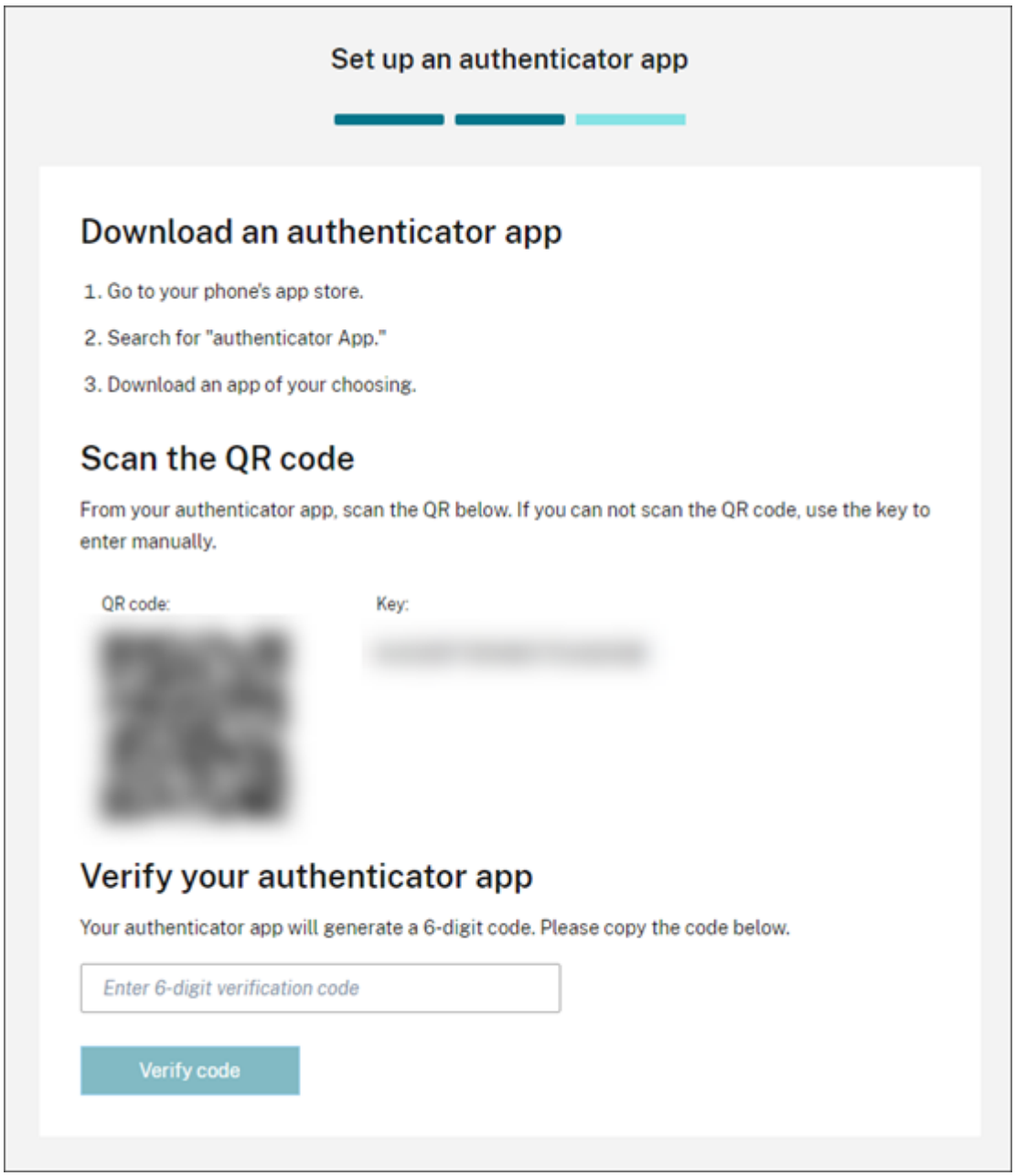
Citrix Cloud vous envoie un e-mail avec un code de vérification.



3. Après avoir reçu l'e-mail, entrez le code de vérification à 6 chiffres et votre mot de passe Citrix Cloud, puis sélectionnez **Vérifier**.

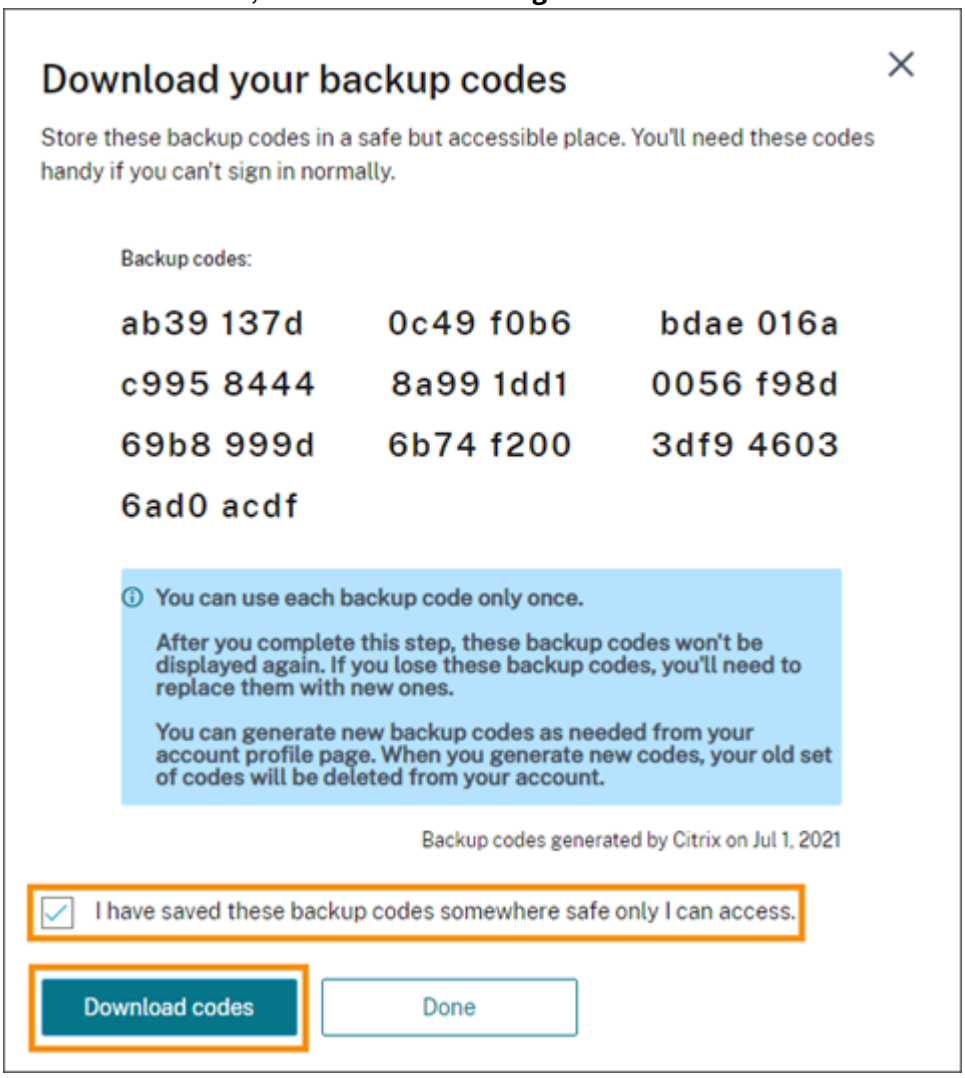


4. À partir de l'application d'authentification, scannez le code QR ou saisissez la clé manuellement. Votre application d'authentification affiche une entrée pour Citrix Cloud et génère un code à 6 chiffres.



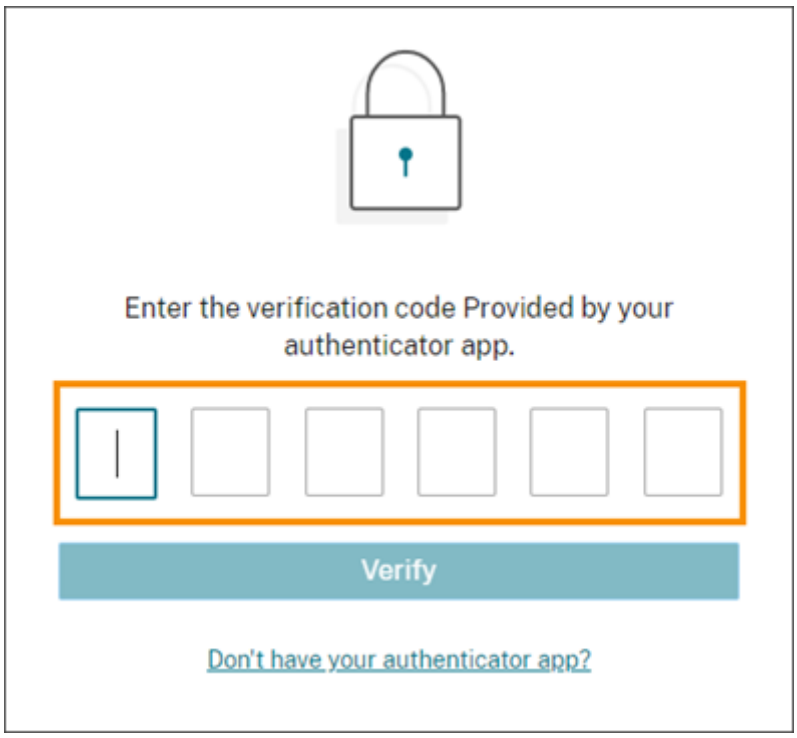
5. Sous **Vérifier votre application d'authentification**, entrez le code de votre application d'authentification et sélectionnez **Vérifier le code**.
6. Configurez les méthodes de récupération de compte suivantes en cas de perte de votre appareil ou si vous ne pouvez pas utiliser votre application d'authentification :
    - N° de téléphone de récupération (obligatoire) : sélectionnez **Ajouter un n° de téléphone de récupération** et entrez un numéro de téléphone qu'un représentant du support Citrix peut utiliser pour vous appeler et vérifier votre identité. Le support Citrix utilise ce numéro de téléphone uniquement lorsque vous demandez de l'aide pour vous connecter. Citrix recommande d'utiliser un numéro de téléphone fixe.

- Codes de secours (requis) : sélectionnez **Générer des codes de secours** pour créer un ensemble de codes de secours à usage unique pour vous aider à vous connecter si vous ne pouvez pas utiliser votre application d'authentification. Lorsque vous y êtes invité, sélectionnez **Télécharger les codes** pour télécharger vos codes de sauvegarde sous forme de fichier texte. Ensuite, sélectionnez **J'ai enregistré ces codes** et sélectionnez **Fermer**.



7. Sélectionnez **Terminer** pour terminer l'inscription.

La prochaine fois que vous vous connectez avec vos informations d'identification d'administrateur Citrix Cloud, Citrix Cloud vous invite à entrer le code de vérification à partir de votre application d'authentification.



Gérer l'inscription de votre appareil

Si vous devez inscrire un autre appareil, générer d'autres codes de secours ou mettre à jour votre numéro de téléphone de récupération ultérieurement, vous pouvez effectuer ces tâches à partir de votre page Mon profil. Pour de plus amples informations, consultez les articles suivants :

- Changer d'appareil pour l'authentification multifacteur
- Gérer vos méthodes de vérification.

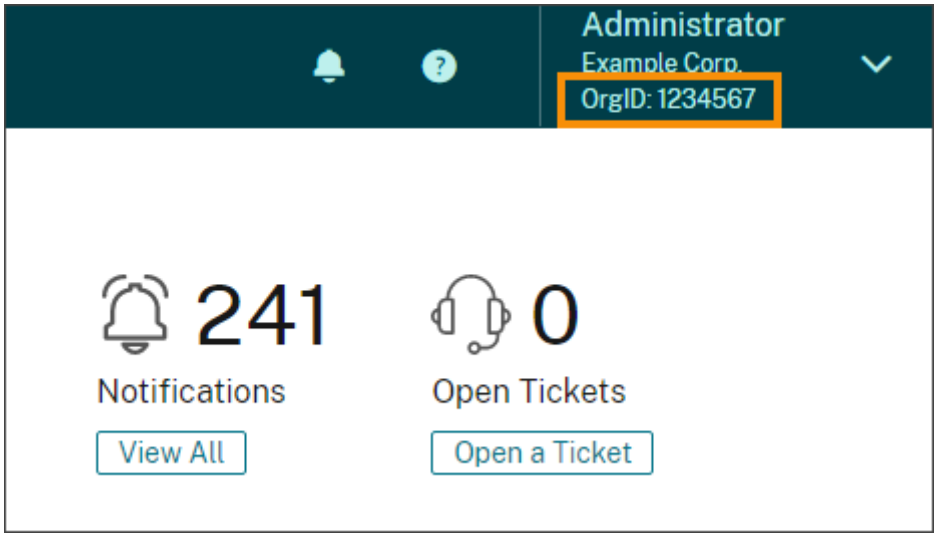
Étape 6 : Vérifier votre OrgID et inviter des administrateurs

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

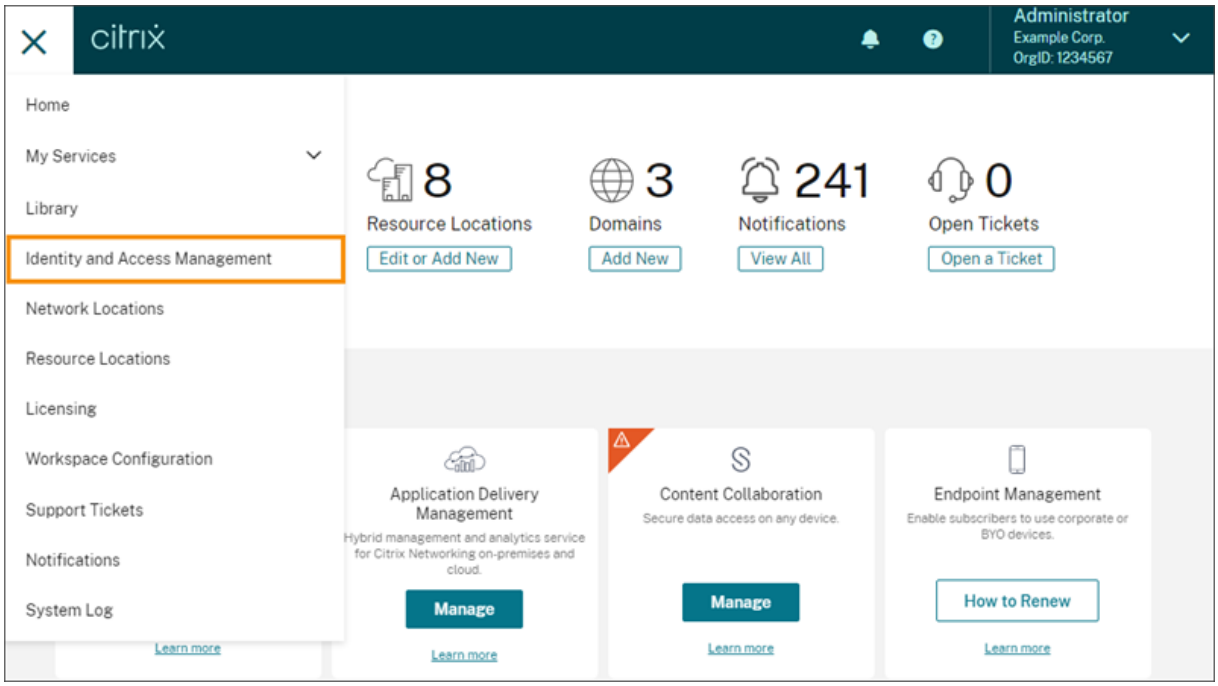
Assurez-vous que l'OrgID de votre compte correspond à l'OrgID que vous utilisez pour passer des commandes. L'un des avantages de Citrix Cloud est que si vous testez un service (tel que Virtual Apps and Desktops Service) et décidez de l'acheter, toutes les configurations que vous avez effectuées dans 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.

Votre OrgID apparaît dans le coin supérieur droit de la console de gestion, sous le nom de votre compte.



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 plus d'informations, consultez Ajouter des administrateurs à un compte Citrix Cloud.



Étape 7 : 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 version d'évaluation pour le service que vous souhaitez tester. Pour plus d'informations, consultez Évaluations de services Citrix Cloud.

Considérations géographiques

July 21, 2021

Cet article traite des régions commerciales utilisées par Citrix Cloud et de la présence de services commerciaux Citrix Cloud dans chaque région.

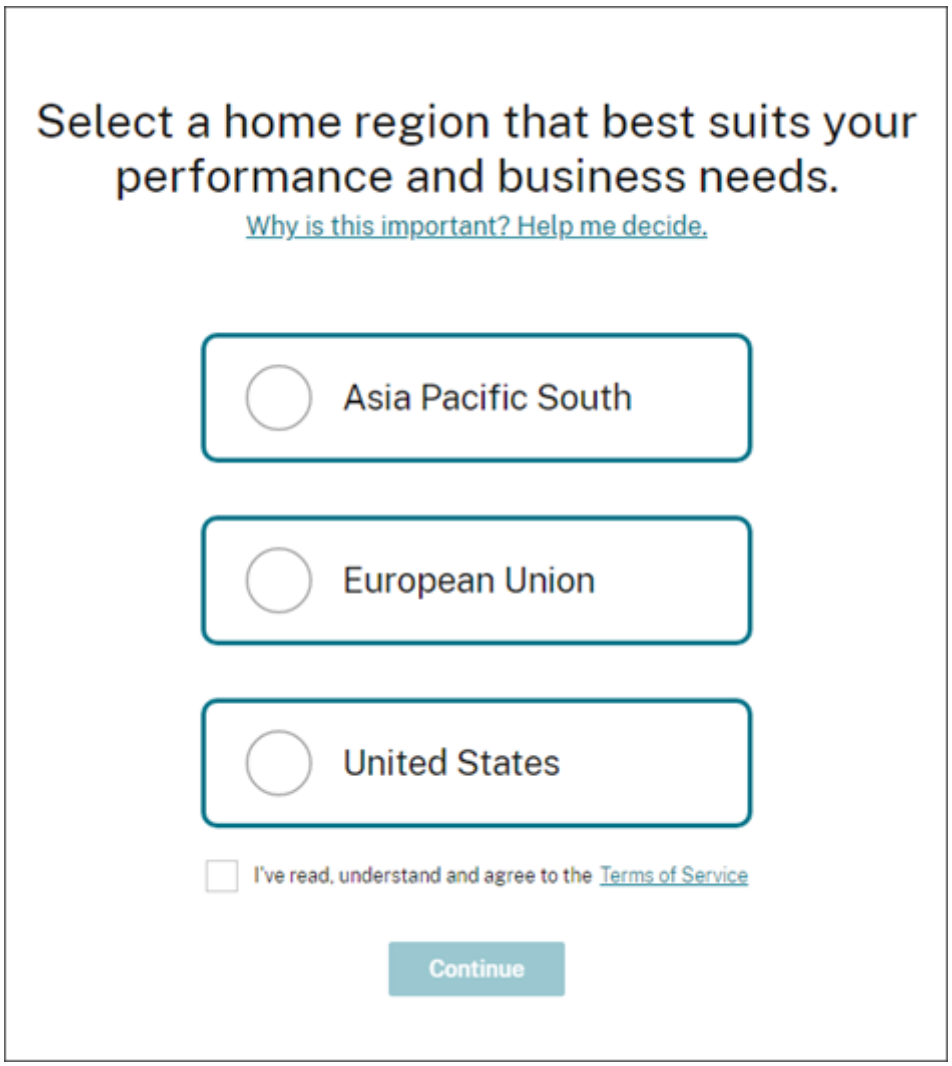
Pour plus d'informations sur les régions géographiques et la présence de services pour les plates-formes cloud du secteur public et dédiées de Citrix, consultez Autres plates-formes cloud de Citrix dans cet article.

Choisir une région

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.



Remarques importantes :

- 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.
- Si vous vous trouvez dans une région et que vous utilisez un service dans une autre région, les impacts sur les performances sont minimes. Les services Citrix Cloud sont conçus pour être utilisés à l'échelle mondiale. Par exemple, les clients des États-Unis qui ont des utilisateurs et des connecteurs en Australie observeront un impact minimal en termes de latence.
- Si vous ne vous trouvez pas dans une région prise en charge par Citrix Cloud, vous pouvez toujours utiliser Citrix Cloud. 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.

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 connecteur 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. En outre, vos données peuvent être traitées à l'échelle mondiale par les filiales ou sous-traitants Citrix si nécessaire pour exécuter les services. 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.

Lorsqu'un service n'est pas disponible dans la région 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
Citrix Analytics	Oui	Oui	Non (Utilise la région États-Unis)

Service	États-Unis	UE	Asie Pacifique Sud
Application Delivery Management	Oui	Oui	Oui
Citrix Content Collaboration	Oui ⋆⋆⋆	Oui ⋆⋆⋆	Non - Sélectionnez États-Unis ou UE ⋆⋆
Citrix Endpoint Management	Oui ⋆⋆	Oui ⋆⋆	Oui ⋆⋆
SD-WAN Orchestrator	Oui	Oui	Non (Utilise la région États-Unis)
Secure Browser Service	Oui ⋆	Oui ⋆	Oui ⋆
Citrix Virtual Apps and Desktops Service	Oui ⋆	Oui ⋆	Oui ⋆
Citrix Virtual Apps and Desktops Standard pour Azure	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	Oui	Non (Utilise la région États-Unis)
Services de réseau	Oui	Non (Utilise la région États-Unis)	Non (Utilise la région États-Unis)
License Usage Insights (CSP uniquement)	Réplication globale	Réplication globale	Réplication globale

Service	États-Unis	UE	Asie Pacifique Sud
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
Nœuds/POP pour le service Accès Internet sécurisé de Citrix	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. Voir Emplacements de Endpoint Management Service dans cet article.

*** La zone de stockage peut être sélectionnée à partir de plusieurs emplacements. Voir Emplacements Content Collaboration et zones de stockage dans cet article.

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 pour le services Accès Internet sécurisé

Le trafic est acheminé vers les emplacements du service Accès Internet sécurisé suivants en fonction de la disponibilité et de la proximité de l'utilisateur afin d'assurer une expérience optimale.

Amérique du Nord

- Sterling, VA, États-Unis
- Toronto, Canada
- Los Angeles, CA, États-Unis
- Irvine, CA, États-Unis
- Seattle, WA, États-Unis
- Denver, CO, États-Unis
- Charlotte, NC, États-Unis
- Dallas, TX, États-Unis
- Allen, TX, États-Unis
- Miami, FL, États-Unis
- Chicago, IL, États-Unis
- New York, NY, États-Unis
- Boston, MA, États-Unis
- Vancouver, Canada

Amérique du Sud

- Queretaro, Mexique
- Sao Paulo, Brésil
- Buenos Aires, Argentine
- Bogota, Colombie

Asie-Pacifique

- Perth, Australie
- Sydney, Australie
- Tokyo, Japon
- Singapour, Singapour
- Mumbai, Inde
- Delhi, Inde

Afrique

Johannesburg, Afrique du Sud

Moyen-Orient

- Dubaï, Émirats arabes unis
- Istanbul, Turquie

Europe occidentale

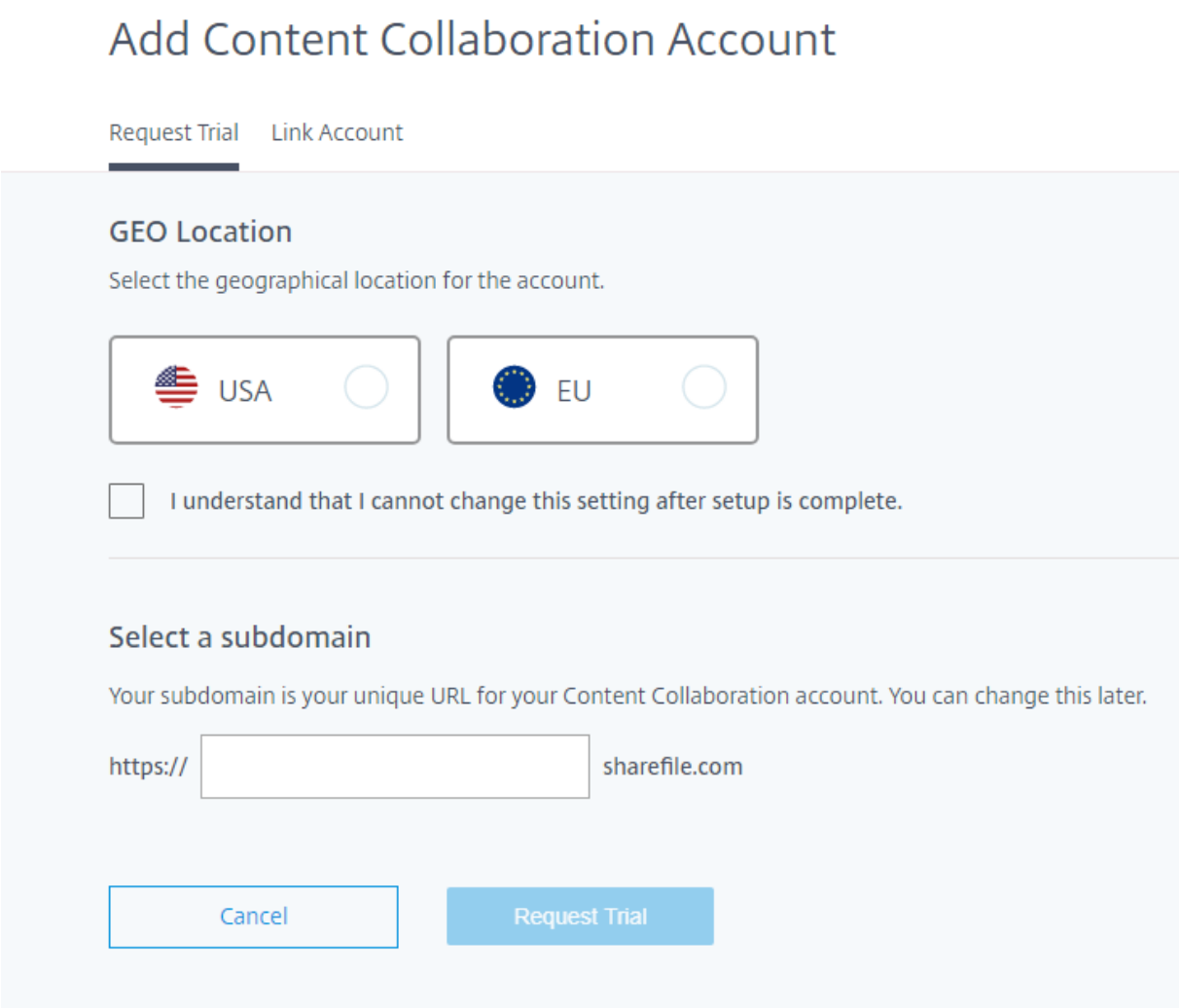
- Londres, Royaume-Uni
- Manchester, Royaume-Uni
- Francfort, Allemagne
- Düsseldorf, Allemagne
- Mannheim, Allemagne
- Paris, France

Europe

- Helsinki, Finlande
- Amsterdam, Pays-Bas
- Stockholm, Suède
- Varsovie, Pologne
- Madrid, Espagne
- Sofia, Bulgarie
- Zurich, Suisse
- Milan, Italie

Emplacements Content Collaboration et zones de stockage

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 zone de stockage par défaut est initialement située dans la région États-Unis.

Pour les comptes ShareFile Enterprise créés en dehors de Citrix Cloud, votre zone de stockage 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 zones de stockage dans le monde entier, ainsi que choisir une nouvelle zone par défaut. Vous pouvez également spécifier une valeur par défaut spécifique aux utilisateurs ou aux dossiers individuels en fonction des zones de stockage 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

Autres plates-formes cloud de Citrix

En plus de Citrix Cloud, Citrix propose d'autres clouds isolés et séparés de Citrix Cloud.

Citrix Cloud Government

Citrix Cloud Government permet aux agences gouvernementales américaines et à d'autres clients du secteur public aux États-Unis d'utiliser les services cloud Citrix conformément aux exigences réglementaires et de conformité. Citrix Cloud Government représente 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 Government. Citrix peut utiliser plusieurs clouds publics ou privés situés dans un ou plusieurs états aux États-Unis pour fournir des services.

Citrix Cloud Government et les services proposés ne sont disponibles qu'aux États-Unis.

Pour plus d'informations, consultez la documentation produit Citrix Cloud Government.

Citrix Cloud Japan

Citrix Cloud Japan permet aux clients japonais d'utiliser les services Citrix Cloud dans un environnement dédié géré par Citrix. Citrix Cloud Japan représente 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 Cloud Japan et les services proposés ne sont disponibles qu'au Japon.

Pour plus d'informations, consultez la documentation produit Citrix Cloud Japan.

Vérifier votre adresse e-mail pour Citrix Cloud

June 17, 2019

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 Citrix Cloud 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.

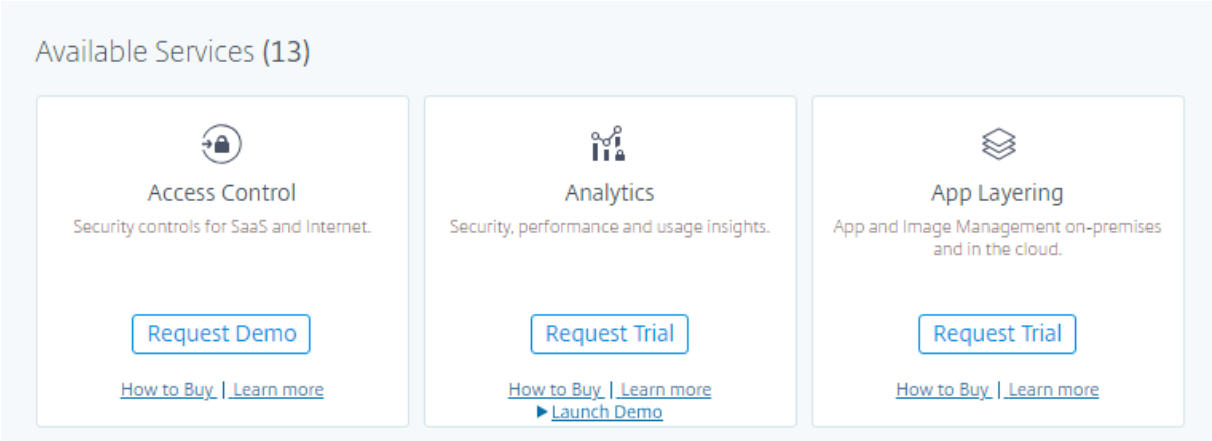
Contacter l'assistance technique Citrix

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

Évaluations de services Citrix Cloud

July 20, 2021

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. Pour certains services, vous devez demander une démo avant de recevoir une version d'évaluation. Pour plus d'informations, consultez la section Demander une démo de service dans cet article.

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.

> **Conseil :**
>
> Le module de formation « Getting Started with Citrix Cloud », inclus dans le cours Fundamentals of Citrix Cloud, fournit une courte vidéo qui vous guide tout au long de la demande d'évaluation. Le cours complet vous fournit également une base solide pour comprendre Citrix Cloud, ses avantages pour votre organisation et les principaux cas d'utilisation utilisés par les services Citrix Cloud.

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	Illimité
Intégration locale à Microsoft Active Directory	Oui

	Évaluation de Citrix Cloud
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
Personnalisable	Oui

*Version d'évaluation non disponible actuellement.

Demander une démo de service

Pour certains services, vous devez demander une démo à un représentant Citrix avant de pouvoir essayer le service. La demande de démo vous permet de discuter des besoins de service de cloud de votre organisation avec un représentant Citrix et de disposer ainsi de toutes les informations nécessaires pour essayer le service avec succès.

1. Connectez-vous à votre compte Citrix Cloud.
2. À partir de la console de gestion, cliquez sur **Demander une démo** pour le service que vous souhaitez tester. La page de demande de démo du service apparaît.
3. Remplissez le formulaire et envoyez-le. Un représentant Citrix vous contactera pour vous fournir plus d'informations et vous aider à utiliser le service.

Demander une version d'évaluation de service

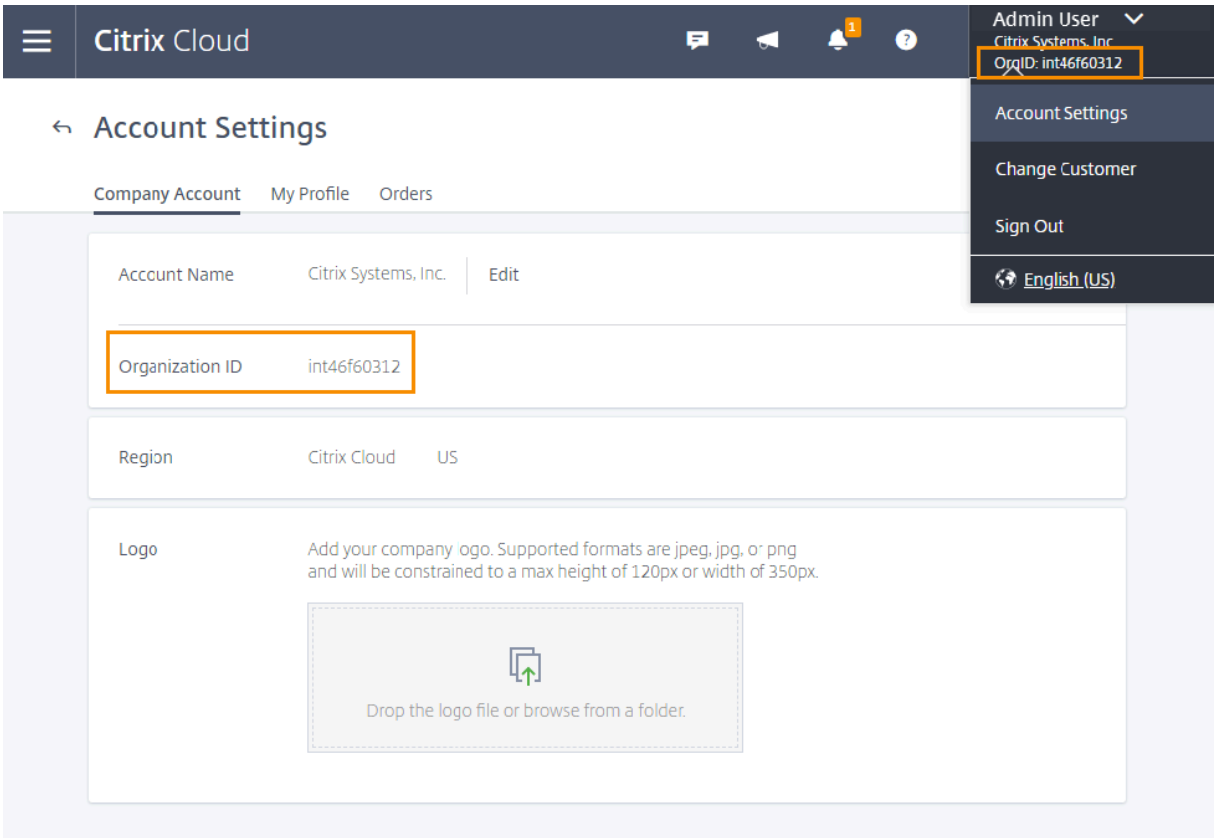
Pour demander une version d'évaluation, connectez-vous à votre compte Citrix Cloud. À partir de la console de gestion, cliquez sur **Demander version d'évaluation** pour le service que vous souhaitez tester. Lorsque votre version d'évaluation est approuvée et prête à être utilisée, vous recevrez une 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/.

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

July 20, 2021

Cet article décrit les notifications d'expiration aux services de Citrix Cloud et comment prolonger votre abonnement. La manière dont un service expire est différente pour les services achetés sous forme d'abonnements mensuels, tels que Virtual Apps et Desktops Essentials, et les services achetés en tant qu'abonnements annuels ou pluriannuels, tels que le service Virtual Apps and Desktops Service.

Dans cet article, les *abonnements mensuels* font référence aux services achetés sur une base mensuelle. Les *abonnements annuels* font référence aux services achetés sur une base annuelle. Les *abon-*

nements pluriannuels font référence aux services achetés sur une base pluriannuelle.

> **Conseil :**
>
> Le module de formation « Getting Started with Citrix Cloud », inclus dans le cours Fundamentals of Citrix Cloud, fournit une courte vidéo qui vous guide tout au long du processus d'expiration de l'abonnement. Le cours complet vous fournit également une base solide pour comprendre Citrix Cloud, ses avantages pour votre organisation et les principaux cas d'utilisation utilisés par les services Citrix Cloud.

Avant l'expiration

Pour les abonnements mensuels, Citrix Cloud n'envoie pas de notifications avant l'expiration.

Pour les abonnements annuels et pluriannuels, Citrix Cloud vous avertit à certains intervalles lorsque votre abonnement existant approche de son expiration. Ces notifications vous invitent à prolonger l'abonnement pour éviter toute interruption 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 votre abonnement au service expire, Citrix fournit des périodes de grâce qui vous permettent de prolonger votre abonnement ou de supprimer vos données du service. Le délai de grâce prévu est différent pour les abonnements mensuels et les abonnements annuels.

Abonnements mensuels au service

Si vous annulez votre abonnement mensuel au service, Citrix vous envoie un e-mail de notification d'expiration à la date d'expiration. La date d'expiration est le dernier jour du mois au cours duquel vous annulez l'abonnement. Après l'expiration, Citrix permet aux administrateurs et aux utilisateurs de continuer à accéder au service pendant cinq jours. Pendant cette période, les administrateurs sont limités aux fonctions d'énumération et de suppression uniquement. Citrix vous facture les frais que vous encourrez lors de l'utilisation des ressources pendant la période de grâce de 5 jours.

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

- 1 jour après l'expiration (5 jours avant le blocage du service)
- 3 jours après l'expiration (2 jours avant le blocage du service)

Une fois la période de grâce écoulée, toutes les ressources associées au service sont arrêtées et mises hors tension. Si vous souhaitez récupérer les données que vous avez ajoutées au service après la fin de la période de grâce, vous pouvez soumettre une demande au support technique Citrix dans les 30 jours suivant la date d'expiration du service.

Abonnements aux services annuels et pluriannuels

Pour les abonnements annuels et pluriannuels, Citrix vous permet de continuer à accéder au service pendant 30 jours après l'expiration de votre abonnement. 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 de 30 jours, les modalités de l'abonnement commencent à la date d'expiration initiale du service. Par exemple, si le service expire le 31 mai et que vous prolongez votre abonnement le 25 juin (avant la fin de la période de grâce), votre abonnement prolongé débute le 31 mai.

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

Si l'abonnement au service n'est pas prolongé pendant la période de grâce, Citrix bloque l'accès au service de la manière suivante :

- Lorsque les abonnements mensuels expirent, les administrateurs et les utilisateurs n'ont plus accès cinq jours après la date d'expiration.
- Lorsque les abonnements annuels et pluriannuels expirent, les administrateurs et les utilisateurs n'ont plus accès 30 jours après la date d'expiration.

Citrix conserve les données que vous avez ajoutées au service pendant 30 jours après la date d'expiration du service. Si vous prolongez votre abonnement avant la fin de la période de rétention de 30 jours, vos administrateurs et vos utilisateurs peuvent accéder au service et les données sont préservées. Votre abonnement prolongé commence comme suit :

- Pour les abonnements mensuels, la date de début de votre premier mois d'abonnement est la date à laquelle vous avez acheté l'extension. Par la suite, votre abonnement est automatiquement renouvelé le 1er de chaque mois.
- Pour les abonnements annuels et pluriannuels, la date de début de votre abonnement prolongé est la date à laquelle vous achetez l'extension.

Si vous ne prolongez pas votre abonnement avant la fin de la période de rétention de 30 jours, Citrix réinitialise le service et supprime les données que vous avez ajoutées. Si vous avez accepté d'autoriser Citrix à gérer votre déploiement cloud (par exemple, lors de l'utilisation de Citrix Essentials Service ou de l'option Déploiement rapide d'Azure dans Virtual Apps and Desktops Service), Citrix effectue les actions suivantes après la fin de la période de rétention de 30 jours :

- Supprime toutes les données relatives au client des bases de données Citrix.
- Supprime toutes les ressources liées aux services Citrix Cloud, y compris les VM gérées par Citrix que Citrix a provisionnées dans votre environnement de cloud. Pour obtenir une description des composants gérés par Citrix qui sont inclus dans des services Citrix Cloud spécifiques, reportez-vous à la documentation du service.

Abonnements Azure gérés par le client

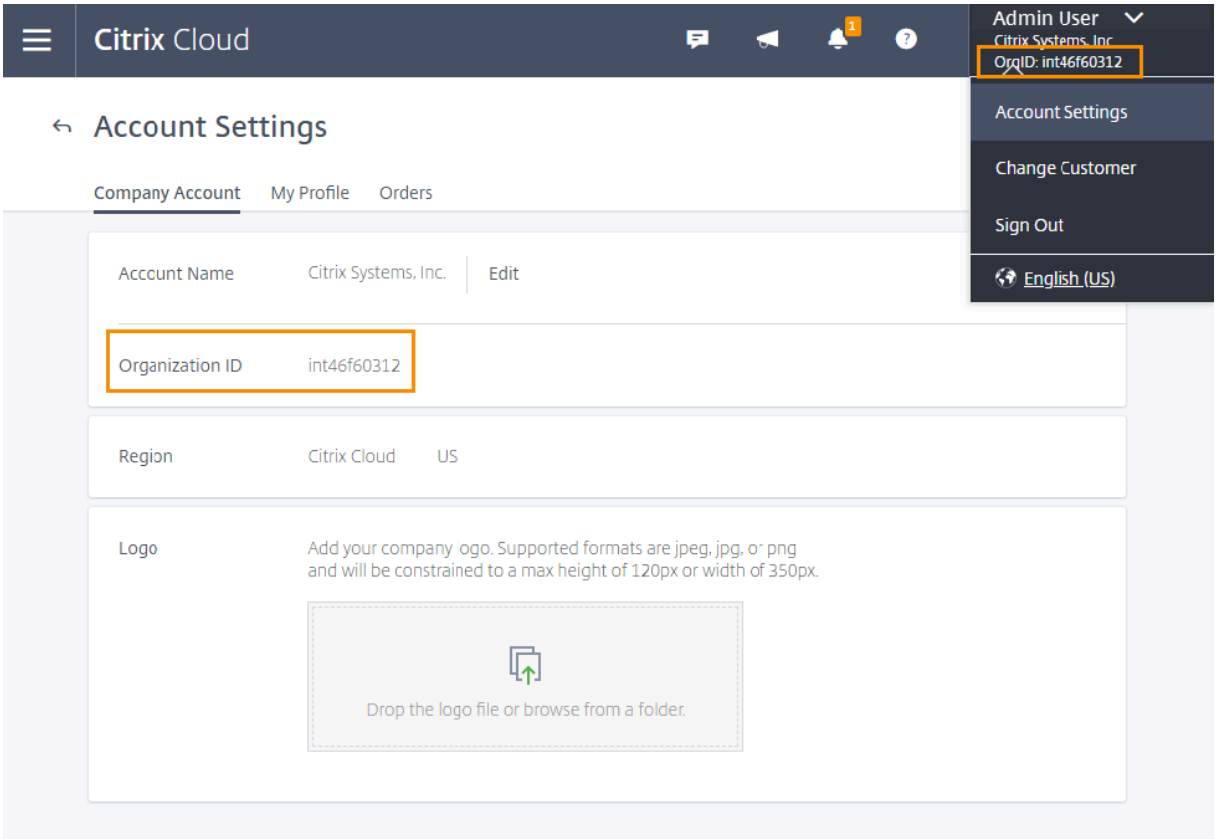
Si vous utilisez votre propre abonnement Azure avec un service Citrix Cloud, le service installe une application lorsque vous connectez votre abonnement Azure au service. Si vous ne prolongez pas votre abonnement au service Citrix Cloud, Citrix ne supprime pas cette application de votre abonnement Azure après la fin de la période de rétention de 30 jours. Vous devez supprimer cette application pour supprimer complètement le service de votre abonnement Azure. Vous pouvez supprimer l'application en utilisant une des méthodes suivantes :

- Si l'accès des administrateurs au service n'est pas encore bloqué, supprimez cette application à partir du service.
- Si l'accès des administrateurs au service est bloqué, supprimez cette application à partir du portail Azure.

Acheter des extensions de service

Pour prolonger votre abonnement aux services Citrix Cloud, accédez au site https://www.citrix.com/products/citrix-cloud/.

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



Configuration requise pour le système et la connectivité

July 21, 2021

Citrix Cloud fournit des fonctions administratives (via un navigateur Web) et des requêtes opérationnelles (provenant d'autres composants installés) qui se connectent aux ressources de votre déploiement. Cet article décrit la configuration système requise, les adresses Internet contactables requises et les considérations à prendre en compte pour établir la connectivité entre vos ressources et Citrix Cloud.

Configuration système requise

Citrix Cloud requiert la configuration minimale suivante :

- Un domaine Active Directory
- Deux machines physiques ou virtuelles, jointes à votre domaine, pour Citrix Cloud Connector. Pour de plus amples informations, consultez Détails techniques sur 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 sur la configuration système requise pour des services spécifiques, reportez-vous à la documentation Citrix de chaque service.

Pour plus d'informations sur les exigences liées au dimensionnement et à la scalabilité, consultez la section Considérations sur le dimensionnement et la scalabilité des Cloud Connector.

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

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.

Notifications de la console

La console de gestion utilise Pendo pour afficher des alertes critiques, des notifications sur les nouvelles fonctionnalités et des conseils intégrés au produit pour certaines fonctionnalités et certains services. Pour garantir de pouvoir afficher le contenu Pendo dans la console de gestion, Citrix recommande que l'adresse `https://citrix-cloud-content.customer.pendo.io/` soit contactable.

Les services qui affichent du contenu Pendo sont les suivants :

- Analytics
- Content Collaboration
- Virtual Apps and Desktops
- Workspace

Pendo est un sous-traitant tiers utilisé par Citrix pour fournir des services de cloud et de support aux clients Citrix. Pour obtenir la liste complète de ces sous-traitants, consultez Sous-traitants pour Citrix Cloud & services de support et filiales Citrix.

Délais d'expiration de la session

Une fois qu'un administrateur se connecte à Citrix Cloud, la session de la console de gestion expire à l'issue des intervalles suivants :

- Sessions inactives (aucune activité de console détectée) : 60 minutes
- Délai maximal d'expiration de la session (quelle que soit l'activité de la console) : 24 heures

Après l'expiration du délai maximal de session, toutes les modifications de configuration non enregistrées sont perdues et l'administrateur doit se connecter à nouveau.

Enregistrement de produits locaux

Si vous utilisez Citrix Cloud avec le serveur de licences Citrix pour enregistrer vos produits locaux, assurez-vous que les adresses suivantes peuvent être contactées :

- `https://trust.citrixnetworkapi.net` (pour récupérer un code)
- `https://trust.citrixworkspacesapi.net/` (pour confirmer que le serveur de licences est enregistré)
- `https://cis.citrix.com` (pour le téléchargement de données)
- `https://core-eastus-release-a.citrixworkspacesapi.net`
- `https://core.citrixworkspacesapi.net`
- `ocsp.digicert.com port 80`
- `crl3.digicert.com port 80`
- `crl4.digicert.com port 80`
- `ocsp.entrust.net port 80`

- `crl.entrust.net port 80`

Si vous utilisez un serveur proxy avec le serveur de licences Citrix, assurez-vous que le serveur proxy est configuré comme décrit à la section Configurer un serveur proxy de la documentation produit de Gestion des licences.

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 connaître la configuration requise pour l'installation du Cloud Connector, consultez la section Configuration système requise. 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.

Pour obtenir de l'aide sur la résolution des problèmes de connectivité entre Cloud Connector et Citrix Cloud, utilisez l'utilitaire Cloud Connector Connectivity Check Utility. Cet utilitaire exécute une série de vérifications sur la machine Cloud Connector pour vérifier qu'elle peut atteindre Citrix Cloud et les services associés et vous aide à ajouter les adresses de connectivité manquantes à la zone Sites de confiance dans Internet Explorer. Si vous utilisez un serveur proxy dans votre environnement, toutes les vérifications de connectivité sont tunnelisées via votre serveur proxy. Pour télécharger l'utilitaire, consultez CTX260337 dans le centre de connaissances du support Citrix.

Exigences en termes de connectivité des services communs de Cloud Connector

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. Pour de plus amples informations, consultez Configuration du pare-feu et du proxy d'un Cloud Connector.

Les adresses de chaque service dans cet article doivent pouvoir être contactées afin d'utiliser et de consommer correctement le service. La liste suivante répertorie les adresses communes à la plupart des services Citrix Cloud et leur fonction. Ces adresses sont fournies uniquement en tant que noms de domaine, car les services Citrix Cloud sont dynamiques et leurs adresses IP sont sujettes à des modifications de routine.

- `https://*.citrixworkspacesapi.net` (fournit un accès aux API Citrix Cloud utilisées par les services)
- `https://*.cloud.com` (fournit un accès à l'interface de connexion Citrix Cloud)

- `https://*.blob.core.windows.net` (fournit un accès au stockage Blob Azure qui stocke les mises à jour pour Citrix Cloud Connector)
  - Les clients qui ne peuvent pas activer tous les sous-domaines peuvent utiliser les adresses suivantes à la place :
    * `https://cwsproduction.blob.core.windows.net`
    * `https://ccprodaps.blob.core.windows.net`
    * `https://ccprodeu.blob.core.windows.net`
- `https://*.servicebus.windows.net` (fournit un accès à Azure Service Bus, qui est utilisé pour la journalisation, l'agent Active Directory et Machine Creation Services)

Il est recommandé d'utiliser la stratégie de groupe pour configurer et gérer ces adresses. En outre, configurez uniquement les adresses applicables aux services que vous et vos utilisateurs consommez.

Si vous utilisez Citrix Cloud avec le serveur de licences Citrix pour enregistrer vos produits locaux, consultezEnregistrement de produits locaux dans cet article pour obtenir les adresses contactables requises supplémentaires.

Validation du certificat

Les fichiers binaires et les points de terminaison contactés par Cloud Connector sont protégés par des certificats X.509 vérifiés lors de l'installation du logiciel. Pour valider ces certificats, chaque machine Cloud Connector doit satisfaire aux exigences suivantes :

- Le port HTTP 80 est ouvert sur *.digicert.com. Ce port est utilisé lors de l'installation du Cloud Connector et lors des vérifications périodiques des listes de révocation de certificats.
- Les adresses suivantes doivent pouvoir être contactées :
  - `http://*.digicert.com`
  - `https://*.digicert.com`
  - `https://dl.cacerts.digicert.com/DigiCertAssuredIDRootCA.crt`
  - `https://dl.cacerts.digicert.com/DigiCertSHA2AssuredIDCodeSigningCA.crt`

Pour plus d'informations sur ces certificats, veuillez consulter la section Exigences relatives à la validation des certificats.

Décryptage SSL

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.

Appliance Connector Citrix pour les services cloud

L'appliance Connector est une appliance que vous pouvez déployer dans votre hyperviseur. L'hyperviseur hébergeant l'appliance Connector se trouve dans le réseau sur lequel résident les ressources que vous utilisez avec Citrix Cloud. L'appliance Connector se connecte à Citrix Cloud, ce qui lui permet d'utiliser et de gérer vos ressources selon les besoins.

Pour connaître la configuration requise pour l'installation de l'appliance Connector, consultez la section Configuration système requise.

L'appliance Connector requiert une connectivité sortante sur le port 443 pour fonctionner. Toutefois, afin de fonctionner dans des environnements contenant un serveur proxy Internet ou des restrictions de pare-feu, une configuration supplémentaire peut être nécessaire.

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

- `https://*.cloud.com`
- `https://*.citrixworkspacesapi.net`
- `https://*.citrixnetworkapi.net`
- `https://*.*.nssvc.net`
  - Les clients qui ne peuvent pas activer tous les sous-domaines peuvent utiliser les adresses suivantes à la place
    - `https://*.g.nssvc.net`
    - `https://*.c.nssvc.net`
- `https://*.servicebus.windows.net`
- `https://iwsprodeastusuniconacr.azurecr.io`
- `https://iwsprodeastusuniconacr.eastus.data.azurecr.io`

Connectivité au service Citrix Analytics

- Pour les messages intégrés au produit, y compris les nouvelles fonctionnalités et les communications critiques : `https://citrix-cloud-content.customer.pendo.io/`
- Exigences supplémentaires :Conditions préalables

Pour plus d'informations sur l'intégration de sources de données au service, consultez la section Comment configurer les sources de données.

Connectivité du service Content Collaboration

Emplacements des ressources/Cloud Connector Citrix :

- Exigences en termes de connectivité des services communs de Cloud Connector
- `https://*.sharefile.com`

- Exigences supplémentaires :Adresse IP et configuration du pare-feu de ShareFile (CTX208318)
- Pour les messages intégrés au produit, y compris les nouvelles fonctionnalités et les communications critiques : `https://citrix-cloud-content.customer.pendo.io/`

Console d'administration :

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

Connectivité du service Endpoint Management

Emplacements des ressources/Cloud Connector Citrix :

- Exigences en termes de connectivité des services communs de Cloud Connector
- Exigences supplémentaires :/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 :/fr-fr/citrix-endpoint-management/endpoint-management.html

Connectivité du service Citrix Gateway

- Exigences en termes de connectivité des services communs de Cloud Connector
- `https://*.*.nssvc.net`
  - Les clients qui ne peuvent pas activer tous les sous-domaines peuvent utiliser les adresses suivantes à la place :
    - `https://*.g.nssvc.net`
    - `https://*.c.nssvc.net`

Connectivité du service SD-WAN Orchestrator

Pour connaître les exigences complètes en termes de connexion Internet, consultez la section Conditions préalables à l'utilisation.

Connectivité de Secure Browser Service

Emplacements des ressources/Cloud Connector Citrix :

Exigences en termes de connectivité des services communs de Cloud Connector

Console d'administration :

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

Connectivité du service Citrix Secure Workspace Access

- https://*.netscalergateway.net
- https://*.*.nssvc.net
  - Les clients qui ne peuvent pas activer tous les sous-domaines peuvent utiliser les adresses suivantes à la place :
    * https://*.g.nssvc.net
    * https://*.c.nssvc.net

Connectivité du service Virtual Apps and Desktops

Emplacements des ressources/Cloud Connector Citrix :

- Exigences en termes de connectivité des services communs de Cloud Connector
- https://[customerid].xendesktop.net, où [customerid] est le paramètre ID client affiché dans l'onglet **Clients sécurisés** (**Gestion des identités et des accès > Accès aux API > Clients sécurisés**) de la console de gestion Citrix Cloud.
  - Les clients utilisant Citrix Virtual Apps Essentials doivent utiliser https://*.xendesktop.net à la place.
- https://*.*.nssvc.net
  - Les clients qui ne peuvent pas activer tous les sous-domaines peuvent utiliser les adresses suivantes à la place :
    * https://*.g.nssvc.net
    * https://*.c.nssvc.net

Pour obtenir une vue d'ensemble qui explique la façon dont le Cloud Connector communique avec le service, consultez le diagramme Virtual Apps and Desktops sur le site Web Citrix Tech Zone.

Console d'administration :

- https://*.citrixworkspacesapi.net
- https://*.citrixnetworkapi.net
- https://*.cloud.com
- https://[customerid].xendesktop.net, où [customerid] est le paramètre ID client affiché dans l'onglet **Clients sécurisés** (**Gestion des identités et des accès > Accès aux API > Clients sécurisés**) de la console de gestion Citrix Cloud.

  - Les clients utilisant Citrix Virtual Apps Essentials doivent utiliser `https://*.xendesktop.net` à la place.
- `https://*.*.nssvc.net` (Non requis pour Virtual Apps and Desktops Standard pour Azure)
  - Les clients qui ne peuvent pas activer tous les sous-domaines peuvent utiliser les adresses suivantes à la place :
    * `https://*.g.nssvc.net`
    * `https://*.c.nssvc.net`
- Pour les messages intégrés au produit, y compris les nouvelles fonctionnalités et les communications critiques : `https://citrix-cloud-content.customer.pendo.io/`

Connectivité de Citrix Workspace Service

- `https://*.cloud.com`
- `https://*.citrixdata.com`
- Pour les messages intégrés au produit, y compris les nouvelles fonctionnalités et les communications critiques : `https://citrix-cloud-content.customer.pendo.io/`

Pour s'assurer que les abonnés peuvent accéder à leur contenu dans Citrix Files and Content Collaboration via Workspace, Citrix recommande d'autoriser les domaines répertoriés dans l'article CTX208318.

Authentification unique pour Workspace avec le service d'authentification fédérée de Citrix

La console et le service FAS accèdent aux adresses suivantes à l'aide du compte de l'utilisateur et du compte de service réseau, respectivement.

- Console d'administration FAS, sous le compte utilisateur
  - `*.cloud.com`
  - `*.citrixworkspacesapi.net`
  - Adresses requises par un fournisseur d'identité tiers, si elles sont utilisées dans votre environnement
- Service FAS, sous le compte de service réseau : `*.citrixworkspacesapi.net`

Si votre environnement inclut des serveurs proxy, configurez le proxy utilisateur avec les adresses de la console d'administration FAS. Assurez-vous également que l'adresse du compte de service réseau est configurée en fonction de votre environnement.

Connectivité de Workspace Environment Management Service

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

Se connecter à Citrix Cloud

July 21, 2020

La connexion de vos ressources à Citrix Cloud implique le déploiement de connecteurs dans votre environnement et la création d'*emplacements de ressources*.

Les emplacements de ressources contiennent les ressources requises pour fournir des services cloud à vos abonnés. Vous pouvez gérer ces ressources à partir de la console Citrix Cloud. Les emplacements de ressources contiennent des ressources différentes selon les services Citrix Cloud que vous utilisez et les services que vous souhaitez fournir à vos abonnés.

Pour créer un emplacement de ressources, installez au moins deux composants Cloud Connector dans votre domaine. Les composants Cloud Connector sont requis pour établir la communication entre Citrix Cloud et vos ressources. Pour plus d'informations sur le déploiement de Cloud Connector, consultez les articles suivants :

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. Différentes ressources utilisent différents types de connecteur. La plupart des services utilisent Citrix Cloud Connector, mais certains services spécifiques nécessitent une appliance Connector.

Services qui utilisent Citrix Cloud Connector

Par exemple, si vous souhaitez fournir un accès aux applications et aux bureaux via le service Virtual Apps and Desktops, votre emplacement de ressources peut inclure les éléments suivants :

- Utilisateur et domaine de ressources Active Directory
- Hyperviseur tel que Citrix Hypervisor
- Serveurs exécutant Virtual Desktop Agent (VDA)
- Instance Citrix Gateway locale ou Citrix Gateway Service pour un accès externe sécurisé aux ressources
- Serveur StoreFront local permettant aux utilisateurs d'accéder aux ressources via un magasin d'applications unique et facile à utiliser

Pour obtenir une vue d'ensemble qui explique la façon dont le Cloud Connector communique avec le service, consultez le diagramme Citrix Tech Zone.

Pour obtenir la liste des services Citrix Cloud qui utilisent Cloud Connector, consultez la section Services qui requièrent le Cloud Connector.

Services qui utilisent une appliance Connector

Par exemple, si vous souhaitez envoyer des actions et des notifications à partir de vos applications directement dans votre espace de travail ou dans d'autres canaux, votre emplacement de ressources peut inclure :

- Accès du service de micro-apps Citrix Workspace aux systèmes résidant dans votre emplacement de ressources
- Accès du service des micro-apps Citrix Workspace aux systèmes externes à partir de votre emplacement de ressources

Il peut y avoir d'autres services dans la version Technical Preview qui dépendent également de l'appliance 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.

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.

Restrictions de dénomination

Les noms que vous attribuez aux emplacements de ressources doivent respecter les restrictions suivantes :

- Longueur maximale : 64 caractères
- Caractères non autorisés :
  - ##, $, %, ^, &, ?, +
  - Accolades : [], { }
  - Barres verticales (|)
  - Symbole inférieur à (<) et symbole supérieur à (>)
  - Barres obliques et barres obliques inverses (/, \)
- Ne doit pas correspondre à un autre nom d'emplacement de ressources (non sensible à la casse) dans le compte Citrix Cloud

Emplacements de ressources principaux

Un emplacement de ressources principal est un emplacement de ressources que vous désignez comme étant « l'emplacement préféré » pour certaines communications entre votre domaine et Citrix Cloud. Les Cloud Connector dans un emplacement de ressources principal sont utilisés pour les ouvertures de session des utilisateurs et les opérations de provisioning. L'emplacement de ressources que vous sélectionnez comme « principal » doit disposer de composants 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 Sélectionner un emplacement de ressources principal.

Citrix Cloud Connector

July 21, 2020

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. Pour obtenir une vue d'ensemble qui explique la façon dont le Cloud Connector communique avec le service, consultez le diagramme Vir-

tual Apps and Desktops dans Citrix Tech Zone.

Citrix Endpoint Management requiert le Cloud Connector pour la connectivité d'entreprise au Endpoint Management Service. Secure Browser Service requiert le Cloud Connector pour les applications Web externes authentifiées.

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 catalogues de machines** : 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.

Communication avec le Cloud Connector

Le Cloud Connector authentifie et crypte toutes les communications entre Citrix Cloud et vos emplacements de ressources. Une fois installé, le Cloud Connector initie la communication avec Citrix Cloud via une connexion sortante. 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.

Disponibilité et gestion de la charge du Cloud Connector

Pour garantir une disponibilité continue et pour gérer la charge, installez plusieurs composants Cloud Connector dans chacun de vos emplacements de ressources. Citrix recommande au moins deux 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. 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.

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.

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 ?

Consultez la section Configuration système requise pour connaître les plates-formes, systèmes d'exploitation et versions pris en charge.

Installez le Cloud Connector sur une machine dédiée exécutant Windows Server 2012 R2, Windows Server 2016 ou Windows Server 2019. Cette machine doit être jointe à votre domaine et capable de communiquer avec les ressources que vous souhaitez gérer depuis Citrix Cloud.

> **Important :**
>
> - N'installez pas Cloud Connector, ni aucun autre composant Citrix, sur un contrôleur de domaine Active Directory.
> - N'installez pas le Cloud Connector sur des machines faisant partie d'autres déploiements Citrix (par exemple, Delivery Controller dans un déploiement Virtual Apps and Desktops).

Pour plus d'informations sur le déploiement, consultez les articles suivants :

- Scénarios de déploiement de Cloud Connector dans Active Directory
- Installation de Cloud Connector

Détails techniques sur Citrix Cloud Connector

July 21, 2021

Le Citrix Cloud Connector est un composant comprenant divers services Windows installés sur Windows Server 2012 R2, Windows Server 2016 ou Windows Server 2019.

Configuration système requise

Les machines hébergeant Cloud Connector doivent satisfaire aux exigences suivantes : Citrix recommande fortement l'installation d'au moins deux logiciels Cloud Connector dans chaque emplacement de ressources afin de garantir une haute disponibilité.

Systèmes d'exploitation

Les systèmes d'exploitation suivants sont pris en charge :

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

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

Configuration requise pour .NET

Microsoft .NET Framework 4.7.2 ou version ultérieure est requis. Téléchargez la dernière version à partir du site Web de Microsoft.

> **Remarque :**
>
> N'utilisez pas Microsoft .NET Core avec Cloud Connector. Si vous utilisez .NET Core au lieu de .NET Framework, l'installation de Cloud Connector peut échouer. Utilisez uniquement .NET Framework avec Cloud Connector.

Éléments requis sur les serveurs

Si vous utilisez Cloud Connector avec Virtual Apps and Desktops Service, reportez-vous à la section Considérations sur le dimensionnement et la scalabilité des Cloud Connector pour obtenir des conseils sur la configuration de la machine.

Les exigences suivantes s'appliquent à toutes les machines sur lesquelles le Cloud Connector est installé :

- Utilisez des machines dédiées pour héberger Cloud Connector. N'installez aucun autre composant sur ces machines.
- Les machines **ne sont pas** configurées en tant que contrôleurs de domaine Active Directory. L'installation de Cloud Connector sur un contrôleur de domaine n'est pas prise en charge.
- L'horloge du serveur doit être définie sur l'heure UTC correcte.
- La configuration de sécurité renforcée d'Internet Explorer (IE ESC) est désactivée. Si cette configuration est activée, le Cloud Connector ne pourra pas se connecter à Citrix Cloud.
- Citrix recommande vivement d'activer Windows Update sur toutes les machines hébergeant le Cloud Connector. Lors de la configuration de Windows Update, configurez Windows pour télécharger et installer automatiquement les mises à jour en dehors des heures ouvrables, mais n'autorisez pas les redémarrages automatiques pendant au moins 4 heures. La plate-forme Citrix Cloud gère les redémarrages de machine lorsqu'elle identifie qu'une mise à jour est en attente d'un redémarrage ; si c'est le cas, la plate-forme autorise un redémarrage pour un seul Cloud Connector à la fois. Vous pouvez configurer un redémarrage de secours à l'aide d'une stratégie de groupe ou d'un outil de gestion système pour les cas où la machine doit être redémarrée après une mise à jour. Pour plus d'informations, consultez https://docs.microsoft.com/en-us/windows/deployment/update/waas-restart.

Exigences relatives à la validation des certificats

Les fichiers binaires et les points de terminaison contactés par Cloud Connector sont protégés par des certificats X.509 émis par les autorités de certification d'entreprise (CA) les plus reconnues. La vérification des certificats dans l'infrastructure de clé publique (PKI) inclut la liste de révocation de certificats. Lorsqu'un client reçoit un certificat, le client vérifie s'il approuve l'autorité de certification qui a émis les certificats et si le certificat est sur une liste de révocation de certificats. Si le certificat figure sur une liste de révocation de certificats, le certificat est révoqué et ne doit pas être approuvé, même s'il apparaît valide.

Les serveurs de liste de révocation de certificats utilisent HTTP sur le port 80 au lieu de HTTPS sur le port 443. Les composants Cloud Connector, eux-mêmes, ne communiquent pas sur le port externe 80. Le besoin d'un port externe 80 est un sous-produit du processus de vérification du certificat effectué par le système d'exploitation.

Les certificats X.509 sont vérifiés lors de l'installation de Cloud Connector. Par conséquent, toutes les machines Cloud Connector doivent être configurées pour approuver ces certificats afin de garantir que le logiciel Cloud Connector peut être installé correctement.

Les points de terminaison Citrix Cloud sont protégés par des certificats émis par DigiCert ou par l'une des autorités de certification racine utilisées par Azure. Pour plus d'informations sur les autorités de certification racine utilisées par Azure, consultez https://docs.microsoft.com/fr-fr/azure/security/fundamentals/tls-certificate-changes

Pour valider les certificats, chaque machine Cloud Connector doit satisfaire aux exigences suivantes :

- Le port HTTP 80 est ouvert aux adresses suivantes. Ce port est utilisé lors de l'installation du Cloud Connector et lors des vérifications périodiques des listes de révocation de certificats. Pour plus d'informations sur la façon de tester la connectivité entre les listes de révocation de certificats et OCSP, consultez https://www.digicert.com/kb/util/utility-test-ocsp-and-crl-access-from-a-server.htm sur le site Web DigiCert.
  - http://crl3.digicert.com
  - http://crl4.digicert.com
  - http://ocsp.digicert.com
  - http://www.d-trust.net
  - http://root-c3-ca2-2009.ocsp.d-trust.net
  - http://crl.microsoft.com
  - http://oneocsp.microsoft.com
  - http://ocsp.msocsp.com
- La communication avec les adresses suivantes est activée :
  - https://*.digicert.com
- Les certificats suivants sont installés :
  - https://dl.cacerts.digicert.com/DigiCertAssuredIDRootCA.crt
  - https://dl.cacerts.digicert.com/DigiCertSHA2AssuredIDCodeSigningCA.crt
  - https://cacerts.digicert.com/DigiCertGlobalRootG2.crt
  - https://cacerts.digicert.com/DigiCertGlobalRootCA.crt
  - https://cacerts.digicert.com/BaltimoreCyberTrustRoot.crt
  - https://www.d-trust.net/cgi-bin/D-TRUST_Root_Class_3_CA_2_2009.crt
  - https://www.microsoft.com/pkiops/certs/Microsoft%20RSA%20Root%20Certificate%20Authority%202017.crt
  - https://www.microsoft.com/pkiops/certs/Microsoft%20EV%20ECC%20Root%20Certificate%20Authority%202017.crt

Pour obtenir des instructions complètes sur le téléchargement et l'installation des certificats, reportez-vous à la section CTX223828.

Configuration requise pour Active Directory

- 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. Pour les environnements multi-domaines, consultez la section Scénarios de déploiement de Cloud Connector dans Active Directory dans cet article.
- Chaque forêt Active Directory que vous prévoyez d'utiliser avec Citrix Cloud doit être accessible par deux Cloud Connector à tout moment.

- Le Cloud Connector doit pouvoir accéder aux contrôleurs de domaine à la fois dans le domaine racine de la forêt et dans les domaines que vous avez l'intention d'utiliser avec Citrix Cloud. 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
  - Section « Ports des services système » dans Vue d'ensemble des services et exigences de ports réseau pour Windows

Configuration réseau requise

- Être connectée à un réseau qui peut contacter les ressources que vous utiliserez dans votre emplacement de ressources. Pour plus d'informations, consultez Configuration du pare-feu et du proxy d'un Cloud Connector.
- Être connectés à Internet. Pour plus d'informations, consultez Configuration requise pour le système et la connectivité.

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

Niveau fonctionnel de la forêt	Niveau fonctionnel du domaine	Contrôleurs de domaine pris en charge
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)

Cloud Connector prend actuellement en charge les algorithmes cryptographiques validés par FIPS qui sont utilisés sur les machines compatibles FIPS. Seule la dernière version du logiciel Cloud Connector disponible dans Citrix Cloud inclut cette prise en charge. Si vous disposez de machines Cloud Connector dans votre environnement (installées avant novembre 2018) et que vous souhaitez activer le mode FIPS sur ces machines, effectuez les actions suivantes :

1. Désinstallez le logiciel Cloud Connector sur chaque machine de votre emplacement de ressources.
2. Activez le mode FIPS sur chaque machine.
3. Installez la dernière version de Cloud Connector sur chaque machine compatible FIPS.

> **Important :**
>
> - N'essayez pas de mettre à niveau des installations Cloud Connector existantes vers la dernière version. Commencez toujours par désinstaller l'ancien Cloud Connector, puis installez la version la plus récente.
> - N'activez pas le mode FIPS sur une machine hébergeant une ancienne version de Cloud Connector. Les logiciels Cloud Connector antérieurs à la version 5.102 ne prennent pas en charge le mode FIPS. L'activation du mode FIPS sur une machine avec un ancien Cloud Connector installé empêche Citrix Cloud d'effectuer des mises à jour de maintenance régulières sur Cloud Connector.

Pour obtenir des instructions sur le téléchargement de la dernière version de Cloud Connector, consultez la section Où obtenir le Cloud Connector ?.

Services installés Cloud Connector

Cette section décrit les services installés avec Cloud Connector et leurs privilèges système.

Pendant l'installation, l'exécutable Citrix Cloud Connector installe et définit la configuration de service nécessaire sur les paramètres par défaut requis pour fonctionner. Si la configuration par défaut est modifiée manuellement, Cloud Connector peut ne pas fonctionner comme prévu. Dans ce cas, la

configuration se réinitialise à l'état par défaut lorsque la prochaine mise à jour Cloud Connector se produit, en supposant que les services qui gèrent le processus de mise à jour peuvent toujours fonctionner.

Citrix Cloud Agent System facilite tous les appels élevés nécessaires au fonctionnement des autres services Cloud Connector et ne communique pas directement sur le réseau. Lorsqu'un service sur Cloud Connector doit effectuer une action nécessitant des autorisations de système local, il le fait via un ensemble prédéfini d'opérations que Citrix Cloud Agent System peut effectuer.

Nom du service	Description	S'exécute en tant que
Citrix Cloud Agent System	Gère les appels système nécessaires pour les agents locaux. Inclut l'installation, les redémarrages et l'accès au registre. Ne peut être appelé que par Citrix Cloud Services Agent WatchDog.	Système local
Citrix Cloud Services Agent WatchDog	Surveille et met à niveau les agents locaux (evergreen).	Service réseau
Citrix Cloud Services Agent Logger	Offre une infrastructure de journalisation dédiée aux services Citrix Cloud Connector.	Service réseau
Citrix Cloud Services AD Provider	Permet à Citrix Cloud de faciliter la gestion des ressources associées aux comptes de domaine Active Directory dans lesquels il est installé.	Service réseau
Découverte de l'agent Citrix Cloud Services	Permet à Citrix Cloud de faciliter la gestion des produits Citrix locaux existants XenApp et XenDesktop.	Service réseau
Citrix Cloud Services Credential Provider	Gère le stockage et la récupération des données chiffrées.	Service réseau

Nom du service	Description	S'exécute en tant que
Citrix Cloud Services WebRelay Provider	Permet aux requêtes HTTP reçues depuis le service WebRelay Cloud d'être transférées aux serveurs Web locaux.	Service réseau
Citrix CDF Capture Service	Capture les traces CDF de tous les produits et composants configurés.	Service réseau
Citrix Config Synchronizer Service	Copie la configuration de négociation localement pour le mode de haute disponibilité.	Service réseau
Service d'échange de location de connexion Citrix	Permet l'échange de fichiers de location de connexion entre l'application Workspace et Cloud Connector pour la continuité du service pour Workspace	Service réseau
Citrix High Availability Service	Assure la continuité du service pendant les interruptions du site central.	Service réseau
Citrix ITSM Adapter Provider	Automatise le provisioning et la gestion des applications et bureaux virtuels.	Service réseau
Citrix NetScaler Cloud Gateway	Fournit une connectivité Internet aux applications et bureaux locaux sans avoir besoin d'ouvrir les règles de trafic entrant du pare-feu ou de déployer des composants dans la DMZ.	Service réseau
Citrix Remote Broker Provider	Permet la communication avec un Remote Broker Service depuis des VDA locaux et des serveurs StoreFront.	Service réseau

Nom du service	Description	S'exécute en tant que
Citrix Remote HCL Server	Communications par proxy entre le Delivery Controller et le(s) hyperviseur(s).	Service réseau
Citrix WEM Cloud Authentication Service	Fournit un service d'authentification aux agents Citrix WEM pour qu'ils se connectent aux serveurs d'infrastructure cloud.	Service réseau
Citrix WEM Cloud Messaging Service	Fournit un service cloud Citrix WEM pour recevoir des messages des serveurs d'infrastructure cloud.	Service réseau

Scénarios de déploiement de Cloud Connector dans Active Directory

Si vous avez un seul domaine dans une même forêt, l'installation de Cloud Connector dans ce domaine est tout ce dont vous avez besoin pour établir un emplacement de ressources. Si vous avez plusieurs domaines dans votre environnement, vous devrez déterminer où installer les Cloud Connector afin que vos utilisateurs puissent accéder aux ressources que vous mettez à disposition.

> **Remarque :**
>
> Les emplacements de ressources ci-dessous constituent un schéma qui peut devoir être répété dans d'autres emplacements physiques en fonction de l'endroit où vos ressources sont hébergées.

Domaine unique dans une forêt unique avec un seul groupe de Cloud Connector

Dans ce scénario, un seul domaine contient tous les objets ressource et utilisateur (forest1.local). Un groupe de Cloud Connector est déployé dans un seul emplacement de ressources et joint au domaine forest1.local.

- Relation d'approbation : aucune - domaine unique
- Domaines répertoriés dans **Gestion des identités et des accès** : forest1.local
- Connexions utilisateur à Citrix Workspace : pris en charge pour tous les utilisateurs
- Connexions utilisateur à un StoreFront local : pris en charge pour tous les utilisateurs

Domaines parents et enfants dans une forêt unique avec un seul groupe de Cloud Connector

Dans ce scénario, un domaine parent (forest1.local) et son domaine enfant (user.forest1.local) résident dans une seule forêt. Le domaine parent agit en tant que domaine de ressources et le domaine enfant est le domaine utilisateur. Un groupe de Cloud Connector est déployé dans un seul emplacement de ressources et joint au domaine forest1.local.

- Relation d'approbation : approbation du domaine parent/enfant
- Domaines répertoriés dans **Gestion des identités et des accès** : forest1.local, user.forest1.local
- Connexions utilisateur à Citrix Workspace : pris en charge pour tous les utilisateurs
- Connexions utilisateur à un StoreFront local : pris en charge pour tous les utilisateurs

> **Remarque :**
>
> Vous devrez peut-être redémarrer les Cloud Connector pour vous assurer que Citrix Cloud enregistre le domaine enfant.

Utilisateurs et ressources dans des forêts distinctes (avec approbation) avec un seul groupe de Cloud Connector

Dans ce scénario, une forêt (forest1.local) contient votre domaine de ressources et une forêt (forest2.local) contient votre domaine utilisateur. Il existe entre ces forêts une approbation qui permet aux utilisateurs de se connecter aux ressources. Un groupe de Cloud Connector est déployé dans un seul emplacement de ressources et joint au domaine forest1.local.

- Relation d'approbation : approbation de forêt
- Domaines répertoriés dans **Gestion des identités et des accès** : forest1.local
- Connexions utilisateur à Citrix Workspace : uniquement pris en charge pour les utilisateurs de forest1.local
- Connexions utilisateur à un StoreFront local : pris en charge pour tous les utilisateurs

> **Remarque :**
>
> La relation d'approbation entre les deux forêts doit permettre à l'utilisateur dans la forêt utilisateur de se connecter aux machines de la forêt de ressources.

Étant donné que les Cloud Connector ne peuvent pas traverser les approbations au niveau de la forêt, le domaine forest2.local n'est pas affiché sur la page **Gestion des identités et des accès** dans la console Citrix Cloud. Cela comporte les limites suivantes :

- Les ressources ne peuvent être publiées que pour les utilisateurs et les groupes situés dans forest1.local dans Citrix Cloud. Toutefois, les utilisateurs de forest2.local peuvent être imbriqués dans les groupes de sécurité de forest1.local pour atténuer ce problème.
- Citrix Workspace ne peut pas authentifier les utilisateurs provenant du domaine forest2.local.

Pour contourner ces limitations, déployez les logiciels Cloud Connector comme décrit dans la section Utilisateurs et ressources dans des forêts distinctes (avec approbation) avec un groupe de Cloud Connector dans chaque forêt.

Utilisateurs et ressources dans des forêts distinctes (avec approbation) avec un groupe de Cloud Connector dans chaque forêt

Dans ce scénario, une forêt (forest1.local) contient votre domaine de ressources et une forêt (forest2.local) contient votre domaine utilisateur. Il existe entre ces forêts une approbation qui permet aux utilisateurs de se connecter aux ressources. Un groupe de Cloud Connector est déployé dans le domaine forest1.local et un second groupe est déployé dans le domaine forest2.local.

- Relation d'approbation : approbation de forêt
- Domaines répertoriés dans **Gestion des identités et des accès** : forest1.local, forest2.local
- Connexions utilisateur à Citrix Workspace : pris en charge pour tous les utilisateurs
- Connexions utilisateur à un StoreFront local : pris en charge pour tous les utilisateurs

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

Cloud Connector génère certains messages d'événements que vous pouvez afficher via l'Observateur d'événements Windows. Si vous souhaitez activer votre logiciel de surveillance préféré pour rechercher ces messages, vous pouvez les télécharger sous forme d'archive ZIP. Le téléchargement ZIP inclut ces messages dans les fichiers XML suivants :

- Citrix.CloudServices.Agent.Core.dll.xml (Connector Agent Provider)
- Citrix.CloudServices.AgentWatchDog.Core.dll.xml (Connector AgentWatchDog Provider)

Téléchargez les messages d'événements Cloud Connector.

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.

Résolution des problèmes

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.

Connectivité Cloud Connector

Si Cloud Connector est « déconnecté », l'utilitaire Cloud Connector Connectivity Check Utility peut vous aider à vérifier que Cloud Connector peut atteindre Citrix Cloud et ses services associés.

L'utilitaire Cloud Connector Connectivity Check Utility s'exécute sur la machine hébergeant le Cloud Connector. Si vous utilisez un serveur proxy dans votre environnement, l'utilitaire peut vous aider à vérifier la connectivité via votre serveur proxy en tunnelisant toutes les vérifications de connectivité. Si nécessaire, l'utilitaire peut également ajouter les sites de confiance Citrix manquants à la zone Sites de confiance dans Internet Explorer.

Pour plus d'informations sur le téléchargement et l'utilisation de cet utilitaire, consultez CTX260337 dans le centre de connaissances du support Citrix.

Installation

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, consultez l'article CTX221535.

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

June 10, 2021

Le Cloud Connector prend en charge la connexion à Internet via un serveur proxy Web non authentifié. 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.

Exigences en termes de connectivité

Utilisez le port 443 pour le trafic HTTP (en sortie uniquement). Pour obtenir la liste des adresses contactables requises, consultez la section Configuration requise pour le système et la connectivité. Pour

obtenir la liste des adresses communes à la plupart des services Citrix Cloud et leur fonction, consultez la section Configuration requise pour la connectivité des services communs de Cloud Connector.

Les adresses contactables requises pour Citrix Cloud sont spécifiées en tant que noms de domaine, et non en tant qu'adresses IP. Étant donné que les adresses IP peuvent changer, l'autorisation des noms de domaine garantit que la connexion à Citrix Cloud reste stable. De plus, Citrix améliore et renforce continuellement la plate-forme Citrix Cloud en autorisant ces domaines via l'utilisation de caractères génériques (par exemple, *.citrixworkspacesapi.net), au lieu d'utiliser des adresses plus spécifiques (par exemple, trust.citrixworkspacesapi.net). Ainsi, les clients peuvent bénéficier de ces améliorations sans que leur connectivité à Citrix Cloud ne soit affectée. Certaines fonctions critiques de la plate-forme, telles que le basculement de trafic basé sur la région géographique, reposent sur la capacité d'acheminer les appels sous plusieurs sous-domaines. La spécification de sous-domaines autorisés au lieu de domaines génériques autorisés augmente le risque d'interruption car ces fonctions peuvent utiliser des sous-domaines que le client n'a pas explicitement autorisés. La spécification du domaine générique permet à ces fonctions de fonctionner sans imposer au client la nécessité d'autoriser un grand nombre de sous-domaines pour chaque service Citrix Cloud.

> **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.

Vérifier la connectivité Cloud Connector

L'utilitaire de vérification de la connectivité Cloud Connector (Cloud Connector Connectivity Check Utility) permet de vérifier la connectivité entre Cloud Connector et Citrix Cloud à l'aide d'une série de vérifications de connectivité. Si vous utilisez un serveur proxy dans votre environnement, l'utilitaire peut vous aider à configurer les paramètres proxy sur Cloud Connector et à tester la connectivité via le serveur proxy. Lorsqu'un serveur proxy est configuré, les tests de connectivité sont tunnellisés via le serveur proxy.

Pour plus d'informations sur le téléchargement et l'utilisation de Cloud Connector Connectivity Check Utility, consultez la section CTX260337.

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.

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 obtenir des instructions complètes, consultez la page Netsh Commands for Windows Hypertext Transfer Protocol (WINHTTP).

> **Remarque :**
>
> Les scripts de détection automatique ou PAC ou les proxy authentifiés ne sont pas pris en charge.

Connexions avec les ressources internes

En raison de la configuration du proxy Windows, Cloud Connector peut tenter d'accéder aux ressources internes via le proxy Web. Ces ressources peuvent ne pas être en mesure de se connecter au Cloud Connector et au service Virtual Apps and Desktops, même si les URL de connectivité requises ont été autorisées. En outre, le proxy Web peut bloquer les connexions entre Cloud Connector et Azure Service Bus car une adresse IP est utilisée comme URL dans la commande HTTP Connect. Par conséquent, certaines fonctions de ressources peuvent échouer. Par exemple, Citrix Provisioning ne parvient pas à créer de catalogues de machines.

Pour vous assurer que ces ressources internes peuvent se connecter comme prévu, ajoutez le nom de domaine complet ou l'adresse IP de chaque ressource à la liste de contournement proxy sur la machine Cloud Connector. Pour plus d'informations sur ce problème, consultez l'article CTX241222 dans le Centre de connaissances du support Citrix.

Connexions entre Citrix Federated Authentication Service et Citrix Cloud

La console et le service FAS accèdent aux adresses suivantes à l'aide du compte de l'utilisateur et du compte de service réseau, respectivement.

- Console d'administration FAS, sous le compte utilisateur
  - `*.cloud.com`

  - `*.citrixworkspacesapi.net`
  - Adresses requises par un fournisseur d'identité tiers, si elles sont utilisées dans votre environnement
- Service FAS, sous le compte de service réseau : `*.citrixworkspacesapi.net`

Si votre environnement inclut des serveurs proxy, configurez le proxy utilisateur avec les adresses de la console d'administration FAS. Assurez-vous également que l'adresse du compte de service réseau est configurée à l'aide de netsh ou d'un outil similaire.

Installation de Cloud Connector

July 21, 2021

Vous pouvez installer le logiciel Cloud Connector de manière interactive ou en utilisant la ligne de commande.

L'installation s'effectue avec les privilèges de l'utilisateur qui lance l'installation. Le Cloud Connector requiert l'accès au cloud pour :

- Authentifier l'utilisateur qui effectue l'installation
- Valider les autorisations du programme d'installation
- Télécharger et configurer les services Cloud Connector

Informations à consulter avant l'installation

- Configuration système requise : pour préparer les machines utilisées pour héberger Cloud Connector.
- Section Antivirus Exclusions de l'article Tech Zone Endpoint Security and Antivirus Best Practices : fournit des recommandations pour vous aider à déterminer l'équilibre approprié entre la sécurité et les performances des logiciels Cloud Connector dans votre environnement. Citrix recommande fortement de partager ces recommandations avec les équipes chargées des programmes antivirus et de la sécurité de votre organisation, et d'effectuer des tests rigoureux dans un environnement de laboratoire avant de les appliquer à un environnement de production.
- Configuration requise pour le système et la connectivité : pour vous assurer que toutes les machines hébergeant Cloud Connector peuvent communiquer avec Citrix Cloud.
- Configuration du pare-feu et du proxy d'un Cloud Connector : si vous installez Cloud Connector dans un environnement doté d'un proxy Web ou de règles de pare-feu strictes.
- Considérations sur le dimensionnement et la scalabilité des Cloud Connector : fournit des détails sur les capacités maximales testées, ainsi que des recommandations sur les meilleures pratiques pour configurer des machines qui hébergent Cloud Connector.

Considérations et conseils en matière d'installation

- 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 appartenant à 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.
- Le programme d'installation du Cloud Connector est téléchargé depuis Citrix Cloud. Par conséquent, votre navigateur doit autoriser le téléchargement de fichiers exécutables.
- Après l'installation, ne déplacez pas la machine qui héberge le Cloud Connector dans un autre domaine. Si vous souhaitez joindre la machine à un autre domaine, désinstallez le Cloud Connector et réinstallez-le une fois que la machine est jointe à l'autre domaine.
- Une fois l'installation effectuée, conservez tous les Cloud Connector sous tension à tout moment pour garantir une connexion permanente à Citrix Cloud.

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 prise 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.

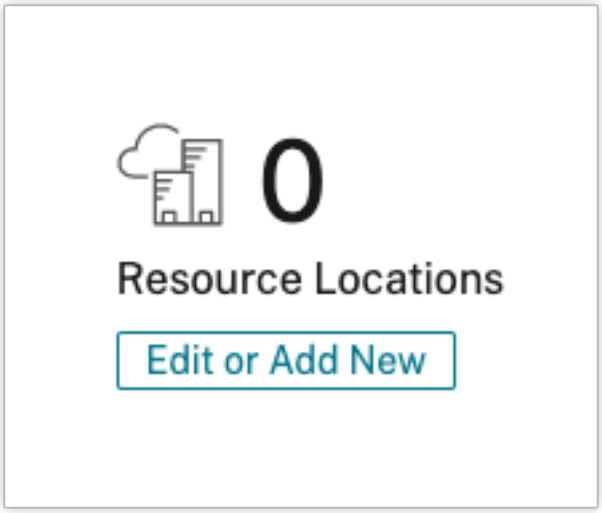
Installation interactive

Vous pouvez télécharger et installer les Cloud Connector à l'aide de l'interface graphique du programme d'installation. Avant de procéder, vous devez créer un ou plusieurs emplacements de

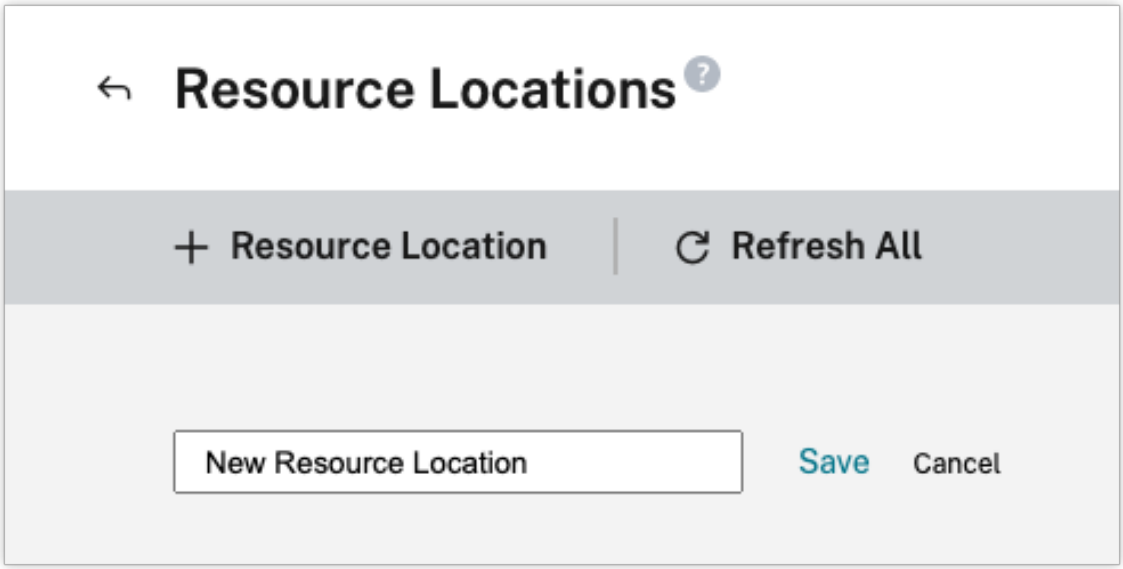
ressources dans la console de gestion Citrix Cloud sur lesquels déployer les Cloud Connector. Pour plus d'informations sur les emplacements de ressources, consultez Emplacement des ressources.

Créer un emplacement de ressources

1. Connectez-vous en tant qu'administrateur Windows sur la machine sur laquelle vous souhaitez installer les Citrix Cloud Connector.
2. Accédez à https://citrix.cloud.com et connectez-vous à votre compte administrateur.
3. Dans la console Citrix Cloud, accédez à **Emplacements de ressources** dans le menu principal ou sélectionnez **Modifier ou ajouter** sous **Emplacements de ressources** en haut de la page.



4. Dans Emplacements de ressources, sélectionnez **+ Emplacement de ressources** en haut de la page et enregistrez-le avec un nom unique.

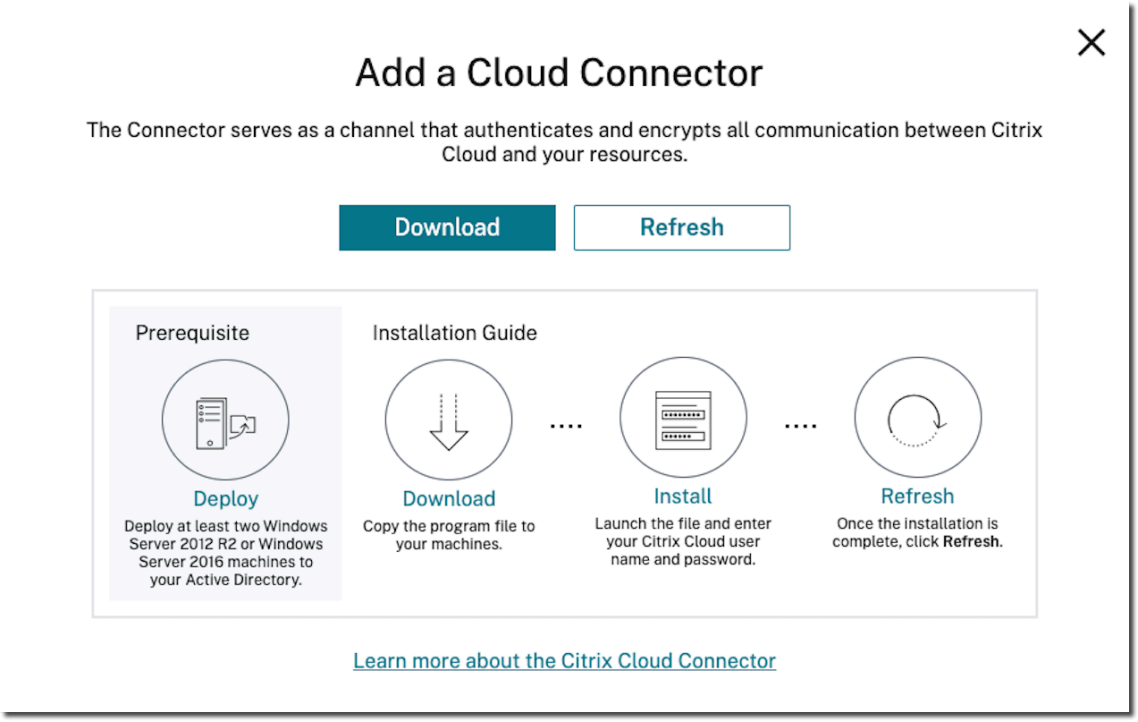


5. Répétez ces étapes sur chaque machine que vous souhaitez utiliser en tant que Cloud Connector.

Téléchargez le logiciel Citrix Cloud Connector

1. Localisez l'emplacement de ressources que vous souhaitez gérer et sélectionnez **+ Cloud Connector**.

2. Sélectionnez **Télécharger** dans la fenêtre qui s'ouvre. Enregistrez le fichier **cwcconnector.exe** dans un emplacement de fichier local sur la machine du Connector.



Installer le logiciel Citrix Cloud Connector

1. Cliquez avec le bouton droit sur **cwcconnector.exe**, puis sélectionnez **Exécuter en tant qu'administrateur**. Le programme d'installation vérifie la connectivité pour s'assurer que vous pouvez vous connecter à Citrix Cloud.
2. Connectez-vous à Citrix Cloud lorsque vous y êtes invité.

3. Pour installer et configurer Cloud Connector, suivez les instructions de l'assistant. Une fois l'installation terminée, le programme d'installation vérifie une dernière fois la connectivité pour vérifier la communication entre Cloud Connector et Citrix Cloud.
4. Répétez ces étapes sur les autres machines que vous souhaitez utiliser en tant que Citrix Cloud Connector. Citrix recommande d'installer au moins deux composants Cloud Connector pour chaque emplacement de ressources pour garantir une haute disponibilité.

Citrix Cloud affiche le Cloud Connector nouvellement installé sur la page **Connecteurs** de votre emplacement de ressources.

Après l'installation, Citrix Cloud enregistre votre domaine dans **Gestion des identités et des accès > Domaines**. Pour plus d'informations, consultez 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

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

Exigences

Pour utiliser l'installation par ligne de commande avec Citrix Cloud, vous devez fournir les informations suivantes :

- ID client du compte Citrix Cloud pour lequel vous installez le Cloud Connector. Cet ID apparaît en haut de l'onglet **Accès aux API** dans **Gestion des identités et des accès**.
- ID client et secret du client API sécurisé que vous souhaitez utiliser pour installer le Cloud Connector. Pour acquérir ces valeurs, vous devez d'abord créer un client sécurisé. L'ID client et le secret garantissent que votre accès à l'API Citrix Cloud est sécurisé de manière appropriée. Lorsque vous créez un client sécurisé, le client fonctionne avec le même niveau d'autorisations d'administrateur que vous. Pour installer un Cloud Connector, vous devez utiliser un client sécurisé qui a été créé par un administrateur avec accès complet, ce qui signifie que le client sécurisé dispose également d'autorisations d'accès complet.
- ID de l'emplacement de ressources que vous souhaitez associer au Cloud Connector. Pour récupérer cette valeur, cliquez sur le bouton **ID** situé sous le nom de l'emplacement de ressources sur la page **Emplacements des ressources**. Si vous ne fournissez pas cette valeur, Citrix Cloud utilise l'ID de l'emplacement de ressources par défaut.

Créer un client sécurisé

Lors de la création d'un client sécurisé, Citrix Cloud génère un ID client et un secret uniques. Vous devez fournir ces valeurs lorsque vous appelez l'API via la ligne de commande.

1. Dans le menu Citrix Cloud, sélectionnez **Gestion des identités et des accès**, puis sélectionnez **Accès aux API**.
2. Dans l'onglet **Clients sécurisés**, entrez un nom pour votre client et sélectionnez **Créer un client**. Citrix Cloud génère et affiche un ID client et un secret pour le client sécurisé.
3. Sélectionnez **Télécharger** pour télécharger l'ID client et le secret en tant que fichier CSV et les stocker dans un emplacement sécurisé. Vous pouvez également sélectionner **Copier** pour acquérir manuellement chaque valeur. Lorsque vous avez terminé, sélectionnez **Fermer** pour revenir à la console.

Paramètres pris en charge

Pour garantir la sécurité des détails du client sécurisé, un fichier de configuration JSON doit être fourni au programme d'installation. Ce fichier doit être supprimé une fois l'installation terminée. Les valeurs prises en charge pour le fichier de configuration sont les suivantes :

- **customerName** obligatoire. ID du client affiché sur la page Accès aux API dans la console Citrix Cloud (sous Gestion des identités et des accès).

- **clientId** obligatoire. ID de client sécurisé qu'un administrateur peut créer, situé sur la page Accès aux API
- **clientSecret** obligatoire. Clé secrète sécurisée du client qui peut être téléchargée après création du client sécurisé. Située sur la page Accès aux API.
- **resourceLocationId** recommandé. Identificateur unique d'un emplacement de ressources existant. Sélectionnez le bouton d'ID pour récupérer l'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** obligatoire. Doit être réglé sur **true**.

Exemple de fichier de configuration :

```
{

"customerName": "\*CustomerID\*",
"clientId": "\*ClientID\*",
"clientSecret": "\*ClientSecret\*",
"resourceLocationId": "\*ResourceLocationId\*",
"acceptTermsOfService": "true"
 }
```

Exemple de ligne de commande qui installe à l'aide du fichier de paramètres :

```
CWCConnector.exe /q /ParametersFilePath:c:\cwcconnector_install_params.
   json
```

Utilisez **Start /Wait CWCConnector.exe /ParametersFilePath:value** pour examiner un code d'erreur potentiel en cas de défaillance. Vous pouvez utiliser le mécanisme standard d'exécution de **echo %ErrorLevel%** une fois l'installation terminée.

> **Remarque :**
>
> L'utilisation de paramètres pour transmettre l'ID client et le secret client n'est plus prise en charge, le fichier de configuration doit être utilisé pour les installations automatisées.

Étapes suivantes

1. Configurez le programme de mise à jour Citrix Cloud Connector. Pour plus d'informations sur les mises à jour Citrix Cloud Connector et la gestion des programmes de mises à jour, accédez à Mises à jour de Connector

2. Configurez un fournisseur d'identité pour authentifier les abonnés de votre espace de travail. Vous pouvez remplacer le fournisseur d'identité Citrix défini par défaut par Active Directory ou d'autres fournisseurs d'identité dans la console Gestion des identités et des accès**. Pour plus d'informations, consultez Connecter Azure Active Directory à Citrix Cloud.

Résolution des problèmes d'installation

Cette section détaille différentes façons de diagnostiquer et de résoudre les problèmes que vous pourriez rencontrer lors de l'installation. Pour plus d'informations sur la résolution des problèmes d'installation, consultez le Guide de dépannage de Citrix Cloud Connector.

Journaux d'installation

Vous pouvez résoudre les problèmes rencontrés lors de l'installation en consultant d'abord les fichiers journaux disponibles.

Les événements survenus pendant l'installation sont disponibles dans l'**Observateur d'événements Windows**. Vous pouvez également consulter les journaux d'installation de Cloud Connector en accédant à **%LOCALAPPDATA%\Temp\CitrixLogs\CloudServicesSetup**.
Les journaux sont ajoutés à **%ProgramData%\Citrix\WorkspaceCloud\InstallLogs** après l'installation.

Codes de sortie

Les codes de sortie suivants peuvent être renvoyés en fonction du succès ou de l'échec du processus d'installation :

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

Erreur d'installation

Si vous installez le logiciel Citrix Cloud Connector en cliquant deux fois sur le programme d'installation, le message d'erreur suivant peut s'afficher :

```
Can't reach this page.
```

Cette erreur peut se produire même si vous êtes connecté en tant qu'administrateur à la machine sur laquelle vous installez Citrix Cloud Connector. Pour éviter cette erreur, exécutez le logiciel Citrix Cloud Connector en tant qu'administrateur en cliquant avec le bouton droit sur le programme d'installation et en sélectionnant Exécuter en tant qu'administrateur.

Échecs de connectivité

Pour garantir que Cloud Connector peut communiquer avec Citrix Cloud, vérifiez que les services Citrix suivants sont définis sur l'état **Démarré** :

- Citrix Cloud AD Provider
- Citrix Cloud Agent Logger
- Citrix Cloud Agent System
- Citrix Cloud Agent Watchdog
- Citrix Cloud Credential Provider
- Citrix Config Synchronizer Service
- Citrix High Availability Service
- Citrix NetScaler Cloud Gateway
- Citrix Remote Broker Provider
- Citrix Remote HCL Server
- Citrix Session Manager Proxy

Pour plus d'informations sur ces services, consultez la section Services installés.

Si vous continuez à rencontrer des échecs de connectivité, utilisez l'utilitaire Cloud Connector Connectivity Check Utility disponible dans le centre de connaissances du support Citrix. Pour plus d'informations, consultez CTX260337 sur le site Web du centre de connaissances.

L'outil peut être utilisé pour effectuer les tâches suivantes :

- Tester si Citrix Cloud et ses services associés sont accessibles
- Vérifier les paramètres dont la configuration est souvent incorrecte
- Configurer les paramètres de proxy sur Citrix Cloud Connector

Pour plus d'informations sur la façon de résoudre un échec de vérification de connectivité, consultez l'article CTX224133 : Cloud Connector Connectivity Check Failed.

Collecte de journaux pour Citrix Cloud Connector

June 10, 2021

Les journaux CDF sont utilisés à des fins de dépannage dans les produits Citrix. Le support Citrix utilise des traces CDF pour identifier les problèmes liés à la négociation des applications et des bureaux, à l'authentification des utilisateurs, à l'enregistrement de Virtual Delivery Agent (VDA). Cet article explique comment capturer des données Cloud Connector qui peuvent être utilisées pour résoudre les problèmes que vous pourriez rencontrer dans votre environnement.

> **Remarques importantes :**
>
> - Activez la journalisation sur toutes les machines Cloud Connector dans vos emplacements de ressources.
> - Pour vous assurer de capturer la totalité des données, Citrix recommande d'utiliser l'outil de capture CDFControl qui réside sur le VDA. Pour plus d'informations, veuillez consulter CTX111961 dans le centre de connaissances du support Citrix. Pour plus d'informations sur la collecte de journaux pour l'application Citrix Workspace, CTX141751.
> - Pour soumettre des traces CDF à Citrix, vous devez avoir ouvert un dossier de support Citrix. Les techniciens du support Citrix ne peuvent pas examiner les traces CDF qui ne sont pas liées à un dossier de support existant.

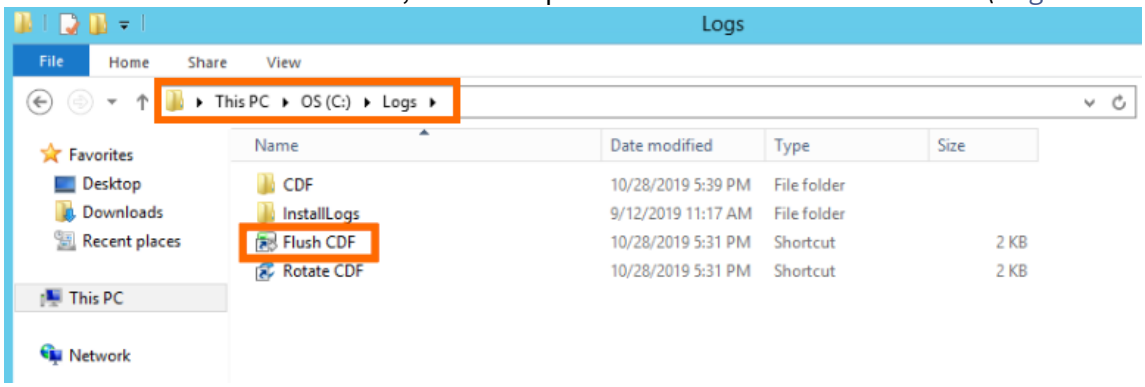
Étape 1 : Recréer le problème

Au cours de cette étape, vous recréez le problème que vous rencontrez dans votre environnement. Si le problème est lié au lancement ou à la négociation d'applications, recréez l'échec de lancement. Si le problème est lié à l'enregistrement VDA, recréez la tentative d'enregistrement VDA en redémarrant manuellement Citrix Desktop Service sur l'ordinateur VDA.

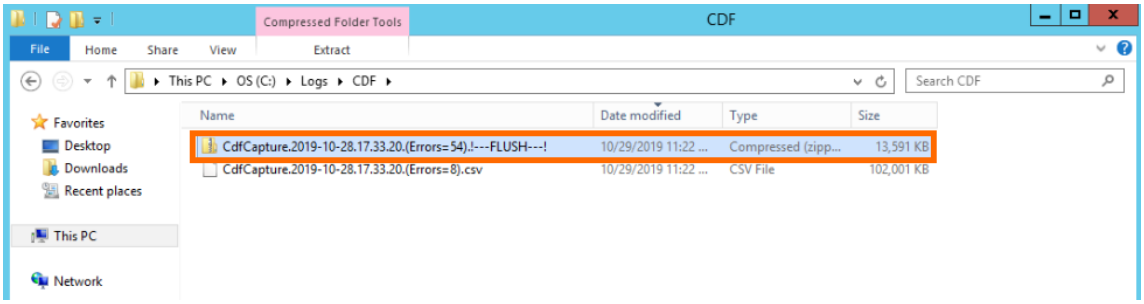
Étape 2 : Recueillir des traces CDF

Au cours de cette étape, vous collectez des traces de purge CDF à partir de chaque Cloud Connector de votre emplacement de ressources.

1. Accédez à la machine Cloud Connector en initiant une connexion RDP à l'aide d'un compte d'administrateur de domaine ou d'administrateur local.
2. Sur l'ordinateur Cloud Connector, ouvrez l'Explorateur de fichiers et accédez à `C:\logs`.



3. Exécutez **Flush CDF**. Une icône apparaît brièvement dans la barre des tâches de l'ordinateur Cloud Connector, puis disparaît.
4. Dans l'Explorateur de fichiers, accédez à C:\logs\CDF et identifiez le dossier le plus récent se terminant par **! - FLUSH—!**.

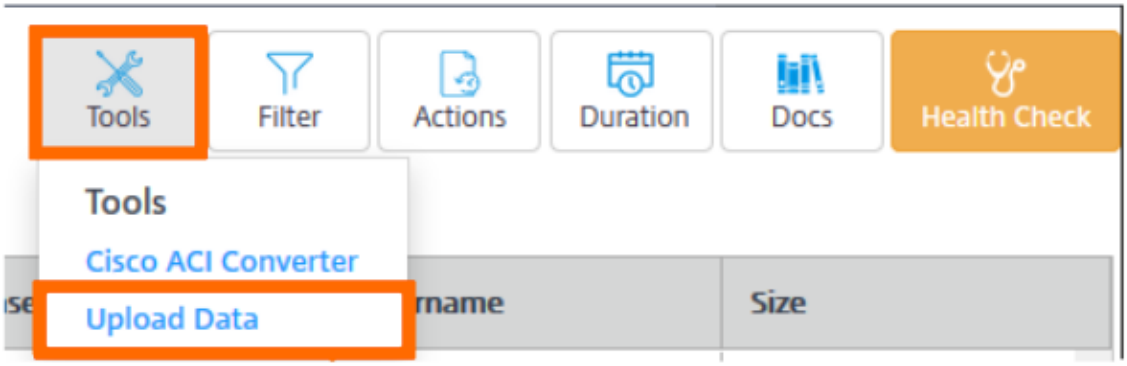


5. Effectuez les étapes 1 à 5 sur chaque machine Cloud Connector de votre emplacement de ressources et combinez toutes les traces de Cloud Connector dans une seule archive ZIP. Si vous ne créez pas d'archive ZIP des traces de purge à partir de toutes vos machines Cloud Connector, vous devrez les soumettre une par une à Citrix.

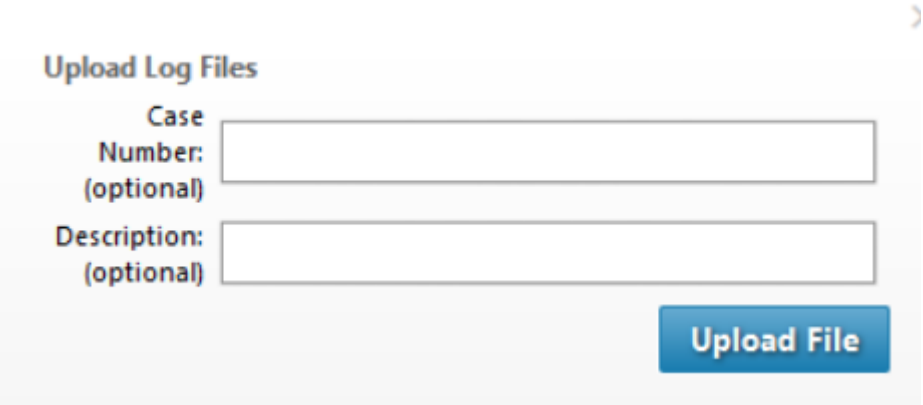
Étape 3 : Soumettre les données à Citrix

Au cours de cette étape, vous joignez vos traces à votre dossier de support Citrix et les soumettez pour examen.

1. Visitez https://cis.citrix.com/ et connectez-vous à l'aide de vos informations d'identification Citrix.com.
2. Sélectionnez **Diagnostics**.
3. Sélectionnez **Outils**, puis **Télécharger données**.



4. Dans **Numéro de dossier**, entrez le numéro du dossier de support Citrix existant. Les techniciens du support Citrix ne peuvent pas examiner les traces CDF de manière appropriée sans un numéro de dossier associé au téléchargement des données.



5. Dans **Description** (facultatif), vous pouvez entrer une brève description ou laisser ce champ vide.
6. Sélectionnez **Télécharger le fichier** et sélectionnez l'archive ZIP que vous avez créée précédemment. Si vous n'avez pas créé d'archive ZIP des traces de purge pour toutes vos machines Cloud Connector, répétez les étapes 3 à 6 pour joindre chaque trace de purge que vous souhaitez soumettre.

Après avoir soumis vos traces de purge, Citrix Insight Services les traite et les joint au dossier de support que vous avez spécifié. Ce processus peut prendre jusqu'à 24 heures, selon la taille des fichiers.

Appliance Connector pour Cloud Services

July 21, 2021

L'appliance Connector est un composant Citrix hébergé dans votre hyperviseur. Elle 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. L'appliance Connector vous permet de gérer et d'axer la priorité sur les ressources qui apportent de la valeur à vos utilisateurs.

L'appliance Connector fournit les fonctions suivantes :

- Le **service de micro-apps Citrix Workspace** fournit des actions et des notifications depuis vos applications directement dans votre instance Workspace ou dans d'autres canaux.

  Créez des intégrations à partir de vos sources de données applicatives vers le service de micro-apps, ce qui vous permet d'extraire des actions de vos applications dans Workspace. Les micro-apps fournissent ensuite des formulaires et des notifications interactifs qui utilisent la réécriture active vers le système source pour compléter le workflow de l'application. Pour plus d'informations, consultez Micro-apps.

Le service de micro-apps Citrix Workspace utilise l'appliance Connector pour diffuser du contenu à partir des emplacements suivants :

- Applications locales
- Systèmes externes se connectant via votre emplacement de ressources

Il peut y avoir d'autres services dans la version Technical Preview qui dépendent également de l'appliance Connector.

Disponibilité et gestion de la charge de l'appliance Connector

Pour garantir une disponibilité continue et pour gérer la charge, installez plusieurs appliances Connector dans chacun de vos emplacements de ressources. Citrix recommande au moins deux appliances Connector dans chaque emplacement de ressources. Si une appliance Connector n'est pas disponible à un moment donné, les autres appliances Connector peuvent maintenir la connexion. Étant donné que chaque appliance Connector est sans état, la charge peut être distribuée sur toutes les appliances Connector disponibles. Il n'est pas nécessaire de configurer cette fonction d'équilibrage de charge. Le processus est automatisé. Tant qu'une appliance Connector est disponible, il n'y a aucune perte de communication avec Citrix Cloud.

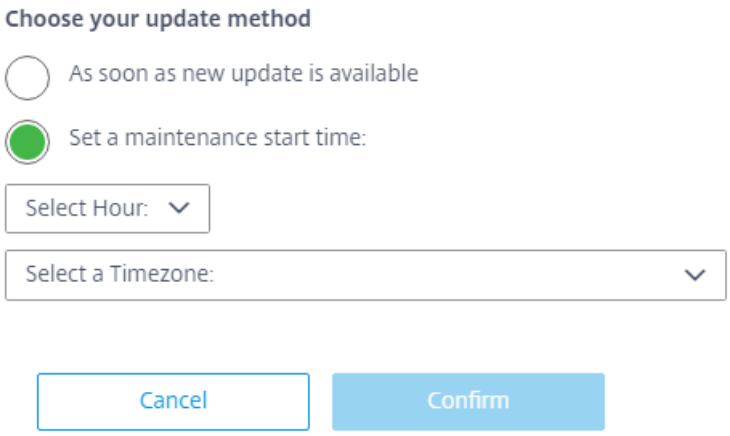
Si un seul connecteur est configuré pour un emplacement de ressources, Citrix Cloud affiche un avertissement sur la page **Emplacements des ressources** et **Connectors**.

Mises à jour d'appliance Connector

L'appliance Connector est mise à jour automatiquement. Vous n'êtes pas obligé de prendre des mesures pour mettre à jour votre connecteur.

Vous pouvez configurer votre emplacement de ressources pour appliquer les mises à jour immédiatement dès qu'elles sont disponibles ou pendant une fenêtre de maintenance spécifique. Pour configurer la fenêtre de maintenance, procédez comme suit :

1. Sur l'emplacement de ressources, accédez au menu des points de suspension (…) et sélectionnez **Gérer l'emplacement des ressources**.
2. Dans la section **Choisissez votre méthode de mise à jour**, sélectionnez **Définissez une heure de début de la maintenance**.
3. Choisissez l'heure de début et le fuseau horaire dans les listes.
4. Cliquez sur **Confirmer**.



Dans le cadre de la mise à jour, l'appliance Connector devient temporairement indisponible. La mise à jour automatique ne met à jour qu'une seule appliance Connector dans un emplacement de ressources à la fois. Pour cette raison, il est important d'enregistrer au moins deux appliances Connector dans chaque emplacement de ressources pour s'assurer qu'au moins une appliance Connector est toujours disponible.

Communication de l'appliance Connector

L'appliance Connector authentifie et crypte toutes les communications entre Citrix Cloud et vos emplacements de ressources. Une fois installé, l'appliance Connector initie la communication avec Citrix Cloud via une connexion sortante. Toutes les connexions sont établies depuis l'appliance Connector vers le cloud à l'aide du port HTTPS standard (443) et du protocole TCP. Aucune connexion entrante n'est acceptée.

L'appliance Connector peut communiquer avec les systèmes locaux de votre emplacement de ressources et avec les systèmes externes. Si vous définissez un ou plusieurs proxy Web lors de l'enregistrement d'appliance Connector, seul le trafic entre l'appliance Connector et les systèmes externes est acheminé via ce proxy Web. Si votre système local se trouve dans un espace d'adressage privé, le trafic d'appliance Connector vers ce système n'est pas acheminé via le proxy Web.

L'appliance Connector définit les espaces d'adressage privés avec les plages d'adresses IPv4 suivantes :

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

Exigences en termes de connexion Internet

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.

Les adresses suivantes doivent pouvoir être contactées avec des connexions HTTPS non modifiées afin d'utiliser et de consommer correctement les services Citrix Cloud.

- https://*.cloud.com
- https://*.citrixworkspacesapi.net
- https://*.citrixnetworkapi.net
- https://*.nssvc.net
- https://*.servicebus.windows.net
- https://iwsprodeastusuniconacr.azurecr.io
- https://iwsprodeastusuniconacr.eastus.data.azurecr.io

Configuration système requise

L'appliance Connector est prise en charge sur les hyperviseurs suivants :

- Citrix XenServer 7.1 CU2 LTSR
- Citrix Hypervisor 8.2 LTSR
- VMware ESXi version 6.5
- Hyper-V sur Windows Server 2016 ou Windows Server 2019
- Microsoft Azure

Votre hyperviseur doit fournir les fonctionnalités minimales suivantes :

- Disque racine de 20 Gio
- 2 processeurs virtuels
- Mémoire de 4 Gio
- Un réseau IPv4

Assurez-vous que votre environnement dispose de la configuration suivante :

- Le réseau permet à l'appliance Connector d'utiliser DHCP pour obtenir des serveurs DNS, une adresse IP, un nom d'hôte et un nom de domaine.
- Le réseau n'est pas configuré pour utiliser les plages IP locales de liaison 169.254.0.1/24, 169.254.64.0/18 ou 169.254.192.0/18 qui sont utilisées en interne par l'appliance Connector.
- L'horloge de l'hyperviseur est définie sur le temps universel coordonné (UTC) et est synchronisée avec un serveur de temps.
- Si vous utilisez un proxy avec l'appliance Connector, le proxy doit être non authentifié.

Vous pouvez héberger plusieurs appliances Connector sur le même hôte hyperviseur. Le nombre

d'appliances Connector sur le même hôte est limité uniquement par l'hyperviseur et les limitations matérielles.

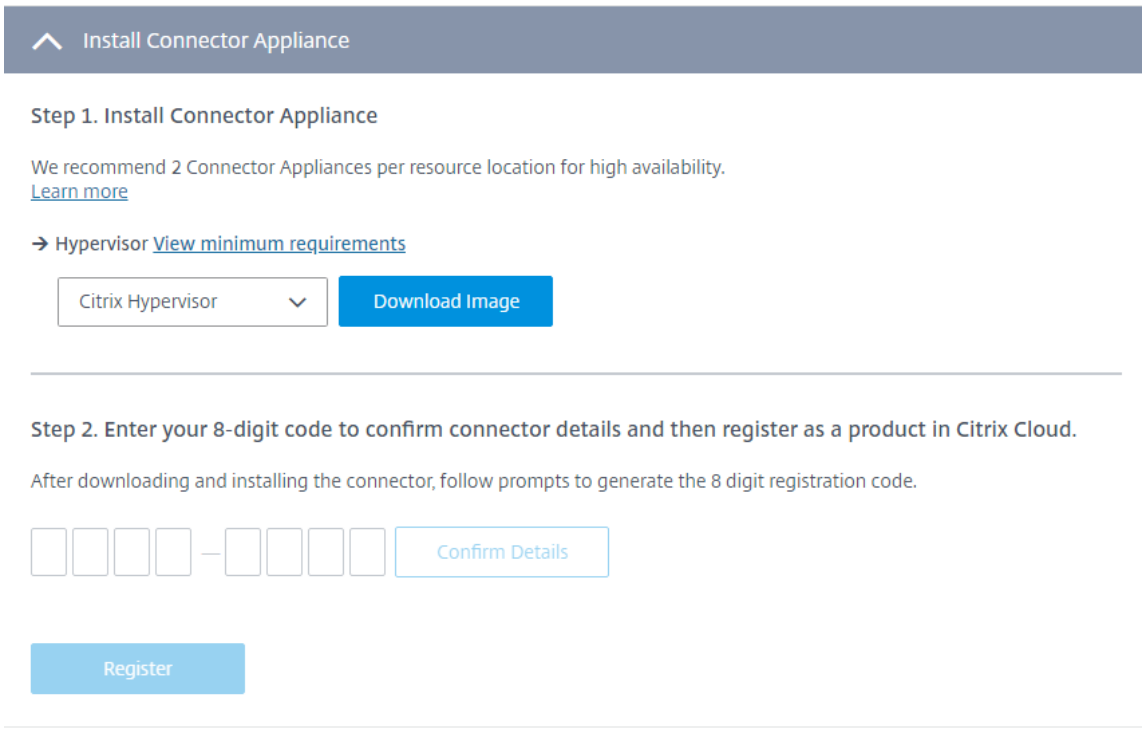
> **Remarque :**
>
> Le clonage, la suspension et la prise d'instantanés de la machine virtuelle d'appliance Connector ne sont pas pris en charge.

Obtenir l'appliance Connector

Téléchargez le logiciel Appliance 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 n'avez pas encore d'emplacement de ressources, cliquez sur l'icône plus (+) ou sélectionnez **Ajouter un emplacement de ressources**.
4. Dans l'emplacement de ressources où vous souhaitez enregistrer l'appliance Connector, cliquez sur l'icône Plus (+) de **Appliances Connector**.

   La tâche **Installer appliance Connector** s'ouvre.

5. Dans la liste **Hyperviseur** de l'**étape 1**, choisissez le type d'hyperviseur que vous utilisez pour héberger votre appliance Connector. Cliquez sur **Télécharger l'image**.
6. Consultez le contrat de service de l'utilisateur final Citrix et, si vous êtes d'accord, sélectionnez **Accepter et continuer**.

7. Lorsque vous y êtes invité, enregistrez le fichier de l'appliance Connector fourni.

   L'extension du nom du fichier de l'appliance Connector dépend de l'hyperviseur que vous choisissez.

8. Gardez la tâche **Installer appliance Connector** ouverte. Après avoir installé l'appliance Connector, vous entrez votre code d'enregistrement à l'**étape 2**.

Vous pouvez également accéder à la tâche **Installer appliance Connector** à partir de la page **Connectors**. Sélectionnez l'icône plus (+) pour ajouter un connecteur et choisissez d'ajouter une appliance Connector.

Installer l'appliance Connector sur votre hyperviseur

Le fichier XVA, OVA ou ZIP que vous avez téléchargé à partir de Citrix Cloud contient une appliance Connector autonome que vous pouvez héberger sur votre hyperviseur.

- Citrix Hypervisor
- VMware ESXi
- Hyper-V
- Microsoft Azure

Citrix Hypervisor

Cette section décrit comment importer l'appliance Connector sur un serveur Citrix Hypervisor à l'aide de XenCenter.

1. Connectez-vous à votre serveur ou pool Citrix Hypervisor à l'aide de XenCenter sur un système qui a accès au fichier XVA d'appliance Connector téléchargé.
2. Sélectionnez **Fichier** > **Importer**.
3. Spécifiez ou accédez au chemin d'accès où se trouve le fichier XVA de l'appliance Connector. Cliquez sur **Suivant**.
4. Sélectionnez le serveur Citrix Hypervisor sur lequel vous souhaitez héberger l'appliance Connector. Vous pouvez également sélectionner le pool dans lequel héberger l'appliance Connector et Citrix Hypervisor choisit un serveur disponible approprié. Cliquez sur **Suivant**.
5. Spécifiez le référentiel de stockage à utiliser pour votre appliance Connector. Cliquez sur **Importer**.
6. Cliquez sur **Ajouter** pour ajouter une interface réseau virtuelle. Dans la liste **Réseau**, sélectionnez le réseau que l'appliance Connector doit utiliser. Cliquez sur **Suivant**.
7. Passez en revue les options à utiliser pour déployer l'appliance Connector. En cas d'erreur, utilisez **Précédent** pour modifier ces options.
8. Assurez-vous que **Démarrer la ou les nouvelles machines virtuelles automatiquement dès que l'importation est terminée** est sélectionnée. Cliquez sur **Terminer**.

Une fois l'appliance Connector déployée et démarrée avec succès, sa console affiche une page d'accueil contenant l'adresse IP de l'appliance Connector. Utilisez cette adresse IP pour vous connecter à l'appliance Connector et poursuivre le processus d'installation.

Par défaut, l'appliance Connector utilise DHCP pour définir sa configuration réseau. Si DHCP n'est pas disponible dans votre environnement, vous devez définir la configuration réseau sur la console de l'appliance Connector avant de pouvoir accéder à l'interface utilisateur de l'appliance Connector. Pour plus d'informations, consultez Définir la configuration réseau à l'aide de la console de l'appliance Connector.

VMware ESXi

Cette section décrit comment déployer une appliance Connector sur un hôte VMware ESXi à l'aide de VMware vSphere Client.

1. Connectez-vous à votre hôte ESXi à l'aide de vSphere Client sur un système qui a accès au fichier OVA de l'appliance Connector téléchargé.
2. Sélectionnez **Fichier** > **Déployer le modèle OVF…**
3. Spécifiez ou accédez au chemin d'accès où se trouve le fichier OVA de l'appliance Connector. Cliquez sur **Suivant**.
4. Vérifiez les détails du modèle. Cliquez sur **Suivant**.
5. Vous pouvez spécifier un nom unique pour votre instance d'appliance Connector. Par défaut, le nom est défini sur « Appliance Connector ». Assurez-vous de choisir un nom qui distingue cette instance d'appliance Connector des autres instances hébergées sur cet hôte ESXi. Cliquez sur **Suivant**.
6. Spécifiez le stockage de destination de votre appliance Connector. Cliquez sur **Suivant**.
7. Choisissez le format dans lequel stocker les disques virtuels. Cliquez sur **Suivant**.
8. Passez en revue les options à utiliser pour déployer l'appliance Connector. En cas d'erreur, utilisez **Précédent** pour modifier ces options.
9. Sélectionnez **Mise sous tension après le déploiement**. Cliquez sur **Terminer**.

Une fois l'appliance Connector déployée et démarrée avec succès, sa console affiche une page d'accueil contenant l'adresse IP de l'appliance Connector. Utilisez cette adresse IP pour vous connecter à l'appliance Connector et poursuivre le processus d'installation.

Par défaut, l'appliance Connector utilise DHCP pour définir sa configuration réseau. Si DHCP n'est pas disponible dans votre environnement, vous devez définir la configuration réseau sur la console de l'appliance Connector avant de pouvoir accéder à l'interface utilisateur de l'appliance Connector. Pour plus d'informations, consultez Définir la configuration réseau à l'aide de la console de l'appliance Connector.

Hyper-V

Cette section décrit comment déployer l'appliance Connector sur un hôte Hyper-V. Vous pouvez déployer la VM à l'aide du Gestionnaire Hyper-V ou à l'aide du script PowerShell inclus.

Déployer l'appliance Connector à l'aide du Gestionnaire Hyper-V

1. Connectez-vous à l'hôte Hyper-V.
2. Copiez ou téléchargez le fichier ZIP de l'appliance Connector sur l'hôte Hyper-V.
3. Extrayez le contenu du fichier ZIP : un script PowerShell et le fichier `connector-appliance.vhdx`.
4. Copiez le fichier VHDX à l'endroit où vous souhaitez conserver vos disques de VM. Par exemple, `C:\ConnectorApplianceVMs`.
5. Ouvrez le Gestionnaire Hyper-V.
6. Cliquez avec le bouton droit de la souris sur le nom de votre serveur et sélectionnez **Nouveau > Ordinateur virtuel**.
7. Dans l'**Assistant Nouvel ordinateur virtuel**, dans le panneau **Spécifier le nom et l'emplacement**, entrez un nom unique à utiliser pour identifier votre appliance Connector dans le champ **Nom**. Cliquez sur **Suivant**.
8. Dans le panneau **Spécifier la génération**, sélectionnez Génération 1. Cliquez sur **Suivant**.
9. Dans le panneau **Affecter la mémoire** :

   a) Attribuez 4 Go de RAM.
   b) Désactivez la mémoire dynamique.

   Cliquez sur *Suivant*.
10. Dans le panneau **Configurer le réseau**, sélectionnez un commutateur dans la liste, par exemple, Commutateur par défaut. Cliquez sur **Suivant**.
11. Dans le panneau **Connecter un disque dur virtuel**, sélectionnez **Utiliser un disque dur virtuel existant**.
12. Accédez à l'emplacement du fichier `connector-appliance.vhdx` et sélectionnez-le. Cliquez sur **Suivant**.
13. Dans le panneau **Résumé**, passez en revue les valeurs que vous avez choisies et cliquez sur **Terminer** pour créer l'ordinateur virtuel.
14. Dans le panneau **Ordinateurs virtuels**, cliquez avec le bouton droit de la souris sur l'ordinateur virtuel de l'appliance Connector et sélectionnez **Paramètres**.

15. Dans la fenêtre **Paramètres**, accédez à **Matériel > Processeurs**. Définissez la valeur **Nombre de processeurs virtuels** sur 2. Cliquez sur **Appliquer**, puis **sur OK**.
16. Dans le panneau **Ordinateurs virtuels**, cliquez avec le bouton droit de la souris sur l'ordinateur virtuel de l'appliance Connector et sélectionnez **Démarrer**.
17. Cliquez avec le bouton droit de la souris sur l'ordinateur virtuel de l'appliance Connector et sélectionnez **Se connecter** pour ouvrir la console.

Une fois l'appliance Connector déployée et démarrée, connectez-vous à la console à l'aide du Gestionnaire Hyper-V. La console affiche une page d'accueil contenant l'adresse IP de l'appliance Connector. Utilisez cette adresse IP pour vous connecter à l'appliance Connector et poursuivre le processus d'installation.

Par défaut, l'appliance Connector utilise DHCP pour définir sa configuration réseau. Si DHCP n'est pas disponible dans votre environnement, vous devez définir la configuration réseau sur la console de l'appliance Connector avant de pouvoir accéder à l'interface utilisateur de l'appliance Connector. Pour plus d'informations, consultez Définir la configuration réseau à l'aide de la console de l'appliance Connector.

Déployer l'appliance Connector à l'aide d'un script PowerShell

Le fichier `connector-appliance.zip` contient un script PowerShell qui crée et démarre une nouvelle machine virtuelle.

> **Remarque :**
>
> Pour exécuter ce script PowerShell non signé, vous devrez peut-être modifier les stratégies d'exécution sur le système Hyper-V. Pour plus d'informations, consultez https://go.microsoft.com/fwlink/?LinkID=135170. Vous pouvez également utiliser le script fourni comme base pour créer ou modifier votre propre script local.

1. Connectez-vous à l'hôte Hyper-V.
2. Copiez ou téléchargez le fichier ZIP de l'appliance Connector sur l'hôte Hyper-V.
3. Extrayez le contenu du fichier ZIP : un script PowerShell et un fichier VHDX.
4. Dans une console PowerShell, modifiez le répertoire où se trouve le contenu du fichier ZIP et exécutez la commande suivante :

```
1 .\connector-appliance-install.ps1
```

5. Lorsque vous y êtes invité, tapez un nom pour votre machine virtuelle ou appuyez sur Entrée pour accepter la valeur par défaut **Appliance Connector**.

6. Lorsque vous y êtes invité, tapez une destination pour le disque racine ou appuyez sur Entrée pour utiliser le répertoire par défaut du système pour les disques durs virtuels.
7. Lorsque vous y êtes invité, tapez un nom de fichier pour le disque racine ou appuyez sur Entrée pour accepter la valeur par défaut `connector-appliance.vhdx`.
8. Lorsque vous y êtes invité, sélectionnez le commutateur à utiliser. Appuyez sur Entrée.
9. Consultez le résumé des informations d'importation de VM. Si les informations sont correctes, appuyez sur Entrée pour continuer.

   Le script crée et démarre la machine virtuelle de l'appliance Connector.

Une fois l'appliance Connector déployée et démarrée avec succès, sa console affiche une page d'accueil contenant l'adresse IP de l'appliance Connector. Utilisez cette adresse IP pour vous connecter à l'appliance Connector et poursuivre le processus d'installation.

Microsoft Azure

Cette section décrit comment déployer l'appliance Connector dans Microsoft Azure. Vous pouvez déployer la VM à l'aide du script PowerShell inclus.

Le fichier `connector-appliance.zip` contient un script PowerShell qui crée et démarre une nouvelle machine virtuelle. Vous pouvez utiliser le script fourni comme base pour créer ou modifier votre propre script local.

Avant d'exécuter le script, assurez-vous de remplir les conditions préalables suivantes :

- Installez le module Az PowerShell dans votre environnement PowerShell local.
- Exécutez le script PowerShell dans le répertoire où se trouve le fichier VHD.

Procédez comme suit :

1. Copiez ou téléchargez le fichier ZIP de l'appliance Connector sur votre système Windows.
2. Extrayez le contenu du fichier ZIP : un script PowerShell et un fichier VHD.
3. Ouvrez une console PowerShell en tant qu'administrateur.
4. Modifiez le répertoire où se trouve le contenu du fichier ZIP et exécutez la commande suivante :

```
.\connector-appliance-upload.ps1
```

5. Une boîte de dialogue s'affiche, vous invitant à vous connecter à Microsoft Azure. Entrez vos informations d'identification.
6. Lorsque le script PowerShell vous y invite, sélectionnez l'abonnement à utiliser. Appuyez sur Entrée.

7. Suivez les invites du script qui vous guident tout au long du chargement de l'image et de la création d'une machine virtuelle.
8. Après avoir créé la première VM, le script vous demande si vous souhaitez créer une autre VM à partir de l'image chargée.
    - Entrez `y` pour créer une autre VM.
    - Entrez `n` pour quitter le script.

Une fois l'appliance Connector déployée et démarrée avec succès, sa console affiche une page d'accueil contenant l'adresse IP de l'appliance Connector. Utilisez cette adresse IP pour vous connecter à l'appliance Connector et poursuivre le processus d'installation.

Enregistrer votre appliance Connector avec Citrix Cloud

Enregistrez une appliance Connector auprès de Citrix Cloud pour fournir un canal de communication entre Citrix Cloud et vos emplacements de ressources.

Après avoir installé l'appliance Connector sur l'hyperviseur et l'avoir démarrée, la console affiche l'adresse IP de l'appliance Connector. La console affiche également une empreinte SSL que vous pouvez utiliser pour valider votre connexion à l'interface utilisateur de l'appliance Connector.

1. Copiez l'adresse IP de l'appliance Connector dans la barre d'adresse de votre navigateur.

    L'interface utilisateur de l'appliance Connector utilise un certificat auto-signé. Par conséquent, vous pouvez voir un message indiquant que la connexion n'est pas sécurisée. Pour vérifier la connexion à votre appliance Connector, vous pouvez comparer l'empreinte SSL de la console avec l'empreinte que le navigateur reçoit de la page Web.

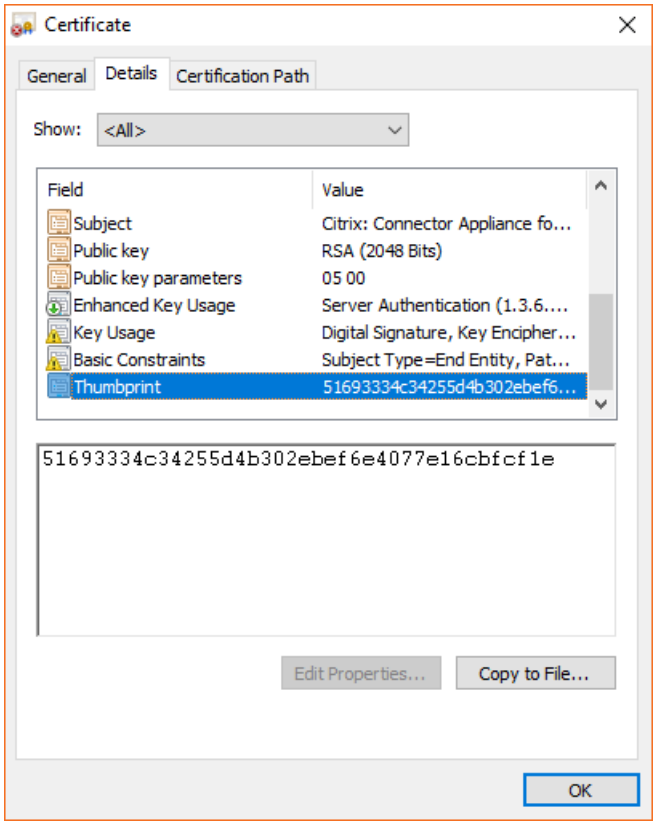
Par exemple, dans le navigateur Google Chrome, procédez comme suit :

a) Cliquez sur le marqueur **Non sécurisé** en regard de la barre d'adresse.

b) Sélectionnez **Certificat**. La fenêtre **Certificat** s'ouvre.

c) Accédez à l'onglet **Détails** et recherchez le champ **Empreinte**.

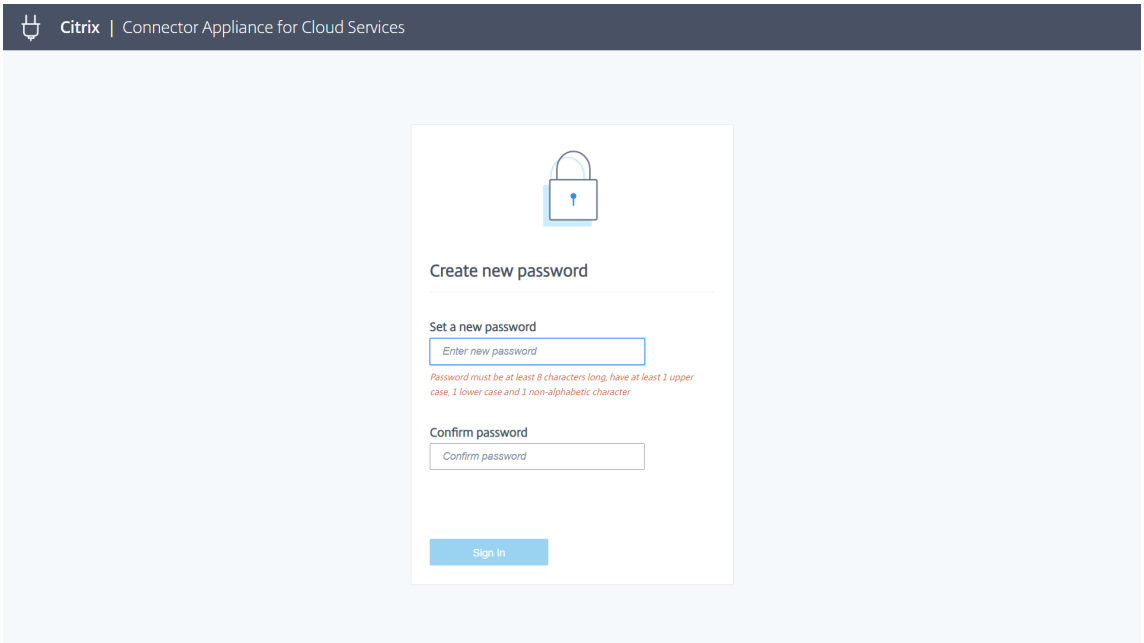
Si la valeur du champ **Empreinte** correspond à l'empreinte SSL fournie dans la console, vous pouvez confirmer que votre navigateur se connecte directement à l'interface utilisateur de l'appliance Connector.



2. Si votre navigateur nécessite une étape supplémentaire pour confirmer que vous souhaitez continuer sur le site, effectuez cette étape maintenant.

   La page Web **Créer un mot de passe** s'ouvre.

3. Créez un mot de passe pour votre interface utilisateur de l'appliance Connector et cliquez sur **Définir le mot de passe**.



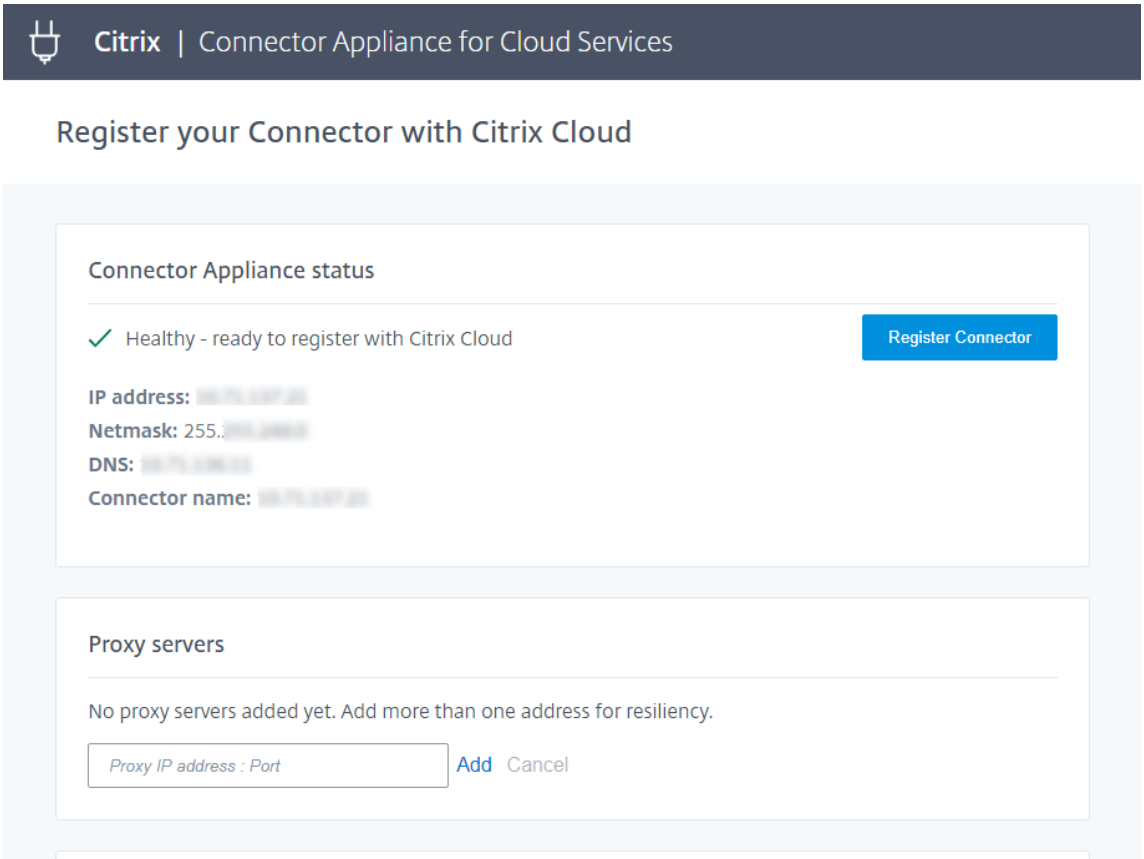
Le mot de passe que vous définissez doit répondre aux conditions suivantes :

- Huit caractères ou plus
- Contient des lettres majuscules et minuscules
- Contient au moins un caractère non alphabétique

Assurez-vous de stocker ce mot de passe dans un endroit sûr pour une utilisation future.

4. Connectez-vous avec le mot de passe que vous venez de définir.

   La **page d'administration de l'appliance Connector** s'ouvre.



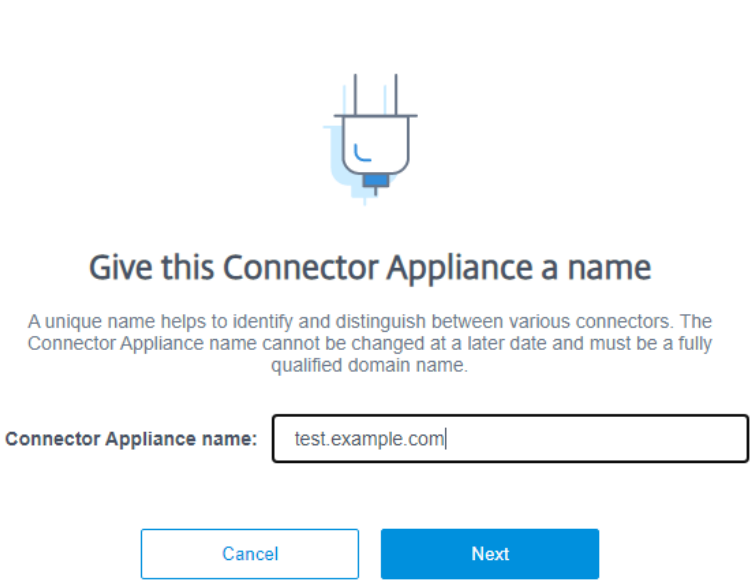
5. (Facultatif) Si vous utilisez un ou plusieurs proxy Web, vous pouvez ajouter les adresses proxy ici. Seuls les proxy non authentifiés sont pris en charge.

   Seul le trafic vers des systèmes externes est acheminé via le proxy Web. Pour plus d'informations, consultez Communication de l'appliance Connector.

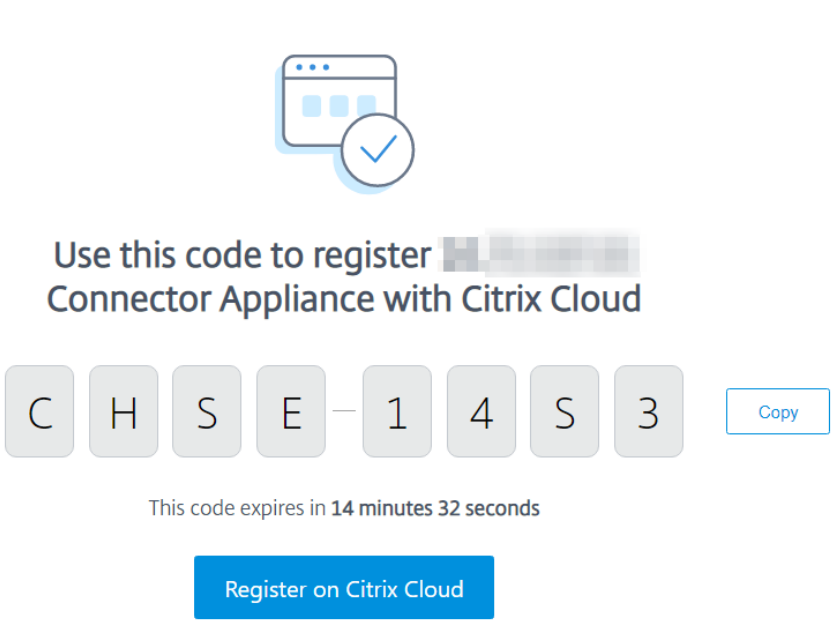
6. Cliquez sur **Enregistrer Connector** pour ouvrir la tâche d'enregistrement.

7. Donnez un nom à votre appliance Connector. Ce nom peut vous aider à distinguer les différentes appliances Connector qui existent dans votre emplacement de ressources. Après avoir enregistré votre appliance Connector, le nom ne peut pas être modifié.

   Entrez le nom dans le champ **Nom de l'appliance Connector**, puis cliquez sur **Suivant**.

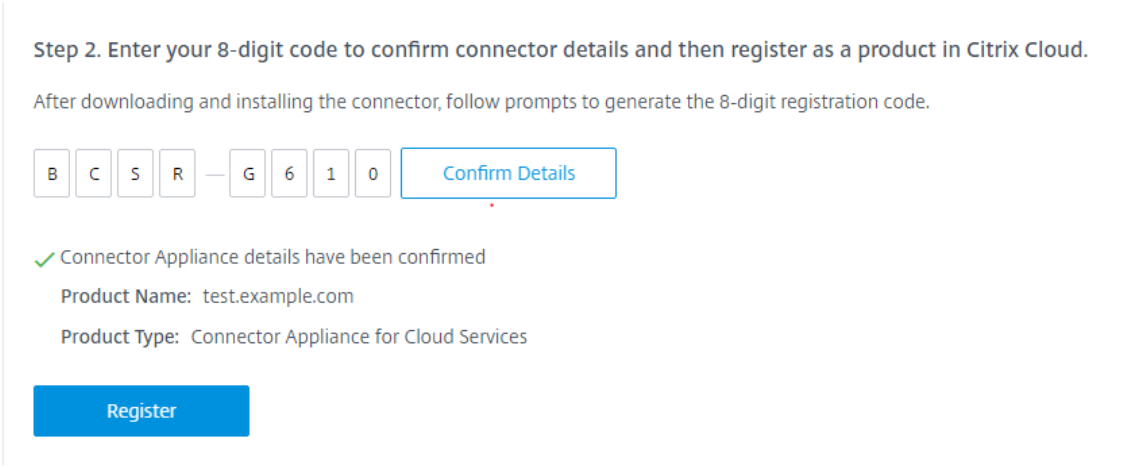


La page Web fournit un code à utiliser pour l'enregistrement auprès de Citrix Cloud. Ce code expire dans 15 minutes.



8. Utilisez le bouton **Copier** pour copier le code dans le Presse-papiers.
9. Revenez à la page Web **Emplacements des ressources**.
10. Collez le code à l'**étape 2** de la tâche **Installer appliance Connector**. Cliquez sur **Confirmer les détails**.

Citrix Cloud vérifie que l'appliance Connector est présente et peut être contactée. Si le code d'enregistrement a expiré, vous êtes invité à générer un nouveau code.



11. Cliquez sur **Enregistrer**.

    La page indique si l'enregistrement a réussi. Si l'enregistrement a échoué, vous êtes invité à réessayer.

12. Cliquez sur **Fermer**.

La **page d'administration de l'appliance Connector** vous permet également de télécharger un rapport de diagnostic pour l'appliance Connector. Pour plus d'informations, consultez Génération d'un rapport de diagnostic.

Après avoir enregistré votre appliance Connector

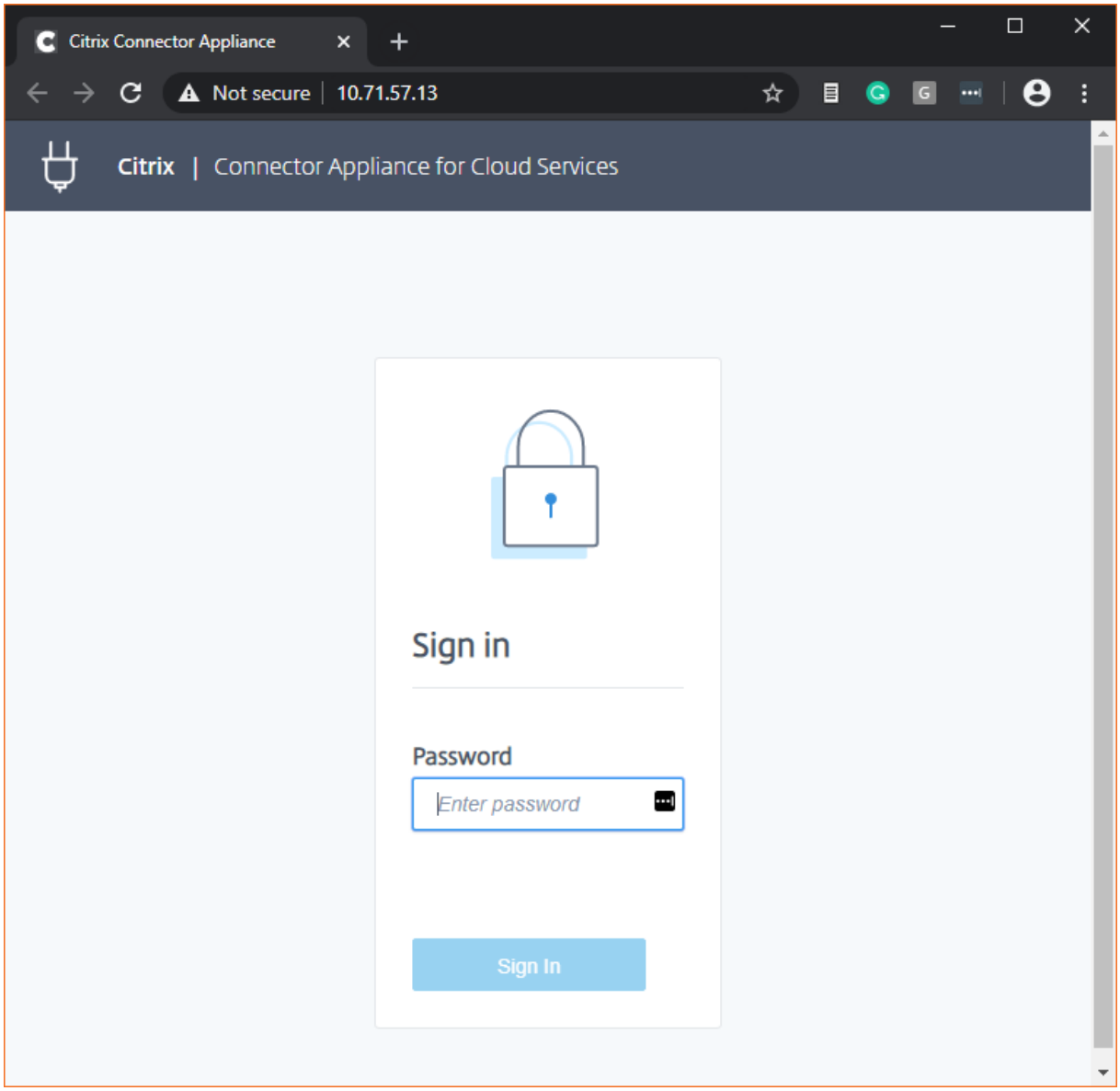
Pour chaque emplacement de ressources, nous vous conseillons d'installer et d'enregistrer au moins deux appliances Connector. Cette configuration garantit une disponibilité continue et permet aux connecteurs d'équilibrer la charge.

Vous ne pouvez pas gérer directement votre appliance Connector.

L'appliance Connector est mise à jour automatiquement. Vous n'êtes pas obligé de prendre des mesures pour mettre à jour votre connecteur. Vous pouvez spécifier l'heure et le jour où les mises à jour de l'appliance Connector doivent être appliquées à votre emplacement de ressources. Pour plus d'informations, consultez Mises à jour de Connector.

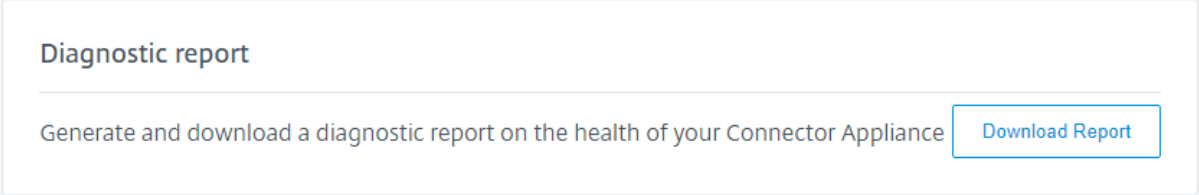
Vous ne devez pas cloner, suspendre ou prendre un instantané de vos machines virtuelles d'appliance Connector. Ces actions ne sont pas prises en charge.

La page **Créer un mot de passe** ne s'affiche que la première fois que vous vous connectez à l'interface utilisateur de l'appliance Connector. Lors des connexions ultérieures à l'interface utilisateur, vous êtes invité à entrer le mot de passe que vous avez défini lors de l'enregistrement de l'appliance Connector.



Génération d'un rapport de diagnostic

Vous pouvez générer et télécharger un rapport de diagnostic à partir de la **page d'administration de l'appliance Connector**.



1. À partir de la console de l'appliance Connector de votre hyperviseur, copiez l'adresse IP dans la barre d'adresse de votre navigateur.

2. Entrez le mot de passe que vous avez défini lors de l'enregistrement de votre appliance Connector.
3. Dans la section **Rapport de diagnostic** de la page, cliquez sur **Télécharger le rapport**.

Les rapports de diagnostic sont fournis dans un fichier `.zip`.

Paramètres réseau de votre appliance Connector

Par défaut, l'adresse IP et les paramètres réseau de votre appliance Connector sont automatiquement attribués à l'aide de DHCP.

Après avoir enregistré votre appliance Connector à l'aide de DHCP, vous pouvez modifier ses paramètres réseau dans la **page d'administration de l'appliance Connector**.

Toutefois, si DHCP n'est pas disponible dans votre environnement ou si vous n'avez pas accès à la **page d'administration de l'appliance Connector**, vous pouvez définir la configuration réseau directement sur la console de l'appliance Connector.

Configuration des paramètres réseau sur la page d'administration de l'appliance Connector

Après avoir enregistré votre appliance Connector à l'aide de DHCP, vous pouvez modifier ses paramètres réseau dans la **page d'administration de l'appliance Connector**.

Pour configurer manuellement vos paramètres réseau, procédez comme suit :

1. Dans la section **Résumé du Connector**, sélectionnez **Modifier les paramètres réseau**.
2. Dans la boîte de dialogue **Paramètres réseau**, choisissez **Configurer vos propres paramètres réseau**.
3. Renseignez les champs **Adresse IP**, **Masque de sous-réseau** et **Passerelle par défaut**.
4. Ajoutez un ou plusieurs **serveurs DNS**.
5. Ajoutez un ou plusieurs **serveurs NTP**.
6. Cliquez sur **Enregistrer**.

Lorsque vous enregistrez les modifications apportées à vos paramètres réseau, l'appliance Connector redémarre. Pendant le redémarrage, l'appliance Connector est temporairement indisponible. Vous êtes déconnecté de la **page d'administration de l'appliance Connector** et l'URL de cette page change. Vous pouvez trouver la nouvelle URL dans la console de l'appliance Connector ou en consultant les informations réseau de votre hyperviseur.

Pour modifier votre configuration réseau afin d'utiliser les valeurs attribuées automatiquement, procédez comme suit :

1. Dans la section **Résumé du Connector**, sélectionnez **Modifier les paramètres réseau**.
2. Dans la boîte de dialogue **Paramètres réseau**, choisissez **Obtenir adresse IP automatiquement**.

3. Cliquez sur **Enregistrer**.

Lorsque vous enregistrez les modifications apportées à vos paramètres réseau, l'appliance Connector redémarre. Pendant le redémarrage, l'appliance Connector est temporairement indisponible. Vous êtes déconnecté de la **page d'administration de l'appliance Connector** et l'URL de cette page change. Vous pouvez trouver la nouvelle URL dans la console de l'appliance Connector ou en consultant les informations réseau de votre hyperviseur.

Définir la configuration réseau à l'aide de la console de l'appliance Connector

Par défaut, l'adresse IP et les paramètres réseau de votre appliance Connector sont automatiquement attribués à l'aide de DHCP. Toutefois, si DHCP n'est pas disponible dans votre environnement ou si vous n'avez pas accès à la **page d'administration de l'appliance Connector**, vous pouvez définir la configuration réseau directement sur la console de l'appliance Connector.

Pour définir la configuration réseau, procédez comme suit :

1. Dans votre hyperviseur, redémarrez l'appliance Connector.
2. Pendant le démarrage de l'appliance Connector, attendez que le message `Welcome to GRUB!` s'affiche sur la console.
3. Lorsque ce message s'affiche, appuyez sur **Échap** pour accéder au menu GRUB.
4. Pour modifier les paramètres de démarrage, appuyez sur **e**.

   L'affichage du message se présente comme suit :

5. Modifiez la ligne qui commence par `linux` pour inclure la configuration réseau requise.

- Pour spécifier la mise en réseau DHCP, ajoutez `network=dhcp` à la fin de la ligne.
- Pour spécifier la mise en réseau statique, ajoutez les paramètres suivants à la fin de la ligne :

```
network=static:ip=<static_ip_address>:netmask=<netmask>:route
   =<default_gateway>:dns=<dns_server_1>,<dns_server_2>:ntp=<
   ntp_server_1>,<ntp_server_2>
```

Remplacez les valeurs de l'espace réservé par les valeurs de votre configuration.

6. Appuyez sur **Ctrl+X** pour démarrer l'appliance Connector avec la nouvelle configuration.

Mises à jour de Connector

July 21, 2021

Citrix publie périodiquement des mises à jour pour améliorer les performances, la sécurité et la fiabilité du Cloud Connector ou de l'appliance Connector. Par défaut, Citrix Cloud installe les mises à jour sur chaque connecteur, une par une, dès qu'elles sont disponibles. Pour vous assurer que les mises à jour sont installées au moment opportun sans affecter l'expérience Citrix Cloud de vos utilisateurs, vous pouvez planifier ces mises à jour sur une heure préférée et un jour préféré de la semaine. Vous pouvez également vérifier que vos connecteurs sont à jour en comparant la version actuelle du connecteur dans votre emplacement de ressources avec la version cible de Citrix Cloud.

Heure préférée

Lorsque vous spécifiez une heure préférée, Citrix Cloud installe les mises à jour 24 heures après leur publication, à votre heure préférée. Par exemple, si votre heure préférée est définie sur 2h00 dans le fuseau horaire USA Pacifique et qu'une mise à jour devient disponible mardi, Citrix Cloud attend 24 heures, puis installe la mise à jour à 2h00 le jour suivant.

Jour préféré de la semaine

Lorsque vous spécifiez un jour préféré de la semaine, Citrix Cloud attend sept jours avant d'installer les mises à jour le jour de votre choix. Cette période d'attente de sept jours vous donne suffisamment de temps pour choisir d'installer la mise à jour à la demande ou d'attendre que Citrix Cloud l'installe le jour de votre choix. Selon le jour de la semaine que vous sélectionnez et le jour où les mises à jour deviennent disponibles, Citrix Cloud peut attendre jusqu'à 13 jours pour installer les mises à jour.

Exemple d'une période d'attente de 8 jours

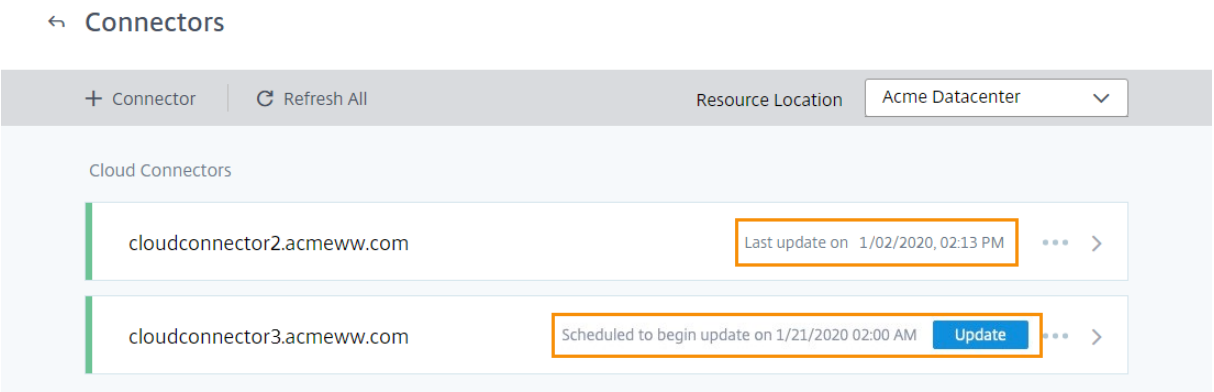
Lundi, vous configurez le mardi à 18h00 comme jour préféré pour les mises à jour. Plus tard dans la journée, Citrix Cloud vous informe qu'une mise à jour est disponible et affiche le bouton **Mettre à jour**. Si vous ne lancez pas la mise à jour, Citrix Cloud attend sept jours, puis installe la mise à jour le jour suivant, le mardi à 18h00.

Exemple d'une période d'attente de 13 jours

Vous avez configuré le lundi à 18h00 comme heure préférée pour les mises à jour. Mardi, Citrix Cloud vous informe qu'une mise à jour est disponible et affiche le bouton **Mettre à jour**. Si vous ne lancez pas la mise à jour, Citrix Cloud attend sept jours, puis installe la mise à jour six jours plus tard, le lundi à 18h00.

Notifications de mise à jour et mises à jour à la demande

Lorsque des mises à jour sont disponibles, Citrix Cloud vous informe avec une alerte dans vos Notifications. En outre, chaque connecteur affiche la date et l'heure auxquelles la mise à jour sera installée.



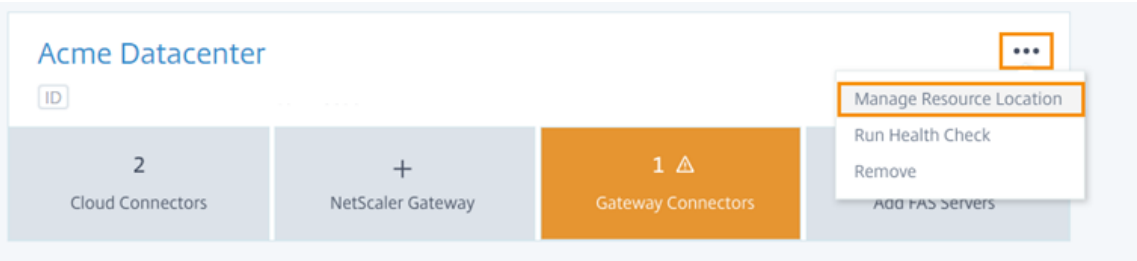
Une fois que Citrix Cloud vous informe d'une mise à jour disponible, chaque connecteur affiche un bouton **Mise à jour** afin que vous puissiez installer la mise à jour plus tôt que votre heure ou jour préféré(e). Après avoir sélectionné **Mettre à jour** pour chaque connecteur, Citrix Cloud met en file d'attente les mises à jour et les installe une à la fois. Vous ne pouvez pas annuler les mises à jour après les avoir lancées.

Une fois la mise à jour terminée, Citrix Cloud affiche la date de la dernière mise à jour. Si certaines mises à jour n'ont pas pu être effectuées, une notification vous est envoyée pour vous en informer.

Choisir une planification de mise à jour

1. Dans le menu Citrix Cloud, sélectionnez **Emplacements des ressources**.

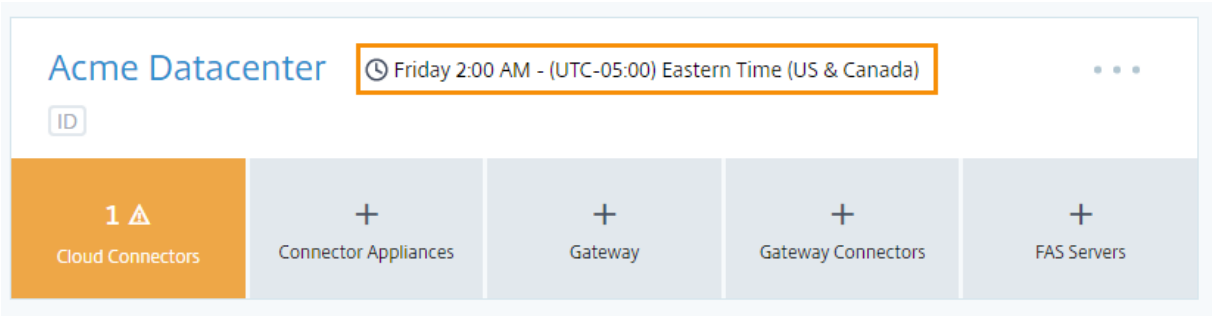
2. Recherchez l'emplacement de ressources à modifier et, dans le menu des points de suspension, sélectionnez **Gérer l'emplacement des ressources**.



3. Sous **Choisissez votre méthode de mise à jour**, sélectionnez **Définissez une heure de début de la maintenance** et choisissez l'heure, le jour et le fuseau horaire pour l'installation des mises à jour.

   - Pour spécifier uniquement une heure préférée, sélectionnez l'heure et le fuseau horaire pendant lesquels vous souhaitez installer les mises à jour. Citrix Cloud installe les mises à jour 24 heures après leur publication, à l'heure de votre choix.
   - Pour spécifier un jour préféré de la semaine, sélectionnez l'heure, le jour et le fuseau horaire. Citrix Cloud attend sept jours après la publication des mises à jour avant de les installer le jour de votre choix.

Après avoir configuré votre planification de mise à jour, Citrix Cloud l'affiche en regard du nom de l'emplacement de ressources.



L'heure de début sélectionnée est appliquée à tous les connecteurs, quel que soit le fuseau horaire dans lequel ils se trouvent. Si vous disposez de connecteurs dans différents fuseaux horaires, Citrix Cloud installe les mises à jour à l'heure et au fuseau horaire que vous avez sélectionnés. Par exemple, si vous planifiez des mises à jour pour 2h00 dans le fuseau horaire USA Pacifique et que vous disposez de connecteurs à Londres, Citrix Cloud commence à installer la mise à jour sur ces connecteurs à 2h00 heure du Pacifique.

> **Remarque :**
>
> Si le connecteur rencontre un problème lors de l'installation de la mise à jour, l'installation s'interrompt jusqu'à ce que le problème soit résolu. Étant donné que les mises à jour sont

> installées sur chaque connecteur, une à la fois, une mise à jour interrompue sur un connecteur peut empêcher les mises à jour sur tous les Cloud Connector restants de votre compte Citrix Cloud.

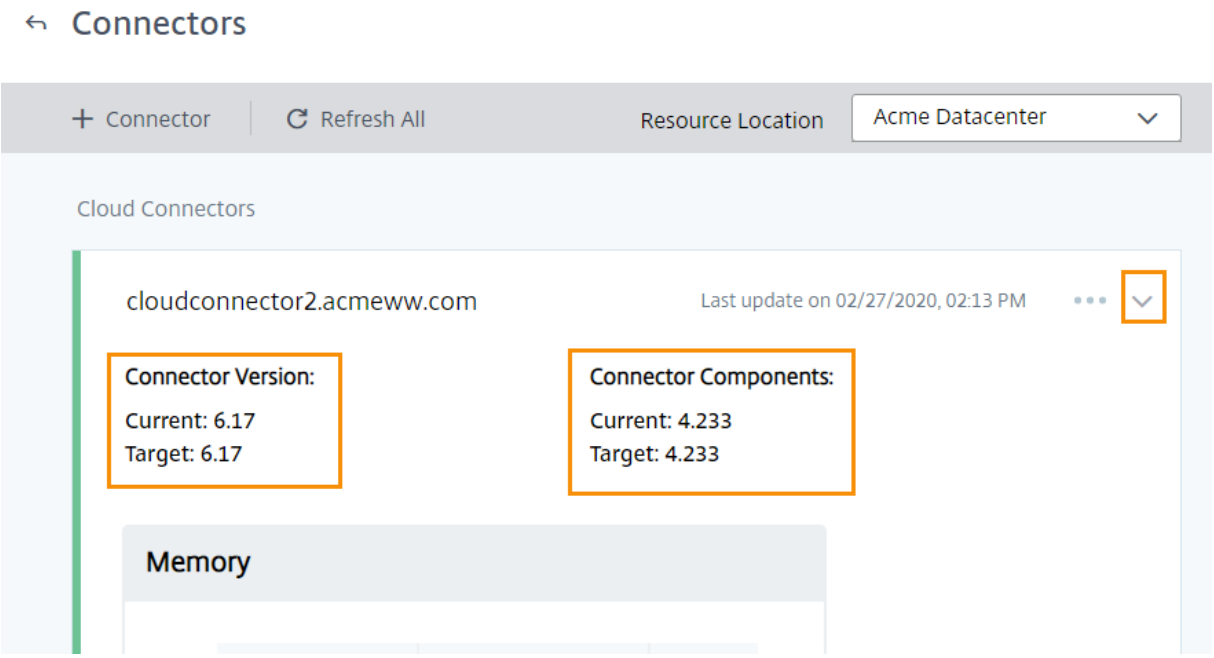
Mises à jour non planifiées

Même si vous choisissez une heure ou un jour préféré(e) pour l'installation des mises à jour, Citrix Cloud peut installer une mise à jour dès que possible après sa publication. Les mises à jour non planifiées se produisent lorsque :

- La mise à jour ne peut pas être installée à l'heure préférée dans les 48 heures suivant sa publication. Par exemple, si votre heure préférée est 2h00 du matin et que le connecteur est hors connexion pendant trois jours suivant la mise à jour, Citrix Cloud installe la mise à jour dès que le connecteur est de nouveau en ligne.
- La mise à jour contient un correctif pour un problème de sécurité ou de fonctionnalité critique.

Comparer les versions de Cloud Connector

Vous pouvez vérifier à tout moment la version du Cloud Connector qui s'exécute dans votre emplacement de ressources. Dans la page **Emplacements des ressources**, sélectionnez la vignette **Cloud Connector** pour l'emplacement de ressources que vous souhaitez gérer. Développez ensuite la vignette Cloud Connector.



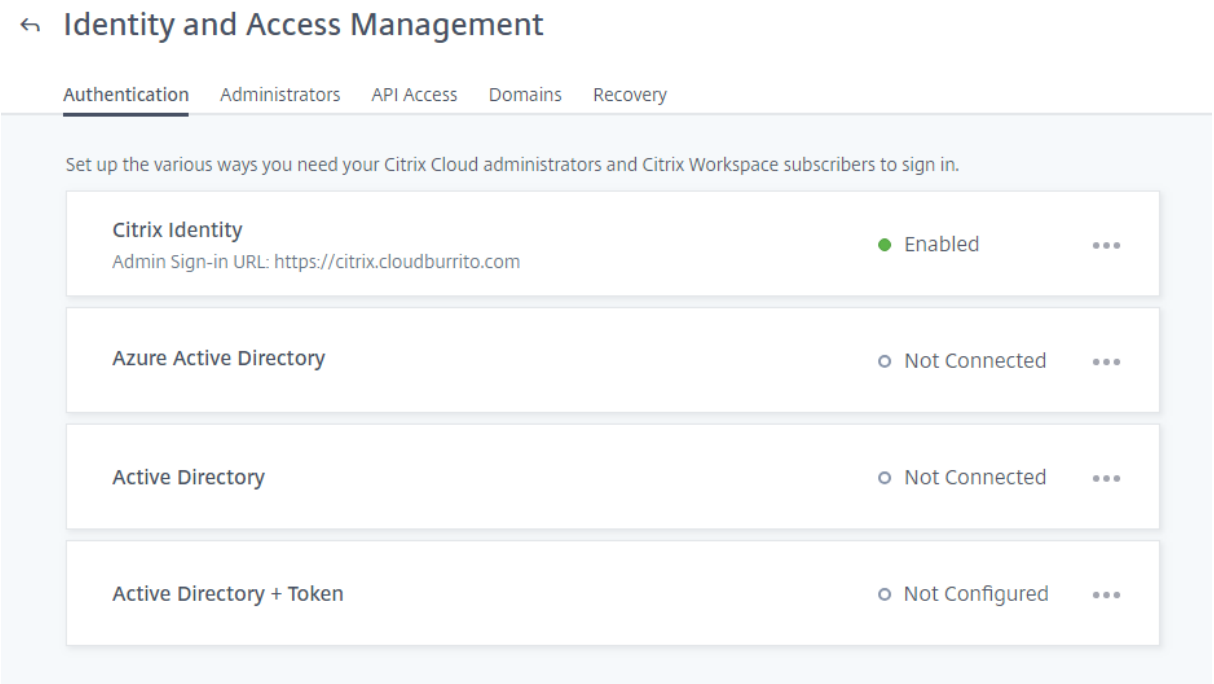
> **Remarque :**
>
> Ces informations ne sont pas disponibles pour les appliances Connector.

Résolution des échecs de maintenance de Cloud Connector

Un logiciel conflictuel installé sur votre machine Cloud Connector ou des erreurs inattendues pendant la maintenance peuvent entraîner l'échec de la mise à jour du Cloud Connector et des pannes de service. Pour plus d'informations sur la gestion d'une mise à jour échouée suite à la maintenance de Cloud Connector, consultez l'article Resolve a Failed Cloud Connector Maintenance.

Gestion des identités et des accès

July 21, 2021



La fonction Gestion des identités et des accès définit les fournisseurs d'identité et les comptes utilisés pour les administrateurs Citrix Cloud et les abonnés à l'espace de travail.

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 cette option pour utiliser l'un des fournisseurs d'identité suivants :

- Répertoire Active Directory local
- Active Directory + jeton
- Azure Active Directory
- Citrix Gateway
- Okta
- SAML 2.0

Citrix Cloud prend également en charge l'utilisation du Service d'authentification fédérée Citrix pour fournir l'authentification unique à Citrix Workspace. Pour plus d'informations, consultez Activer l'authentification unique pour les espaces de travail avec Service d'authentification fédérée de Citrix.

> **Conseil :**
>
> Apprenez-en plus sur les fournisseurs d'identité pris en charge avec le cours de formation Introduction to Citrix Identity and Authentication. Chaque module fournit de courtes vidéos qui vous expliquent comment connecter chaque fournisseur d'identité à Citrix Cloud et activer l'authentification pour Citrix Workspace.

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. En tant qu'administrateur initial, vous pouvez 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 définir leur accès à Citrix Cloud, consultez la section Gérer les administrateurs 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.

Citrix vous demande de réinitialiser votre mot de passe sous certaines conditions pour vous aider à sécuriser votre mot de passe de compte. Pour plus d'informations sur ces conditions, consultez la section Modification de votre mot de passe.

> **Remarque :**
>
> Ajoutez **customerservice@citrix.com** à votre liste d'adresses e-mail autorisées pour vous assurer que les e-mails provenant de Citrix Cloud ne finissent pas dans votre dossier de spam ou la corbeille.

Supprimer des administrateurs

Vous pouvez supprimer des administrateurs de votre compte Citrix Cloud à partir de l'onglet **Administrateurs**. 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 à partir de l'onglet **Domaines**. Si vous prévoyez d'utiliser des domaines de plusieurs forêts, installez au moins deux Citrix Cloud Connector dans chaque forêt. Citrix recommande au moins deux Citrix Cloud Connector pour garantir un environnement de haute disponibilité. Pour plus d'informations sur le déploiement de Cloud Connector dans Active Directory, consultez la section Scénarios de déploiement de Cloud Connector dans Active Directory.

> **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 Citrix 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 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 composants Citrix 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 plus d'informations, consultez Sélectionner un emplacement de ressources principal.

Connecter Active Directory à Citrix Cloud

July 21, 2021

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). En outre, certaines méthodes d'authentification d'espace de travail nécessitent une connexion entre votre AD et Citrix Cloud. Pour plus d'informations, consultez Modifier l'authentification aux espaces de travail.

Citrix Cloud prend en charge l'utilisation de jetons comme deuxième facteur d'authentification pour les abonnés qui se connectent à leurs espaces de travail via Active Directory. Les abonnés à l'espace

de travail peuvent générer des jetons à l'aide de n'importe quelle application conforme à la norme TOTP (mot de passe à usage unique temporaire), telle que Citrix SSO.

Pour plus d'informations sur l'authentification des abonnés à l'espace de travail avec Active Directory et des jetons, consultez la section Active Directory + jeton.

> **Conseil :**
>
> Apprenez-en plus sur les fournisseurs d'identité pris en charge avec le cours de formation Introduction to Citrix Identity and Authentication. Le module « Planning Citrix Identity and Access Management » comprend de courtes vidéos qui vous expliquent comment connecter ce fournisseur d'identité à Citrix Cloud et activer l'authentification pour Citrix Workspace.

Authentification Active Directory

La connexion de votre Active Directory à Citrix Cloud implique l'installation de Cloud Connector dans votre domaine. Citrix recommande d'installer au moins deux composants Cloud Connector pour garantir une haute disponibilité. Pour plus d'informations, consultez les articles suivants :

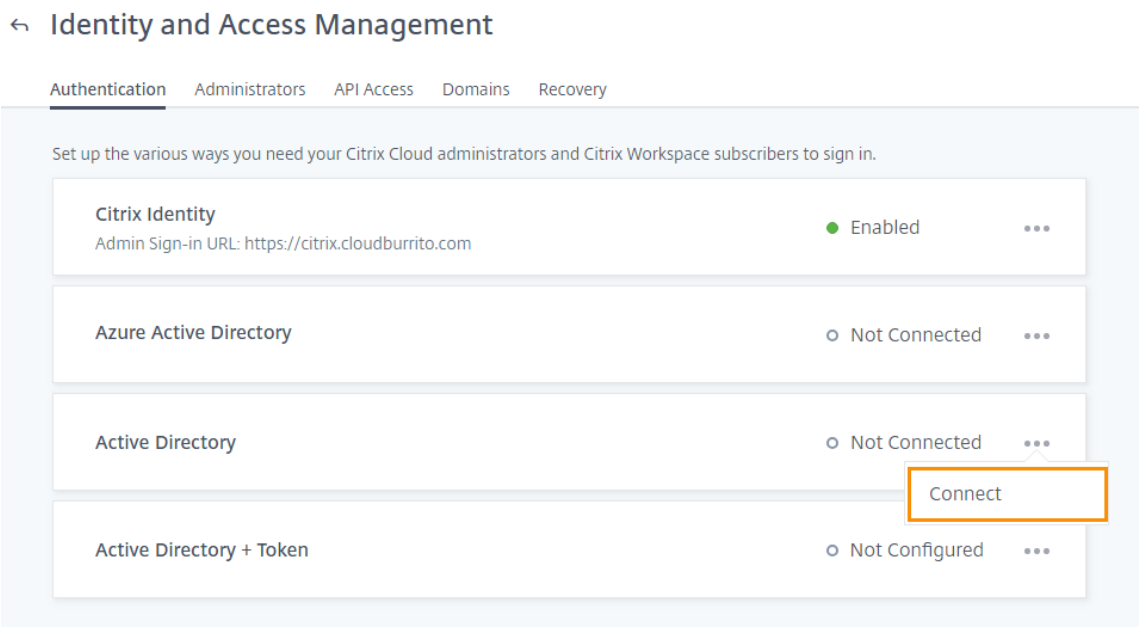
- Détails techniques sur Cloud Connector : pour la configuration système requise et les recommandations de déploiement.
- Installation de Cloud Connector : pour les instructions d'installation à l'aide de l'interface graphique ou de la ligne de commande.

La connexion d'Active Directory à Citrix Cloud implique les tâches suivantes :

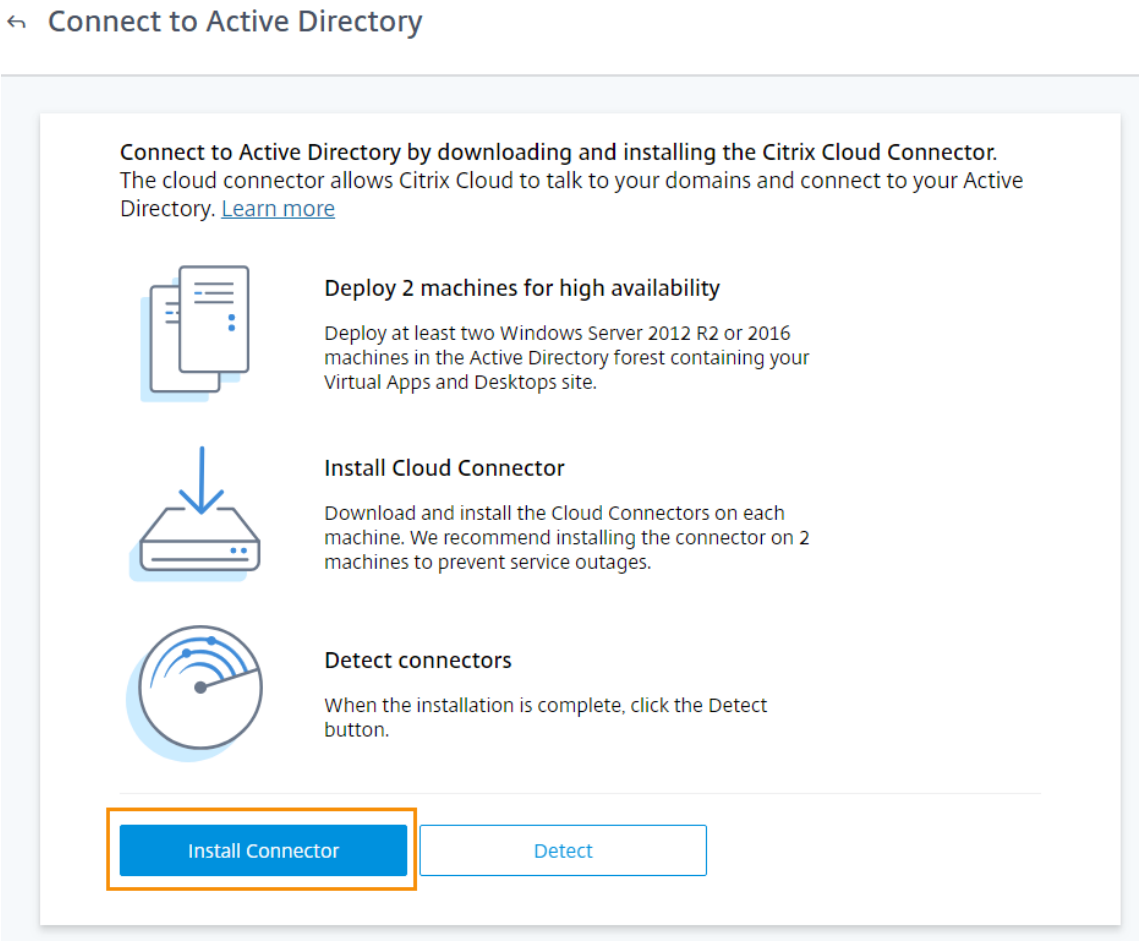
1. Installer des composants Cloud Connector dans votre domaine. Citrix recommande d'installer deux composants Cloud Connector pour garantir une haute disponibilité.
2. Le cas échéant, activez les jetons sur les machines utilisateur. Les abonnés ne peuvent inscrire qu'un seul appareil à la fois.

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.



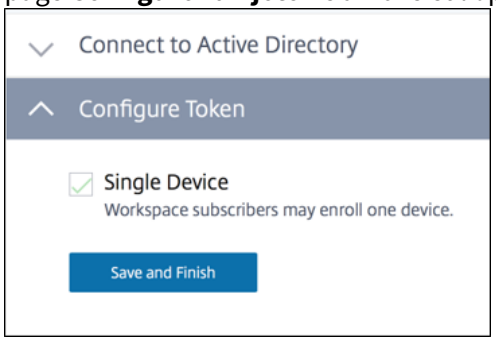
4. Lancez le programme d'installation de Cloud Connector et suivez les instructions de l'assistant

d'installation.

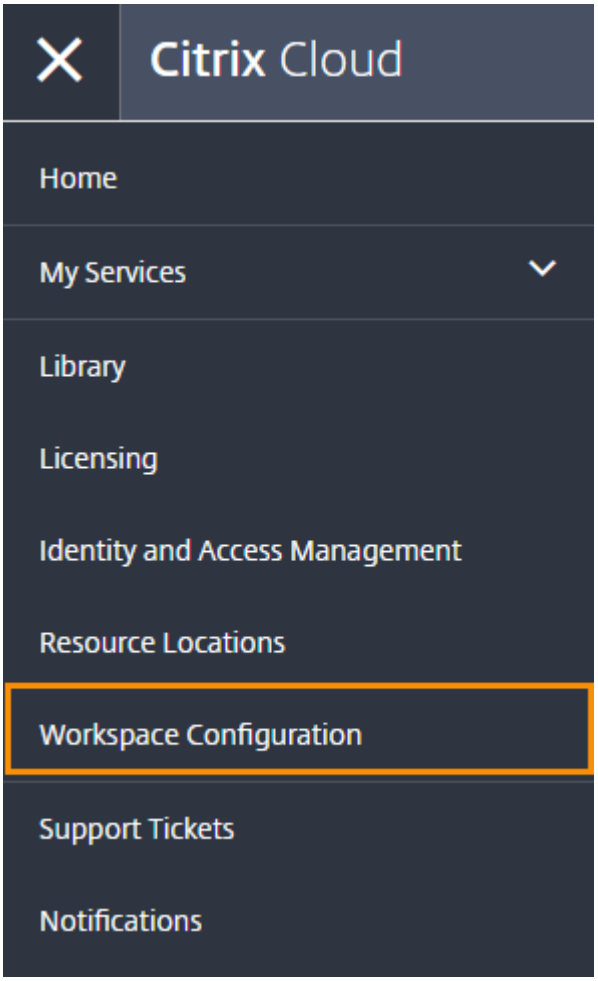
5. Dans la page **Se connecter à Active Directory**, cliquez sur **Détecter**. Après vérification, Citrix Cloud affiche un message indiquant que votre Active Directory est connecté.
6. Cliquez sur **Revenir à l'authentification**. L'entrée **Active Directory** est marquée **Activé** dans l'onglet **Authentification**.

Activer l'authentification Active Directory + jeton

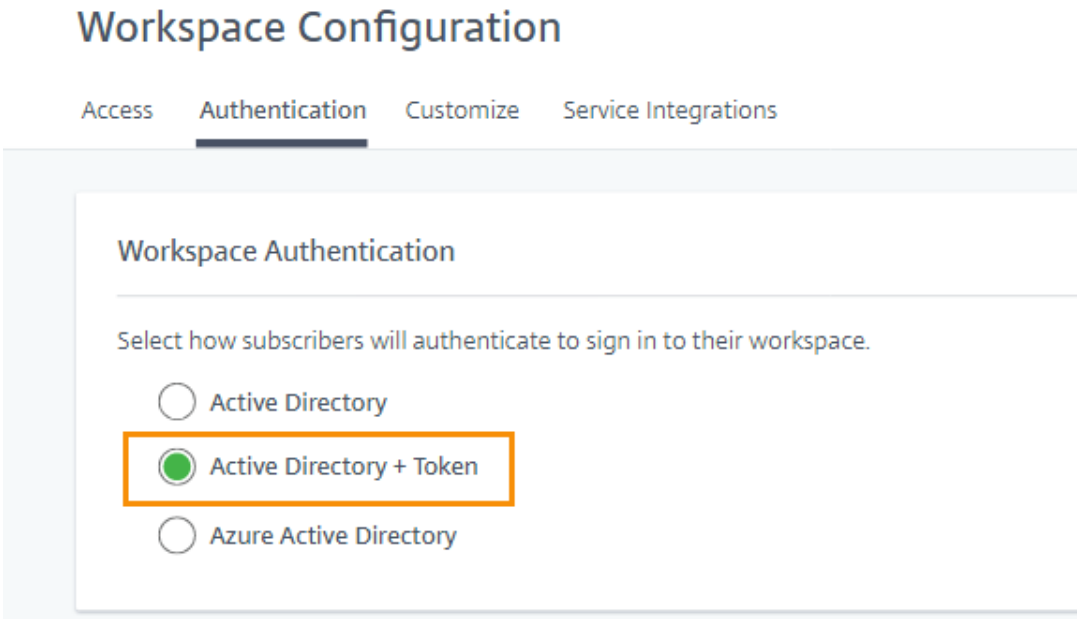
1. Effectuez les étapes 1 à 5 comme décrit à la section Connecter Azure Active Directory à Citrix Cloud.
2. Une fois que Citrix Cloud a vérifié la connexion avec Active Directory, cliquez sur **Suivant**. La page **Configurer un jeton** s'affiche et l'option **Appareil unique** est sélectionnée par défaut.



3. Cliquez sur **Enregistrer et terminer** pour terminer la configuration. Sous l'onglet **Authentification**, l'entrée **Active Directory + jeton** est marquée comme **Activé**.
4. Activer l'authentification par jeton pour les espaces de travail
   a) Dans le menu Citrix Cloud, sélectionnez **Configuration de l'espace de travail**.



b) Dans l'onglet **Authentification**, sélectionnez **Active Directory + jeton**.



Après avoir activé l'authentification Active Directory + jeton, les abonnés de l'espace de travail peu-

vent enregistrer leur appareil et utiliser une application d'authentification pour générer des jetons. Les abonnés ne peuvent enregistrer qu'un seul appareil à la fois. Pour obtenir des instructions sur l'enregistrement des appareils des abonnés, consultez Enregistrer les appareils pour l'authentification à deux facteurs.

Pour connaître les options permettant de réinscrire les appareils des abonnés, reportez-vous à la section Réinscrire des appareils.

Connecter Azure Active Directory à Citrix Cloud

July 21, 2021

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 la section Se reconnecter à Azure AD pour l'application mise à niveau dans cet article.

> **Conseil :**
>
> Apprenez-en plus sur les fournisseurs d'identité pris en charge avec le cours de formation Introduction to Citrix Identity and Authentication. Le module « Planning Citrix Identity and Access Management » comprend de courtes vidéos qui vous expliquent comment connecter ce fournisseur d'identité à Citrix Cloud et activer l'authentification pour Citrix Workspace.

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 n'avez pas de compte Azure, inscrivez-vous à partir de l'adresse 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 obtenir des instructions complètes, consultez la page Prise en main d'Azure AD Connect à l'aide de paramètres express 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. Recherchez Azure Active Directory et sélectionnez **Se connecter** dans le menu des points de suspension.
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 avez intégré Citrix Endpoint Management ou XenMobile Server avec Microsoft Intune, vous devez accorder des autorisations de lecture-écriture liées à Microsoft Intune. Pour de plus amples informations, consultez la section Accepter les invites d'autorisations déléguées.
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 la section Gérer les administrateurs 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 décrivant les 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 du service Azure AD, consultez la section https://azure.microsoft.com/fr-fr/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 mai 2019), 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 ajouter des groupes Azure AD à vos offres de bibliothèque, améliorer les performances de connexion et obtenir d'autres avantages, vous devez accorder à Citrix Cloud des autorisations supplémentaires via le rôle « Administrateur général » dans Azure AD. Pour ce faire, vous devez être un administrateur général dans 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.

> **Important :**
>
> Pour reconnecter votre compte Azure AD à Citrix Cloud, vous devez vous connecter à Citrix Cloud à l'aide d'un compte d'administrateur Citrix Cloud sous le fournisseur d'identité Citrix. Si vous

> êtes connecté à Citrix Cloud avec vos informations d'identification Azure AD, la reconnexion échouera. Si vous utilisez un compte d'administrateur Azure AD avec Citrix Cloud et que vous n'avez pas d'administrateur utilisant le fournisseur d'identité Citrix dans votre compte, vous pouvez en ajouter un temporairement pour effectuer cette reconnexion et le supprimer ultérieurement.

Pour effectuer la reconnexion, connectez-vous à Citrix Cloud avec vos informations d'identification d'administrateur Citrix Cloud. Lorsque vous êtes invité à vous reconnecter, vous pouvez vous connecter à Azure avec vos informations d'identification d'administrateur général.

Connecter une passerelle Citrix Gateway locale en tant que fournisseur d'identité à Citrix Cloud

July 21, 2021

Citrix Cloud prend en charge l'utilisation de Citrix Gateway local en tant que fournisseur d'identité pour authentifier les abonnés qui se connectent à leurs espaces de travail.

En utilisant l'authentification Citrix Gateway, vous pouvez :

- Continuer à authentifier les utilisateurs via votre Citrix Gateway existant afin qu'ils puissent accéder aux ressources de votre déploiement local d'applications et de bureaux virtuels via Citrix Workspace.
- Utilisez les fonctions d'authentification, d'autorisation et d'audit (AAA) de Citrix Gateway avec Citrix Workspace.
- Utilisez des fonctions telles que l'authentification unique, les cartes à puce, les jetons sécurisés, les stratégies d'accès conditionnel, la fédération et bien d'autres, tout en fournissant à vos utilisateurs l'accès aux ressources dont ils ont besoin via Citrix Workspace.

> **Conseil :**
>
> Apprenez-en plus sur les fournisseurs d'identité pris en charge avec le cours de formation Introduction to Citrix Identity and Authentication. Le module « Planning Citrix Identity and Access Management » comprend de courtes vidéos qui vous expliquent comment connecter ce fournisseur d'identité à Citrix Cloud et activer l'authentification pour Citrix Workspace.

Versions prises en charge

L'authentification Citrix Gateway est prise en charge pour une utilisation avec les versions de produit locales suivantes :

- Citrix Gateway 12.1 54.13 Édition Advanced ou ultérieure

- Citrix Gateway 13.0 41.20 Édition Advanced ou ultérieure

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 :

- Les serveurs doivent répondre à la configuration système décrite dans la section 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 plus d'informations, consultez Configuration requise pour le système et la connectivité.
- 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 plus d'informations sur l'installation du Cloud Connector, consultez la section Installation de Cloud Connector.

Active Directory

Avant d'activer l'authentification Citrix Gateway, effectuez les tâches suivantes :

- Vérifiez que vos abonnés à un espace de travail disposent de comptes d'utilisateur dans Active Directory (AD). Les abonnés sans compte AD ne peuvent pas se connecter à leur espace de travail.
- Assurez-vous que les propriétés utilisateur des comptes AD de vos abonnés sont renseignées. Citrix Cloud utilise ces propriétés pour établir le contexte utilisateur lorsque les abonnés se connectent. Si ces propriétés ne sont pas renseignées, les abonnés ne peuvent pas se connecter à leur espace de travail. Ces propriétés comprennent :
  - Adresse e-mail
  - Nom d'affichage
  - Nom commun
  - Nom du compte SAM

  - Nom d'utilisateur principal
  - OID
  - SID
- Connectez votre Active Directory (AD) à votre compte Citrix Cloud. Dans cette tâche, vous installez le logiciel Cloud Connector sur les serveurs que vous avez préparés, comme décrit dans la section Cloud Connector. Les Cloud Connector permettent à Citrix Cloud de communiquer avec votre environnement local. Pour obtenir des instructions, veuillez consulter la section Connecter Active Directory à Citrix Cloud.
- Si vous configurez une fédération avec l'authentification Citrix Gateway, synchronisez vos utilisateurs AD avec le fournisseur de fédération. Citrix Cloud a besoin des attributs d'utilisateur AD pour vos abonnés à un espace de travail afin qu'ils puissent se connecter correctement.

Exigences

Stratégies avancées Citrix Gateway

L'authentification Citrix Gateway nécessite l'utilisation de stratégies avancées sur l'instance Gateway locale en raison de la mise hors service des stratégies classiques. Les stratégies avancées prennent en charge l'authentification multifacteur pour Citrix Cloud, y compris des options telles que le chaînage des fournisseurs d'identité. Si vous utilisez actuellement des stratégies classiques, vous devez créer de nouvelles stratégies avancées pour utiliser l'authentification Citrix Gateway dans Citrix Cloud. Vous pouvez réutiliser la partie Action de la stratégie classique lorsque vous créez la stratégie avancée.

Certificats de signature

Lors de la configuration de Gateway pour l'authentification des abonnés à Citrix Workspace, Gateway agit en tant que fournisseur OpenID Connect. Les messages entre Citrix Cloud et Gateway sont conformes au protocole OIDC, qui inclut la signature numérique de jetons. Par conséquent, vous devez configurer un certificat pour signer ces jetons. Ce certificat doit être délivré par une autorité de certification publique. L'utilisation d'un certificat émis par une autorité de certification privée n'est pas prise en charge car il n'existe aucun moyen de fournir à Citrix Cloud le certificat d'autorité de certification racine privée. Ainsi, la chaîne de certificat de confiance ne peut pas être établie. Si vous configurez plusieurs certificats pour la signature, une rotation des clés est effectuée pour chaque message.

Les clés doivent être liées à **vpn global**. Sans ces clés, les abonnés ne peuvent pas accéder à leur espace de travail après s'être connectés.

Synchronisation de l'horloge

Étant donné que les messages signés numériquement dans OIDC portent un horodatage, Gateway doit être synchronisé avec l'heure NTP. Si l'horloge n'est pas synchronisée, Citrix Cloud suppose que

les jetons sont périmés lors de la vérification de leur validité.

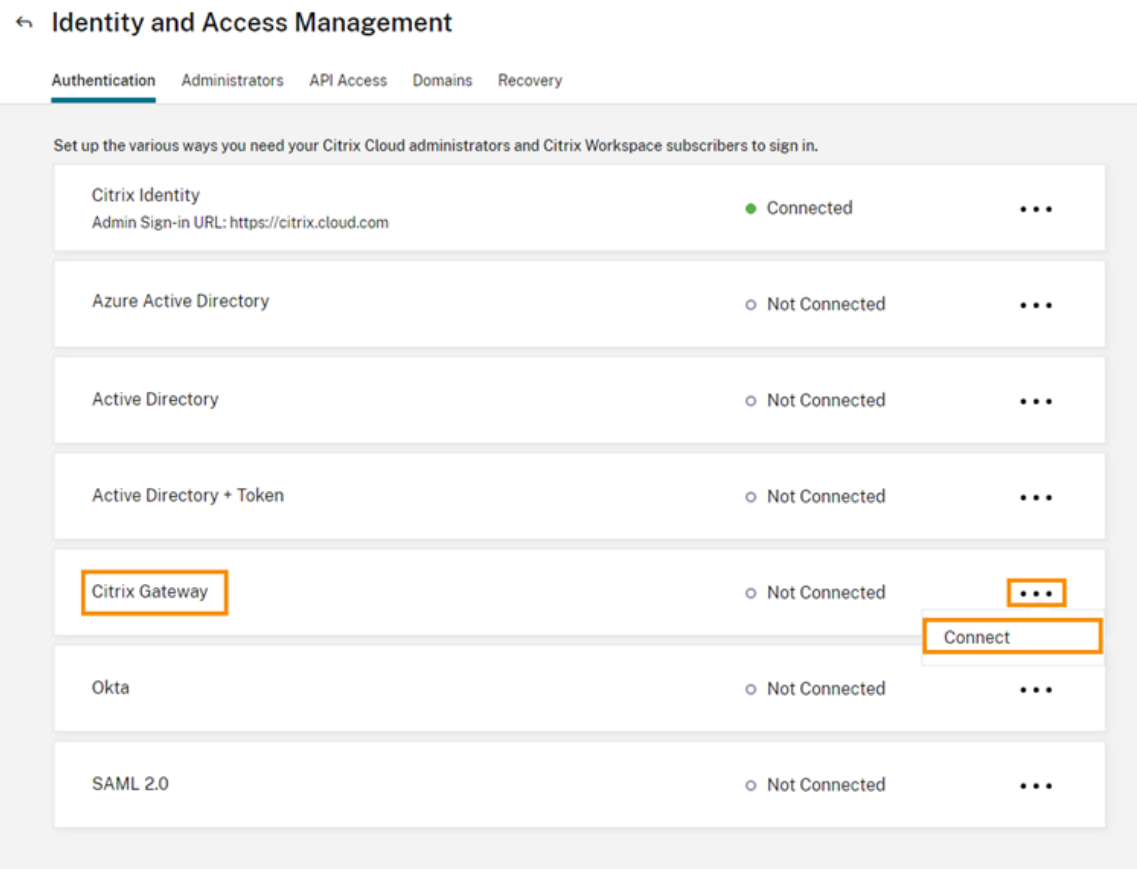
Vue d'ensemble des tâches

Pour configurer l'authentification Citrix Gateway, vous effectuez les tâches suivantes :

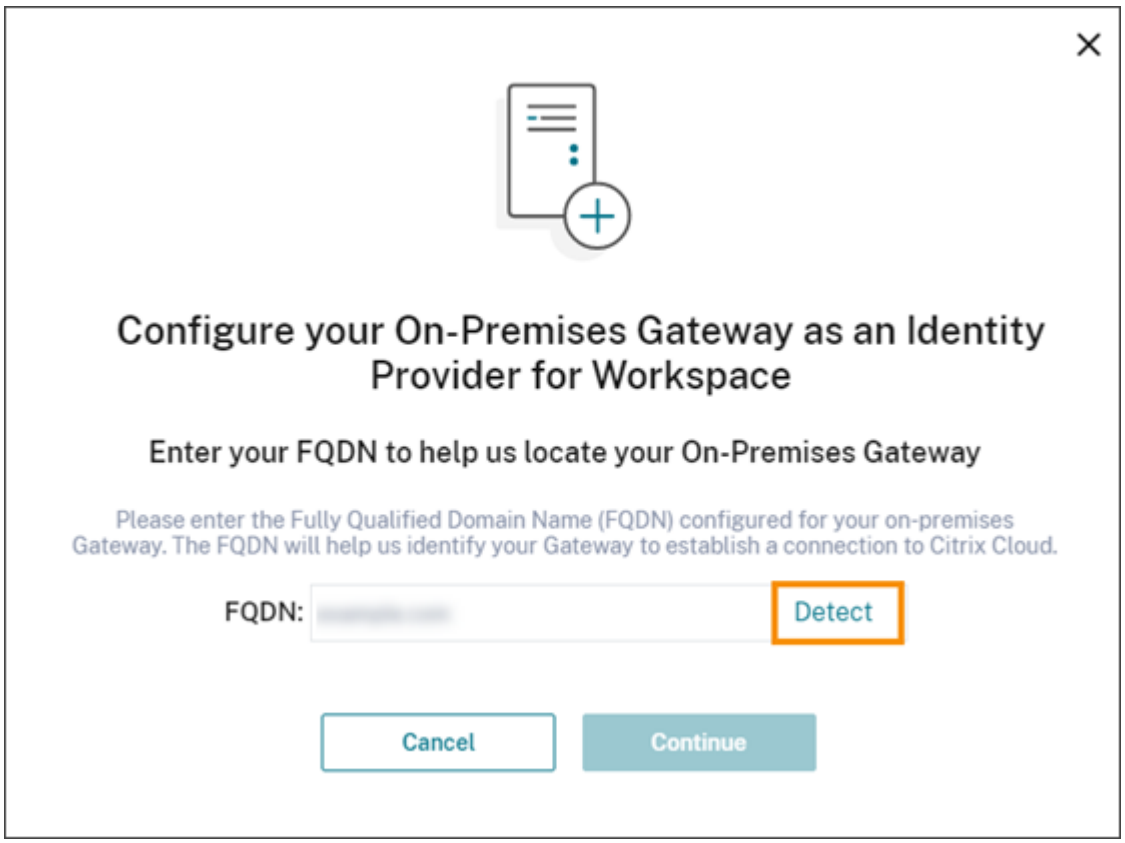
1. Dans **Gestion des identités et des accès**, commencez à configurer la connexion à votre passerelle. Au cours de cette étape, vous générez l'ID client, le secret et l'URL de redirection pour Gateway.
2. Sur Gateway, créez une stratégie avancée de fournisseur d'identité OAuth à l'aide des informations générées à partir de Citrix Cloud. Cela permet à Citrix Cloud de se connecter à votre passerelle Gateway locale. Pour de plus amples informations, consultez les articles suivants :
   - Citrix Gateway 12.1 : Utiliser une passerelle Citrix Gateway locale en tant que fournisseur d'identité pour Citrix Cloud
   - Citrix Gateway 13.0 : Utiliser une passerelle Citrix Gateway locale en tant que fournisseur d'identité pour Citrix Cloud
3. Dans**Configuration de l'espace de travail**, activez l'authentification Citrix Gateway pour les abonnés.

Pour activer l'authentification Citrix Gateway pour les abonnés de l'espace de travail

1. Dans le menu Citrix Cloud, sélectionnez **Gestion des identités et des accès**.
2. Dans l'onglet **Authentification**, dans **Citrix Gateway**, cliquez sur le menu des points de suspension et sélectionnez **Connecter**.

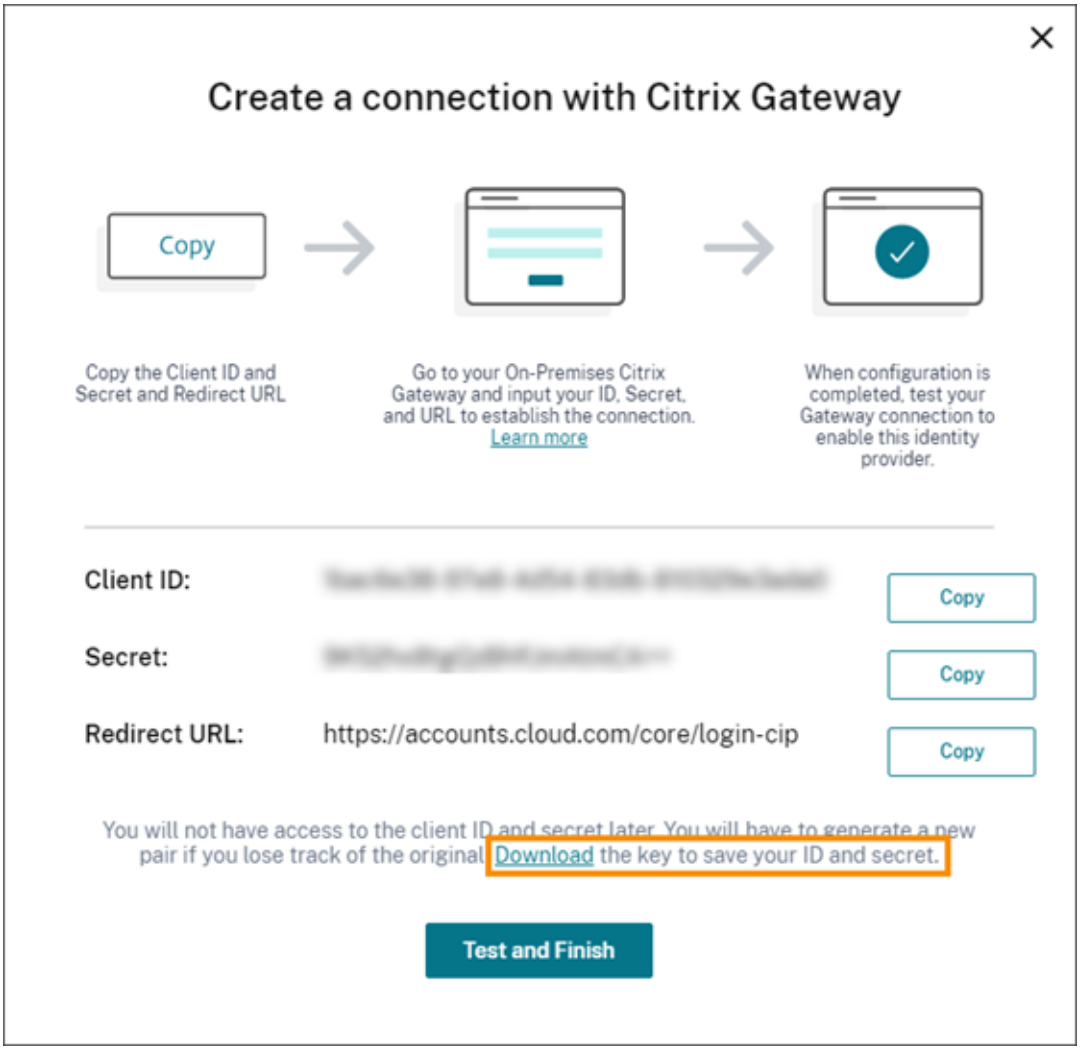


3. Entrez le nom de domaine complet de votre passerelle Gateway locale et cliquez sur **Détecter**.



Une fois que Citrix Cloud l'a détecté correctement, cliquez sur **Continuer**.

4. Créez une connexion avec votre passerelle Gateway locale :
   a) Copiez l'ID client, Secret et URL de redirection affichées par Citrix Cloud.



Téléchargez aussi une copie de ces informations et enregistrez-les en toute sécurité hors ligne pour votre référence. Ces informations ne sont pas disponibles dans Citrix Cloud une fois générées.

b) Sur Gateway, créez une stratégie avancée de fournisseur d'identité OAuth à l'aide de l'ID client, du secret et de l'URL de redirection provenant de Citrix Cloud. Pour de plus amples informations, consultez les articles suivants :
   - Pour Citrix Gateway 12.1 :Utiliser une passerelle Citrix Gateway locale en tant que fournisseur d'identité pour Citrix Cloud
   - Pour Citrix Gateway 13.0 :Utiliser une passerelle Citrix Gateway locale en tant que fournisseur d'identité pour Citrix Cloud

c) Cliquez sur **Tester et terminer**. Citrix Cloud vérifie que votre passerelle Gateway est accessible et configurée correctement.

5. Activez l'authentification Citrix Gateway pour les espaces de travail :
   a) Dans le menu Citrix Cloud, sélectionnez **Configuration de l'espace de travail**.
   b) Dans l'onglet **Authentification**, sélectionnez **Citrix Gateway**.

c) Sélectionnez **Je comprends l'impact sur l'expérience de l'abonné**, puis cliquez sur **Enregistrer**.

Résolution des problèmes

Dans un premier temps, passez en revue les sections Conditions préalables et Exigences de cet article. Vérifiez que vous disposez de tous les composants requis dans votre environnement local et que vous avez effectué toutes les configurations requises. Si l'un de ces composants est manquant ou mal configuré, l'authentification de l'espace de travail avec Citrix Gateway ne fonctionne pas.

Si vous rencontrez un problème lors de l'établissement d'une connexion entre Citrix Cloud et votre passerelle Gateway locale, vérifiez les éléments suivants :

- Le nom de domaine complet de Gateway est accessible depuis Internet.
- Vous avez entré correctement le nom de domaine complet de la passerelle dans Citrix Cloud.
- Vous avez entré correctement l'URL de passerelle dans le paramètre `-issuer` de la stratégie OAuth IDP. Exemple : `-issuer https://GatewayFQDN.com`
- Les valeurs d'ID client, de secret et d'URL de redirection provenant de Citrix Cloud sont saisies correctement dans les champs ID client, Clé secrète client, Redirection URL et Audience de la stratégie de fournisseur d'identité OAuth. Vérifiez que l'ID client correct a été saisi dans le champ Audience de la stratégie.
- La stratégie d'authentification de fournisseur d'identité OAuth est configurée correctement. Pour de plus amples informations, consultez les articles suivants :
  - Citrix Gateway 12.1 : Utiliser une passerelle Citrix Gateway locale en tant que fournisseur d'identité pour Citrix Cloud
  - Citrix Gateway 13.0 : Utiliser une passerelle Citrix Gateway locale en tant que fournisseur d'identité pour Citrix Cloud
- Vérifiez que la stratégie est liée correctement au serveur d'authentification AAA, comme décrit à la section Liaison des stratégies d'authentification.

Serveurs de catalogues globaux

En plus de récupérer les détails des comptes d'utilisateur, Gateway récupère le nom de domaine des utilisateurs, le nom AD NETBIOS et le nom de domaine AD racine. Pour récupérer le nom AD NETBIOS, Gateway recherche l'AD dans lequel résident les comptes d'utilisateur. Les noms NETBIOS ne sont pas répliqués sur les serveurs de catalogues globaux.

Si vous utilisez des serveurs de catalogues globaux dans votre environnement AD, les actions LDAP configurées sur ces serveurs ne fonctionnent pas avec Citrix Cloud. Vous devez configurer les AD individuels dans l'action LDAP. Si vous avez plusieurs domaines ou forêts, vous pouvez configurer plusieurs stratégies LDAP.

Recherche AD pour l'authentification unique avec Kerberos ou le chaînage de fournisseurs d'identité

Si vous utilisez Kerberos ou un fournisseur d'identité externe qui utilise les protocoles SAML ou OIDC pour la connexion des abonnés, vérifiez que la recherche AD est configurée. Gateway utilise des recherches AD pour récupérer les propriétés des utilisateurs AD et les propriétés de configuration AD des abonnés.

Assurez-vous que des stratégies LDAP sont configurées, même si l'authentification est gérée par des serveurs tiers. Pour configurer ces stratégies, vous ajoutez un second facteur d'authentification à votre profil de schéma de connexion existant en effectuant les tâches suivantes :

1. Créez un serveur d'authentification LDAP qui effectue uniquement l'extraction d'attributs et de groupes à partir d'Active Directory.
2. Créez une stratégie d'authentification avancée LDAP.
3. Créez une étiquette de stratégie d'authentification.
4. Définissez l'étiquette de stratégie d'authentification comme facteur suivant, après le fournisseur d'identité principal.

Ajouter LDAP en tant que second facteur d'authentification

1. Créez le serveur d'authentification LDAP :
   a) Sélectionnez **System > Authentication > Basic Policies > LDAP > Servers > Add**.
   b) Sur la page **Create Authentication LDAP Server**, entrez les informations suivantes :
      - Sous **Choose Server Type**, sélectionnez **LDAP**.
      - Sous **Name**, entrez un nom convivial pour le serveur.
      - Sélectionnez **Server IP**, puis entrez l'adresse IP du serveur LDAP.
      - Sous **Security Type**, sélectionnez le type de sécurité LDAP requis.
      - Sous **Server Type**, sélectionnez **AD**.
      - Dans **Authentification**, ne cochez pas la case. Cette case doit être désactivée car ce serveur d'authentification sert uniquement à extraire les attributs et les groupes utilisateur à partir d'Active Directory, et non à l'authentification.
   c) Sous **Other Settings**, entrez les informations suivantes :
      - Sous **Server Logon Name Attribute**, saisissez **UserPrincipalName**.
      - Sous **Group Attribute**, sélectionnez **memberOf**.
      - Sous **Sub Attribute Name**, sélectionnez **cn**.
2. Créez la stratégie d'authentification avancée LDAP :
   a) Sélectionnez **Security > AAA - Application Traffic > Policies > Authentication > Advanced Policies > Policy > Add**.
   b) Sur la page **Create Authentication Policy**, entrez les informations suivantes :
      - Sous **Name**, entrez un nom convivial pour la stratégie.
      - Sous **Action Type**, sélectionnez **LDAP**.

- Sous **Action**, sélectionnez le serveur d'authentification LDAP que vous avez créé précédemment.
- Sous **Expression**, saisissez **TRUE**.

c) Cliquez sur **Create** pour enregistrer la configuration.

3. Créez l'étiquette de stratégie d'authentification :
   a) Sélectionnez **Security > AAA – Application Traffic > Policies > Authentication > Advanced Policies > Policy Label > Add**.
   b) Sous **Name**, entrez un nom convivial pour l'étiquette de stratégie d'authentification.
   c) Sous Login Schema, sélectionnez **LSCHEMA_INT**.
   d) Sous **Policy Binding** > **Select Policy**, sélectionnez la stratégie d'authentification avancée LDAP que vous avez créée précédemment.
   e) Sous **GoTo Expression**, sélectionnez **END**.
   f) Cliquez sur **Bind** pour terminer la configuration.
4. Définissez l'étiquette de stratégie d'authentification LDAP comme facteur suivant, après le fournisseur d'identité principal :
   a) Sélectionnez **System > Security > AAA - Application Traffic > Virtual Servers**.
   b) Sélectionnez le serveur virtuel qui contient la liaison pour votre fournisseur d'identité principal et sélectionnez **Edit**.
   c) Sous **Advanced Authentication Policies**, sélectionnez les liaisons de stratégie d'authentification existantes (**Authentication Policy**).
   d) Sélectionnez la liaison pour votre fournisseur d'identité principal, puis sélectionnez **Edit Binding**.
   e) Sur la page **Policy Binding** > **Select Next Factor**, sélectionnez l'étiquette de stratégie d'authentification LDAP que vous avez créée précédemment.
   f) Cliquez sur **Bind** pour enregistrer la configuration.

Mot de passe par défaut pour l'authentification multifacteur

Si vous utilisez l'authentification multifacteur pour les abonnés d'espace de travail, Gateway utilise le mot de passe du dernier facteur comme mot de passe par défaut pour l'authentification unique. Ce mot de passe est envoyé à Citrix Cloud lorsque les abonnés se connectent à leur espace de travail. Si l'authentification LDAP est suivie d'un autre facteur dans votre environnement, vous devez configurer le mot de passe LDAP comme mot de passe par défaut envoyé à Citrix Cloud. Activez **SSOCredentials** sur le schéma de connexion correspondant au facteur LDAP.

Connecter Okta en tant que fournisseur d'identité à Citrix Cloud

July 21, 2021

Citrix Cloud prend en charge l'utilisation de Okta en tant que fournisseur d'identité pour authentifier les abonnés qui se connectent à leurs espaces de travail. En connectant votre organisation Okta à Citrix Cloud, vous pouvez offrir à vos abonnés une expérience de connexion commune pour l'accès aux ressources dans Citrix Workspace.

Après avoir activé l'authentification Okta dans Configuration de l'espace de travail, les abonnés ont une expérience de connexion différente. La sélection de l'authentification Okta fournit une connexion fédérée, et non une authentification unique. Les abonnés se connectent aux espaces de travail à partir d'une page de connexion Okta, 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. Pour activer l'authentification unique et empêcher une deuxième invite d'ouverture de session, vous devez utiliser le Service d'authentification fédérée Citrix avec Citrix Cloud. Pour plus d'informations, consultez Connecter le Service d'authentification fédérée Citrix à Citrix Cloud.

> **Conseil :**
>
> Apprenez-en plus sur les fournisseurs d'identité pris en charge avec le cours de formation Introduction to Citrix Identity and Authentication. Le module « Planning Citrix Identity and Access Management » comprend de courtes vidéos qui vous expliquent comment connecter ce fournisseur d'identité à Citrix Cloud et activer l'authentification pour Citrix Workspace.

Conditions préalables

Cloud Connector

Vous devez disposer d'au moins deux (2) serveurs dans votre domaine Active Directory sur lesquels installer le logiciel Citrix Cloud Connector. Les Cloud Connector sont requis pour établir la communication entre Citrix Cloud et votre emplacement de ressources. Citrix recommande deux serveurs pour garantir la haute disponibilité de Cloud Connector. Ces serveurs doivent satisfaire aux exigences suivantes :

- Répondre à la configuration décrite dans la section 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.
- Appartenir à votre domaine Active Directory (AD). Si vos ressources et vos utilisateurs d'espace de travail résident dans plusieurs domaines, vous devez installer au moins deux Cloud Connector dans chaque domaine. Pour plus d'informations, consultez Scénarios de déploiement de Cloud Connector dans Active Directory.
- Être connectés à un réseau pouvant contacter les ressources auxquelles les utilisateurs accèdent via Citrix Workspace.
- Être connectés à Internet. Pour plus d'informations, consultez Configuration requise pour le système et la connectivité.

Pour plus d'informations sur l'installation des composants Cloud Connector, consultez la section Installation de Cloud Connector.

Domaine Okta

Lorsque vous connectez Okta à Citrix Cloud, vous devez fournir le domaine Okta pour votre organisation. Citrix prend en charge les domaines Okta suivants :

- okta.com
- okta-eu.com
- oktapreview.com

Vous pouvez également utiliser des domaines personnalisés Okta avec Citrix Cloud. Passez en revue les points importants à prendre en compte pour l'utilisation de domaines personnalisés dans Personnaliser le domaine URL Okta sur le site Web Okta.

Pour savoir comment trouver le domaine personnalisé de votre organisation, reportez-vous à Trouver votre domaine Okta sur le site Web Okta.

Application Web Okta OIDC

Pour utiliser Okta comme fournisseur d'identité, vous devez d'abord créer une application Web Okta OIDC avec des informations d'identification client que vous pouvez utiliser avec Citrix Cloud. Après avoir créé et configuré l'application, notez l'ID client et le secret client. Vous fournissez ces valeurs à Citrix Cloud lorsque vous connectez votre organisation Okta.

Pour créer et configurer cette application, consultez les sections suivantes de cet article :

- Créer une application Web Okta OIDC
- Configurer l'application Web Okta OIDC

URL Workspace

Lors de la création de l'application Okta, vous devez fournir l'URL de votre espace de travail à partir de Citrix Cloud. Pour obtenir l'URL de l'espace de travail, sélectionnez **Configuration de l'espace de travail** dans le menu Citrix Cloud. L'URL de l'espace de travail est affichée dans l'onglet **Accès**.

> **Important :**
>
> Si vous modifiez l'URL de l'espace de travail plus tard, vous devez mettre à jour la configuration de l'application Okta avec la nouvelle URL. Sinon, vos abonnés peuvent rencontrer des problèmes lors de la déconnexion de leur espace de travail.

Jeton API Okta

L'utilisation d'Okta comme fournisseur d'identité avec Citrix Cloud nécessite un jeton API pour votre organisation Okta. Créez ce jeton à l'aide d'un compte Administrateur en lecture seule dans votre organisation Okta. Ce jeton doit pouvoir lire les utilisateurs et les groupes de votre organisation Okta.

Pour créer le jeton API, reportez-vous à Créer un jeton API Okta dans cet article. Pour plus d'informations sur les jetons API, voir Créer un jeton API sur le site Web Okta.

> **Important :**
>
> Lorsque vous créez le jeton API, notez la valeur du jeton (par exemple, copiez temporairement la valeur dans un document en texte brut). Okta n'affiche cette valeur qu'une seule fois, vous pouvez donc créer le jeton juste avant d'effectuer les étapes décrites dans Connecter Citrix Cloud à votre organisation Okta.

Synchroniser les comptes avec l'agent Okta AD

Pour utiliser Okta comme fournisseur d'identité, vous devez d'abord intégrer votre AD local à Okta. Pour ce faire, vous installez l'agent Okta AD dans votre domaine et ajoutez votre AD à votre organisation Okta. Pour obtenir des conseils sur le déploiement de l'agent Okta AD, reportez-vous à Démarrer avec l'intégration d'Active Directory sur le site Web Okta. Vous importez ensuite vos utilisateurs et groupes AD dans Okta. Lors de l'importation, incluez les valeurs SID, UPN et OID associées à vos comptes AD.

> Remarque :
>
> Si vous utilisez le service Citrix Gateway avec Workspace, vous n'avez pas besoin de synchroniser vos comptes AD avec votre organisation Okta.

Pour synchroniser vos utilisateurs et groupes AD avec votre organisation Okta :

1. Installez et configurez l'agent Okta AD. Pour obtenir des instructions complètes, consultez les articles suivants sur le site Web Okta :
   - Installer l'agent Okta Active Directory
   - Configurer les paramètres d'importation et de compte Active Directory
   - Configurer les paramètres de provisioning Active Directory
2. Ajoutez vos utilisateurs et groupes AD à Okta en effectuant une importation manuelle ou une importation automatisée. Pour plus d'informations sur les méthodes d'importation Okta et des instructions, consultez la section Gérer les utilisateurs et les groupes Active Directory sur le site Web Okta.

Créer une application Web Okta OIDC

1. Dans la console de gestion Okta, sous **Applications**, sélectionnez **Applications**.

2. Cliquez sur **Add Application**, puis sur **Create New App**.
3. Dans **Sign in method**, sélectionnez **OpenID Connect**, puis cliquez sur **Create**. La valeur par défaut de la **plate-forme** (**Web**) ne change pas.
4. Entrez le nom de l'application.
5. Dans **Login redirect URIs**, entrez `https://accounts.cloud.com/core/login-okta`.
6. Dans **Logout redirect URIs**, entrez l'URL de votre espace de travail à partir de Citrix Cloud.
7. Cliquez sur **Enregistrer**.

Configurer l'application Web Okta OIDC

Dans cette étape, vous configurez votre application Web Okta OIDC avec les paramètres requis pour Citrix Cloud. Citrix Cloud requiert ces paramètres pour authentifier vos abonnés via Okta lorsqu'ils se connectent à leurs espaces de travail.

1. Dans la page de configuration de l'application Okta, dans **General Settings**, cliquez sur **Edit**.
2. Dans **Allowed grant types**, sélectionnez les options suivantes :
   - Authorization Code
   - Refresh Token
   - Implicit (Hybrid)
   - Allow ID Token with implicit grant type
   - Allow Access Token with implicit grant type
3. Cliquez sur **Enregistrer**.
4. Accordez un accès groupe ou utilisateur à l'application :
   a) Dans l'onglet **Assignments**, sélectionnez **Assign**, puis sélectionnez **Assign to People** ou **Assign to Groups**.
   b) Sélectionnez les utilisateurs ou les groupes auxquels vous souhaitez donnez accès aux espaces de travail. Pour autoriser l'accès à tous les utilisateurs, sélectionnez **Assign to Groups**, puis **Everyone**.
5. Cliquez sur **Terminé**.
6. Ajoutez des attributs d'application. Les attributs sont sensibles à la casse.
   a) Dans le menu de la console Okta, sélectionnez **Directory > Profile Editor**.
   b) Recherchez le profil **user** Okta et sélectionnez **Profile**. Sous **Attributes**, sélectionnez **Add attribute**.
   c) Entrez les informations suivantes :
      - Nom complet : cip_sid
      - Nom de la variable : cip_sid
      - Description : Identificateur de sécurité de l'utilisateur AD
      - Longueur de l'attribut : supérieure à 1
      - Attribut requis : Oui
   d) Cliquez sur **Save and Add Another**.

e) Entrez les informations suivantes :
   - Nom complet : cip_upn
   - Nom de la variable : cip_upn
   - Description : Nom principal de l'utilisateur AD
   - Longueur de l'attribut : supérieure à 1
   - Attribut requis : Oui

f) Cliquez sur **Save and Add Another**.

g) Entrez les informations suivantes :
   - Nom complet : cip_oid
   - Nom de la variable : cip_oid
   - Description : GUID utilisateur AD
   - Longueur de l'attribut : supérieure à 1
   - Attribut requis : Oui

h) Cliquez sur **Enregistrer**.

7. Modifiez les mappages d'attributs pour l'application :
   a) Dans la console Okta, sélectionnez **Directory > Directory Integrations**.
   b) Sélectionnez l'AD que vous avez précédemment intégré. Pour de plus amples informations, consultez Synchroniser les comptes avec l'agent Okta AD
   c) Sous l'onglet **Settings**, sélectionnez **Edit Mappings**.
   d) Mappez les attributs suivants :
      - Sélectionnez `appuser.objectSid` et mappez avec l'attribut `cip_sid`.
      - Sélectionnez `appuser.userName` et mappez avec l'attribut `cip_upn`.
      - Sélectionnez `appuser.externalId` et mappez avec l'attribut `cip_oid`.
   e) Cliquez sur **Save Mappings**.
   f) Cliquez sur **Apply updates now**.

Créer un jeton API Okta

1. Connectez-vous à la console Okta à l'aide d'un compte Administrateur en lecture seule.
2. Dans le menu de la console Okta, sélectionnez **Security > API**.
3. Sélectionnez l'onglet **Tokens**, puis sélectionnez **Create Token**.
4. Entrez un nom pour le jeton.
5. Cliquez sur **Create Token**.
6. Copiez la valeur du jeton. Vous fournissez cette valeur lorsque vous connectez votre organisation Okta à Citrix Cloud.

Connecter Citrix Cloud à votre organisation Okta

1. Connectez-vous à Citrix Cloud sur https://citrix.cloud.com.
2. Dans le menu Citrix Cloud, sélectionnez **Gestion des identités et des accès**.

3. Localisez **Okta** et sélectionnez **Connecter** dans le menu des points de suspension.
4. Dans **URL Okta**, entrez votre domaine Okta.
5. Dans **Jeton API Okta**, entrez le jeton API de votre organisation Okta.
6. Dans **ID du client** et **Clé secrète client**, entrez les informations d'identification de votre application Okta. Pour copier ces valeurs à partir de la console Okta, sélectionnez **Applications** et recherchez votre application Okta. Sous **Informations d'identification du client**, utilisez le bouton **Copier dans le presse-papiers** pour chaque valeur.
7. Cliquez sur **Tester et terminer**. Citrix Cloud vérifie vos détails Okta et teste la connexion.

Activer l'authentification Okta pour les espaces de travail

1. Dans le menu Citrix Cloud, sélectionnez **Configuration de l'espace de travail > Authentification**.
2. Sélectionnez **Okta**. Lorsque vous y êtes invité, sélectionnez **Je comprends l'impact sur l'expérience des abonnés**.
3. Cliquez sur **Accepter** pour accepter la demande d'autorisations.

Connecter SAML en tant que fournisseur d'identité à Citrix Cloud (Technical Preview)

July 21, 2021

Citrix Cloud prend en charge l'utilisation de SAML (Security Assertion Markup Language) en tant que fournisseur d'identité pour authentifier les abonnés qui se connectent à leurs espaces de travail. Vous pouvez utiliser le fournisseur SAML de votre choix avec votre répertoire Active Directory (AD) local, à condition qu'il prenne en charge SAML 2.0.

> **Remarques :**
>
> - Cette fonctionnalité est actuellement disponible dans la version Technical Preview. Citrix recommande d'utiliser les fonctionnalités Technical Preview uniquement dans les environnements de test.
> - Cet article décrit la configuration de SAML 2.0 dans Citrix Cloud avec Active Directory uniquement. Si vous envisagez d'utiliser l'authentification unique (SSO) avec SAML 2.0, consultez Comment intégrer Azure AD avec SAML 2.0 Tech Preview (CTX312150).

Conditions préalables

L'utilisation de l'authentification SAML avec Citrix Cloud exige les conditions suivantes :

- Fournisseur SAML prenant en charge SAML 2.0
- Domaine Active Directory local
- Deux Cloud Connector déployés sur un emplacement de ressources et associés à votre domaine AD local. Les Cloud Connector sont utilisés pour garantir que Citrix Cloud peut communiquer avec votre emplacement de ressources.
- Intégration AD avec votre fournisseur SAML

Cloud Connector

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

- Les serveurs doivent répondre à la configuration système décrite dans la section 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.
- Les serveurs doivent être associés au domaine sur lequel résident vos ressources. Si les utilisateurs accèdent aux ressources dans plusieurs domaines, vous devez installer au moins deux Cloud Connector dans chaque domaine.
- Les serveurs doivent être connectés à un réseau pouvant contacter les ressources auxquelles les utilisateurs accèdent via Citrix Workspace.
- Être connectés à Internet. Pour de plus amples informations, consultez Configuration requise pour le système et la connectivité.

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

Active Directory

Avant de configurer l'authentification SAML, effectuez les tâches suivantes :

- Vérifiez que vos abonnés à un espace de travail disposent de comptes d'utilisateur dans Active Directory (AD). Les abonnés sans compte AD ne peuvent pas se connecter à leurs espaces de travail lorsque l'authentification SAML est configurée.
- Assurez-vous que les propriétés utilisateur des comptes AD de vos abonnés sont renseignées. Citrix Cloud utilise ces propriétés pour établir le contexte utilisateur lorsque les abonnés se connectent à Citrix Workspace. Si ces propriétés ne sont pas renseignées, les abonnés ne peuvent pas se connecter. Ces propriétés comprennent :
  - Adresse e-mail
  - Nom d'affichage (facultatif)

  - Nom commun
  - Nom du compte SAM
  - Nom d'utilisateur principal
  - GUID d'objet
  - SID
- Connectez votre répertoire Active Directory (AD) à votre compte Citrix Cloud en déployant Cloud Connector dans votre répertoire AD local.
- Synchronisez vos utilisateurs AD avec le fournisseur SAML. Citrix Cloud a besoin des attributs d'utilisateur AD pour vos abonnés à un espace de travail afin qu'ils puissent se connecter correctement.

Intégration SAML avec Active Directory

Avant d'activer l'authentification SAML, vous devez intégrer votre répertoire AD local à votre fournisseur SAML. Cette intégration permet au fournisseur SAML de transmettre les attributs utilisateur AD requis suivants à Citrix Cloud dans l'assertion SAML :

- SecurityIDentifier (SID)
- objectGUID (OID)
- userPrincipalName (UPN)
- Mail (adresse e-mail)

Bien que les étapes d'intégration spécifiques varient d'un fournisseur SAML à l'autre, le processus d'intégration comprend généralement les tâches suivantes :

1. Installez un agent de synchronisation dans votre domaine AD pour établir une connexion entre votre domaine et votre fournisseur SAML.
2. Si vous ne disposez pas déjà d'attributs personnalisés mappés sur les attributs utilisateur AD décrits ci-dessus, créez les attributs personnalisés et mappez-les à AD. À titre de référence, les étapes générales de cette tâche sont décrites à la section Créer et mapper des attributs SAML personnalisés de cet article.
3. Synchronisez vos utilisateurs AD avec votre fournisseur SAML.

> **Remarque :**
>
> Si vous avez déjà créé des attributs personnalisés qui correspondent aux attributs utilisateur AD requis répertoriés précédemment dans cette section, vous n'avez pas besoin de créer et de mapper d'autres attributs personnalisés. Utilisez plutôt vos attributs personnalisés existants lorsque vous configurez les métadonnées de votre fournisseur SAML dans Citrix Cloud.

Pour plus d'informations sur l'intégration de votre répertoire AD avec votre fournisseur SAML, consultez la documentation produit de votre fournisseur SAML.

Vue d'ensemble des tâches

Pour configurer l'authentification SAML pour les abonnés de l'espace de travail, effectuez les tâches suivantes :

1. Dans **Gestion des identités et des accès**, connectez votre répertoire AD local à Citrix Cloud comme décrit à la section Connecter Active Directory à Citrix Cloud.
2. Intégrez votre fournisseur SAML à votre répertoire AD local comme décrit à la section Intégration SAML avec Active Directory de cet article.
3. Dans **Gestion des identités et des accès**, configurez l'authentification SAML dans Citrix Cloud. Cette tâche consiste à configurer les métadonnées SAML de Citrix Cloud dans votre fournisseur SAML, puis à configurer les métadonnées de votre fournisseur SAML dans Citrix Cloud pour créer la connexion SAML.
4. Dans **Configuration de l'espace de travail**, sélectionnez la méthode d'authentification SAML.

Créer et mapper des attributs SAML personnalisés

Si vous disposez déjà d'attributs personnalisés pour les attributs SID, UPN, OID et E-mail configurés dans votre fournisseur SAML, vous n'avez pas à effectuer cette tâche. Passez à l'étape Créer une application de connecteur SAML et utilisez vos attributs SAML personnalisés existants à l'étape 8.

> **Remarque :**
>
> Les étapes de cette section décrivent les actions que vous effectuez dans la console d'administration de votre fournisseur SAML. Les commandes spécifiques que vous utilisez pour effectuer ces actions peuvent varier des commandes décrites dans cette section, en fonction du fournisseur SAML choisi. Les commandes du fournisseur SAML de cette section ne sont fournies qu'à titre d'exemples. Reportez-vous à la documentation de votre fournisseur SAML pour plus d'informations sur les commandes correspondantes de votre fournisseur SAML.

1. Connectez-vous à la console d'administration de votre fournisseur SAML et sélectionnez l'option permettant de créer des attributs utilisateur personnalisés. Par exemple, en fonction de la console de votre fournisseur SAML, vous pouvez sélectionner **Users > Custom User Fields > New User Field**.
2. Ajoutez les attributs suivants :
   - cip_sid
   - cip_upn
   - cip_oid
   - cip_email
3. Sélectionnez le répertoire AD que vous avez connecté à Citrix Cloud. Par exemple, en fonction de la console de votre fournisseur SAML, vous pouvez sélectionner **Users > Directories**.
4. Sélectionnez l'option permettant d'ajouter des attributs de répertoire. Par exemple, en fonction de la console de votre fournisseur SAML, vous pouvez sélectionner **Directory Attributes**.

5. Sélectionnez l'option permettant d'ajouter des attributs et mappez les attributs AD suivants aux attributs utilisateur personnalisés que vous avez créés à l'étape 2 :
   - Sélectionnez `objectSid` et mappez avec l'attribut `cip_sid`.
   - Sélectionnez `userPrincipalName` et mappez avec l'attribut `cip_upn`.
   - Sélectionnez `ObjectGUID` et mappez avec l'attribut `cip_oid`.
   - Sélectionnez `mail` et mappez avec l'attribut `cip_email`.

Configurer les métadonnées du fournisseur SAML

Dans cette tâche, vous créez une application de connecteur à l'aide des métadonnées SAML de Citrix Cloud. Après avoir configuré l'application SAML, vous utilisez les métadonnées SAML de votre application connecteur pour configurer la connexion SAML à Citrix Cloud.

> **Remarque :**
>
> Certaines étapes de cette section décrivent les actions que vous effectuez dans la console d'administration de votre fournisseur SAML. Les commandes spécifiques que vous utilisez pour effectuer ces actions peuvent varier des commandes décrites dans cette section, en fonction du fournisseur SAML choisi. Les commandes du fournisseur SAML de cette section ne sont fournies qu'à titre d'exemples. Reportez-vous à la documentation de votre fournisseur SAML pour plus d'informations sur les commandes correspondantes de votre fournisseur SAML.

Créer une application de connecteur SAML

1. Connectez-vous à Citrix Cloud sur https://citrix.cloud.com.
2. Dans le menu Citrix Cloud, sélectionnez **Gestion des identités et des accès**.
3. Localisez **SAML 2.0** et sélectionnez **Connecter** dans le menu des points de suspension. L'écran **Configurer SAML** s'affiche.
4. À partir de la console d'administration de votre fournisseur SAML, ajoutez une application pour un fournisseur d'identité en incluant des attributs et une réponse signée. Par exemple, en fonction de la console de votre fournisseur, vous pouvez sélectionner **Applications > Applications > Add App**, puis sélectionner **SAML Test Connector (IdP w/ attr w/ sign response)**.
5. Le cas échéant, entrez un nom complet et enregistrez l'application.
6. Dans l'écran **Configurer SAML** dans Citrix Cloud, dans le champ **Métadonnées SAML**, sélectionnez **Télécharger**. Le fichier XML de métadonnées apparaît dans un autre onglet du navigateur.
7. Entrez les détails suivants pour l'application de connecteur :
   - Dans le champ **Audience**, entrez `https://saml.cloud.com`.
   - Dans le champ **Destinataire**, entrez `https://saml.cloud.com/saml/acs`.

- Dans le champ Validateur URL ACS, entrez `https://saml.cloud.com/saml/acs`.
- Dans le champ URL ACS, entrez `https://saml.cloud.com/saml/acs`.
- Dans le champ URL de déconnexion unique, entrez `https://saml.cloud.com/saml/logout/callback`.

8. Ajoutez vos attributs SAML personnalisés en tant que valeurs de paramètre dans l'application :

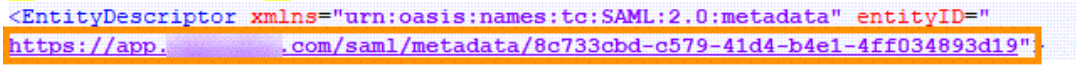
Créer ce champ	Attribuer cet attribut personnalisé
cip_sid	cip_sid ou votre attribut SID existant
cip_upn	cip_upn ou votre attribut UPN existant
cip_oid	cip_oid ou votre attribut OID existant
cip_email	cip_email ou votre attribut e-mail existant

9. Ajoutez vos abonnés Workspace en tant qu'utilisateurs pour leur permettre d'accéder à l'application.

Ajouter des métadonnées du fournisseur SAML à Citrix Cloud

1. Obtenez les métadonnées SAML auprès de votre fournisseur SAML. L'image suivante montre à quoi ce fichier peut ressembler :

2. Sur l'écran **Configurer SAML** dans Citrix Cloud, entrez les valeurs suivantes à partir du fichier de métadonnées de votre fournisseur SAML :
    - Sous **ID de l'entité**, entrez la valeur **entityID** de l'élément **EntityDescriptor** dans les métadonnées.

    - Sous **Signer demande d'authentification**, sélectionnez **Oui** pour autoriser Citrix Cloud à signer les demandes d'authentification, certifiant qu'elles proviennent de Citrix Cloud et non d'un acteur malveillant. Sélectionnez **Non** si vous préférez ajouter l'URL Citrix ACS à une liste d'autorisation utilisée par votre fournisseur SAML pour publier des réponses SAML en toute sécurité.
    - Dans **URL du service SSO**, entrez l'URL du mécanisme de liaison que vous souhaitez utiliser. Vous pouvez utiliser la liaison HTTP-POST ou HTTP-Redirect. Dans le fichier de métadonnées, recherchez les éléments **SingleSignOnService** dont les valeurs de liaison sont **HTTP-POST** ou **HTTP-Redirect**.

- Dans **Mécanisme de liaison**, sélectionnez le mécanisme qui correspond à la liaison de l'URL du service SSO que vous avez choisie dans le fichier de métadonnées.
- Dans **Réponse SAML**, sélectionnez la méthode de signature utilisée par votre fournisseur SAML pour la réponse SAML et l'assertion SAML. Par défaut, Citrix Cloud rejette toutes les réponses qui ne sont pas signées de la manière spécifiée dans ce champ.

3. Dans la console d'administration de votre fournisseur SAML, effectuez les opérations suivantes :
   - Sélectionnez **SHA-256** pour l'algorithme de signature SAML.
   - Téléchargez le certificat X.509 en tant que fichier PEM.
4. Sur l'écran **Configurer SAML** dans Citrix Cloud, sélectionnez **Charger le fichier** et sélectionnez le fichier PEM que vous avez téléchargé à l'étape précédente.
5. Sélectionnez **Continuer** pour terminer le chargement.
6. Sous **Contexte d'authentification**, sélectionnez le contexte que vous souhaitez utiliser et le degré de rigueur avec lequel vous souhaitez que Citrix Cloud applique ce contexte. Sélectionnez **Minimum** pour appliquer l'authentification avec le contexte sélectionné ainsi que dans des contextes plus stricts. Sélectionnez **Exact** pour appliquer l'authentification uniquement avec le contexte sélectionné. Par exemple, si vous sélectionnez le contexte **Transport Layer Security (TLS)** et le niveau **Minimum**, Citrix Cloud accepte les réponses SAML avec le contexte de TLS, de certificat X.509, d'authentification Windows intégrée et de Kerberos. Les réponses utilisant les contextes Nom d'utilisateur et Mot de passe, et Transport protégé par mot de passe sont rejetées. Si votre fournisseur SAML ne prend pas en charge les contextes d'authentification ou si vous choisissez de ne pas les utiliser, sélectionnez **Non spécifié** et **Minimum**.
7. Sous **URL de déconnexion**, recherchez l'élément **SingleSignOnService** avec la liaison HTTP-Redirect dans le fichier de métadonnées de votre fournisseur SAML et entrez l'URL.
8. Vérifiez que les valeurs d'attribut des noms par défaut suivantes dans Citrix Cloud correspondent aux valeurs d'attribut dans la console d'administration de votre fournisseur SAML. Si votre fournisseur SAML utilise des valeurs différentes, vous pouvez modifier ces valeurs dans Citrix Cloud pour vous assurer qu'elles correspondent à celles de votre fournisseur SAML.
   - **Nom d'attribut du nom d'affichage de l'utilisateur** : `displayName`
   - **Nom d'attribut du prénom de l'utilisateur** : `givenName`
   - **Nom d'attribut du nom de famille de l'utilisateur** : `familyName`
9. Dans Citrix Cloud, entrez les attributs SAML personnalisés de votre fournisseur SAML :
   - Sous **Nom d'attribut de l'identificateur de sécurité (SID)**, entrez votre nom d'attribut SID personnalisé. La valeur par défaut est `cip_sid`.
   - Sous **Nom d'attribut du nom d'utilisateur principal (UPN)**, entrez votre nom d'attribut UPN personnalisé. La valeur par défaut est `cip_upn`.
   - Sous **Nom d'attribut de l'e-mail**, entrez votre nom d'attribut E-mail personnalisé. La valeur par défaut est `cip_email`.
   - Sous **Nom d'attribut de l'identificateur d'objet AD (OID)**, entrez votre nom d'attribut OID

personnalisé. La valeur par défaut est `cip_oid`.

10. Sélectionnez **Tester et terminer** pour vérifier que vous avez correctement configuré la connexion.

Activer l'authentification SAML pour les espaces de travail

1. Dans le menu Citrix Cloud, sélectionnez **Configuration de l'espace de travail**.
2. Sélectionnez l'onglet **Authentification**
3. Sélectionnez **SAML 2.0**.

Sélectionner un emplacement de ressources principal

November 10, 2020

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 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**.

Gérer les administrateurs Citrix Cloud

July 20, 2021

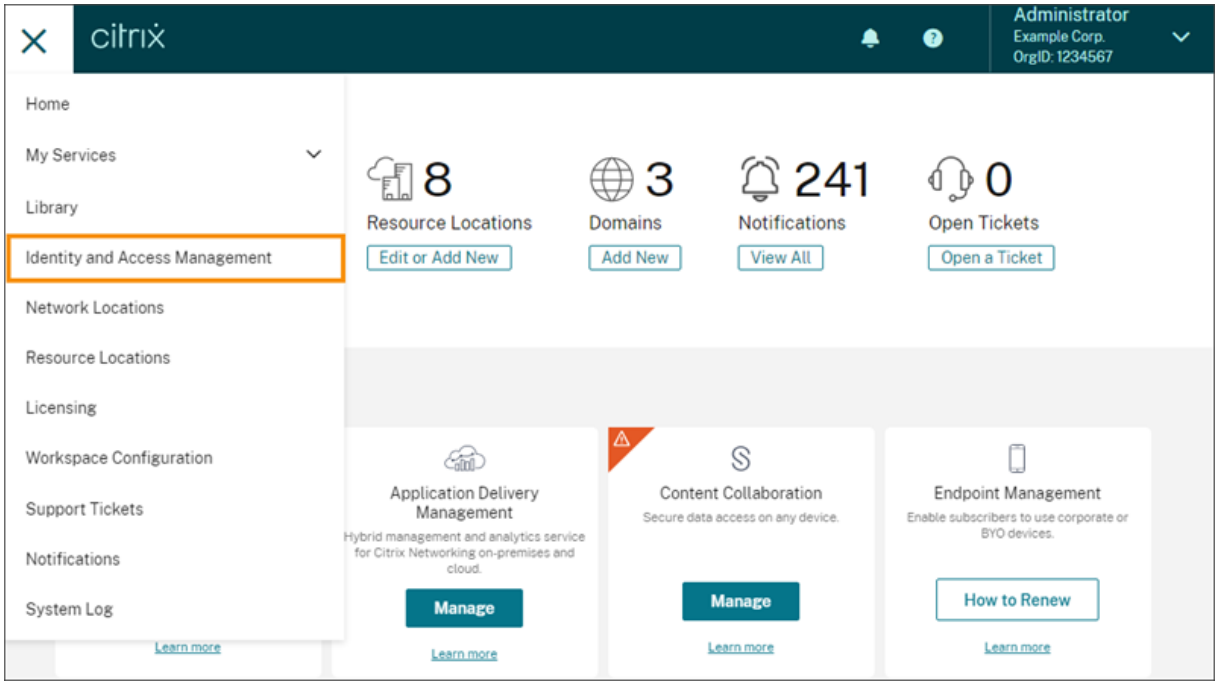
Les administrateurs sont gérés à partir de la console Citrix Cloud. Si vous souhaitez être ajouté en tant qu'administrateur à un compte Citrix Cloud existant, un administrateur du compte doit vous inviter.

Citrix Cloud prend également en charge l'utilisation de jetons en tant que deuxième facteur d'authentification pour les administrateurs Citrix Cloud. Après avoir été ajouté en tant qu'administrateur, vous pouvez inscrire votre appareil à l'authentification multifacteur et générer des jetons à l'aide de n'importe quelle application conforme à la norme TOTP (mot de passe à usage unique temporaire), telle que Citrix SSO ou Google Authenticator.

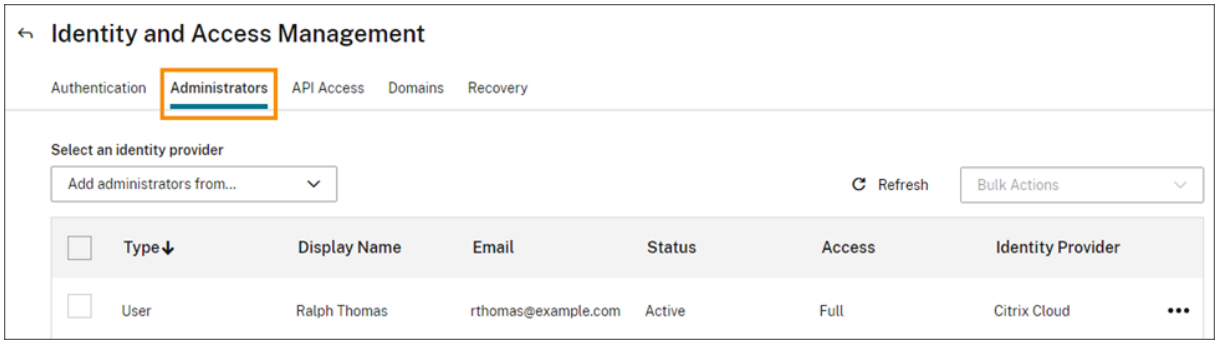
> **Conseil :**
>
> Le module « Citrix Cloud Platform », inclus dans le cours Fundamentals of Citrix Cloud, fournit de courtes vidéos qui vous guident dans l'administration de Citrix Cloud et de ses services associés. Le cours complet vous fournit également une base solide pour comprendre Citrix Cloud, ses avantages pour votre organisation et les principaux cas d'utilisation utilisés par les services Citrix Cloud.

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 :

1. Dans la zone **Ajouter admin. de**, sélectionnez le fournisseur d'identité à partir duquel vous souhaitez sélectionner l'administrateur. Selon le fournisseur d'identité sélectionné, Citrix Cloud peut vous inviter à vous connecter d'abord au fournisseur d'identité (par exemple, Azure Active Directory).
2. Si **Citrix Identity** est sélectionné, entrez l'adresse e-mail de l'utilisateur, puis cliquez sur **Inviter**.
3. Si Azure Active Directory est sélectionné, entrez le nom de l'utilisateur que vous souhaitez ajouter, puis cliquez sur **Inviter**. L'invitation d'utilisateurs invités AAD n'est pas prise en charge.
4. Configurez les autorisations appropriées de l'administrateur. L'option **Accès complet** (sélectionnée par défaut) permet de contrôler toutes les fonctions Citrix Cloud, ainsi que tous les services souscrits. L'option **Accès personnalisé** permet de contrôler les fonctions et les services que vous sélectionnez.
5. Cliquez sur **Envoyer invitation**.

Citrix Cloud envoie une invitation à l'utilisateur que vous avez spécifié et ajoute l'administrateur à la liste. L'e-mail est envoyé depuis cloud@citrix.com et explique comment accéder au compte. Citrix Cloud affiche également l'état de l'invitation afin que vous puissiez voir si l'utilisateur l'a acceptée et s'est connecté à Citrix Cloud.

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.

Modifier les autorisations d'administrateur

Lorsque vous ajoutez des administrateurs à votre compte Citrix Cloud, vous définissez les autorisations d'administrateur appropriées selon leur rôle dans votre organisation. Toutefois, il se peut que vous deviez parfois attribuer un niveau d'accès différent à un administrateur existant.

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

Pour modifier les autorisations d'administrateur existantes :

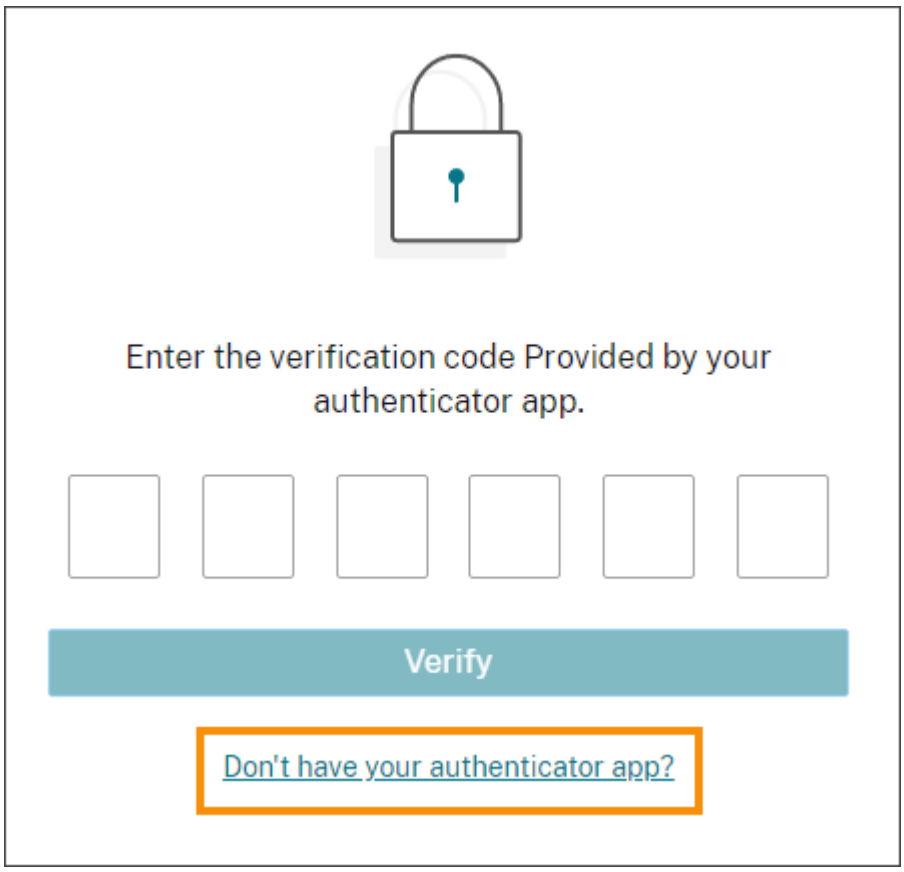
1. Connectez-vous à Citrix Cloud sur https://citrix.cloud.com.
2. Dans le menu Citrix Cloud, sélectionnez **Gestion des identités et des accès**, puis sélectionnez **Administrateurs**.
3. Recherchez l'administrateur que vous souhaitez gérer, cliquez sur le bouton représentant des points de suspension et sélectionnez **Modifier l'accès**.
4. Pour autoriser ou interdire des autorisations spécifiques, sélectionnez **Accès personnalisé**.
5. Pour chaque autorisation, sélectionnez ou désélectionnez la case à cocher selon vos besoins.
6. Cliquez sur **Enregistrer**.

Changer d'appareil pour l'authentification multifacteur

Si vous perdez votre appareil inscrit, si vous souhaitez utiliser un autre appareil avec Citrix Cloud ou réinitialiser votre application d'authentification, vous pouvez vous réinscrire à l'authentification multifacteur Citrix Cloud.

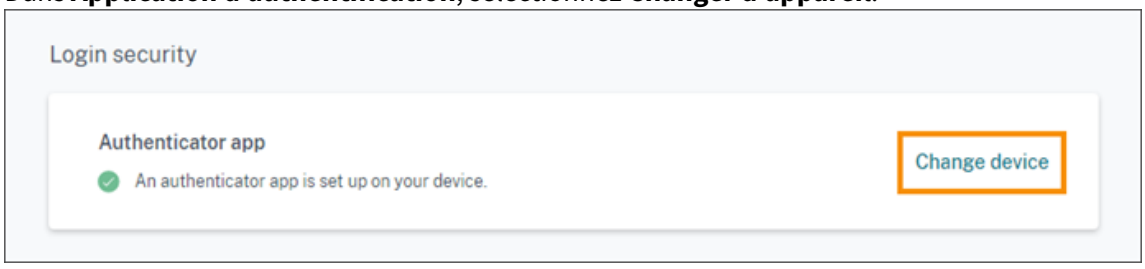
> **Remarques**
>
> - Le changement d'appareil supprime l'inscription de l'appareil actuel et génère une nouvelle clé d'application d'authentification.
> - Si vous réinscrivez avec la même application d'authentification à partir de votre inscription d'origine, supprimez l'entrée Citrix Cloud de votre application d'authentification avant de vous réinscrire. Les codes affichés dans cette entrée ne fonctionneront plus une fois la réinscription terminée. Si vous ne supprimez pas cette entrée avant ou après la réinscription, votre application d'authentification affiche deux entrées Citrix Cloud avec des codes différents, ce qui peut causer de la confusion lors de la connexion à Citrix Cloud.
> - Si vous vous réinscrivez avec un nouvel appareil et que vous ne disposez pas d'une application d'authentification, vous pouvez en télécharger une à partir du magasin d'applications de votre appareil. Pour une expérience plus fluide, Citrix vous recommande d'installer une application d'authentification avant de réinscrire votre appareil.

1. Connectez-vous à Citrix Cloud et saisissez le code fourni par votre application d'authentification.



Si vous n'avez pas votre application d'authentification, cliquez sur **Vous n'avez pas d'application d'authentification ?** et sélectionnez une méthode de récupération pour vous aider à vous connecter. Selon la méthode de récupération sélectionnée, entrez le code de récupération que vous avez reçu ou un code de secours inutilisé et sélectionnez **Vérifier**.

2. Si vous êtes administrateur pour plusieurs organisations clientes, sélectionnez une de ces organisations.
3. Dans le menu supérieur droit, sélectionnez **Mon profil**.
4. Dans **Application d'authentification**, sélectionnez **Changer d'appareil**.



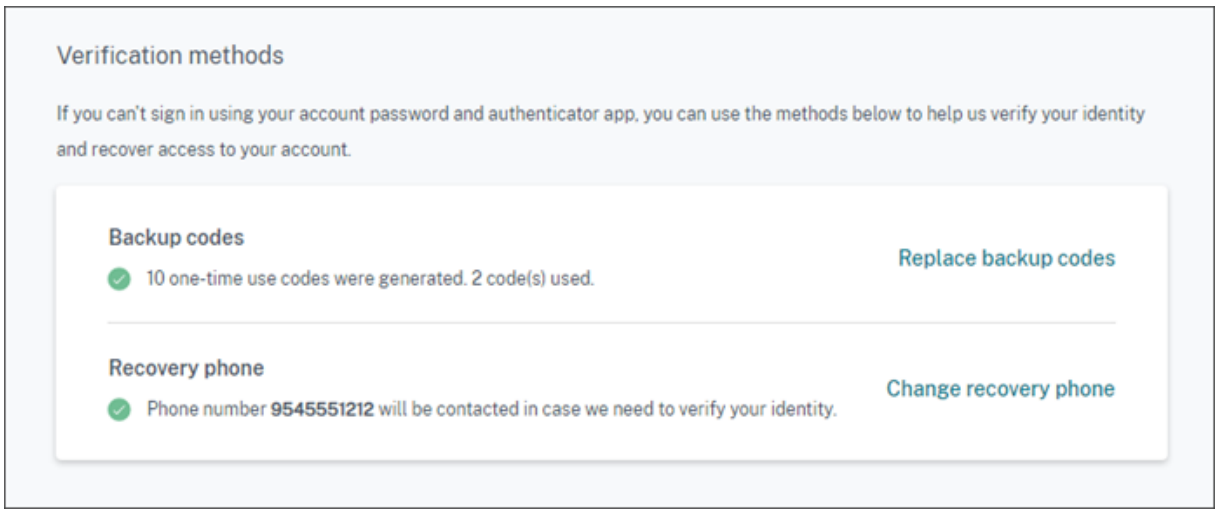
5. Lorsque vous êtes invité à confirmer le changement d'appareil, sélectionnez **Oui, changer d'appareil**.
6. Vérifiez votre identité en entrant un code de vérification fourni par votre application

d'authentification. Si vous n'avez pas d'application d'authentification, sélectionnez **Vous n'avez pas d'application d'authentification ?** et sélectionnez une méthode de récupération. Selon la méthode de récupération que vous sélectionnez, entrez le code de vérification ou le code de récupération que vous recevez ou un code de secours inutilisé. Sélectionnez **Vérifier**.

7. Si vous utilisez l'appareil que vous avez inscrit à l'origine et votre application d'authentification d'origine, supprimez l'entrée Citrix Cloud existante de votre application d'authentification.
8. Si vous inscrivez un nouvel appareil et que vous n'avez pas d'application d'authentification, téléchargez-en une depuis le magasin d'applications de votre appareil.
9. Depuis votre application d'authentification, scannez le code QR avec votre appareil ou saisissez la clé manuellement.
10. Saisissez le code de vérification à 6 chiffres de votre application d'authentification et sélectionnez **Vérifier le code**.

Gérer vos méthodes de vérification

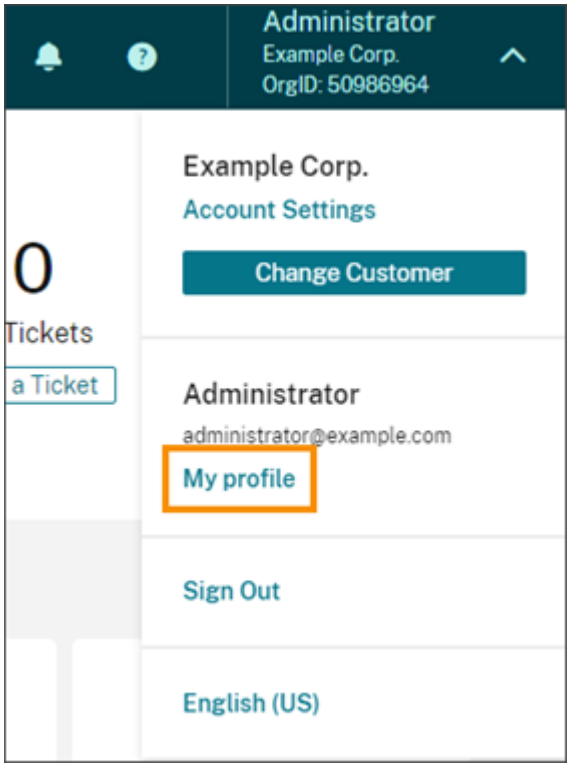
> **Important :**
>
> Pour garantir la sécurité de votre compte Citrix Cloud, maintenez vos méthodes de vérification à jour avec des informations correctes. Si vous perdez l'accès à votre application d'authentification, ces méthodes de vérification sont la seule façon de récupérer l'accès à votre compte.



Générer de nouveaux codes de secours

Si vous perdez ou avez besoin de générer plus de codes de secours à usage unique, vous pouvez générer un nouvel ensemble de codes de secours à tout moment. Après avoir généré de nouveaux codes de secours, assurez-vous de les stocker dans un endroit sûr.

1. Connectez-vous à Citrix Cloud et saisissez le code fourni par votre application d'authentification.
2. Si vous êtes administrateur pour plusieurs organisations clientes, sélectionnez une de ces organisations.
3. Dans le menu supérieur droit, sélectionnez **Mon profil**.



4. Sous **Méthodes de vérification**, dans **Codes de secours**, sélectionnez **Remplacer les codes de secours**.
5. Vérifiez votre identité en entrant un code de vérification fourni par votre application d'authentification.
6. Lorsque vous êtes invité à remplacer vos codes de secours, sélectionnez **Oui, les remplacer**. Citrix Cloud génère et affiche un nouvel ensemble de codes de secours.
7. Sélectionnez **Télécharger les codes** pour télécharger vos nouveaux codes sous forme de fichier texte. Ensuite, sélectionnez **J'ai enregistré ces codes** et sélectionnez **Fermer**.

> **Remarque :**
>
> Vous ne pouvez modifier les autorisations des administrateurs de Citrix Endpoint Management (CEM) qu'après que l'administrateur a accepté l'invitation d'un administrateur et a cliqué sur **Gérer** dans la vignette CEM. Comme tous les administrateurs Citrix Cloud, les administrateurs CEM disposent d'un accès complet par défaut.

Modifier votre numéro de téléphone de récupération

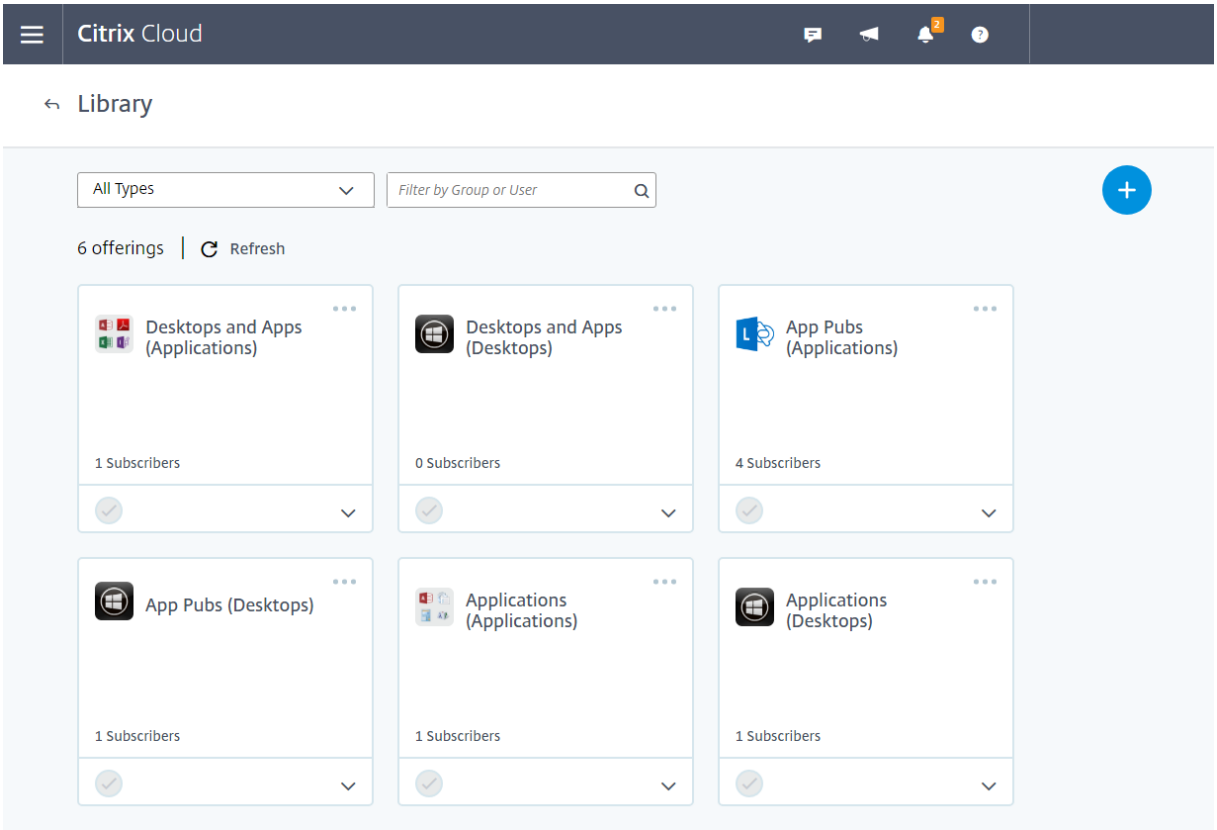
1. Connectez-vous à Citrix Cloud et saisissez le code fourni par votre application d'authentification.
2. Si vous êtes administrateur pour plusieurs organisations clientes, sélectionnez l'organisation cliente à partir de laquelle vous vous êtes initialement inscrit à l'authentification multifacteur.
3. Dans le menu supérieur droit, sélectionnez **Mon profil**.
4. Sous **Méthodes de vérification**, dans **N° de téléphone de récupération**, sélectionnez **Changer le n° de téléphone de récupération**.
5. Saisissez le nouveau numéro de téléphone que vous souhaitez utiliser, puis sélectionnez **Enregistrer**.

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

January 24, 2020

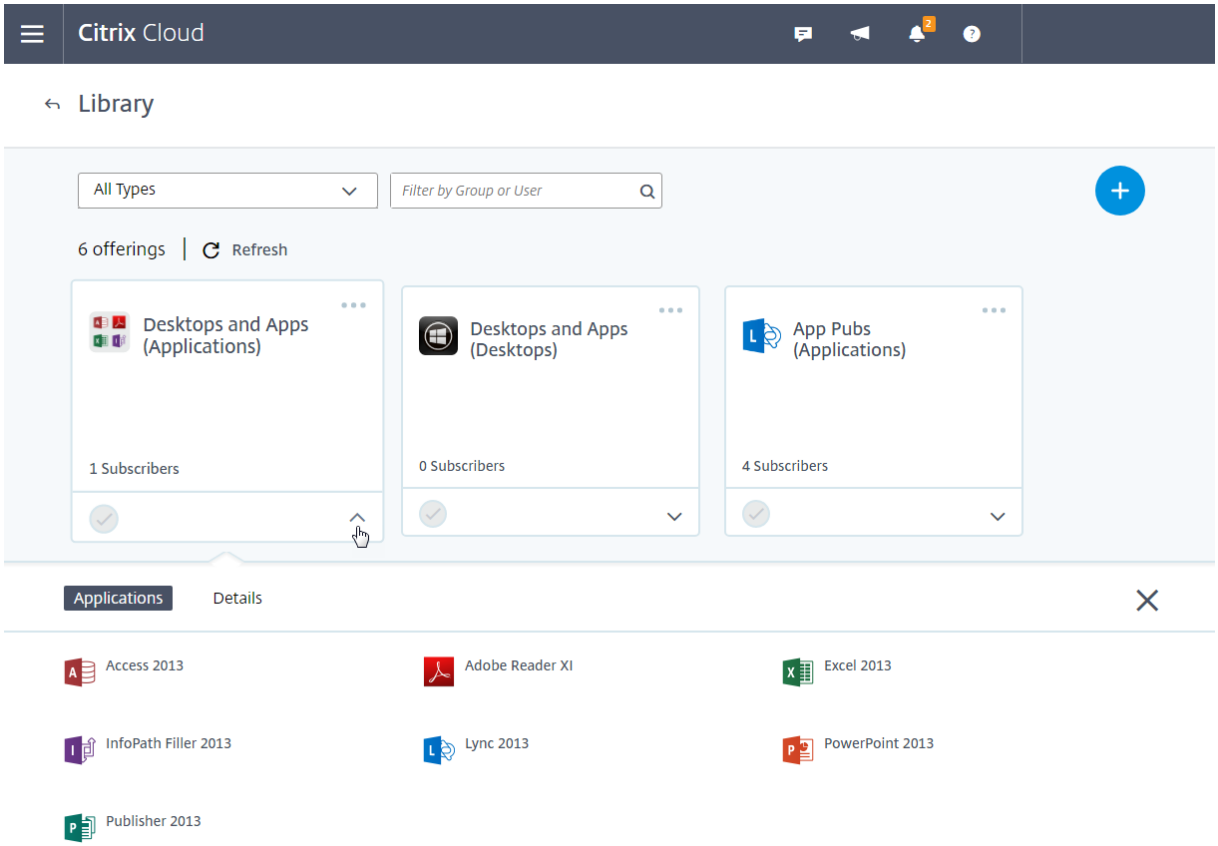
Vous pouvez attribuer des ressources ou d'autres éléments que vous configurez dans un service (par exemple, les bureaux ou les applications configurés dans Virtual Apps and Desktops Service) à vos utilisateurs et groupes Active Directory à l'aide de la bibliothèque.

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.



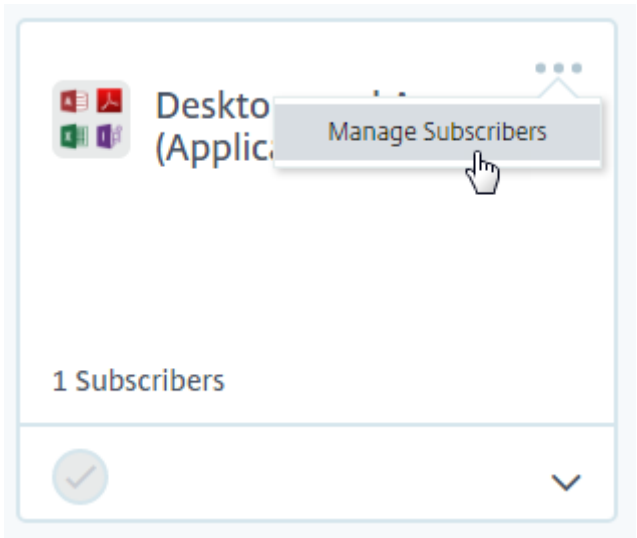
Afficher les détails d'une offre

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.



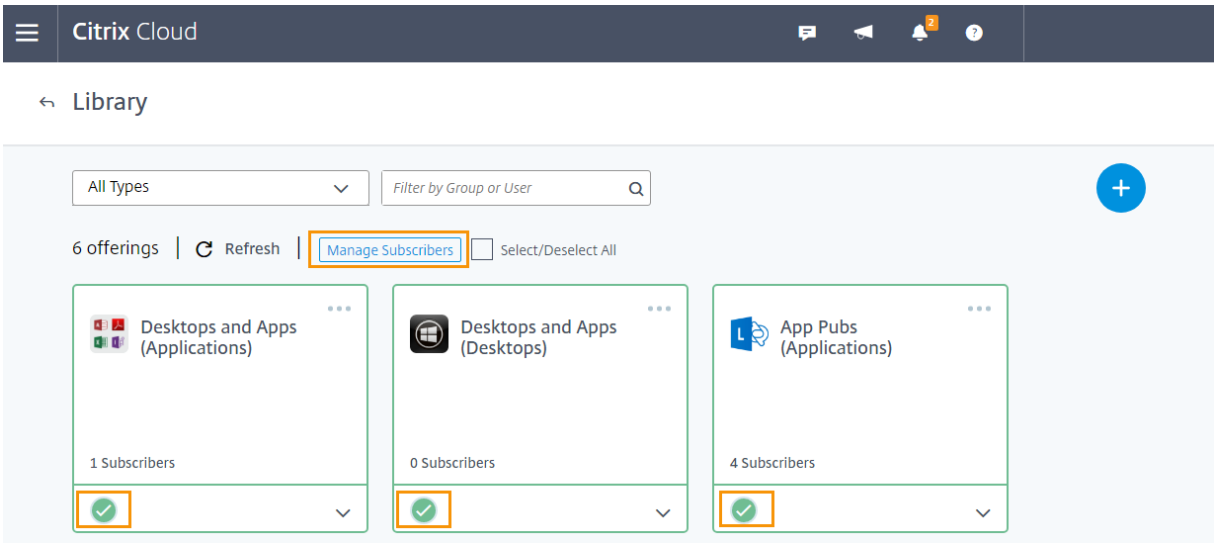
Ajouter ou supprimer des abonnés

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

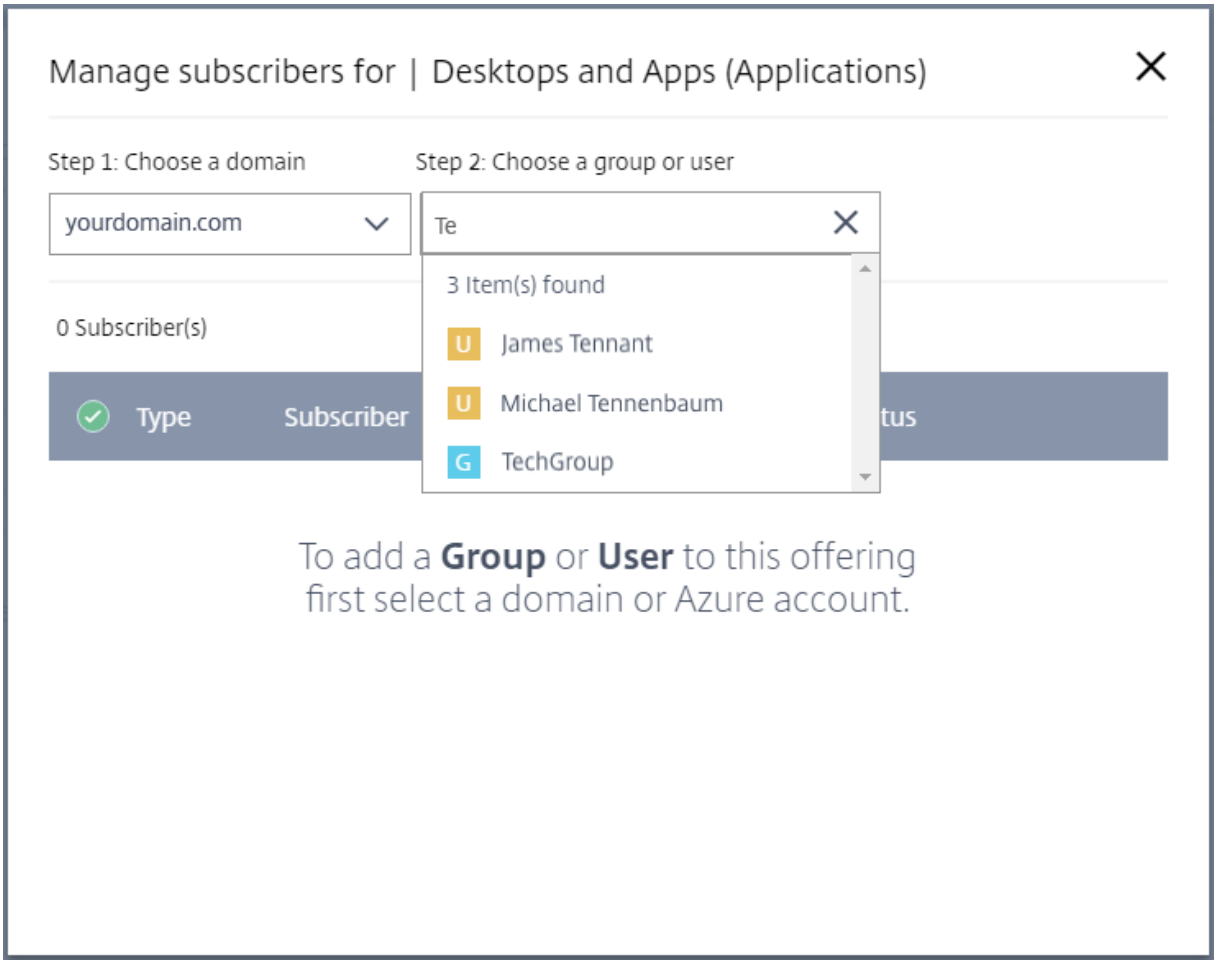


Pour gérer les abonnés pour plusieurs offres, sélectionnez la coche de chaque offre et cliquez sur

Gérer les abonnés.

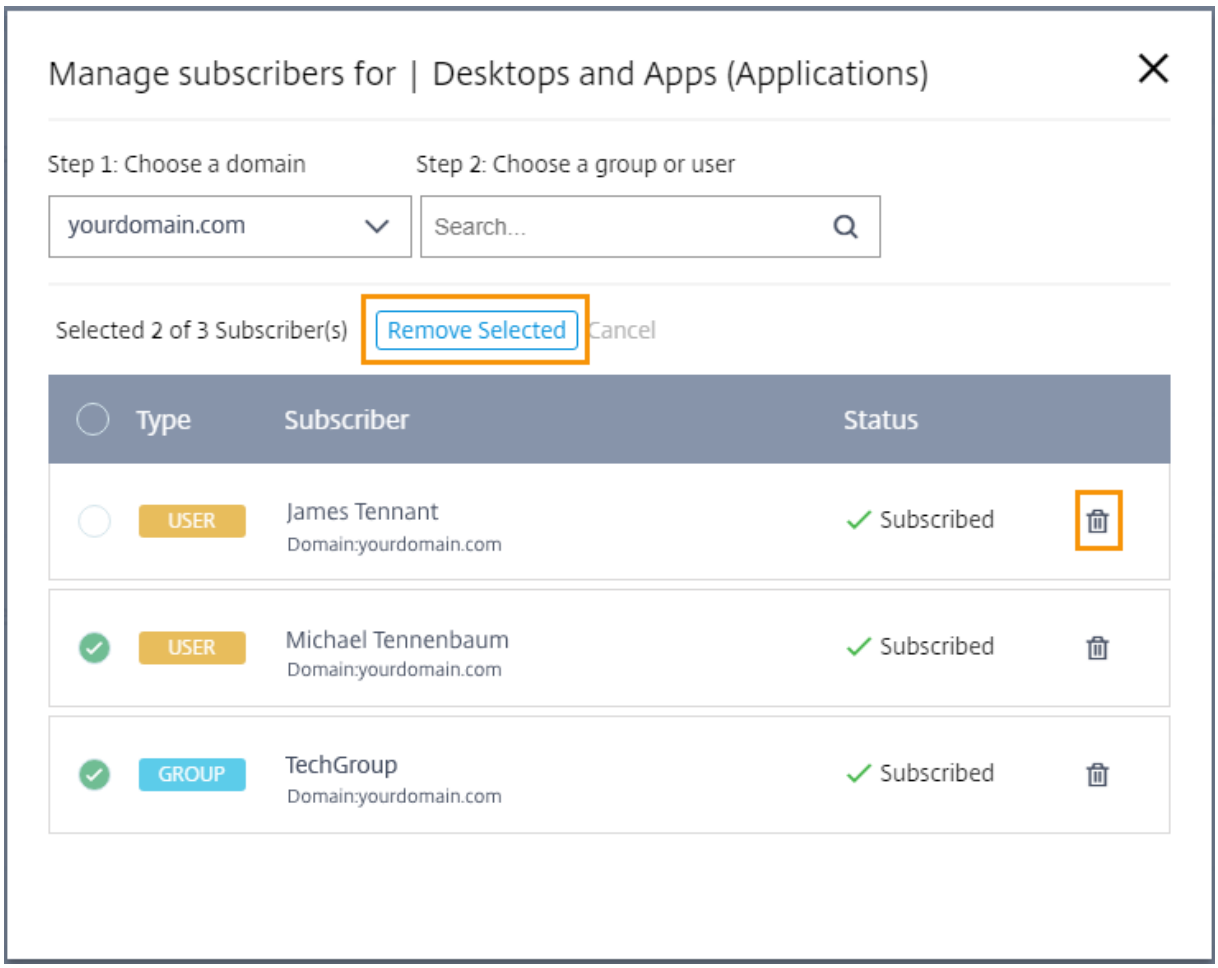


Pour ajouter des abonnés à l'offre, choisissez un domaine et sélectionnez les utilisateurs ou groupes que vous souhaitez ajouter.



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

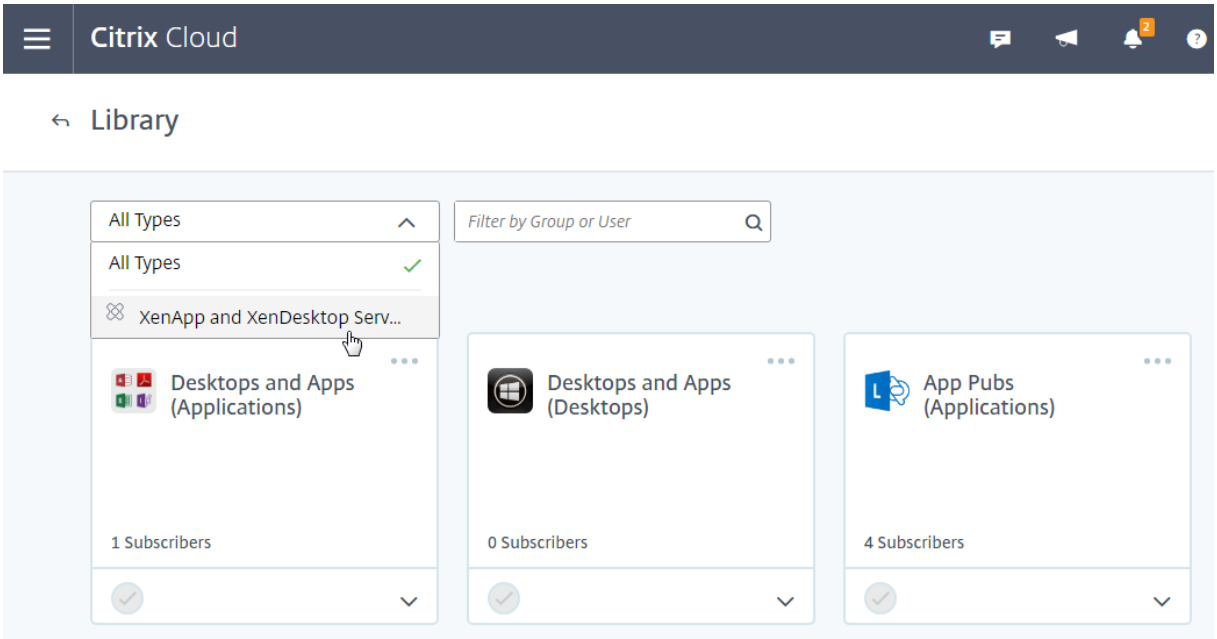
supprimer plusieurs abonnés, sélectionnez les utilisateurs ou groupes et cliquez sur **Supprimer la sélection**.



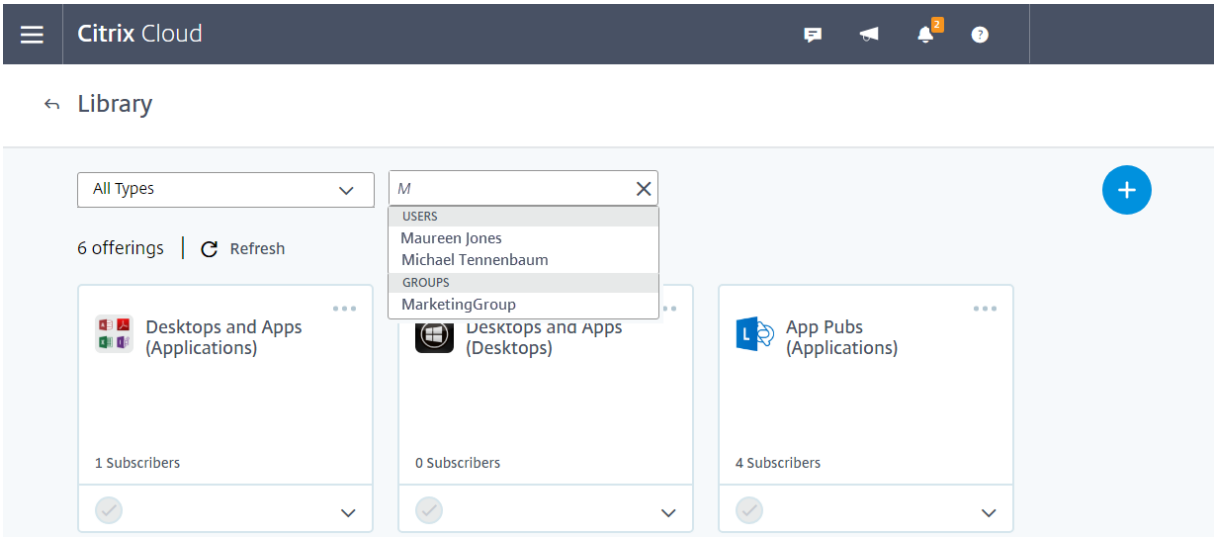
Après avoir ajouté ou supprimé des abonnés d'une offre, la carte d'offre affiche le nombre actuel d'abonnés.

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.



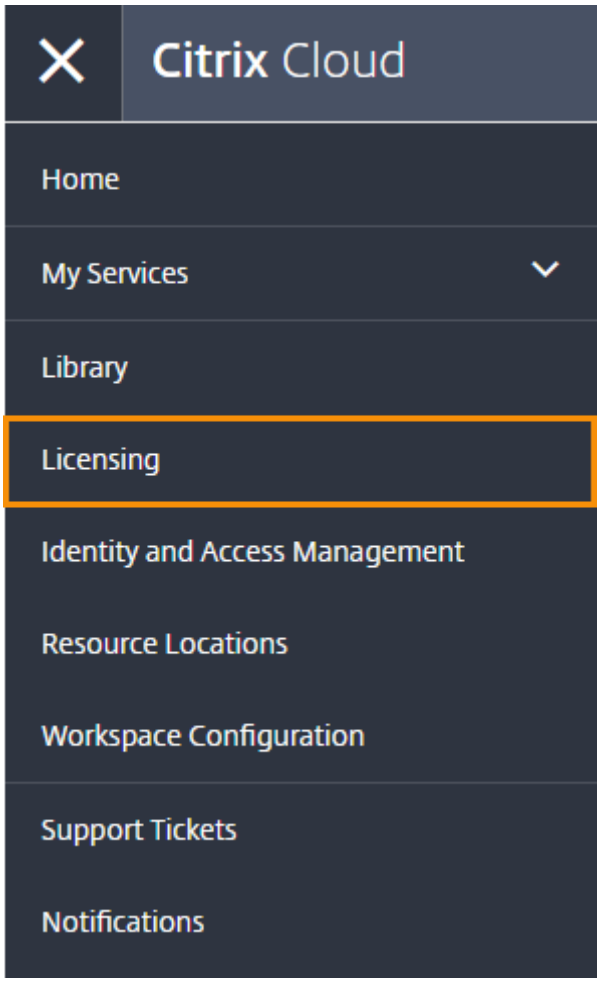
Surveiller les licences et l'utilisation active pour les services cloud

July 21, 2021

Le système de licences dans Citrix Cloud vous permet de surveiller de près la consommation de licences des services cloud que vous avez achetés. Le résumé et les rapports détaillés vous permettent :

- D'afficher la disponibilité et les affectations de licences
- D'afficher les tendances quotidiennes et mensuelles d'utilisation active des services cloud applicables
- 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

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



> **Remarque :**
>
> Cet article couvre les fonctionnalités Système de licences communes à tous les services Citrix Cloud pris en charge. Certains aspects de l'option Système de licences peuvent être différents, selon le service (par exemple, l'attribution de licence). Pour plus d'informations sur les licences et l'utilisation de chaque service, consultez les articles suivants :
>
> - Surveiller les licences et l'utilisation active de Virtual Apps and Desktops Service (utilisateur/appareil)
> - Surveiller les licences et l'utilisation maximale de Virtual Apps and Desktops Service (simul-

tané)
- Surveiller les licences et l'utilisation active de Virtual Apps and Desktops Standard pour Azure
- Surveiller les licences et l'utilisation active du service Endpoint Management

Régions et services cloud pris en charge

L'option Système de licences est disponible pour les services pris en charge dans les régions suivantes : États-Unis, Union Européenne et Asie Pacifique Sud.

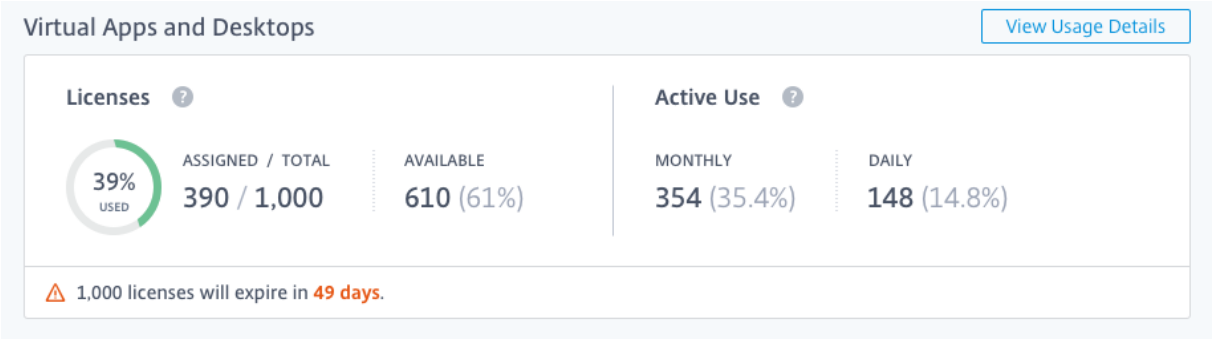
L'option Système de licences est prise en charge pour les services cloud suivants :

- Virtual Apps and Desktops (modèles de licences utilisateur/appareil et simultanés)
- Virtual Apps and Desktops Standard pour Azure (modèle de licence utilisateur/appareil)
- Endpoint Management
- Gateway

Attribution de licence

En général, les utilisateurs se voient attribuer une licence lors de la première utilisation du service cloud. Certains services peuvent attribuer des licences différemment en fonction du modèle de licence qu'ils utilisent. Pour plus d'informations sur la façon dont les licences sont affectées à chaque service, consultez les articles Système de licences référencés en haut de celui-ci.

Résumé et détails de l'option Système de licences



L'écran de résumé de l'option Système de licences fournit une vue d'ensemble des informations suivantes pour chaque service pris en charge :

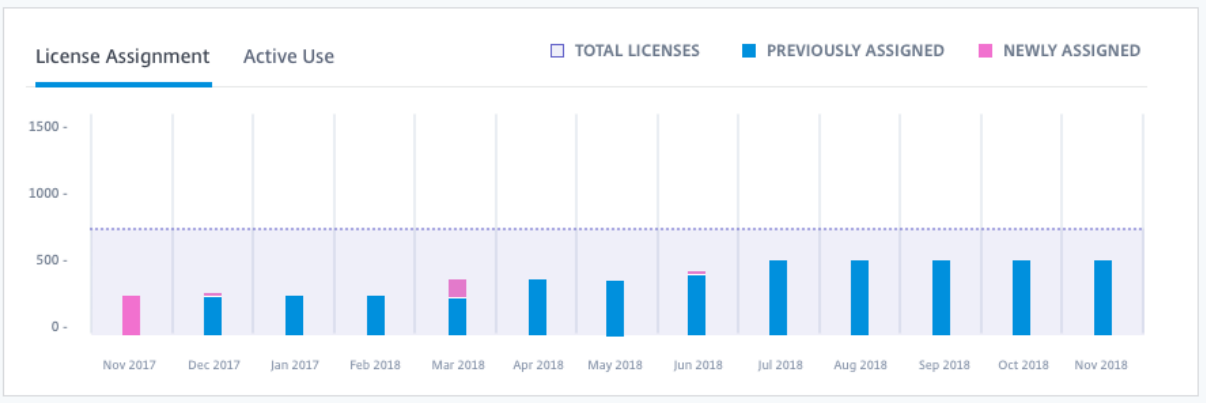
- Pourcentage du nombre total de licences achetées attribuées. Lorsque le pourcentage approche 100 %, le pourcentage passe du vert au jaune. Si le pourcentage dépasse 100 %, il devient rouge.
- Rapport entre les licences attribuées et les licences achetées et le nombre de licences disponibles restantes.

- Temps restant avant expiration de l'abonnement au service cloud. Si l'abonnement expire dans les 90 jours suivants, un message d'avertissement apparaît.

Pour certains services, ce résumé peut inclure des informations supplémentaires telles que l'utilisation active. Pour plus d'informations sur les détails spécifiques au service, consultez les articles Système de licences référencés en haut de celui-ci.

Tendances d'utilisation et activité des licences

Pour obtenir une vue détaillée des licences de votre service cloud, cliquez sur **Afficher détails d'utilisation**. Vous pouvez ensuite voir une répartition des tendances d'utilisation et des consommateurs de licences de service cloud.



Cette répartition affiche des informations variables, selon le service cloud. Pour plus d'informations sur les tendances d'utilisation et l'activité des licences spécifiques au service, consultez les articles Système de licences référencés en haut de celui-ci.

Libérer des licences attribuées

En général, une licence attribuée peut être libérée si l'utilisateur n'a pas utilisé le service cloud pendant 30 jours consécutifs. Lorsqu'une licence est libérée, le nombre de licences restantes augmente et le nombre de licences attribuées diminue en conséquence.

Pour certains services, les licences peuvent être libérées différemment, selon le modèle de licence utilisé. Pour plus d'informations sur la libération de licences pour un service spécifique, consultez les articles Système de licences référencés en haut de celui-ci.

Questions fréquentes

- **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 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.
- **Les licences multitypes sont-elles prises en charge avec Virtual Apps and Desktops Service (par exemple, en utilisant à la fois les modèles Utilisateur/machine et Utilisateurs simultanés) ?** Si les deux modèles de licences sont introduits dans un compte Citrix Cloud unique, la vignette Virtual Apps and Desktops n'apparaît plus sur la page de la console de licences dans Citrix Cloud. En raison de cette perte de visibilité au niveau des licences pour Virtual Apps and Desktops Service, Citrix ne recommande pas d'utiliser des licences multitypes.
- **Les licences multi-éditions sont-elles prises en charge avec Virtual Apps and Desktops Service ? Par exemple, puis-je utiliser les éditions Premium et Advanced sur le même compte Citrix Cloud ?** Non, ce cas d'utilisation n'est pas pris en charge. Un site Virtual Apps and Desktops ne peut détenir de licence que pour une seule édition.
- **Quelle est la différence entre les rapports de monitoring (dans Director) et les insights sur les licences simultanées ?** Le rapport de monitoring et l'explication des sessions simultanées fournissent une interprétation et des mesures différentes de celles des mesures des licences simultanées en cours d'utilisation. Dans la plupart des cas, l'utilisation du nombre de sessions simultanées au sein de Director comme représentation ou prévision de l'utilisation maximale des licences simultanées surestime considérablement le nombre de licences simultanées nécessaires. N'utilisez pas le rapport de monitoring de Director en tant que substitut à un rapport sur l'utilisation simultanée des licences. Les deux principales différences entre les outils de reporting sont les suivantes :
  - **Durée de l'échantillonnage :** la période d'échantillonnage des licences est de cinq minutes. Toutes les cinq minutes, Citrix Cloud compte les appareils uniques connectés au service. Toutes les périodes d'échantillonnage de cinq minutes sont regroupées pour déterminer l'utilisation maximale au cours d'une période de 24 heures, d'une période mensuelle et d'une période contractuelle. Le rapport de monitoring dans Director peut afficher des intervalles allant jusqu'à deux heures en fonction de la manière dont le rapport est exécuté.
  - **Unicité :** le système de gestion des licences recherche le caractère unique des appareils lorsque les sessions sont lancées. Le rapport de monitoring ne tient pas compte des appareils uniques.

Surveiller les licences et l'utilisation active du service Endpoint Management

May 28, 2020

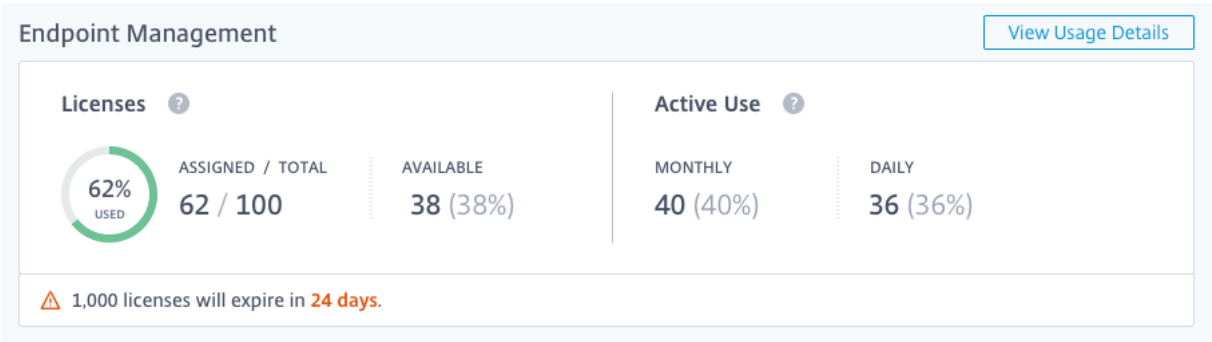
Attribution de licence

En général, les utilisateurs se voient attribuer une licence lors de la première utilisation du service cloud. Pour Endpoint Management, une licence est attribuée lorsqu'un utilisateur inscrit un appareil. Une fois qu'un appareil est inscrit, l'appareil est enregistré périodiquement avec Citrix Cloud. Citrix Cloud utilise ensuite cette « impulsion d'enregistrement » pour calculer l'utilisation mensuelle et informe les administrateurs de l'utilisation des services la plus récente des utilisateurs.

La première utilisation a lieu la première fois qu'un utilisateur inscrit un appareil ou la première fois qu'une « impulsion d'enregistrement » se produit sur l'appareil.

Les licences sont attribuées par utilisateur. Ainsi, si deux utilisateurs s'inscrivent et utilisent le même appareil, deux licences sont attribuées.

Résumé et détails de l'option Système de licences



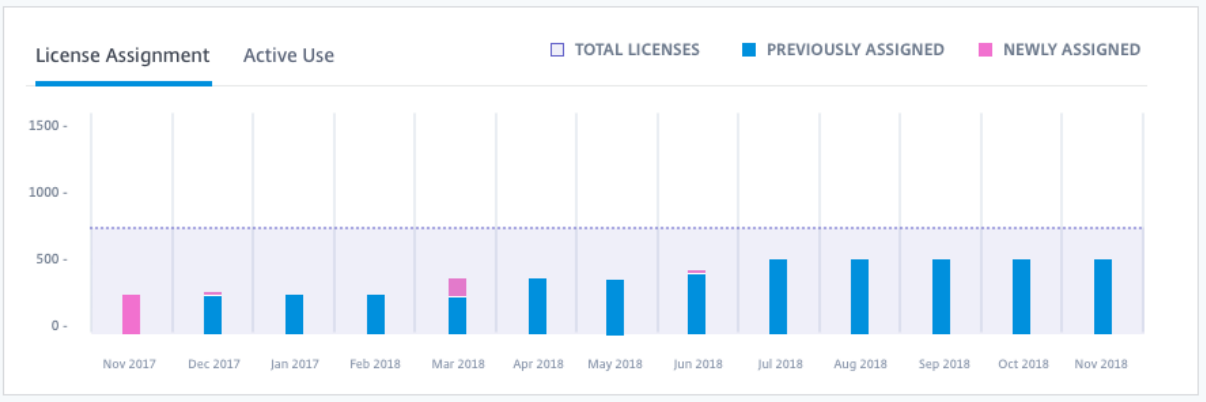
L'écran de résumé de l'option Système de licences fournit une vue d'ensemble des informations suivantes pour chaque service pris en charge :

- Pourcentage du nombre total de licences achetées attribuées. Lorsque le pourcentage approche 100 %, le pourcentage passe du vert au jaune. Si le pourcentage dépasse 100 %, il devient rouge.
- Rapport entre les licences attribuées et les licences achetées et le nombre de licences disponibles restantes.
- Statistiques d'utilisation active sur une base mensuelle et quotidienne :
  - L'utilisation active mensuelle fait référence au nombre d'utilisateurs uniques qui ont utilisé le service au cours des 30 derniers jours.

  - L'utilisation active quotidienne fait référence au nombre d'utilisateurs uniques qui ont utilisé le service au cours des dernières 24 heures.
- Temps restant avant expiration de l'abonnement au service cloud. Si l'abonnement expire dans les 90 jours suivants, un message d'avertissement apparaît.

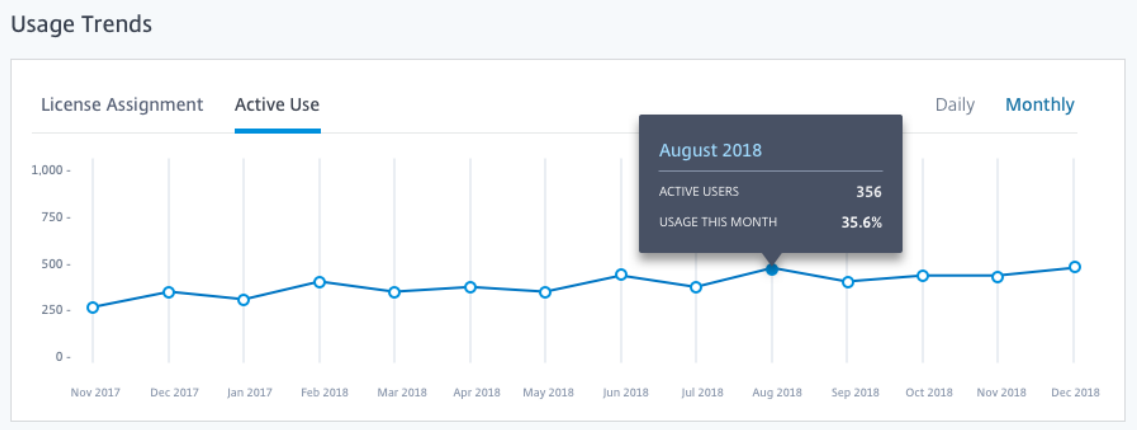
Tendances d'utilisation et activité des licences

Pour obtenir une vue détaillée des licences, cliquez sur **Afficher détails d'utilisation**. Vous pouvez ensuite voir une répartition des tendances d'utilisation et des utilisateurs et des appareils individuels qui consomment des licences de service cloud.



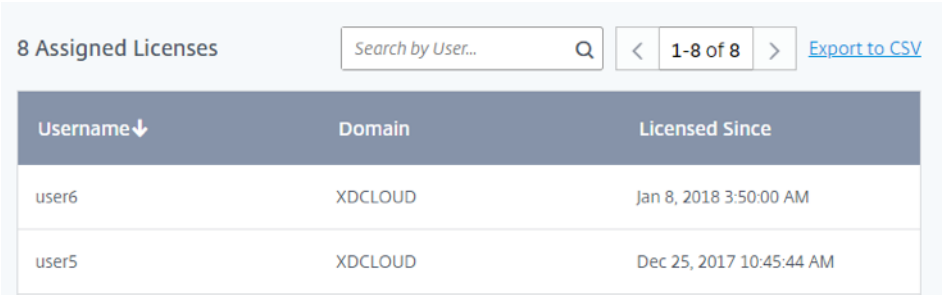
Cette répartition vous montre les informations suivantes :

- **Nombre total de licences :** nombre total de licences achetées pour le service cloud pour toutes les prestations.
- **Précédemment attribuée :** 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 « Précédemment attribuée » 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.
- **Utilisation active :** tendances quotidiennes et mensuelles de l'utilisation active au cours du mois civil et de l'année civile précédente, respectivement.



La section **Activité des licences** affiche également les informations suivantes :

- Liste des consommateurs individuels qui ont attribué des licences
- Date à laquelle les licences ont été attribuées
- Nombre d'appareils inscrits et date du dernier enregistrement pour chaque utilisateur



Pour afficher le nombre d'appareils inscrits pour un utilisateur spécifique, vous pouvez cliquer sur le bouton représentant des points de suspension et sélectionner **Afficher appareils**. Citrix Cloud affiche la liste des appareils inscrits pour l'utilisateur et la date du dernier enregistrement pour chaque appareil.

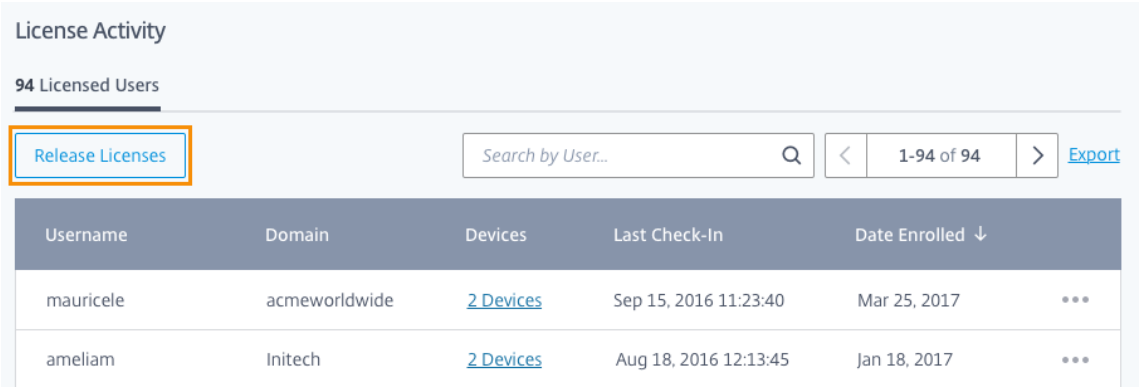
Libérer des licences attribuées

Vous pouvez libérer des licences pour les utilisateurs qui n'ont pas inscrit un nouvel appareil et si un appareil existant ne s'est pas connecté avec Citrix Cloud au cours des 30 derniers jours. Vous pouvez libérer plusieurs licences en bloc ou individuellement.

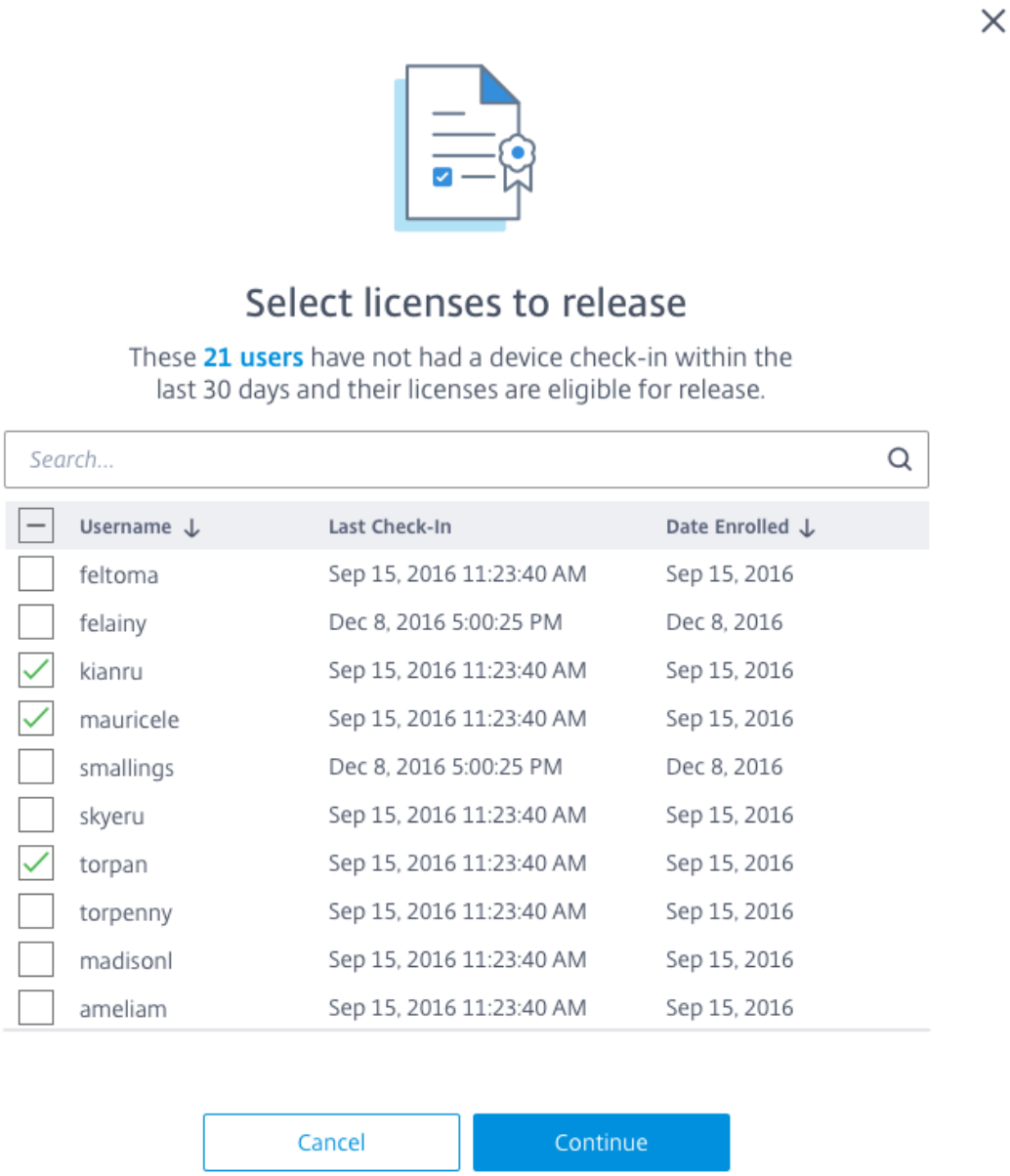
Lorsqu'une licence est libérée, le nombre de licences restantes augmente et le nombre de licences attribuées diminue en conséquence. Une fois la licence d'un utilisateur libérée, l'utilisateur peut acquérir une autre licence en inscrivant un appareil.

Pour libérer plusieurs licences attribuées

1. Sous **Activité des licences**, sélectionnez **Libérer licences**.



2. Dans la liste, sélectionnez les utilisateurs que vous souhaitez gérer et sélectionnez **Continuer**.



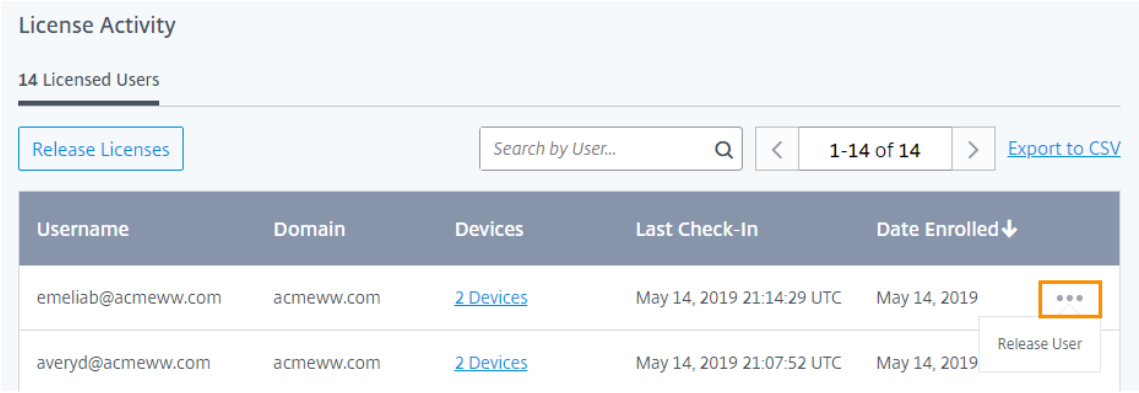
3. Lorsque vous êtes invité à confirmer la libération, cliquez sur **Libérer**.

Pour libérer une seule licence attribuée

Vous pouvez libérer des licences individuelles à partir de la liste **Utilisateurs sous licence**. Cette liste affiche des boutons de points de suspension sur lesquels peuvent cliquer uniquement les utilisateurs disposant de licences pouvant être libérées. Le bouton représentant des points de suspension est inactif pour les utilisateurs qui ont inscrit un nouvel appareil et si un appareil existant s'est connecté avec Citrix Cloud au cours des 30 derniers jours.

1. Sous **Activité des licences**, sélectionnez l'onglet **Utilisateurs sous licence**.

2. Localisez l'utilisateur que vous voulez gérer.
3. Cliquez sur le bouton des points de suspension et sélectionnez **Libérer utilisateur**.



4. Vérifiez l'utilisateur sélectionné et sélectionnez **Continuer**.
5. Lorsque vous êtes invité à confirmer la libération, cliquez sur **Libérer**.

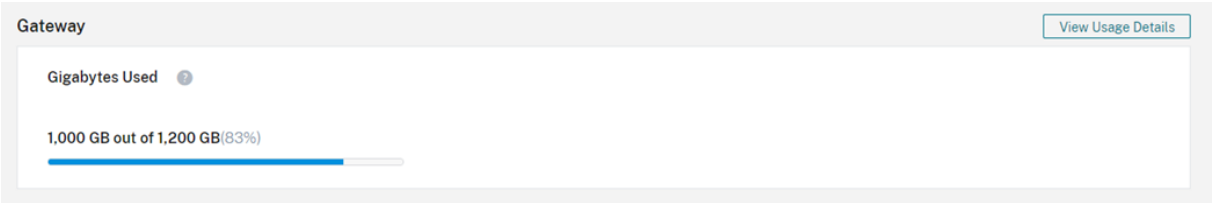
Surveiller l'utilisation de la bande passante pour Gateway Service (version Technical Preview)

July 21, 2021

> **Remarque :**
>
> La surveillance de l'utilisation de la bande passante pour Gateway Service est actuellement en version Technical Preview. Pendant cette période, les limites de licence ne seront pas appliquées ou n'interféreront pas avec les charges de travail de production.

Cet article concerne Gateway Service lorsqu'il est utilisé conjointement avec Citrix Virtual Apps and Desktops Service et Citrix Workspace. La consommation de bande passante de Gateway Service inclus avec le service Virtual Apps Essentials n'est pas affichée sur la page **Licences** de la console de gestion Citrix Cloud.

Résumé de l'option Système de licences



Le résumé de l'option Système de licences pour Gateway Service fournit une vue d'ensemble des informations suivantes :

- Quantité de bande passante consommée par rapport à la quantité totale de bande passante pour tous les abonnements
- Temps restant avant expiration de l'abonnement au service cloud. Si l'abonnement expire dans les 90 jours suivants, un message d'avertissement apparaît.

Licences et bande passante utilisées

Pour les abonnements à Gateway Service, chaque utilisateur a accès à 1 Go de bande passante par mois (12 Go par utilisateur et par an). Cette bande passante est regroupée selon le nombre de licences et la période d'abonnement. Par exemple, si vous achetez 100 licences sur 3 ans, vous disposez de 3 600 Go de bande passante totale (1 200 Go par an). Cette bande passante est répartie entre tous les utilisateurs sous licence pendant la période de 3 ans. Si vous achetez des abonnements supplémentaires, Citrix Cloud affiche le nombre total de licences et de bande passante sur tous vos abonnements.

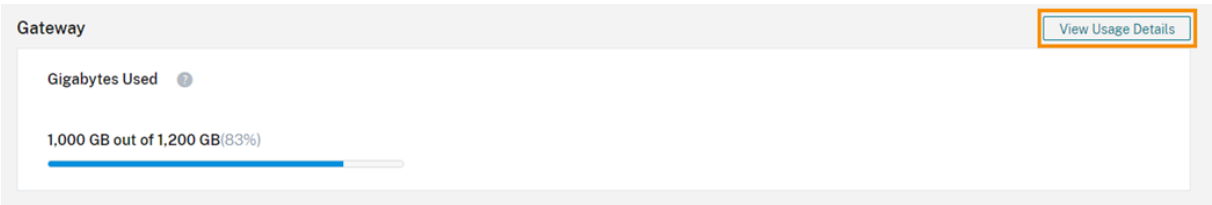
Pour les essais Gateway Service, 50 Go de bande passante sont regroupés entre 25 utilisateurs pendant la période d'essai de 60 jours.

Si vous n'utilisez pas la totalité de la bande passante pendant la période d'abonnement, Citrix Cloud ne reporte pas la bande passante inutilisée lors du renouvellement.

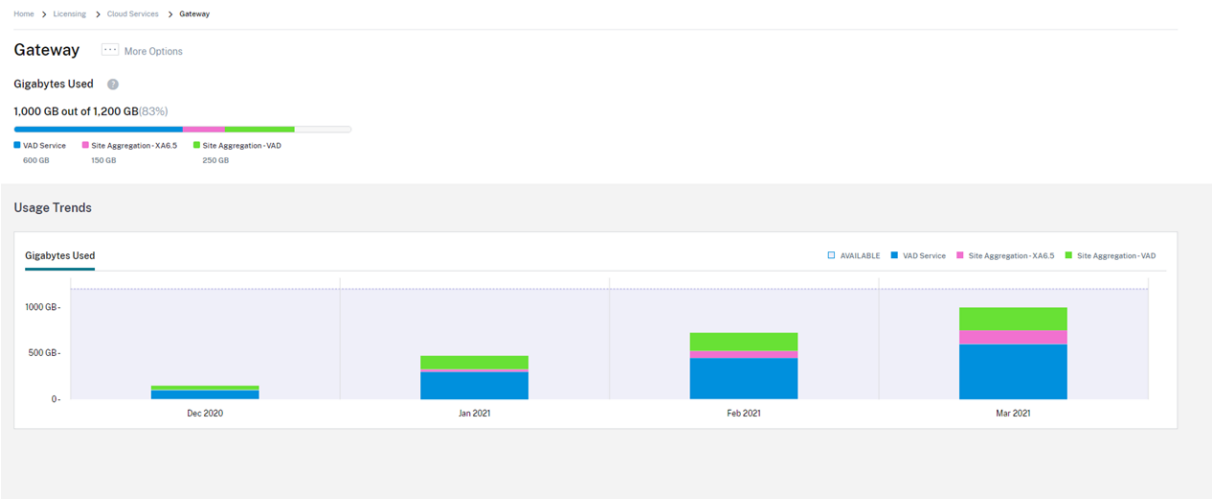
Pour plusieurs abonnements dont les conditions se chevauchent, la quantité de bande passante associée à chaque abonnement est supprimée de la licence lorsque chaque abonnement expire. Par exemple, si vous avez acheté deux abonnements, Citrix Cloud affiche le total des licences et de la bande passante entre les deux abonnements. Lorsque le premier abonnement expire, Citrix Cloud affiche uniquement la bande passante associée à l'abonnement non expiré. Lorsque le dernier abonnement expire, Citrix Cloud affiche la bande passante actuellement consommée et la bande passante totale égale à zéro. Cet affichage persiste pendant la période de grâce du service et la période de rétention des données, comme décrit à la section Prolonger les abonnements aux services de Citrix Cloud.

Tendances d'utilisation

Pour obtenir une vue détaillée des licences, cliquez sur **Afficher détails d'utilisation**.



Vous pouvez ensuite voir une répartition des tendances d'utilisation et des utilisateurs individuels qui consomment des licences de service cloud et la bande passante.



Dans la section **Tendances d'utilisation**, l'onglet **Gigaoctets utilisés** affiche la quantité de bande passante consommée à partir de la bande passante totale disponible. La quantité de bande passante consommée est répartie en fonction de l'accès à l'aide des méthodes suivantes :

- Service VAD : quantité de bande passante utilisée pour la connectivité externe par les utilisateurs de Virtual Apps and Desktops.
- Agrégation de sites : quantité de bande passante utilisée pour lancer des applications et des bureaux locaux via Workspace avec agrégation de sites.

> **Remarque :**
>
> Les tendances d'utilisation sont cumulatives pour la durée de la période d'abonnement actuelle.

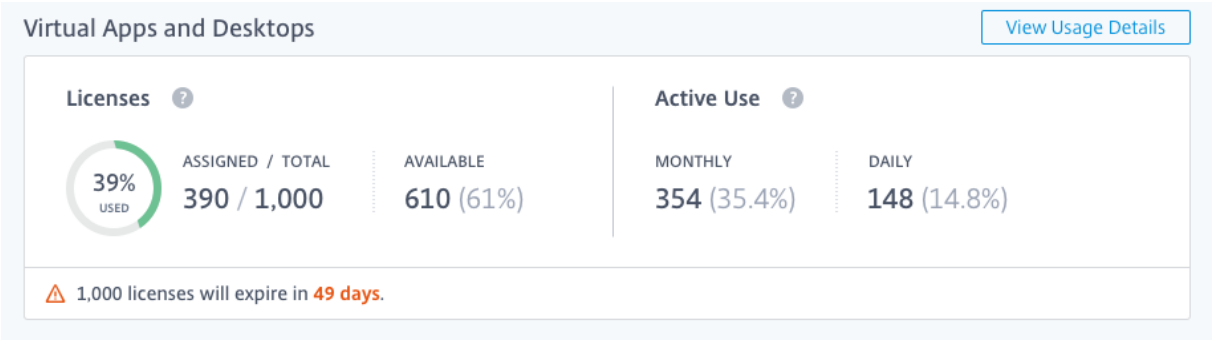
Surveiller les licences et l'utilisation active de Citrix Virtual Apps and Desktops Service (utilisateur/appareil)

November 10, 2020

Attribution de licence

Citrix Cloud attribue une licence lorsqu'un utilisateur unique ou un appareil unique lance une application ou un bureau pour la première fois.

Résumé de l'option Système de licences



Le résumé de l'option Système de licences fournit une vue d'ensemble des informations suivantes :

- Pourcentage du nombre total de licences achetées attribuées. Lorsque le pourcentage approche 100 %, le pourcentage passe du vert au jaune. Si le pourcentage dépasse 100 %, il devient rouge.
- Rapport entre les licences attribuées et les licences achetées et le nombre de licences disponibles restantes.
- Statistiques d'utilisation active sur une base mensuelle et quotidienne :
  - L'utilisation active mensuelle fait référence au nombre d'utilisateurs ou d'appareils uniques qui ont utilisé le service au cours des 30 derniers jours, la valeur la moins élevée étant affichée.
  - L'utilisation active quotidienne fait référence au nombre d'utilisateurs ou d'appareils uniques qui ont utilisé le service au cours des dernières 24 heures, la valeur la moins élevée étant affichée.
- Temps restant avant expiration de l'abonnement au service cloud. Si l'abonnement expire dans les 90 jours suivants, un message d'avertissement apparaît.

Calcul des licences attribuées et de l'utilisation active

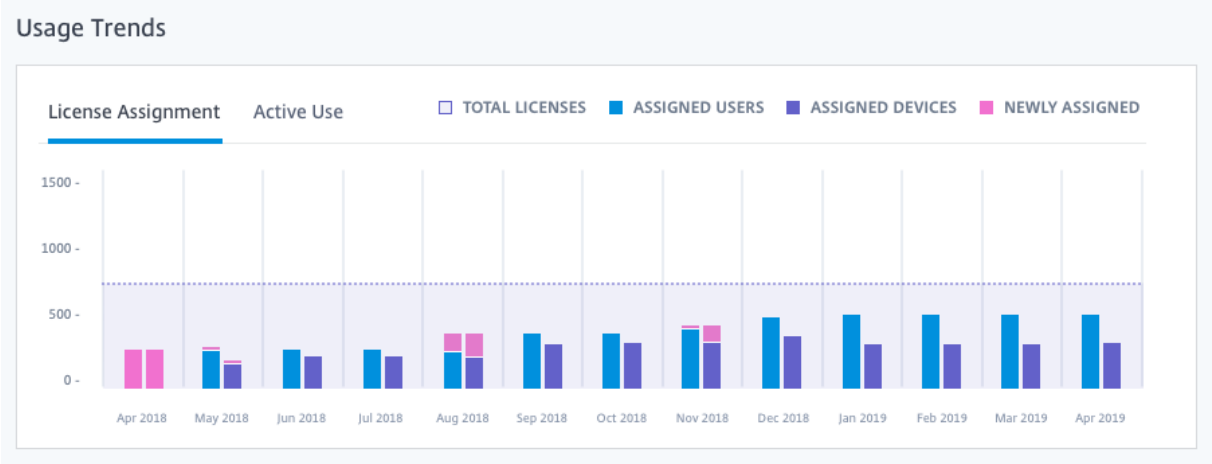
Pour refléter avec précision le modèle de licence Utilisateur/Appareil pour le service Virtual Apps and Desktops, Citrix Cloud compte le nombre d'utilisateurs uniques et d'appareils uniques qui ont utilisé le service. Citrix Cloud utilise la valeur la moins élevée pour mesurer les licences attribuées et l'utilisation active.

Par exemple, si 100 utilisateurs uniques et 50 appareils uniques ont utilisé le service, Citrix Cloud utilise le nombre inférieur (50) pour déterminer le nombre de licences attribuées. Le pourcentage de licences utilisées et le nombre de licences disponibles sont basés sur ces 50 licences attribuées.

Si 10 utilisateurs uniques et 20 appareils uniques ont utilisé le service au cours des 30 derniers jours, Citrix Cloud calcule l'utilisation active mensuelle en fonction du nombre inférieur (10). De même, si 30 utilisateurs uniques et 15 appareils uniques ont été comptés au cours des dernières 24 heures, Citrix Cloud calcule l'utilisation active quotidienne en fonction du nombre inférieur (15).

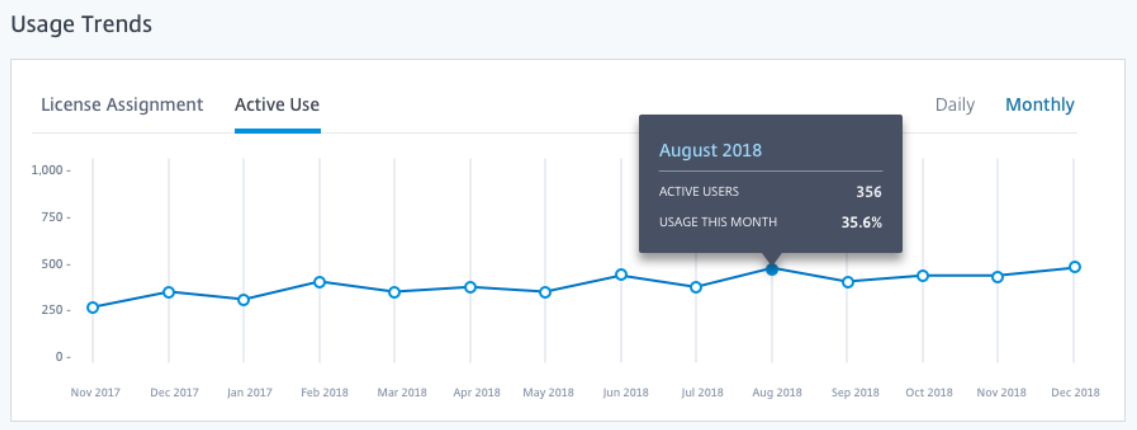
Tendances d'utilisation et activité des licences

Pour obtenir une vue détaillée des licences, cliquez sur **Afficher détails d'utilisation**. Vous pouvez ensuite voir une répartition des tendances d'utilisation et des utilisateurs et des appareils individuels qui consomment des licences de service cloud.



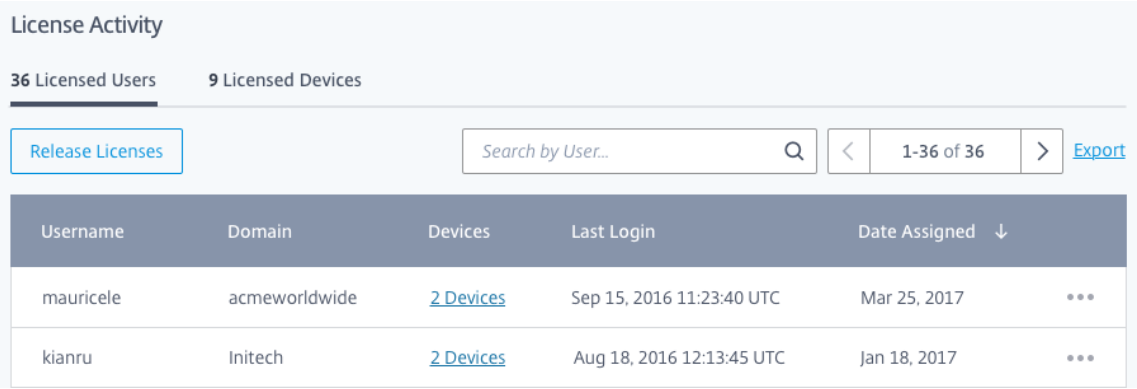
Cette répartition, sous **Tendances d'utilisation**, vous présente les informations suivantes :

- **Nombre total de licences :** nombre total de licences achetées pour le service cloud pour toutes les prestations.
- **Utilisateurs attribués :** nombre cumulé de licences attribuées aux utilisateurs jusqu'au mois en cours.
- **Appareils attribués :** nombre cumulé de licences attribuées aux appareils jusqu'au mois en cours. Si ce nombre semble particulièrement élevé pour un mois donné, cela pourrait être le résultat de lancements d'applications ou de bureaux effectués via un navigateur Web. Pour réduire ce nombre, Citrix recommande d'utiliser une application Workspace native ou un client Receiver à la place.
- **Nouvellement attribuées :** nombre de nouvelles licences qui ont été attribuées chaque mois. Par exemple, un utilisateur accède au service cloud pour la première fois en juillet et se voit attribuer une licence. Cette licence est comptée comme « nouvellement attribuée » pour le mois de juillet.
- **Utilisation active :** tendances quotidiennes et mensuelles de l'utilisation active au cours du mois civil et de l'année civile précédente, respectivement.

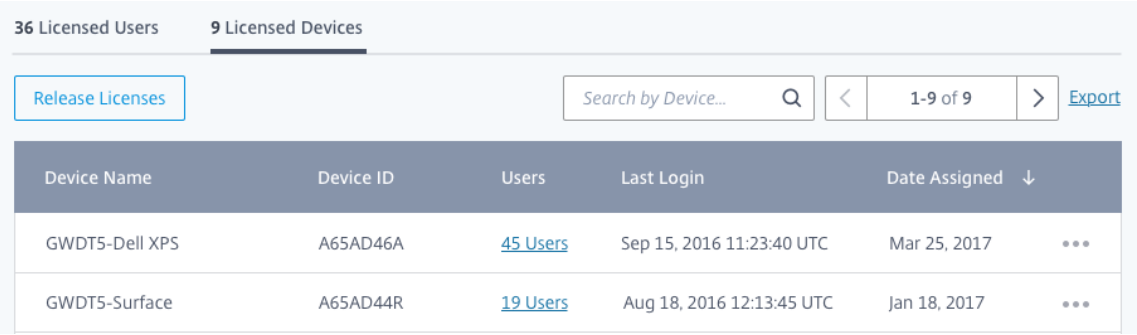


La section **Activité des licences** affiche également les informations suivantes :

- Liste des utilisateurs individuels qui ont attribué des licences, y compris les appareils associés



- Liste des appareils auxquels des licences ont été attribuées, y compris les utilisateurs associés



- Date à laquelle une licence a été attribuée à l'utilisateur ou à l'appareil

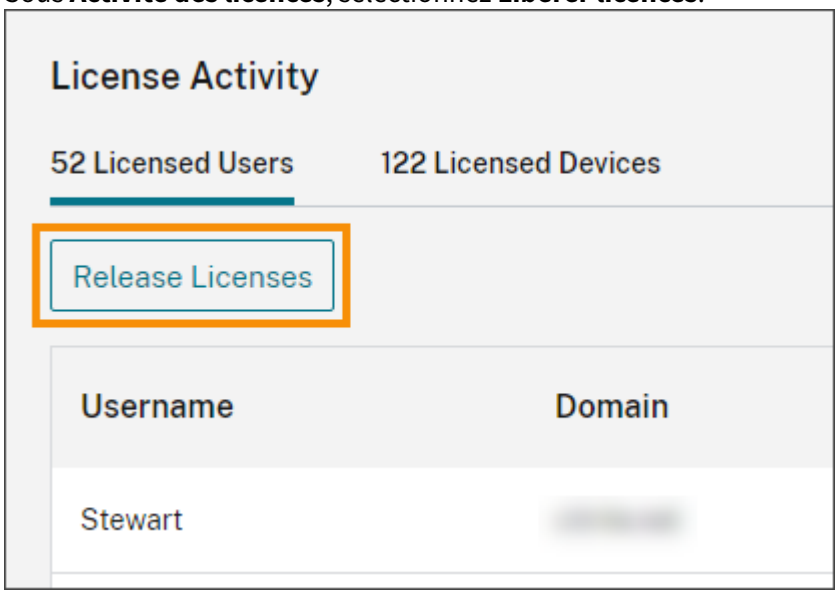
Libérer des licences attribuées

Vous pouvez libérer des licences pour les utilisateurs qui n'ont pas lancé d'application ou de bureau au cours des 30 derniers jours. Vous pouvez libérer des licences pour les appareils si aucune application ou aucun bureau n'a été lancé(e) depuis l'appareil au cours des 30 derniers jours. Vous pouvez libérer plusieurs licences en bloc ou individuellement. (Cela diffère des déploiements Citrix Virtual Apps and Desktops locaux, où les licences inactives sont libérées automatiquement après 90 jours.)

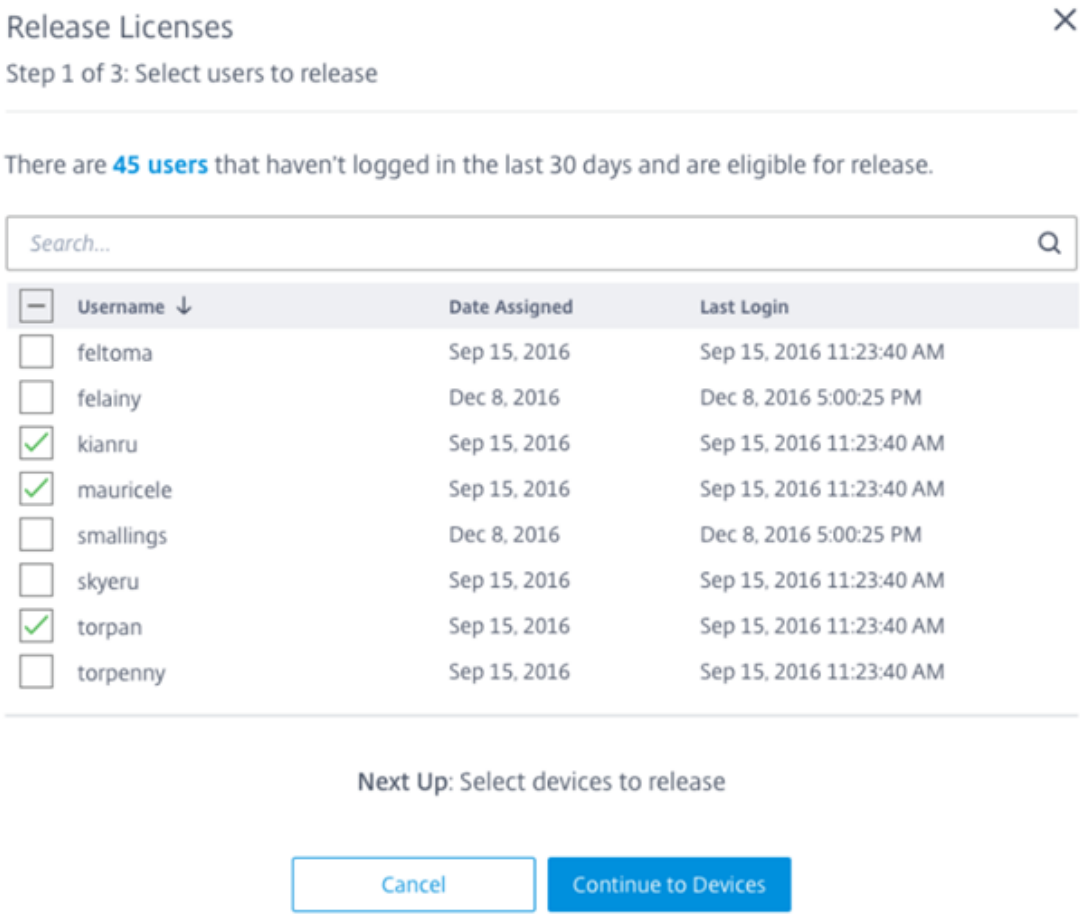
Lorsqu'une licence est libérée, le nombre de licences restantes augmente et le nombre de licences attribuées diminue en conséquence. Après libération d'une licence, l'utilisateur peut acquérir une autre licence en se connectant et en utilisant le service cloud.

Pour libérer plusieurs licences attribuées

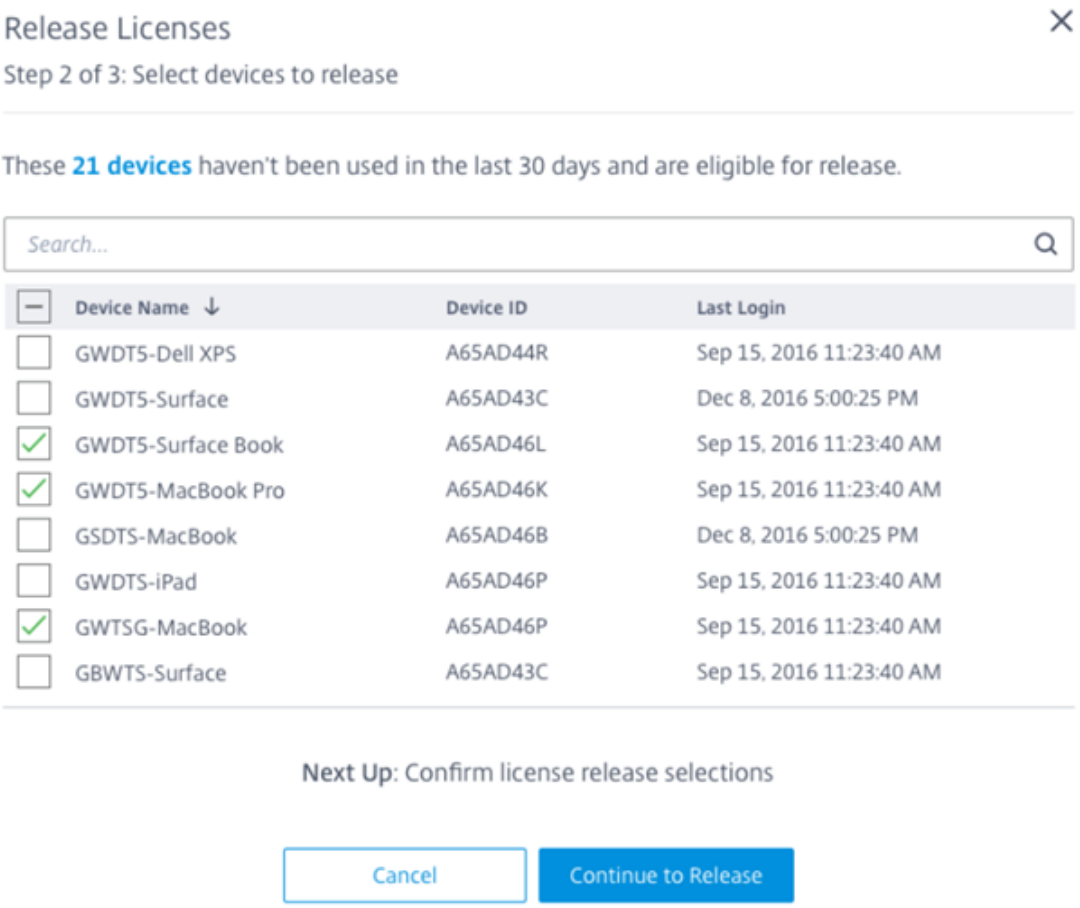
1. Sous **Activité des licences**, sélectionnez **Libérer licences**.



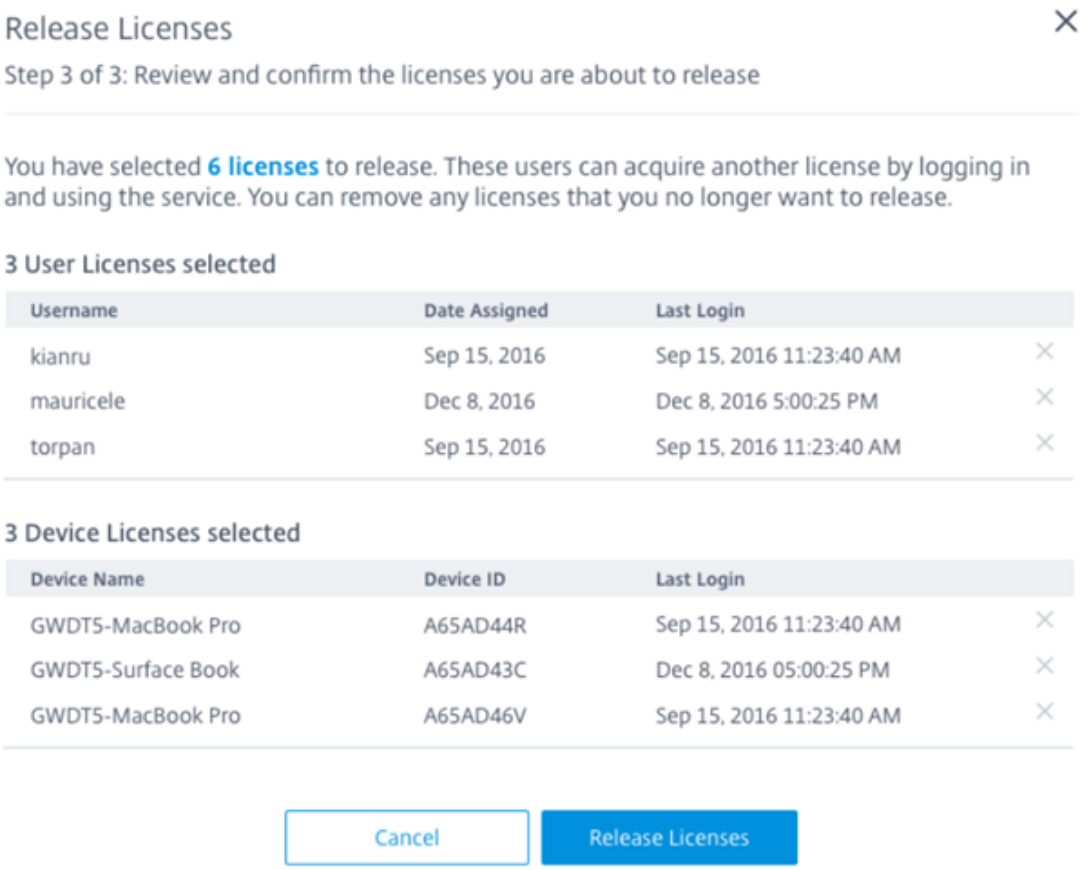
2. Dans la liste, sélectionnez les utilisateurs que vous souhaitez gérer et sélectionnez **Continuer vers Appareils**.



3. Sélectionnez les appareils que vous souhaitez gérer et sélectionnez **Continuer vers Libérer**.



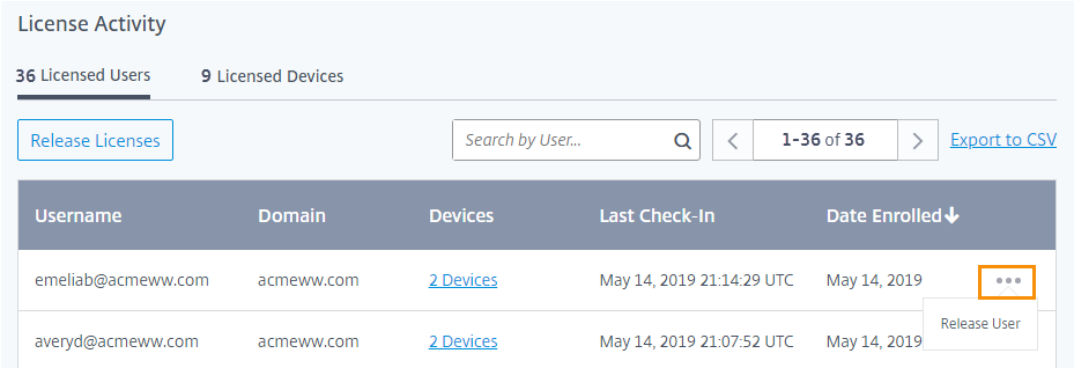
4. Vérifiez les licences que vous avez sélectionnées et sélectionnez **Libérer licences**.



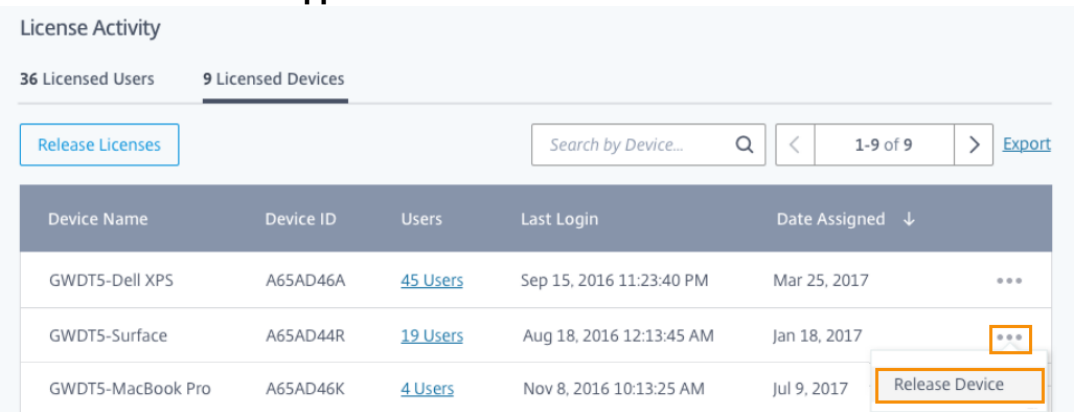
Pour libérer une seule licence attribuée

Vous pouvez libérer des licences individuelles à partir de la liste **Utilisateurs sous licence** ou de la liste **Appareils sous licence**. Ces listes affichent des boutons de points de suspension disponibles uniquement pour les utilisateurs et les appareils disposant de licences pouvant être libérées. Le bouton représentant des points de suspension est inactif pour les utilisateurs individuels et les appareils individuels qui ont lancé une application ou un bureau au cours des 30 derniers jours.

1. Sous **Activité des licences**, sélectionnez l'onglet **Utilisateurs sous licence** ou **Appareils sous licence**.
2. Identifiez l'utilisateur ou l'appareil que vous souhaitez gérer et pour lequel vous souhaitez libérer la licence :
   a) Pour libérer la licence d'un utilisateur unique, cliquez sur le bouton représentant des points de suspension et sélectionnez **Libérer l'utilisateur**.



b) Pour libérer un seul appareil, cliquez sur le bouton représentant des points de suspension et sélectionnez **Libérer appareil**.



3. Vérifiez votre sélection, puis sélectionnez **Continuer**.
4. Lorsque vous êtes invité à confirmer la libération, sélectionnez **Libérer**.

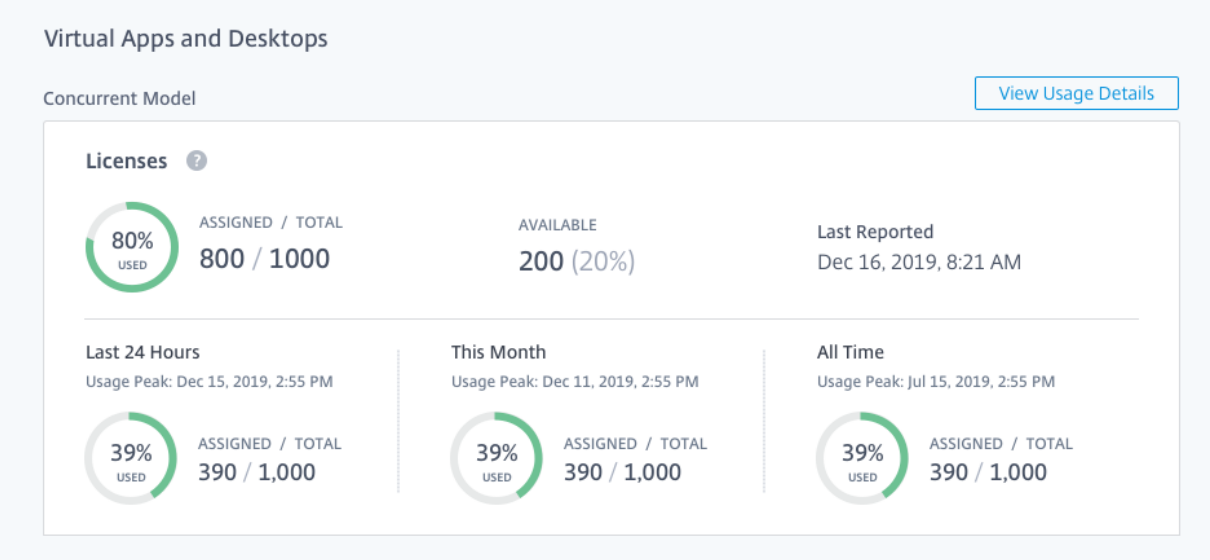
Surveiller les licences et l'utilisation maximale de Citrix Virtual Apps and Desktops Service (simultané)

April 28, 2021

Attribution de licence

Citrix Cloud attribue une licence lorsqu'un utilisateur lance une application ou un bureau sur son appareil. Lorsque l'utilisateur ferme ou se déconnecte de la session, la licence n'est plus attribuée. Étant donné que l'attribution de licences peut changer en fonction du nombre d'appareils accédant aux applications ou aux bureaux à un moment donné, Citrix Cloud évalue le nombre de licences en cours d'utilisation toutes les cinq minutes. Pour plus d'informations sur le modèle de licences simultanées, consultez Licences simultanées.

Résumé de l'option Système de licences



Le résumé de l'option Système de licences fournit une vue d'ensemble des informations suivantes :

- Pourcentage du nombre total de licences achetées actuellement utilisées lors de la dernière évaluation par Citrix Cloud des licences utilisées. Citrix Cloud calcule ce pourcentage toutes les cinq minutes en fonction des appareils uniques disposant de connexions actives au service.
- Ratio entre les licences attribuées et le nombre total de licences achetées et le nombre de licences disponibles restantes. Le **total** indiqué dans ce ratio représente le nombre total de licences actuellement détenues (à la date et à l'heure du « Dernier rapport »).
- Statistiques d'utilisation maximale. Lors du calcul du nombre maximal de licences utilisées, Citrix Cloud récupère le nombre maximal de licences utilisées dans les périodes suivantes :
  - **Dernières 24 heures :** nombre maximal de licences utilisées simultanément au cours de la dernière période de 24 heures.
  - **Ce mois-ci :** nombre maximal de licences utilisées simultanément depuis le début du mois en cours.
  - **Toute période :** nombre maximal de licences utilisées simultanément depuis le début de l'abonnement.

  Le **total** indiqué pour ces périodes d'utilisation maximale représente le nombre total de licences détenues à ce moment donné. Si le nombre total de licences détenues augmente ou diminue, et que cela entraîne une augmentation des licences attribuées, le **total** change pour refléter le nouveau nombre de licences détenues à ce moment donné. Toutefois, s'il n'y a pas de pic d'utilisation correspondant, le **total** ne change pas.

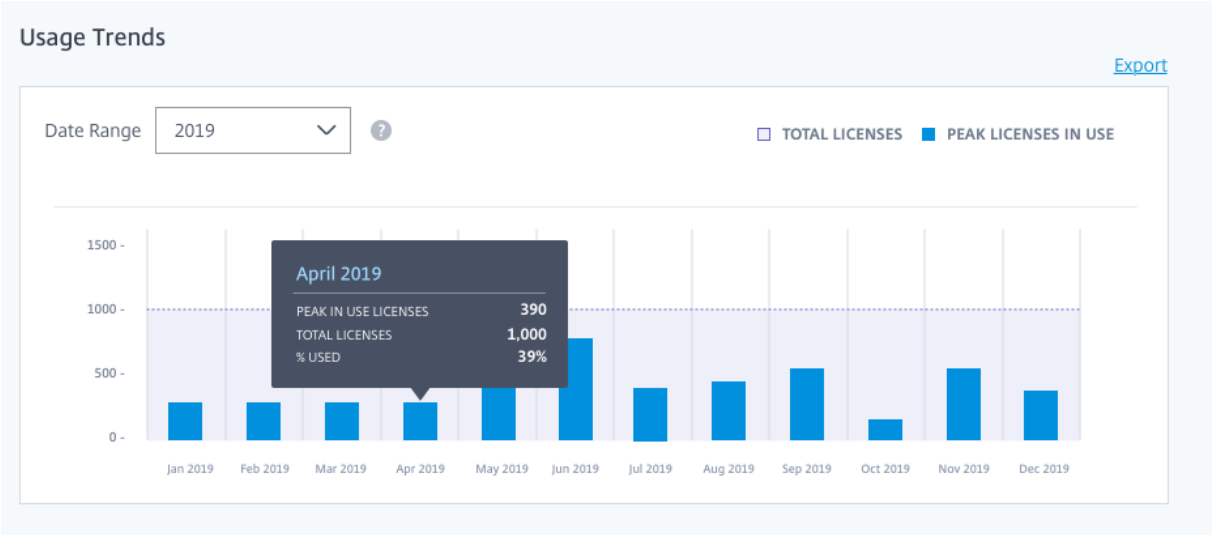
Calcul du nombre maximal de licences utilisées

Pour refléter avec précision le modèle de licences simultanées pour Virtual Apps and Desktops Service, Citrix Cloud compte le nombre d'appareils uniques qui accèdent au service simultanément toutes les cinq minutes. Si le nombre est supérieur à l'utilisation maximale actuelle affichée, Citrix Cloud affiche la nouvelle utilisation maximale avec la date et l'heure auxquelles elle a été atteinte. Si le nombre est inférieur à l'utilisation maximale actuelle, l'utilisation maximale actuelle ne change pas.

> **Important :**
>
> Si vous utilisez la console de surveillance dans Director pour obtenir des informations sur les sessions simultanées, sachez que le rapport de monitoring fournit une interprétation différente des sessions simultanées et ne reflète pas avec précision le nombre de licences simultanées utilisées. Pour plus d'informations sur les différences entre les rapports de monitoring et les rapports de licence, consultez Questions fréquentes.

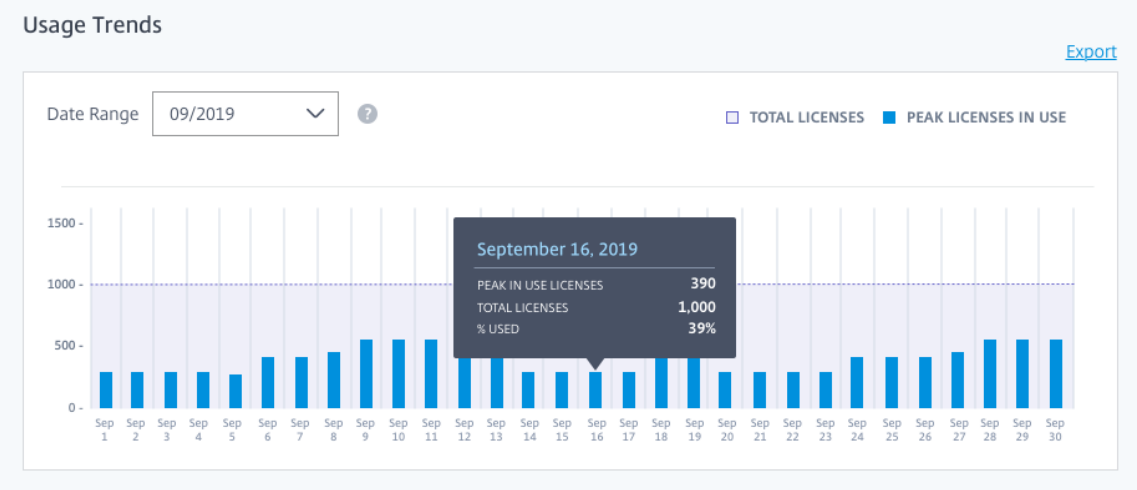
Tendances d'utilisation et activité des licences

Pour afficher l'historique de vos licences, cliquez sur **Afficher détails d'utilisation**.

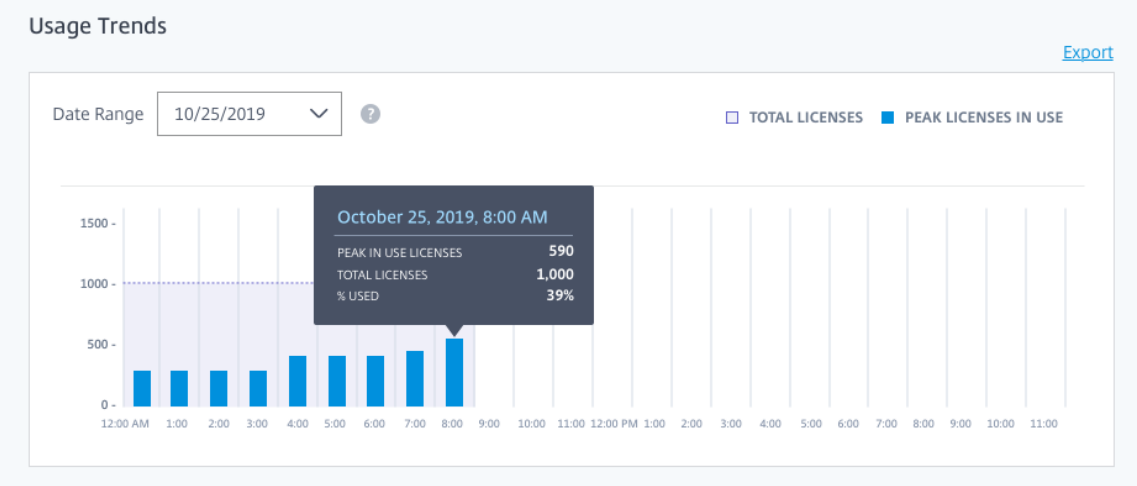


La répartition **Tendances d'utilisation** vous présente les informations suivantes :

- **Nombre total de licences :** nombre total de licences simultanées achetées.
- **Nombre maximal de licences utilisées :** nombre maximal de licences attribuées pour la plage de dates que vous sélectionnez. Par défaut, Citrix Cloud affiche les pics d'utilisation pour chaque mois de l'année civile en cours. Pour accéder à l'utilisation maximale mensuelle ou horaire, sélectionnez le mois ou le jour à afficher dans le menu **Plage de dates**.



Si la plage de dates que vous sélectionnez n'est pas encore terminée, Citrix Cloud affiche l'utilisation maximale actuelle correspondant à la dernière période. Par exemple, si vous accédez à un jour qui n'est pas encore fini, le nombre maximal de licences est affiché pour chaque heure jusqu'à l'instant présent. Si le nombre maximal de licences augmente au cours du prochain intervalle de cinq minutes, Citrix Cloud met à jour l'utilisation maximale pour l'heure actuelle.



Surveiller les licences et l'utilisation active de Citrix Virtual Apps and Desktops Standard pour Azure Service

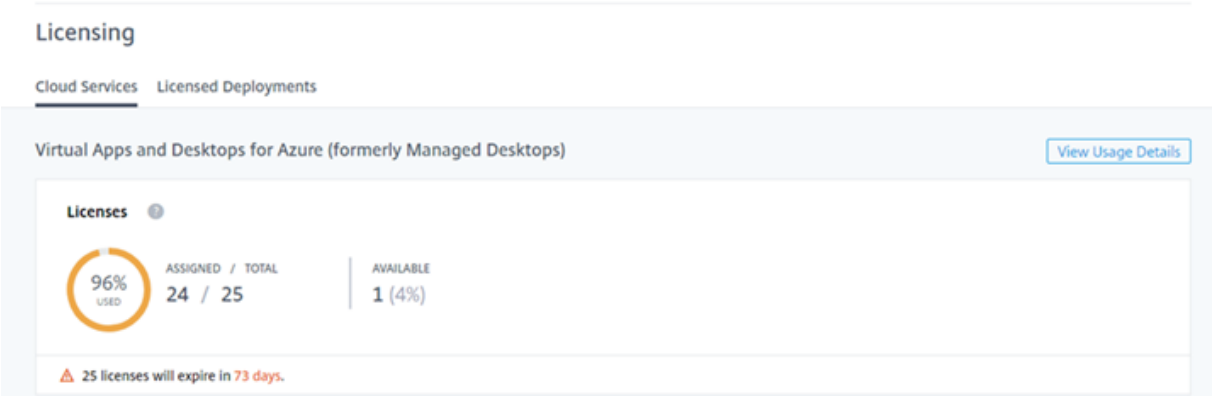
January 22, 2021

Cet article décrit l'expérience de création de rapports sur les licences cloud pour le modèle de licence **utilisateur/périphérique** uniquement.

Attribution de licence

Citrix Cloud attribue une licence lorsqu'un utilisateur unique ou un appareil unique lance un bureau pour la première fois.

Résumé de l'option Système de licences



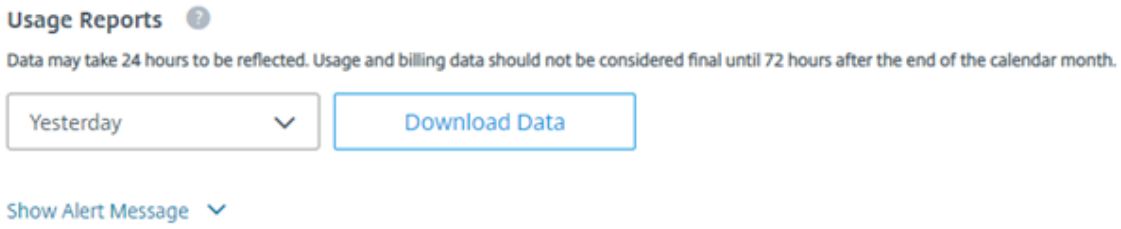
Le résumé de l'option Système de licences fournit une vue d'ensemble des informations suivantes :

- Pourcentage du nombre total de licences achetées attribuées (utilisées). Lorsque le pourcentage approche 100 %, le pourcentage passe du vert au jaune. Si le pourcentage dépasse 100 %, il devient rouge.
- Rapport entre les licences attribuées et les licences achetées et le nombre de licences disponibles restantes.

Cliquez sur **Afficher détails d'utilisation** pour afficher une répartition des rapports et des tendances d'utilisation, ainsi qu'une liste des utilisateurs qui consomment des licences Citrix Virtual Apps and Desktops Standard pour Azure.

> **Remarque :**
>
> Citrix Virtual Apps and Desktops Standard pour Azure est la nouvelle appellation de Citrix Managed Desktops. Certains affichages peuvent contenir l'ancien nom.

Rapports d'utilisation



Vous pouvez télécharger les informations d'utilisation pour un intervalle standard ou spécifié.

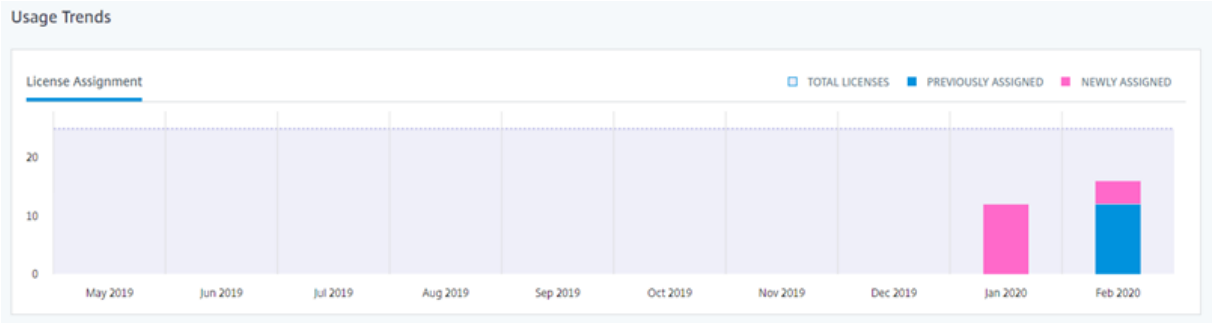
Ces informations comprennent l'utilisation des compteurs pour :

- VM Azure
- Connexions réseau, telles que l'appairage de réseaux virtuels (Vnet)
- Éléments de stockage Azure, tels que les disques gérés, les objets blob de blocs et les objets blob de page

Les données peuvent prendre jusqu'à 72 heures après la fin d'un jour/mois pour refléter toutes les utilisations.

Cliquez sur **Télécharger les données** pour générer et télécharger un fichier CSV sur votre ordinateur local.

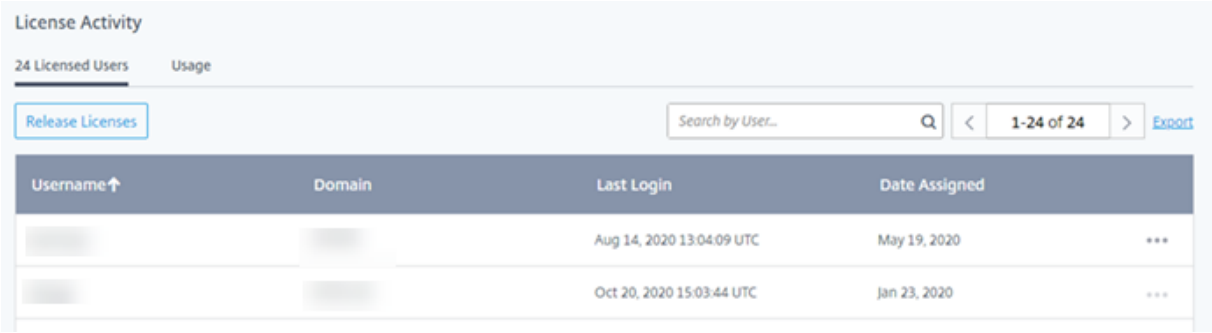
Tendances d'utilisation et activité des licences



La répartition **Tendances d'utilisation** vous présente les informations suivantes :

- **Nombre total de licences :** nombre total de licences achetées pour le service cloud pour toutes les prestations.
- **Précédemment attribuées :** nombre de licences qui ont été attribuées au cours du mois précédent. Par exemple, un utilisateur accède au service cloud pour la première fois en juillet et se voit attribuer une licence. Cette licence est comptée comme « nouvellement attribuée » pour le mois de juillet. Pour le mois d'août, cette licence est comptée comme « précédemment attribuée ».
- **Nouvellement attribuées :** nombre de nouvelles licences qui ont été attribuées chaque mois. Par exemple, un utilisateur accède au service cloud pour la première fois en juillet et se voit attribuer une licence. Cette licence est comptée comme « nouvellement attribuée » pour le mois de juillet.

La section **Activité des licences** affiche la liste des utilisateurs individuels qui ont des licences attribuées, ainsi que la date à laquelle une licence a été attribuée à l'utilisateur.



Libérer des licences attribuées

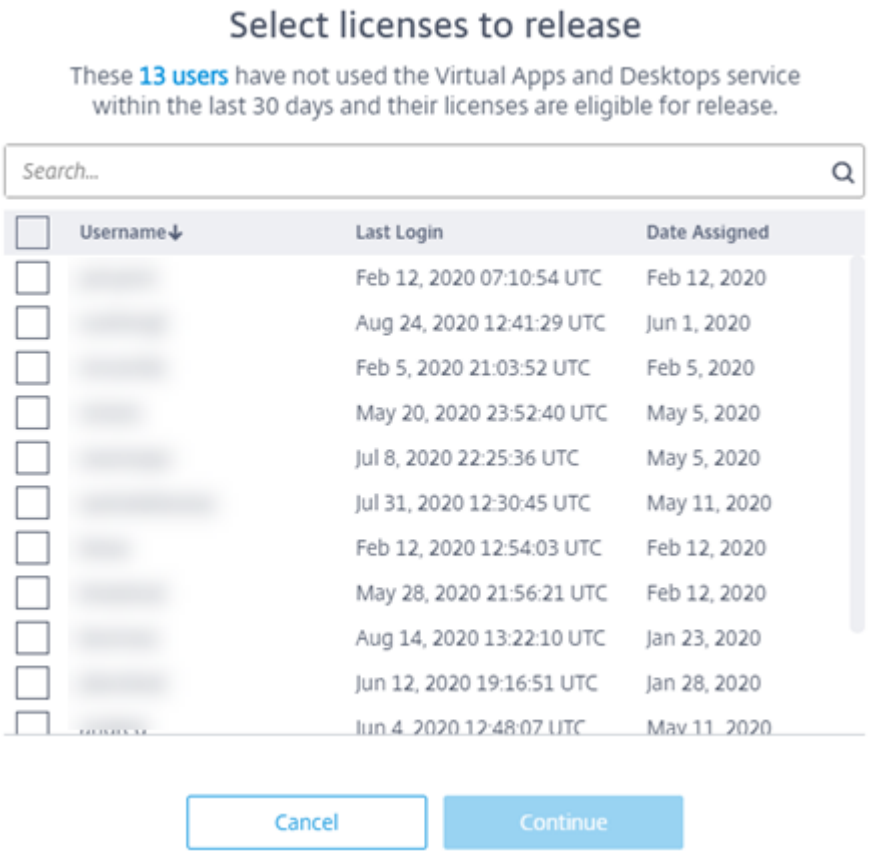
Abonnements annuels au service : si vous disposez d'un abonnement annuel, vous pouvez libérer des licences pour les utilisateurs qui n'ont pas lancé d'application ou de bureau au cours des 30 derniers jours. Vous pouvez libérer plusieurs licences en bloc ou individuellement.

Abonnements mensuels au service: si vous disposez d'un abonnement mensuel, vous pouvez libérer des licences le premier jour de chaque mois, quelle que soit la période d'inactivité.

Lorsqu'une licence est libérée, le nombre de licences restantes augmente et le nombre de licences attribuées diminue en conséquence. Après libération d'une licence, l'utilisateur peut acquérir une autre licence en se connectant et en utilisant le service cloud.

Pour libérer plusieurs licences attribuées

1. Sous **Activité des licences**, sélectionnez **Libérer licences**.
2. Dans la liste, sélectionnez les utilisateurs que vous souhaitez gérer et sélectionnez **Continuer**.



3. Vérifiez les licences que vous avez sélectionnées et sélectionnez **Libérer licences**.

Pour libérer une seule licence attribuée

Vous pouvez libérer des licences individuelles à partir de la liste **Activité des licences**. La liste affiche des boutons de points de suspension sur lesquels uniquement les utilisateurs disposant de licences pouvant être libérées peuvent cliquer.

1. Sous **Activité des licences**, localisez l'utilisateur que vous souhaitez gérer. Dans le menu représentant des points de suspension de cet utilisateur, sélectionnez **Libérer utilisateur**.
2. Vérifiez votre sélection, puis sélectionnez **Continuer**.
3. Lorsque vous êtes invité à confirmer la libération, sélectionnez **Libérer**.

Enregistrer des produits locaux avec Citrix Cloud

July 21, 2021

Vous pouvez facilement enregistrer votre produit Citrix local en utilisant l'activation rapide (code court) via Citrix Cloud. Selon votre produit, ce code à 8 chiffres peut être généré pendant le processus

d'installation du produit ou lorsque vous exécutez la console de gestion du produit. À l'invite de l'enregistrement du produit, le code est demandé à Citrix Cloud, puis affiché. Vous pouvez ensuite copier et coller ce code ou l'entrer manuellement dans Citrix Cloud.

Enregistrer un serveur de licences local

L'enregistrement de produit est actuellement pris en charge avec le serveur de licences Citrix. Pour utiliser cette fonctionnalité, vous devez effectuer les tâches suivantes :

- Activez Call Home.
- Enregistrez votre serveur de licences auprès de Citrix Cloud à partir de la console Citrix Licensing Manager.

Pour enregistrer votre serveur de licences local auprès de Citrix Cloud, consultez Enregistrer et supprimer l'enregistrement de votre serveur de licences Citrix.

Exigences en termes de connectivité

Pour enregistrer vos produits locaux, assurez-vous que les adresses suivantes peuvent être contactées :

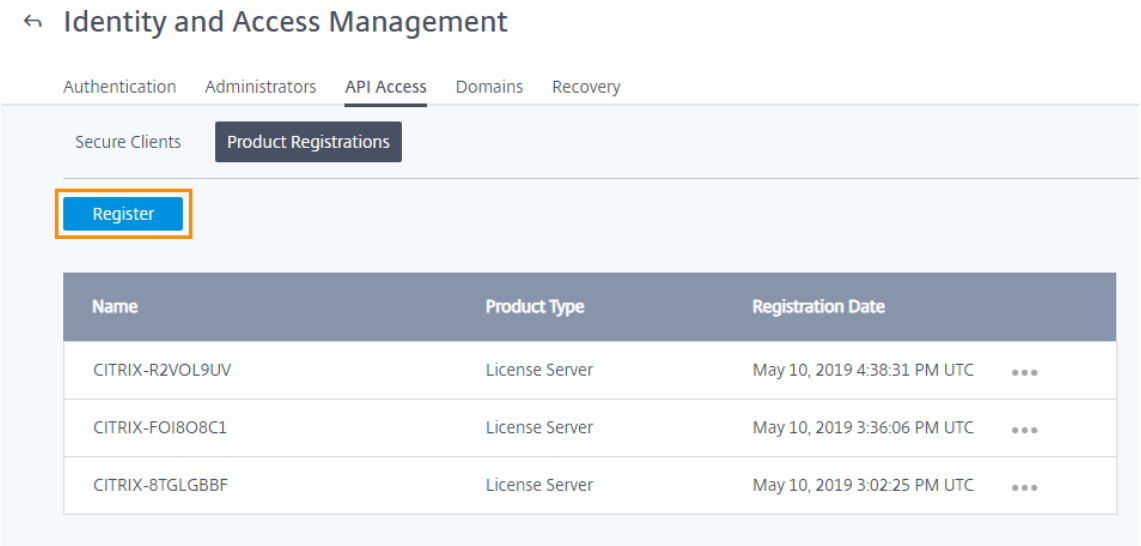
- `https://trust.citrixnetworkapi.net` (pour récupérer un code)
- `https://trust.citrixworkspacesapi.net/` (pour confirmer que le serveur de licences est enregistré)
- `https://cis.citrix.com` (pour le téléchargement de données)
- `https://core-eastus-release-a.citrixworkspacesapi.net`
- `https://core.citrixworkspacesapi.net`
- `ocsp.digicert.com port 80`
- `crl3.digicert.com port 80`
- `crl4.digicert.com port 80`
- `ocsp.entrust.net port 80`
- `crl.entrust.net port 80`

Si vous utilisez un serveur proxy avec le serveur de licences Citrix, assurez-vous que le serveur proxy est configuré comme décrit à la section Configurer un serveur proxy de la documentation produit de Gestion des licences.

Enregistrer un produit

1. Dans le menu Citrix Cloud, sélectionnez **Gestion des identités et des accès**.

2. Sélectionnez **Accès aux API > Enregistrements de produits**, puis sélectionnez **Enregistrer**.

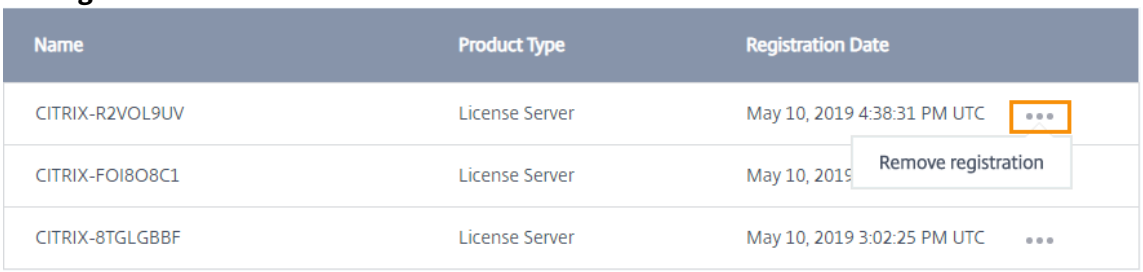


3. Entrez le code d'enregistrement de produit à 8 chiffres pour votre produit Citrix et cliquez sur **Continuer**.
4. Vérifiez les détails de l'enregistrement, puis cliquez sur **Enregistrer**.

Supprimer un enregistrement de produit

Si vous supprimez des serveurs exécutant un produit Citrix enregistré de votre environnement, la page Enregistrements de produits affiche toujours les serveurs. Suivez les étapes suivantes pour supprimer les serveurs de Citrix Cloud. Si nécessaire, vous pouvez enregistrer à nouveau le produit ultérieurement pour afficher les serveurs sur la page Enregistrements de produits.

1. Dans la page Enregistrements de produits, recherchez le serveur à supprimer.
2. Cliquez sur le bouton représentant des points de suspension et sélectionnez **Supprimer l'enregistrement**.



3. Lorsque vous y êtes invité, sélectionnez **Supprimer**.

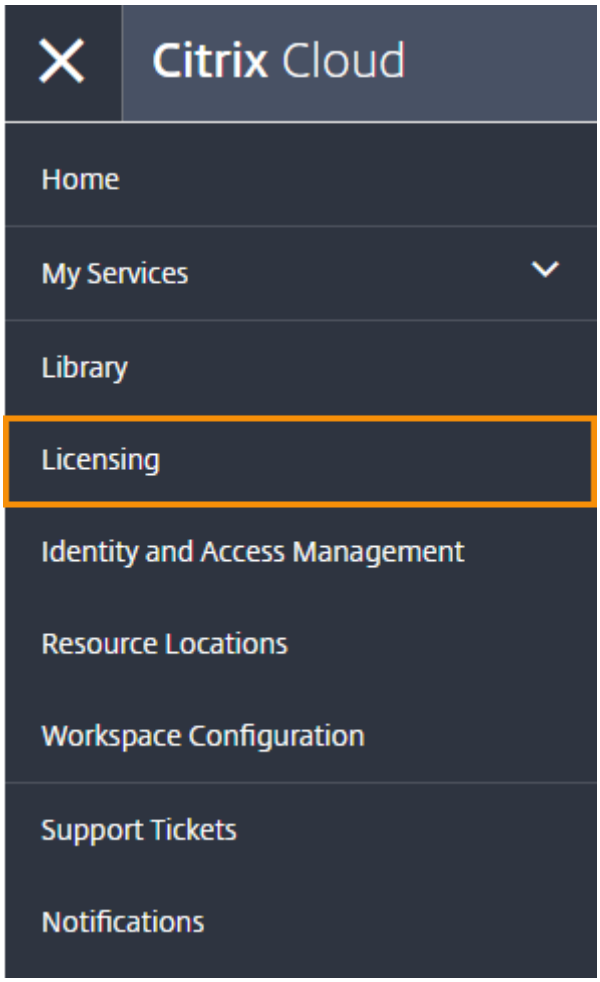
Surveiller les licences et l'utilisation sur les déploiements locaux

May 28, 2020

L'expérience de déploiements sous licence dans Citrix Cloud comprend les tâches suivantes :

- Enregistrement du produit : enregistrez vos serveurs de licences Citrix existants auprès de Citrix Cloud pour obtenir des informations supplémentaires sur l'utilisation et des rapports sur vos déploiements. Pour plus d'informations sur l'enregistrement de vos serveurs de licences, reportez-vous à la section Enregistrer des produits locaux avec Citrix Cloud.
- État du serveur de licences : affichez l'état de vos serveurs de licences Citrix pour identifier ceux qui génèrent avec succès des rapports sur l'utilisation et la date à laquelle ils ont généré des rapports d'utilisation pour la dernière fois à Citrix Cloud.
- Informations sur l'utilisation : affichez le nombre de licences installées et utilisées sur vos serveurs de licences Citrix et découvrez les tendances historiques d'utilisation des licences.

Pour afficher les informations sur l'utilisation du serveur de licences Citrix, sélectionnez **Système de licences** dans le menu de la console, puis sélectionnez **Déploiements sous licence**.



Conditions préalables

Pour utiliser les informations d'utilisation du serveur de licences Citrix, assurez-vous de disposer des éléments suivants :

- Version 11.15.0.0 ou ultérieure du serveur de licences Citrix
- Un compte Citrix Cloud
- Accès réseau du serveur de licences Citrix vers Citrix Cloud

Produits pris en charge

Les informations d'utilisation du serveur de licences Citrix sont disponibles pour toutes les éditions de Virtual Apps and Desktops sous les modèles de licences utilisateur/appareil et de licences simultanées.

Afficher l'utilisation locale des licences produit

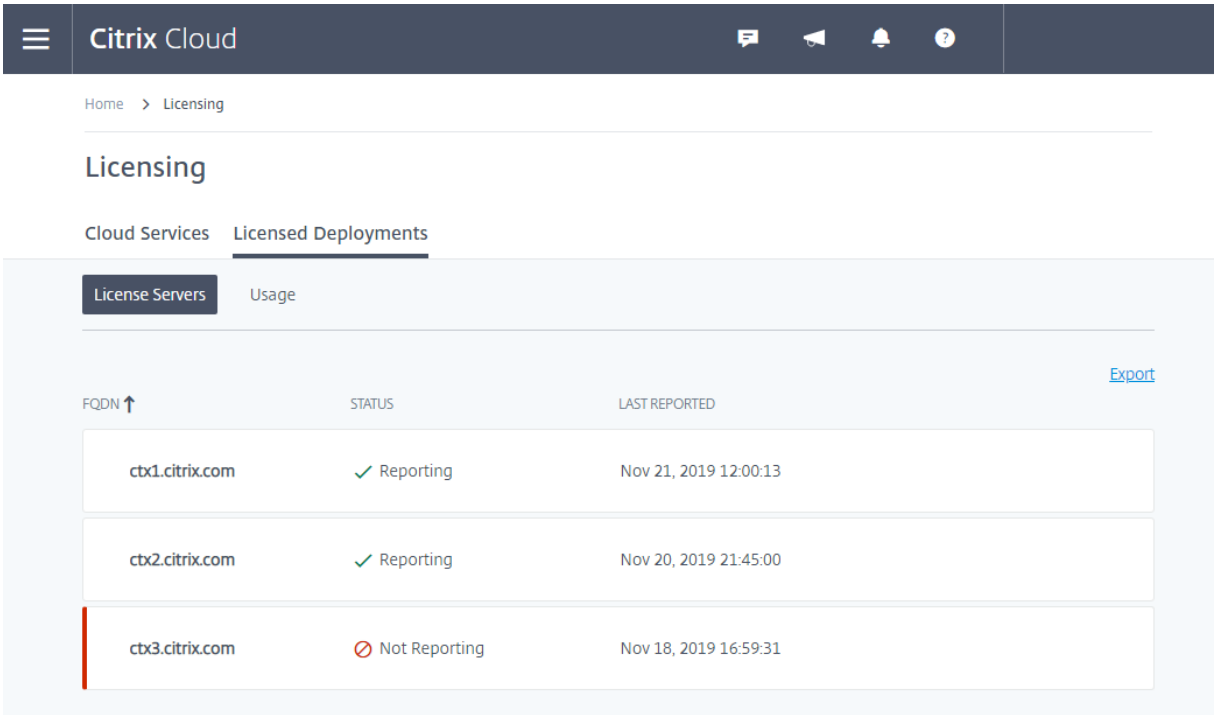
Les informations sur l'utilisation du serveur de licences Citrix fournissent une visibilité sur l'utilisation des licences dans l'ensemble de votre parc Citrix. Après avoir activé les informations d'utilisation pour vos serveurs de licences et les avoir enregistrées auprès de Citrix Cloud, vous pouvez accéder aux rapports d'utilisation. Ces derniers vous permettent de :

- Déterminer le nombre de serveurs de licences déployés et enregistrés et s'ils rapportent des informations d'utilisation à Citrix Cloud.
- Bénéficier d'une visibilité sur l'utilisation des licences utilisateur/appareil et des licences simultanées pour Virtual Apps and Desktops.
- Obtenir un aperçu sur l'utilisation agrégée des licences utilisateur/appareil et des licences simultanées sur de multiples déploiements.
- Comprendre l'utilisation historique des licences et les tendances mensuelles d'utilisation des licences.
- Afficher l'heure de la dernière connexion d'utilisateurs spécifiques.
- Comparer le nombre de licences installées par rapport aux licences utilisées sur les serveurs de licences Citrix.
- Surveiller le découvert de licences.
- Afficher une ventilation de l'utilisation des licences utilisateur/appareil et des licences simultanées.

Pour plus d'informations sur l'enregistrement de vos serveurs de licences, reportez-vous à la section Enregistrer des produits locaux avec Citrix Cloud.

Afficher l'état du serveur de licences

La vue de l'état du serveur de licences affiche chacun des serveurs de licences générant des rapports d'utilisation sur Citrix Cloud.



Les serveurs de licences affichent l'état « Rapports » s'ils ont correctement chargé l'utilisation sur Citrix Cloud au cours des trois derniers jours. Les serveurs de licences affichent l'état « Pas de rapport » s'ils ont signalé une utilisation au cours des 30 derniers jours mais qu'ils n'en n'ont signalé aucune au cours des trois derniers jours. Les serveurs de licences qui n'ont pas signalé d'utilisation au cours des 30 derniers jours sont supprimés de la liste.

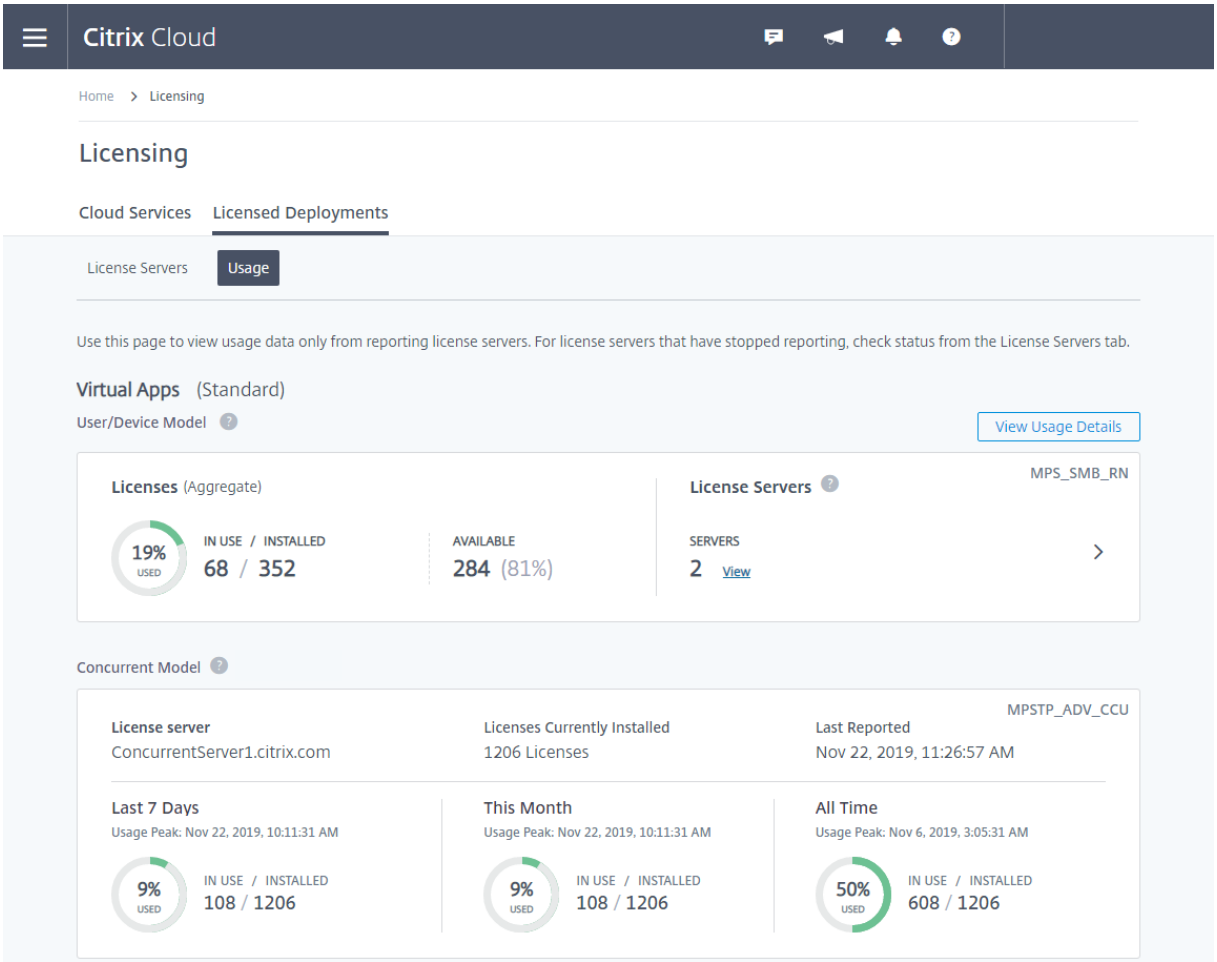
Impact de l'état du serveur de licences sur les vues d'utilisation des licences

L'état des rapports et la date du dernier rapport d'un serveur de licences déterminent si l'utilisation d'un serveur de licences particulier est incluse ou non dans les vues et rapports d'utilisation.

- Les licences installées et en cours d'utilisation sont basées exclusivement sur les données provenant des serveurs de licences de reporting. Si un serveur de licences est répertorié comme « Pas de rapport », les licences installées et en cours d'utilisation à partir de ce serveur de licences ne sont pas reflétées dans l'expérience d'utilisation.
- La date du dernier rapport pour chaque serveur de licences détermine l'état de mise à jour des informations d'utilisation des licences dans l'expérience d'utilisation. Les rapports d'utilisation des licences affichés sont aussi récents que l'heure du Dernier rapport pour chaque serveur de licences.
- Les serveurs de licences Citrix configurés pour générer des rapports d'utilisation et enregistrés auprès de Citrix Cloud actualisent les informations d'utilisation une fois par jour. Si nécessaire, vous pouvez forcer une mise à jour à partir de la console de gestion Citrix Licensing Manager sur le serveur de licences.

Utilisation des licences

L'onglet Utilisation fournit une vue consolidée de l'utilisation des licences dans vos déploiements Citrix. Les informations de licence de chaque serveur de licences de reporting sont combinées dans une seule vue. Cette vue vous offre une vision globale de vos licences sur de nombreux déploiements et serveurs de licences différents.



L'utilisation des licences est organisée et agrégée sur plusieurs serveurs de licences en fonction de l'édition du produit et du modèle de licence. Une fiche récapitulative de l'utilisation des licences est affichée pour chaque édition de licence unique trouvée sur tous les serveurs de licences de reporting. Une fiche récapitulative est affichée pour chaque édition de produit détectée.

Utilisation maximale des licences pour le modèle de licences simultanées

L'expérience de création de rapports pour les licences simultanées est organisée autour des points de données suivants :

- Licences installées : nombre de licences installées sur chaque serveur de licences.

- Nombre maximal de licences utilisées : nombre maximal de licences utilisées dans une période donnée.

Lors du calcul du nombre maximal de licences utilisées, Citrix Cloud récupère le nombre maximal de licences utilisées dans les périodes suivantes :

- 7 derniers jours : nombre maximal de licences utilisées à la fois au cours des sept derniers jours.
- Ce mois-ci : nombre maximal de licences utilisées en même temps au cours du mois en cours.
- En permanence : nombre maximal de licences utilisées en même temps depuis l'enregistrement du serveur de licences auprès de Citrix Cloud.

> **Important :**
>
> Les données de ces périodes peuvent ne pas correspondre au nombre de licences utilisées sur le serveur de licences. Le serveur de licences indique uniquement le nombre de licences utilisées à un moment donné. Citrix Cloud reçoit ces points de données individuels et calcule le nombre maximal pour ces périodes.

Considérations relatives à l'interprétation de l'utilisation des licences

Les licences Citrix prennent en charge de nombreux scénarios d'utilisation et comprennent des informations détaillées. Gardez à l'esprit les considérations suivantes lors de la surveillance de l'utilisation :

- Les informations d'utilisation sont basées sur les licences installées sur chacun des serveurs de licences de reporting. Si un serveur de licences vient à manquer de licences disponibles, vous pouvez allouer et placer des licences supplémentaires sur le serveur de licences pour augmenter le nombre de licences disponibles.
- Les informations disponibles dans la vue sur l'utilisation du serveur de licences Citrix incluent uniquement les informations collectées et rapportées par les serveurs de licences Citrix enregistrés et générant des rapports. L'expérience de déploiements sous licence ne représente pas et peut ne pas correspondre au nombre total de licences que vous possédez ou que vous avez achetées.
- Le pourcentage de licences disponibles est calculé en fonction du nombre de licences utilisées par rapport aux licences installées sur les serveurs de licences de reporting.

Notifications

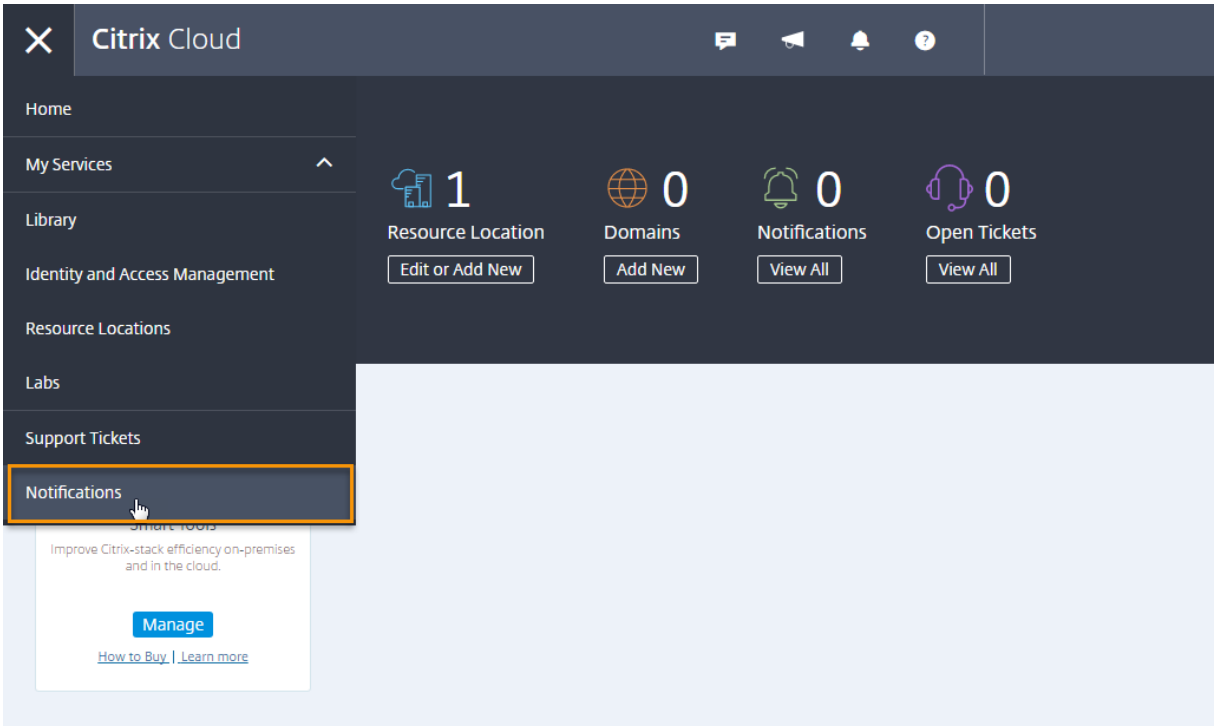
April 9, 2020

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.

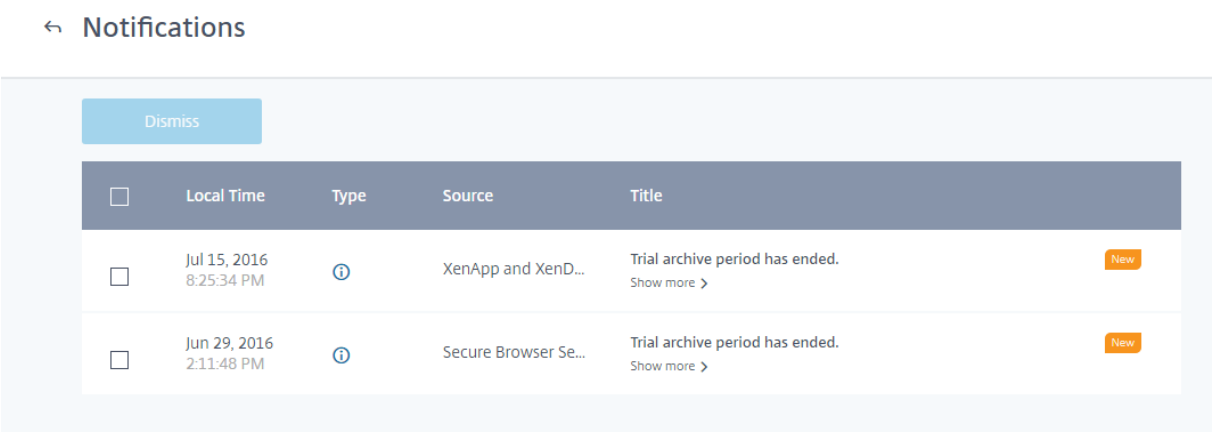
Afficher les notifications

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

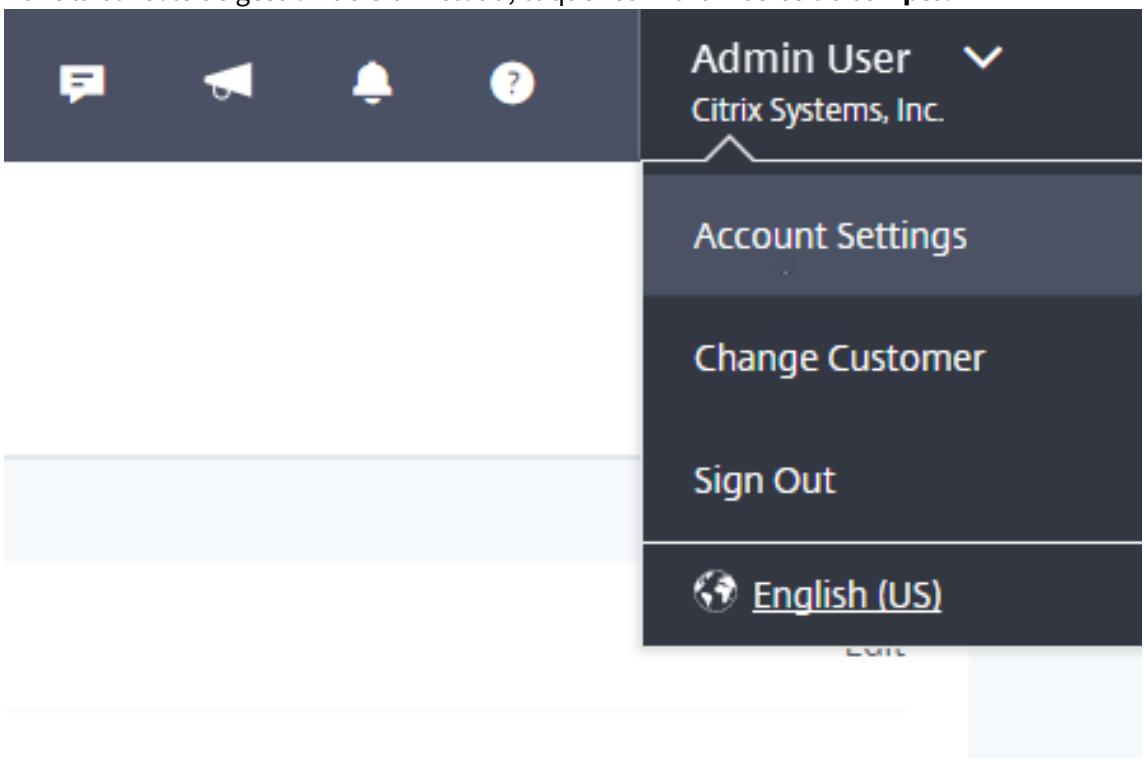
Vous pouvez choisir de recevoir des notifications par e-mail au lieu de vous connecter pour les voir. Par défaut, les notifications par e-mail sont désactivées.

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.

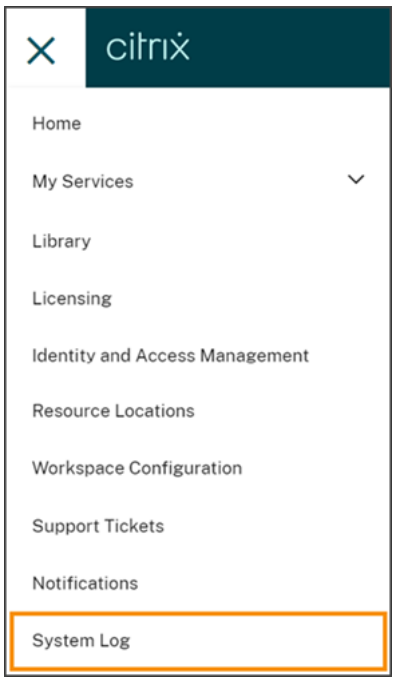
Journal système (version Technical Preview)

July 20, 2021

> **Remarque :**
>
> Le journal système et l'API SystemLog sont en version Technical Preview. Citrix recommande d'utiliser ces fonctionnalités uniquement dans un environnement de non production.

Le journal système affiche une liste horodatée des événements survenus dans Citrix Cloud. Vous pouvez exporter ces modifications sous forme de fichier CSV pour répondre aux exigences de conformité réglementaire de votre organisation ou pour prendre en charge l'analyse de sécurité.

Pour afficher le journal système, sélectionnez **Journal système** dans le menu Citrix Cloud.



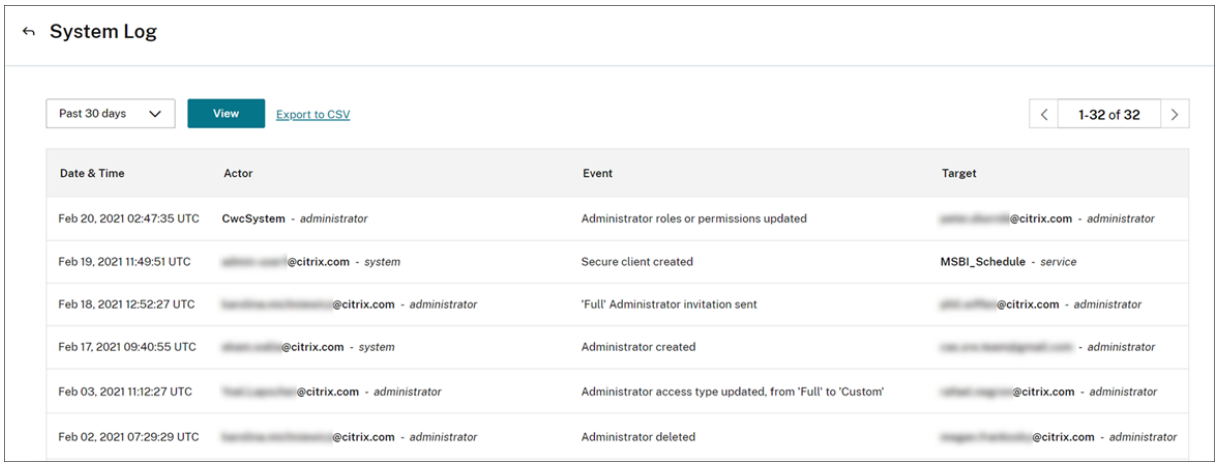
Pour plus d'informations sur la rétention des données dans les journaux système, consultez Rétention des données dans cet article.

Événements enregistrés

Le journal système capture les événements suivants :

- Ajout, modification et suppression d'administrateurs
- Création et suppression de clients sécurisés

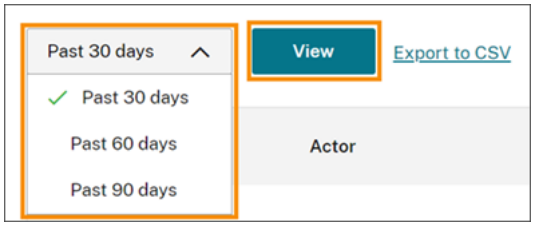
Par défaut, le journal système affiche les événements survenus au cours des 30 derniers jours. Les événements les plus récents sont affichés en premier.



La liste affichée contient les informations suivantes :

- Date et heure (UTC) auxquelles l'événement s'est produit
- Acteur qui a initié l'événement, tel qu'un administrateur ou un client sécurisé. Les entrées avec l'acteur **CwcSystem** indiquent que Citrix Cloud a effectué l'opération.
- Brève description de l'événement, telle que la modification d'un administrateur ou la création d'un nouveau client sécurisé
- Cible de l'événement. La cible est l'objet système qui a été affecté ou modifié à la suite de l'événement. Par exemple, un utilisateur qui a été ajouté en tant qu'administrateur.

Pour afficher des événements passés de plus de 30 jours, filtrez la liste en sélectionnant la période que vous souhaitez afficher et sélectionnez **Afficher**. Vous pouvez afficher les événements qui se sont produits jusqu'aux 90 derniers jours.

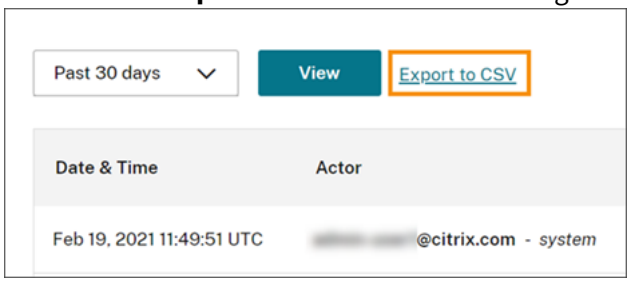


Pour récupérer des événements plus anciens survenus pendant une période spécifiée, vous pouvez utiliser l'API SystemLog. Pour plus d'informations, consultez la section Récupérer des événements pour une période spécifique dans cet article.

Exporter des événements

Vous pouvez exporter un fichier CSV d'événements du journal système qui se sont produits jusqu'aux 90 derniers jours. Le nom du fichier téléchargé suit le format `SystemLog-CustomerName-OrgID-DateTimeStamp.csv`.

1. Dans le menu Citrix Cloud, sélectionnez **Journal système**.
2. Si nécessaire, filtrez la liste pour afficher la période pour laquelle vous souhaitez exporter des événements.
3. Sélectionnez **Exporter au format CSV** et enregistrez le fichier.



Le fichier CSV contient les informations suivantes :

- Horodatage UTC de chaque événement
- Détails de l'acteur qui a initié l'événement, y compris le nom et l'identifiant de l'acteur

- Détails de l'événement, tels que le type d'événement et le texte de l'événement
- Détails de la cible de l'événement, tels que l'ID cible, le nom de l'administrateur ou d'un client sécurisé

Récupérer des événements pour une période spécifique

Si vous souhaitez récupérer des événements pendant des périodes spécifiques, vous pouvez utiliser l'API SystemLog. Avant d'utiliser l'API, vous devez créer un client sécurisé comme décrit dans Getting Started sur le site Web Citrix Developer.

Pour plus d'informations sur l'utilisation de l'API SystemLog, consultez Cloud Services Platform - SystemLog sur le site Web Citrix Developer Docs.

Transférer les événements du journal système

Le module complémentaire Citrix System Log Add-on for Splunk vous permet de connecter votre instance Splunk à Citrix Cloud. Avec cette connexion, vous pouvez transférer les données du journal système vers Splunk. Pour plus d'informations, consultez add-on documentation dans le référentiel Citrix sur GitHub.

Les modules complémentaires pour d'autres solutions de gestion des événements et des informations de sécurité (SIEM, Security Information Event Management) telles que Microsoft Azure Sentinel et IBM QRadar ne sont pas encore disponibles. Veuillez consulter régulièrement les ressources suivantes pour obtenir des mises à jour sur les efforts de développement et les versions :

- Blogs Citrix
- Forum de discussion Citrix Cloud
- Médias sociaux Citrix : Twitter, LinkedIn, Facebook

Rétention des données

Citrix partage la responsabilité avec vous, le client, quant à la rétention des données du journal système capturées par Citrix Cloud.

Citrix conserve les enregistrements du journal système pendant 90 jours après l'enregistrement des événements.

Vous êtes responsable du téléchargement des enregistrements du journal système que vous souhaitez conserver afin de répondre aux exigences de conformité de votre organisation et de stocker ces enregistrements dans une solution de stockage à long terme.

Citrix Workspace

June 10, 2021

Citrix Workspace est une solution complète d'espace de travail numérique qui fournit un accès sécurisé aux informations, applications et autres contenus pertinents pour le rôle d'une personne dans votre organisation. Les utilisateurs s'abonnent aux services que vous mettez à disposition et peuvent y accéder depuis n'importe où, sur n'importe quel appareil. Citrix Workspace vous aide à organiser et à automatiser les détails les plus importants dont vos utilisateurs ont besoin pour collaborer, prendre de meilleures décisions et se concentrer sur leur travail.

Pour obtenir une description complète de chaque édition de Citrix Workspace et des fonctionnalités incluses, consultez le tableau des fonctionnalités de Citrix Workspace.

Mise en route

Citrix Workspace inclut une procédure détaillée pour vous aider à fournir rapidement des espaces de travail. Chaque étape vous guide à travers la console Citrix Cloud en fournissant des instructions pour des tâches telles que la configuration de votre fournisseur d'identité, la sélection de l'authentification de votre espace de travail et l'activation des autres services fournis avec Workspace. La procédure détaillée fournit également un accès rapide aux informations techniques dont vous aurez besoin lorsque vous assemblez votre équipe de déploiement et que vous configurez votre infrastructure et vos ressources. Pour obtenir une vue d'ensemble des tâches que vous allez effectuer et des informations dont vous aurez besoin au fur et à mesure de votre déploiement, consultez la section Mise en route de Citrix Workspace.

Micro-apps

Le service de micro-apps vous permet d'envoyer des notifications pertinentes et exploitables à partir de vos applications directement dans les espaces de travail des utilisateurs. Les utilisateurs gagnent du temps et peuvent se concentrer sur leur travail principal car ils n'ont pas besoin de basculer entre les applications pour interagir avec les principaux systèmes de votre organisation. Créez des intégrations à partir de vos sources de données applicatives pour extraire des actions dans Workspace. Les micro-apps peuvent utiliser la réécriture active vers les systèmes source de sorte que les utilisateurs peuvent gérer ces actions sans quitter leur espace de travail.

Pour de plus amples informations, consultez la documentation du service Micro-apps.

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.

Citrix Endpoint Management

Pour les clients Endpoint Management dont l'expérience d'espace de travail est activée, les utilisateurs qui ouvrent Secure Hub et cliquent sur **Ajouter des applications** sont dirigés vers le magasin d'applications 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 :

- Pour déployer l'expérience d'espace de travail sur de nouveaux appareils, ajoutez-les au groupe de mise à disposition d'espace de travail. Pour de plus amples informations, consultez Intégration de Citrix Endpoint Management à Citrix Workspace.
- 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, consultez 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 la section Authentification domaine ou domaine + jeton de sécurité.
- Activez l'intégration de Workspace pour Endpoint Management. 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 Endpoint Management. Nous vous recommandons de désactiver l'intégration de ShareFile dans la console Endpoint Management avant d'activer l'intégration de Workspace.

Citrix Gateway

Citrix Gateway (anciennement NetScaler Gateway Service) fournit un accès distant sécurisé avec des fonctionnalités de gestion des identités et des accès (IdAM). Citrix Gateway offre une expérience unifiée aux applications SaaS (Software as a Service), ainsi qu'aux applications et aux bureaux virtuels. Suivez les étapes pour configurer Service Citrix Gateway, 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.

Citrix Content Collaboration

Citrix Content Collaboration (anciennement ShareFile) permet d'accéder aux données en toute sécurité, de synchroniser et de partager des fichiers à partir de n'importe quel appareil. Nous regroupons le partage de fichiers de niveau professionnel, les workflows optimisés et la collaboration en temps réel dans un seul emplacement afin que les utilisateurs puissent travailler comme ils le souhaitent.

1. Assurez-vous que vous êtes autorisé à utiliser Content Collaboration.
2. Associez Citrix Workspace à votre compte Content Collaboration. Pour plus d'informations , consultez l'article À propos de Content Collaboration, y compris la section Créer ou associer un compte Content Collaboration (ShareFile) à Citrix Cloud.
3. Activez Content Collaboration dans Citrix Workspace. Reportez-vous à la section Déployer et activer Citrix Content Collaboration dans Citrix Workspace dans la documentation Citrix Content Collaboration. Si ce processus est configuré, l'onglet **Fichiers** s'affiche dans le panneau de navigation de gauche dans l'interface utilisateur Citrix Workspace.

Signature électronique

Citrix offre une fonctionnalité de signature électronique à l'aide de Citrix RightSignature. Une signature électronique, parfois connue sous le nom de « e-signature », correspond à votre signature

manuscrite sur un document papier, mais sous format électronique, à savoir une marque sur un contrat ou un document électronique que vous apposez pour démontrer votre intention d'accepter les conditions de ce document. Pour plus d'informations sur RightSignature, consultez la page répertoriant les questions fréquentes de RightSignature.

Les utilisateurs peuvent envoyer une signature directement à partir de Citrix Workspace via l'intégration Citrix RightSignature à Citrix Content Collaboration. Reportez-vous à Intégration de ShareFile RightSignature Suivez ces étapes :

1. Assurez-vous que vous êtes autorisé à utiliser Content Collaboration et RightSignature.
2. Associez Citrix Workspace à votre compte Content Collaboration et activez Content Collaboration dans Citrix Workspace. Pour plus d'informations, consultez À propos de Content Collaboration, y compris l'article Créer ou associer un compte Content Collaboration (ShareFile) à Citrix Cloud, et Déployer et activer Citrix Content Collaboration dans Citrix Workspace dans la documentation de Citrix Content Collaboration. Si ce processus est configuré, l'onglet **Fichiers** s'affiche dans le panneau de navigation de gauche dans l'interface utilisateur Citrix Workspace.
3. Activez RightSignature pour les utilisateurs. Voir l'article d'assistance Add Users to RightSignature. Si ce processus est configuré, la vignette **Envoyer pour signature** s'affiche pour n'importe quel fichier ouvert à partir de **Fichiers** dans l'interface utilisateur Citrix Workspace.

Citrix RightSignature est également disponible en tant que solution autonome. Pour commencer, reportez-vous à la section RightSignature. Pour la signature électronique dans Content Collaboration, reportez-vous à Citrix Content Collaboration - Signature électronique.

Secure Browser Service

Secure Browser Service protège le réseau de l'entreprise contre les attaques via navigateur en isolant la navigation sur le Web. Lorsque des abonnés accèdent à l'URL fournie par l'administrateur, leurs navigateurs publiés sont affichés, ainsi que d'autres applications et bureaux configurés 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.

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.

Citrix Cloud pour les partenaires

June 10, 2021

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 indique 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.

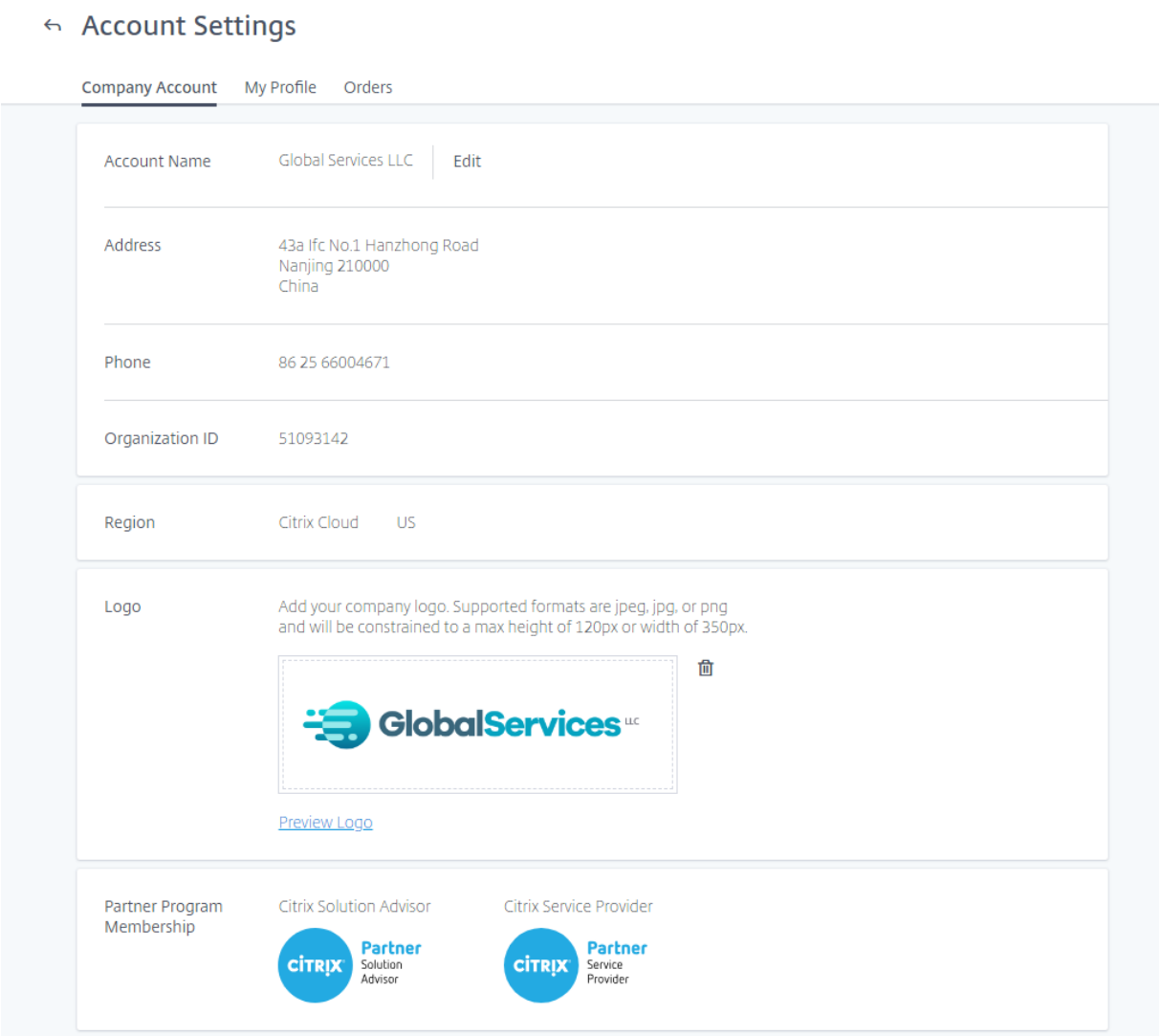
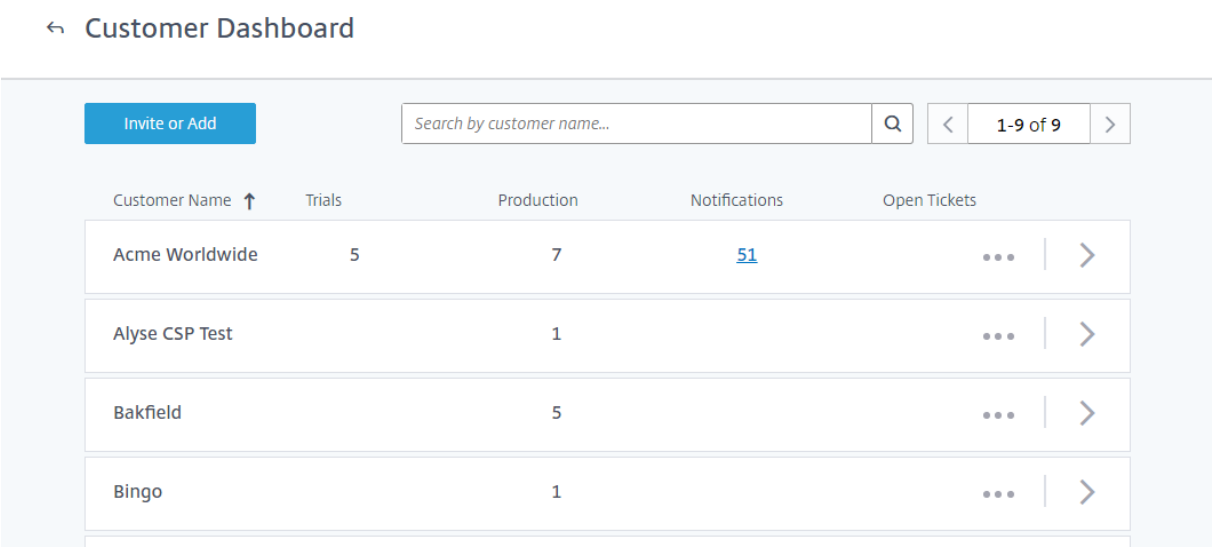


Tableau de bord client

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
- Les partenaires voient les droits d'utilisation des licences et d'utilisation active des services Citrix Cloud

Informations supplémentaires sur les connexions de partenaire :

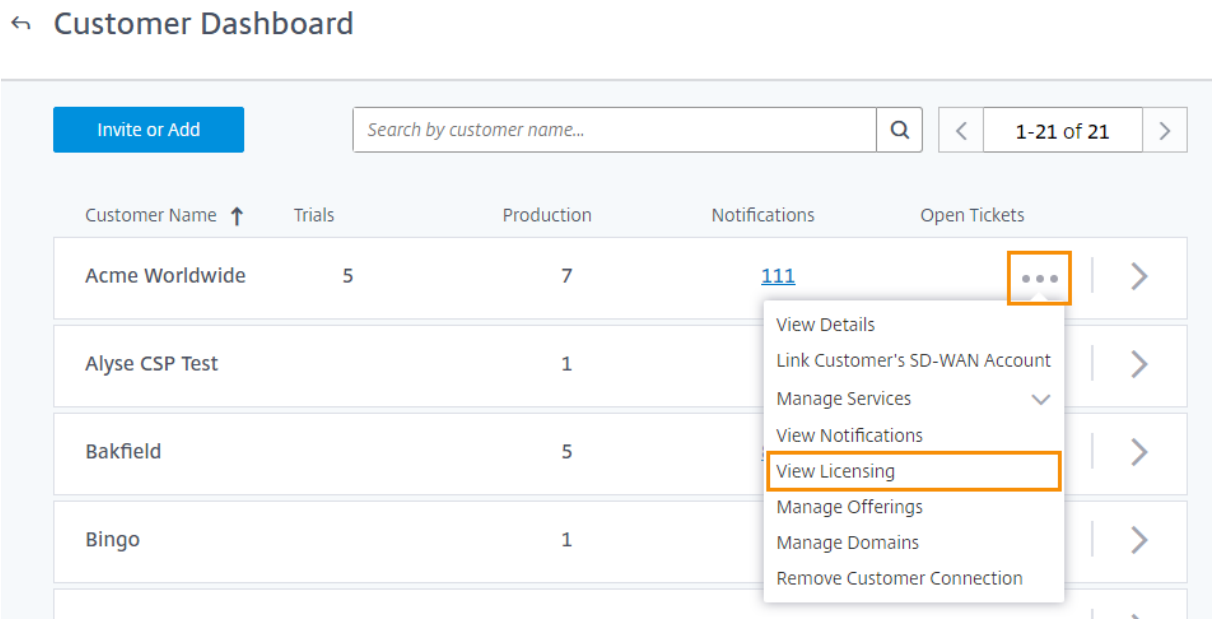
- Les partenaires peuvent établir des connexions avec plusieurs clients
- Les clients peuvent établir des connexions avec plusieurs partenaires
- Il n'y a pas de limite au nombre de connexions client-partenaire
- Les connexions peuvent être annulées à tout moment par le client ou le partenaire
  - Par le client dans la page d'informations de compte
  - Par le partenaire à l'aide du tableau de bord client
- Des notifications Citrix Cloud 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

- En matière de visibilité du système de licences, le partenaire peut afficher uniquement les résumés relatifs aux attributions de licences et aux tendances historiques d'utilisation
- 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 et les dates d'expiration.

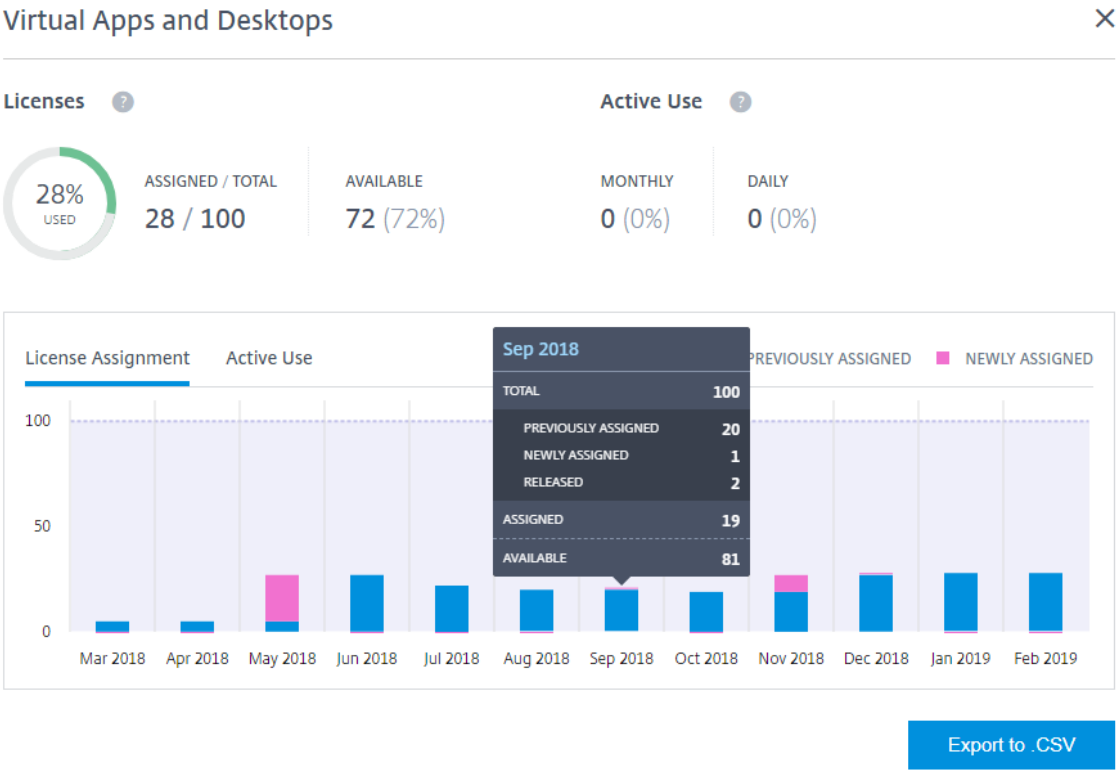
Tendances du système de licences

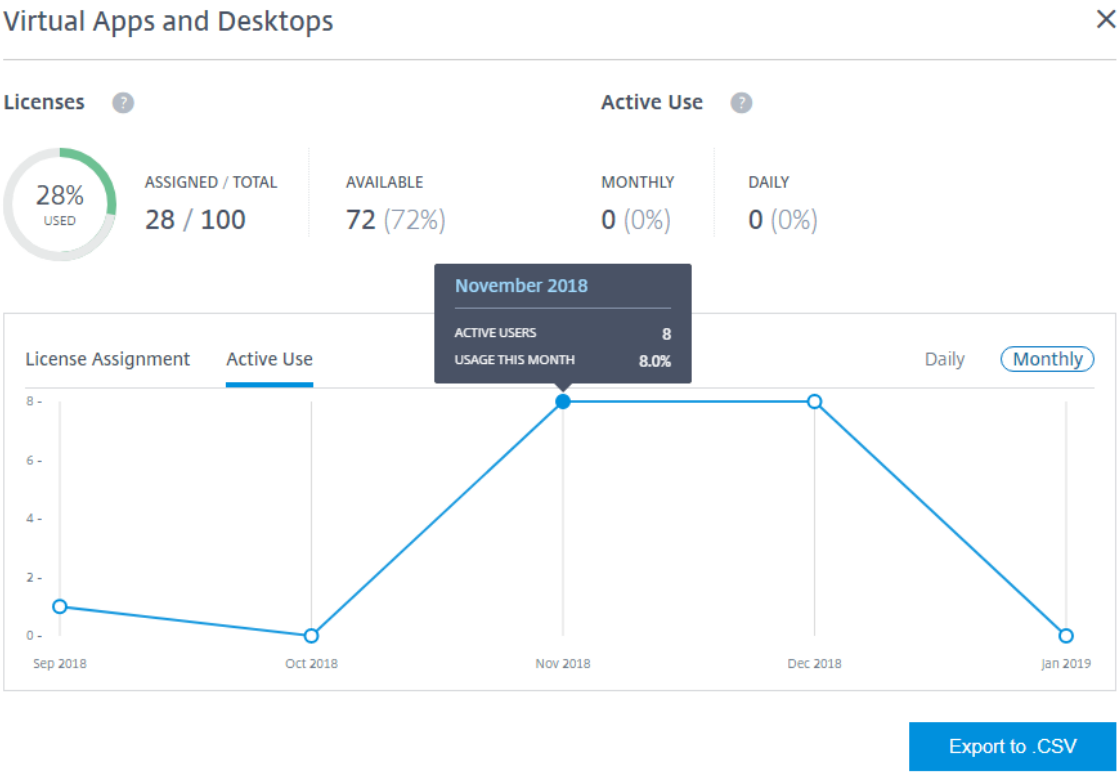
Les partenaires peuvent consulter les informations relatives au système de licences à partir du tableau de bord client en cliquant sur le bouton représentant des points de suspension en regard du nom du client et en sélectionnant **Afficher les licences**.



> **Remarque :**
>
> Les partenaires Citrix ne peuvent afficher que la vue de résumé de l'option Système de licences et les tendances historiques de l'utilisation active. Ils ne peuvent pas afficher les utilisateurs individuels qui consomment des licences pour un service donné.

Pour afficher un résumé, sélectionnez **Afficher tendance d'utilisation** dans l'onglet **Utilisation** de la page client. Le résumé inclut le rapport entre les licences attribuées et le total des licences achetées, une répartition des licences attribuées, ainsi que les utilisateurs actifs mensuels et quotidiens. Si nécessaire, les partenaires peuvent exporter ces informations sous forme de fichier .csv.

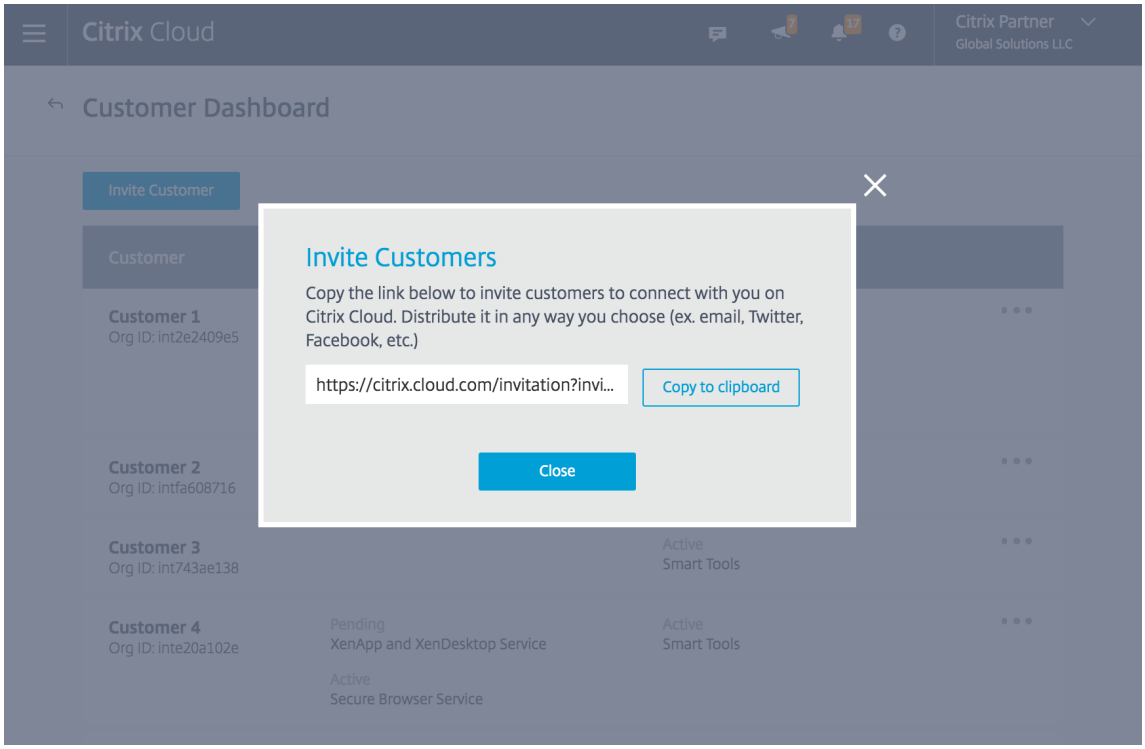




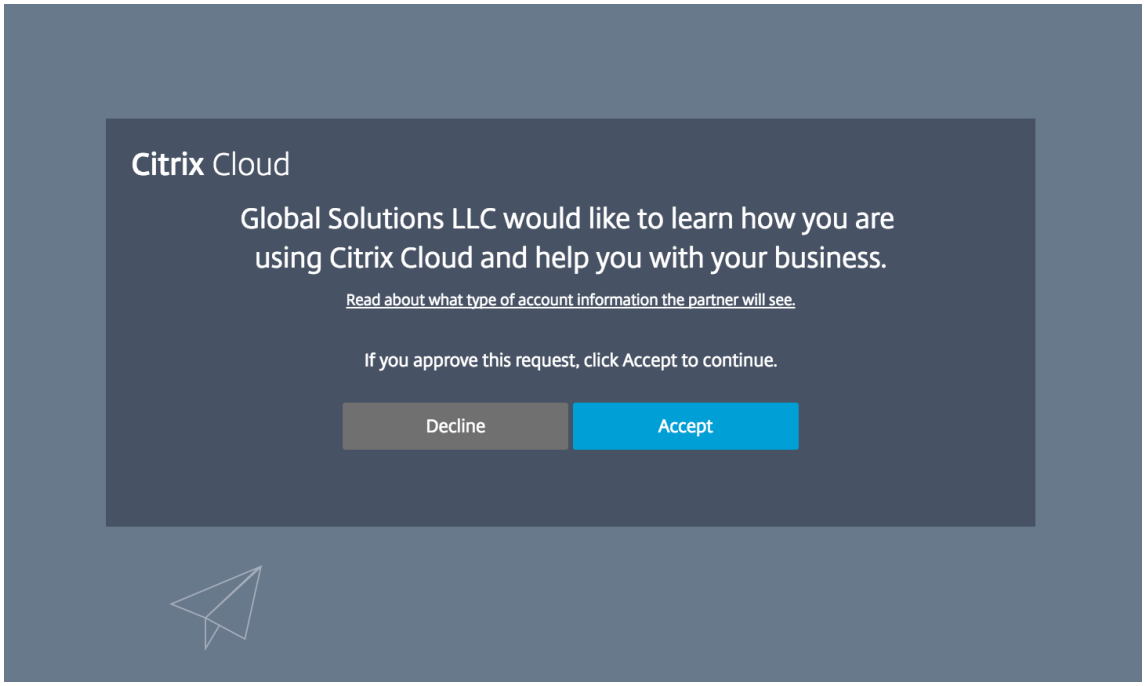
Inviter un client à se connecter

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 reçoivent un lien d'invitation. Le lien est fixe et non personnalisable ou modifiable.

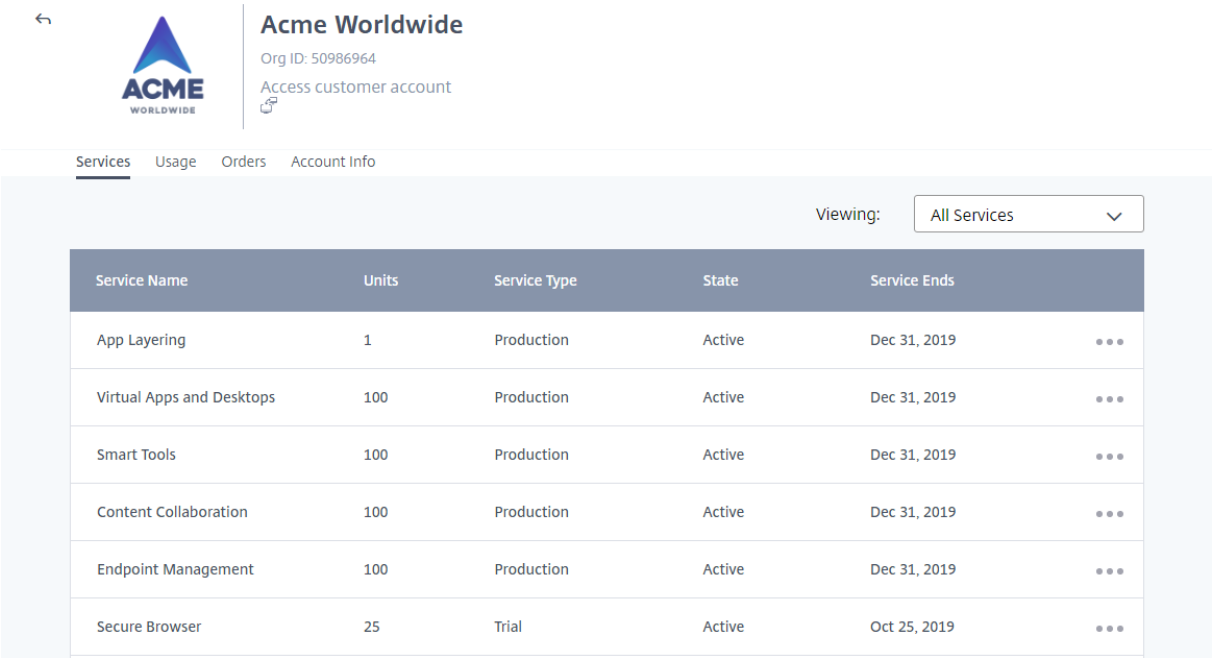
- Il n'existe aucune limite au nombre de fois que le lien peut être utilisé pour établir une connexion.
- Le lien peut être réutilisé si une connexion doit être recréée.
- Le lien n'expire pas.

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 :

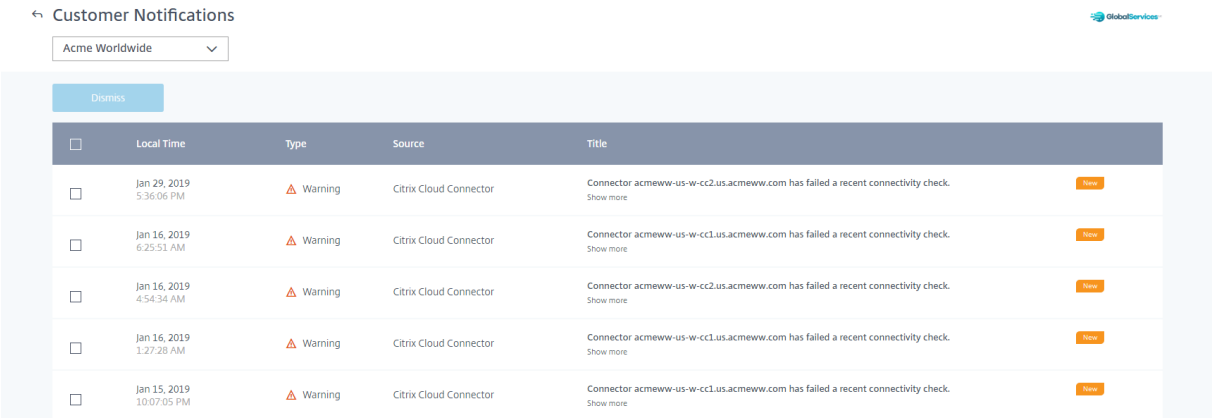
- Évaluations de service en cours
- Demandes d'évaluation de service en attente
- Évaluations de service qui ont expiré
- Droits d'utilisation en cours (services achetés ou autrement autorisés/activés pour le client)
- Nombre de licences et date d'expiration des droits



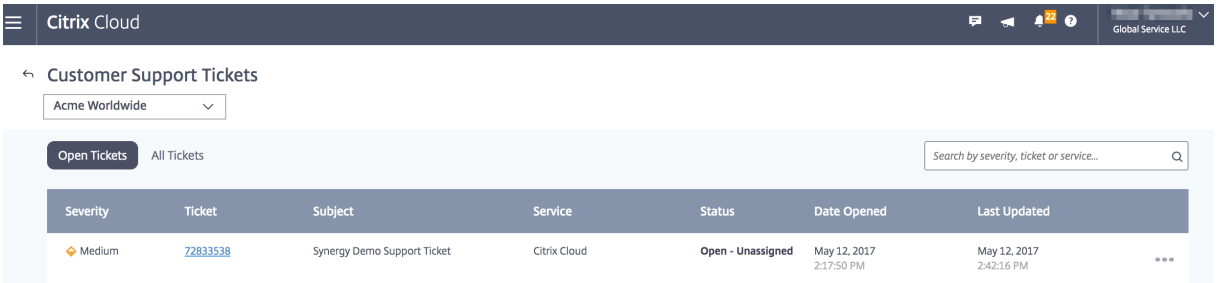
Visibilité des partenaires sur les tickets de support et les notifications des clients

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. Les notifications ignorées ne s'affichent pas pour le partenaire.

Toutefois, les clients peuvent toujours voir la notification dans leur compte une fois qu'ils se sont connectés à Citrix Cloud.



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



Domaines fédérés pour les fournisseurs de services Citrix

Les *domaines fédérés* permettent aux utilisateurs d'utiliser les informations d'identification d'un domaine attaché à votre emplacement de ressources CSP pour se connecter à l'espace de travail. Cela vous permet de fournir des espaces de travail dédiés à vos utilisateurs clients avec une URL d'espace de travail personnalisée, telle que *customer.cloud.com*. L'emplacement des ressources se trouve toujours sur votre compte Citrix Cloud partenaire. Vous pouvez fournir des espaces de travail dédiés en plus de l'espace de travail partagé auxquels les clients peuvent accéder à l'aide de l'adresse URL de votre espace de travail CSP (par exemple, csppartner.cloud.com). Pour permettre aux clients d'accéder à leur espace de travail dédié, vous les ajoutez aux domaines appropriés que vous gérez. Après avoir configuré l'espace de travail, les utilisateurs peuvent se connecter à leur espace de travail et accéder aux applications et aux bureaux que vous avez rendus disponibles via Virtual Apps and Desktops Service.

Lorsque vous supprimez un client d'un domaine fédéré, les utilisateurs ne peuvent plus accéder à leurs espaces de travail à l'aide des informations d'identification du domaine du partenaire.

Pour plus d'informations sur l'utilisation de domaines fédérés pour mettre à disposition des appli-

cations et des bureaux, consultez la section Citrix Virtual Apps and Desktops Service pour les fournisseurs de services Citrix.

Options d'apparence de l'espace de travail pour les fournisseurs de services Citrix

Vous pouvez configurer les couleurs et les logos de votre espace de travail avec des thèmes personnalisés. Pour savoir comment créer des thèmes personnalisés, reportez-vous à la section Personnaliser l'apparence des espaces de travail.

> **Remarque**
>
> Le thème personnalisé est une fonctionnalité mono-locataire. Les Citrix Service Provider avec lesquels les locataires partagent un emplacement de ressources, des Cloud Connector et un domaine Active Directory (multi-locataires) ne sont actuellement pas pris en charge. Les locataires Citrix Service Provider qui disposent de leur propre emplacement de ressources dédié, de leurs propres Cloud Connector et de leur propre domaine Active Directory dédié (locataire unique) sont entièrement pris en charge.

Content Collaboration

January 22, 2021

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 la section 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.

Pour plus d'informations sur l'utilisation de Citrix Files sur chaque plate-forme prise en charge, consultez Citrix Files dans le Centre d'aide utilisateur.

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 l'Accord de niveau de service.

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

July 20, 2021

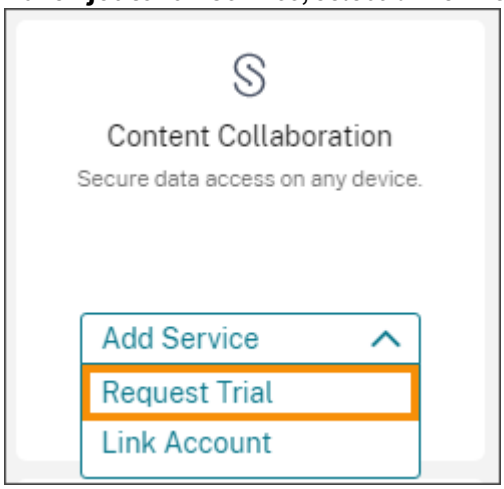
Pour commencer avec Content Collaboration, vous pouvez tirer parti des options suivantes :

- 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 **Mes services**, localisez la vignette **Content Collaboration**.
3. Dans **Ajouter un service**, sélectionnez **Demander version d'évaluation**.



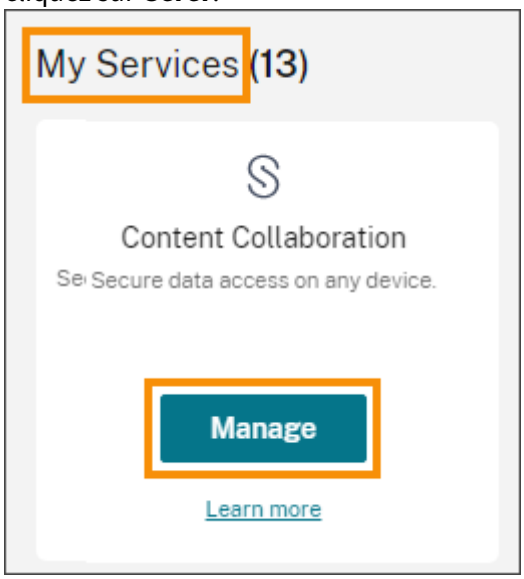
   La page Ajouter compte Content Collaboration apparaît avec l'onglet Demander version d'évaluation sélectionné.
4. Dans la section **Emplacement géographique**, sélectionnez la région du service que vous souhaitez utiliser et confirmez que la région ne peut pas être modifiée après avoir demandé l'évaluation.

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.

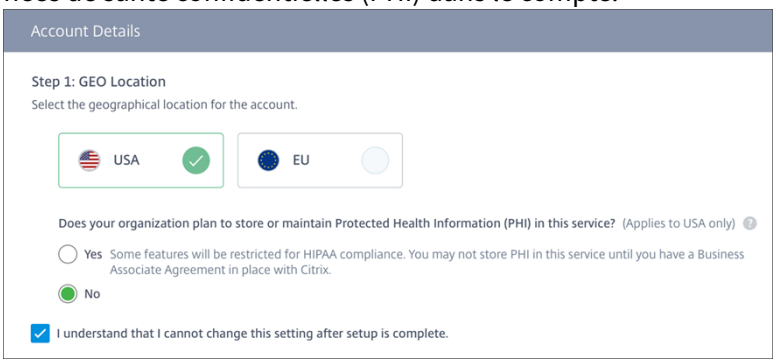
1. Connectez-vous à Citrix Cloud avec vos informations d'identification Citrix Cloud.
2. Dans la console Citrix Cloud, sous **Mes services**, localisez la vignette Content Collaboration et cliquez sur **Gérer**.



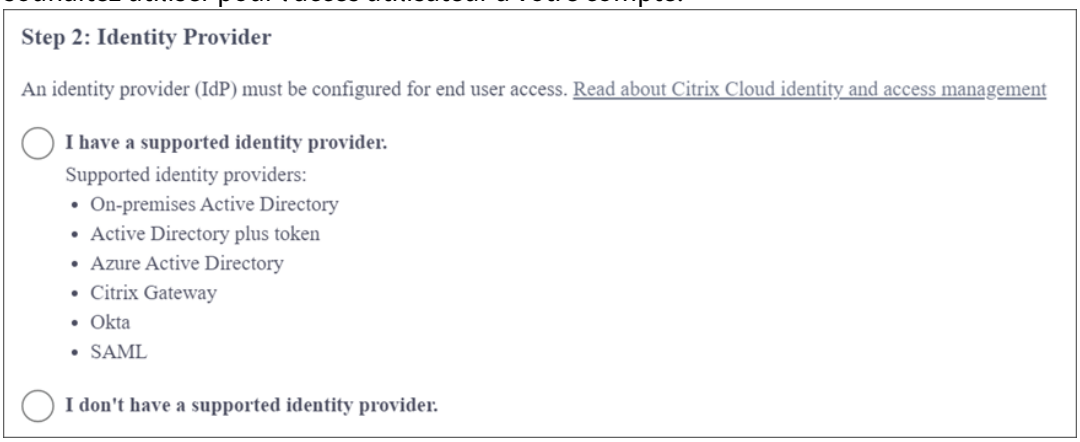
La page Attribuer droits de Content Collaboration affiche tous les nouveaux droits liés à Content Collaboration achetés sous votre OrgID Citrix.

3. Sélectionnez les droits à appliquer au compte, puis cliquez sur **Continuer**.
4. Sous **Nom du compte**, sélectionnez un nouveau compte à affecter au droit d'accès, puis cliquez sur **Attribuer**.

5. Sur la page **Créer un compte Content Collaboration**, sous **Détails du compte**, entrez les informations suivantes :
   a) Dans **Étape 1 : Emplacement géographique**, sélectionnez la région du service pour votre compte. Si vous sélectionnez la région USA, indiquez si vous prévoyez de stocker des données de santé confidentielles (PHI) dans le compte.

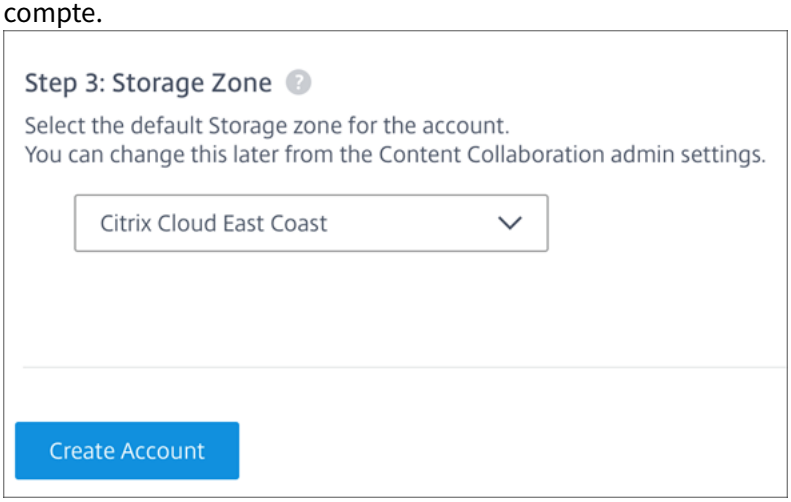


   b) Dans **Étape 2 : Fournisseur d'identité**, sélectionnez le fournisseur d'identité que vous souhaitez utiliser pour l'accès utilisateur à votre compte.



   Si votre fournisseur d'identité n'est pas pris en charge ou si vous n'avez pas de fournisseur d'identité, sélectionnez **Je n'ai pas de fournisseur d'identité pris en charge et j'ai besoin de Citrix pour stocker mon répertoire d'utilisateurs** et choisissez un sous-domaine ShareFile. Citrix vous crée ensuite un compte ShareFile.com.
   c) Dans **Étape 3 : Zone de stockage**, sélectionnez la zone de stockage par défaut pour votre

compte.



6. Sélectionnez **Créer compte.**

Associer un compte ShareFile existant

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

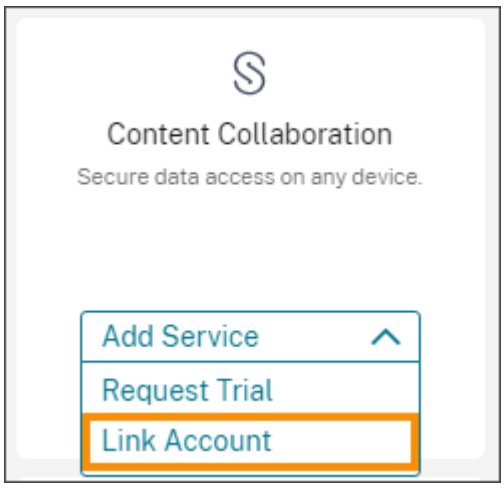
- Vous devez disposer d'autorisations d'administrateur dans Citrix Cloud et ShareFile.
- Vos autorisations d'administrateur ShareFile doivent inclure **Accéder aux autorisations du compte d'entreprise**.
- L'adresse e-mail que vous utilisez pour vous connecter à Citrix Cloud doit correspondre à l'adresse 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.

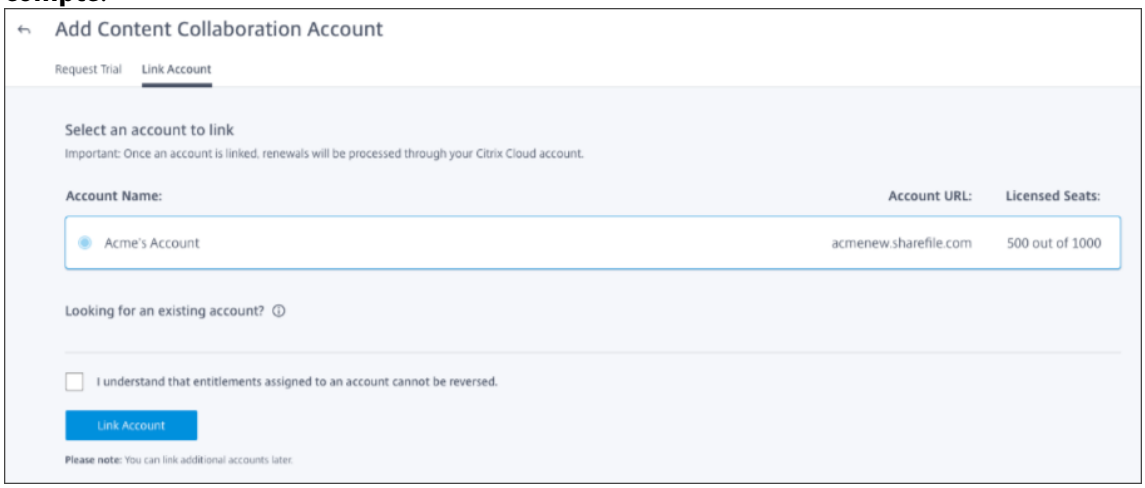
Pour associer votre compte Content Collaboration à Citrix Cloud (pas de nouveaux droits)

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 **Mes services**, 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**.

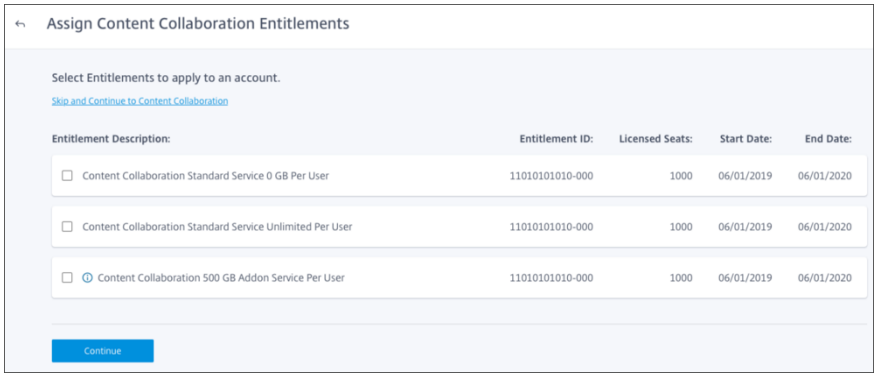


> **Important :**
>
> Si aucun compte ne s'affiche, vérifiez que vous êtes administrateur pour ShareFile et que l'adresse e-mail de Citrix Cloud correspond à celle de Content Collaboration. Pour obtenir une assistance supplémentaire, contactez le support Citrix.

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. Sélectionnez les droits à appliquer au compte, puis cliquez sur **Continuer**.



4. Sélectionnez le compte à appliquer aux droits sélectionnés.

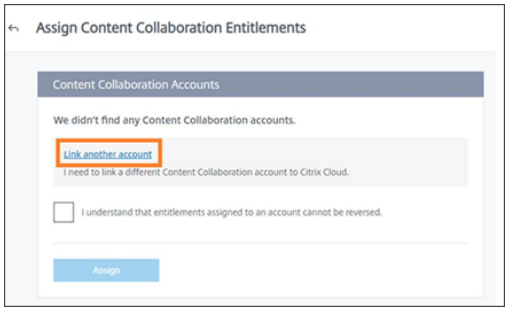
   > **Important :**
   >
   > Si aucun compte ne s'affiche, vérifiez que vous êtes administrateur pour Content Collaboration et que l'adresse e-mail de Citrix Cloud correspond à celle de ShareFile. Pour obtenir une assistance supplémentaire, contactez le support Citrix.
   >
   > Lorsque le message **Nous n'avons trouvé aucun compte Content Collaboration** s'affiche, consultez la section Pour associer un compte qui ne s'est jamais connecté à Citrix Cloud et suivez les étapes décrites.

5. Sélectionnez **Je comprends que les droits attribués à un compte ne peuvent pas être révoqués**.
6. Cliquez sur **Attribuer**. La page Attribuer droits de Content Collaboration affiche le compte attribué au droit.
7. Cliquez sur **Gérer** pour continuer vers la vue d'ensemble de l'administration de Content Collaboration.

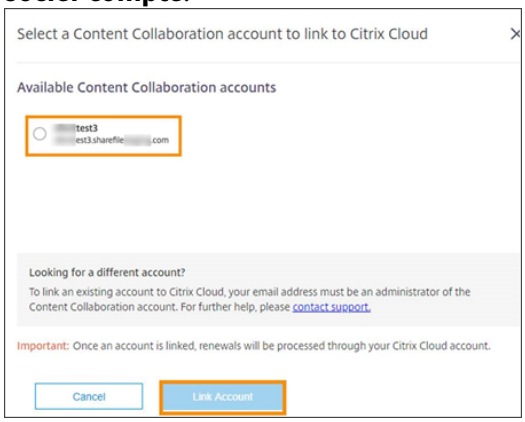
Pour associer un compte qui ne s'est jamais connecté à Citrix Cloud

Suivez les étapes suivantes si vous n'avez jamais associé un compte à 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**. Le message **Nous n'avons trouvé aucun compte Content Collaboration** s'affiche.



3. Sélectionnez **Associer un autre compte**.
4. Sélectionnez le compte Content Collaboration que vous souhaitez associer, puis cliquez sur **Associer compte**.



Configurer ShareFile

June 10, 2021

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 for Policy-Based Administration.

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 de plus amples informations, consultez ShareFile Single Sign-On SSO.

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 Single Sign On for ShareFile with 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 de Citrix Files pour Windows. Citrix Files vous permet d'accéder directement à vos fichiers dans ShareFile via un lecteur mappé, offrant ainsi une expérience identique à l'Explorateur de fichiers Windows natif.

Utilisation de Citrix Files pour Windows

Sur Citrix Virtual Apps and Desktops, vous utilisez Citrix Files pour Windows. Citrix Files pour Windows peut être préinstallé sur votre image de bureau avant le déploiement auprès des utilisateurs. Vous pouvez installer l'application une fois et la propager à toutes les sessions Citrix Virtual Apps and Desktops de votre environnement. Pour plus d'informations sur l'utilisation de Citrix Files pour Windows, consultez les articles suivants :

- Citrix Files sur Citrix Virtual Apps and Desktops
- CTX228273 : Installer et utiliser Citrix Files pour Windows

Accès à ShareFile avec Endpoint Management

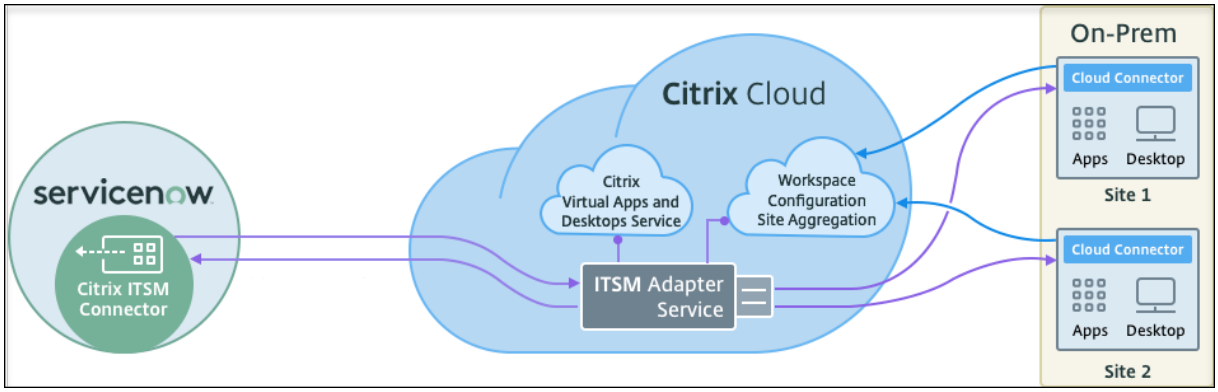
Pour plus d'informations sur l'encapsulation de l'application ShareFile et le déploiement de l'authentification unique entre Endpoint Management et ShareFile, consultez Citrix ShareFile pour Endpoint Management.

IT Service Management (ITSM) Adapter

July 21, 2021

Généralités

ITSM Adapter est un service Citrix Cloud. Avec le connecteur ITSM installé dans ServiceNow, ITSM Adapter offre un moyen facile d'étendre les fonctionnalités de ServiceNow à vos environnements Citrix Virtual Apps and Desktops. Il fournit également des workflows permettant aux équipes informatiques d'automatiser et de gérer facilement les sites cloud et locaux qui se connectent à Citrix Cloud, ce qui les laisse se concentrer sur des projets stratégiques.



Pour vous assurer que le service ITSM Adapter puisse interagir avec ServiceNow, ajoutez l'une des adresses IP suivantes à la liste d'autorisation de votre instance ServiceNow :

Région ITSM Adapter	Adresse IP
États-Unis	52.158.218.132/30
UE	20.54.214.12/30
Asie-Pacifique	20.195.2.68/30

Nouveautés

Juin 2021

- Nous avons mis à jour la version du connecteur ITSM de 1.8.0 à 2106.1.1.
- Nous avons étendu nos options de service pour vous permettre d'ajouter des machines créées par MCS lorsqu'un catalogue de machines demandé manque de machines. Pour plus d'informations, consultez Ajouter des machines créées par MCS.

Avril 2021

- Le service ITSM Adapter prend en charge ServiceNow Quebec.
- Un jeton d'actualisation et un jeton d'accès sont désormais générés automatiquement lorsque vous ajoutez une instance ServiceNow dans Citrix Cloud. Grâce à cette amélioration, vous n'avez

plus besoin d'utiliser un outil séparé pour générer les jetons. Pour plus d'informations, consultez Étape 4 : Ajouter une instance ServiceNow dans Citrix Cloud.

- Nous avons synchronisé les stratégies d'alerte Citrix que vous définissez dans Citrix Virtual Apps and Desktops Service avec ServiceNow sous **Citrix IT Service Management Connector > Settings > Alert Policies**. Lorsque le moniteur webhook est activé pour une stratégie d'alerte, les alertes répondant à la stratégie sont répertoriées dans ServiceNow sous **Citrix IT Service Management Connector > Alerts**. Vous pouvez également créer des incidents et les affecter à des personnes spécifiques. Pour désactiver une stratégie d'alerte dans ServiceNow, cliquez sur **Disable Monitor**. Pour plus d'informations, consultez Accéder aux alertes Citrix depuis ServiceNow.

Novembre 2020

- Nous avons simplifié le déploiement du service ITSM Adapter.
- Le service ITSM Adapter ajoute le tableau de bord **Reporting** pour présenter les statistiques de requête.
- Le service ITSM Adapter ajoute l'onglet **Add users to Application Group(s)** pour permettre aux administrateurs ServiceNow de sélectionner des utilisateurs lors du traitement des demandes d'accès aux applications.
- L'accès à une application spécifique peut être limité à certains utilisateurs d'un groupe Active Directory. Pour faciliter cette configuration, le service ITSM Adapter répertorie tous les groupes Active Directory qui peuvent accéder à une application spécifique dans l'onglet **Add users to Active Directory Group(s)**. Les administrateurs ServiceNow peuvent ajouter un utilisateur à un tel groupe Active Directory lors du traitement des demandes d'accès aux applications.

Juin 2020

- Le service ITSM Adapter prend en charge ServiceNow New York.
- Le service ITSM Adapter met en œuvre le nom d'utilisateur principal (UPN) pour donner aux utilisateurs Active Directory (AD) un format de type adresse e-mail avec lequel ils peuvent se connecter.

Intégration du service ITSM Adapter

L'intégration du service ITSM Adapter comporte les cinq étapes suivantes :

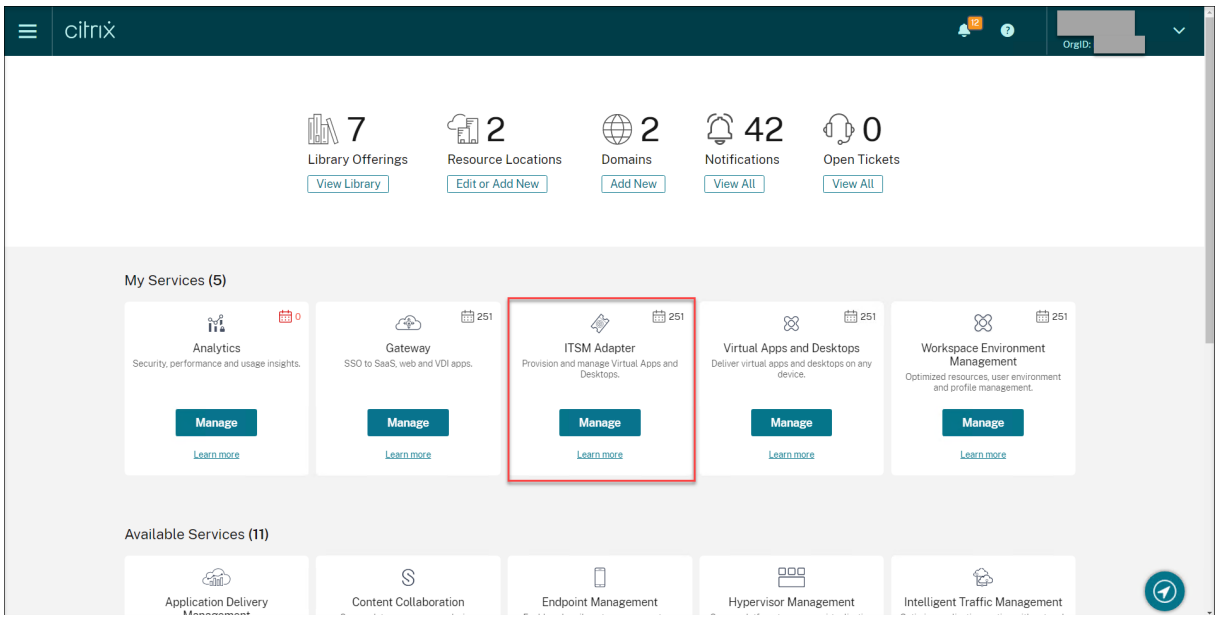
1. Vérifier que vous êtes abonné au Citrix Virtual Apps and Desktops Service
2. Configurer le connecteur ITSM pour ServiceNow

3. (Facultatif) Ajouter des sites locaux à Citrix Cloud via l'agrégation de sites
4. Ajouter une instance ServiceNow dans Citrix Cloud
5. Publier le service ITSM Adapter sur le portail ServiceNow pour que l'utilisateur puisse y accéder

> **Remarque :**
>
> Avant de passer aux étapes suivantes, assurez-vous que vous disposez des privilèges Administrateur ServiceNow et Administrateur Citrix.
>
> - En tant qu'administrateur ServiceNow, vous pouvez avoir l'autorisation d'activer le plug-in ServiceNow Orchestration, et de télécharger et d'installer le plug-in du connecteur ITSM. Vous pouvez également fournir le rôle x_cion_citrix_it_s.ctx_itsm_admin pour configurer le plug-in ITSM Connector dans ServiceNow.
> - En tant qu'administrateur Citrix, vous pouvez accéder au portail de Citrix Virtual Apps and Desktops Service et effectuer les configurations requises comme suit.

Étape 1 : Vérifier que vous êtes abonné au Citrix Virtual Apps and Desktops Service

Connectez-vous à Citrix Cloud à l'aide de vos informations d'identification Citrix ou créez un nouveau compte. Si vous vous êtes inscrit à un essai gratuit ou si vous êtes abonné à Citrix Virtual Apps and Desktops Service, vous pouvez voir le service ITSM Adapter comme illustré dans la capture d'écran suivante. Sinon, vérifiez auprès de vos représentants Citrix.

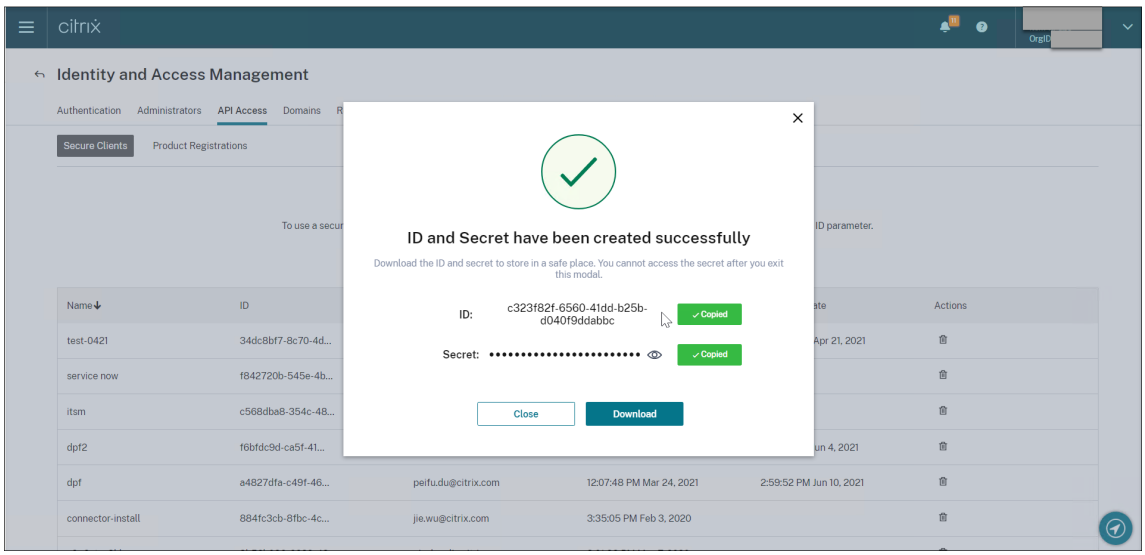


> **Conseil :**

> Le bouton **Manage** est disponible une fois que les droits ont été attribués sur les comptes utilisateur. Si cela n'a pas été effectué, le bouton **Request Demo** s'affiche.

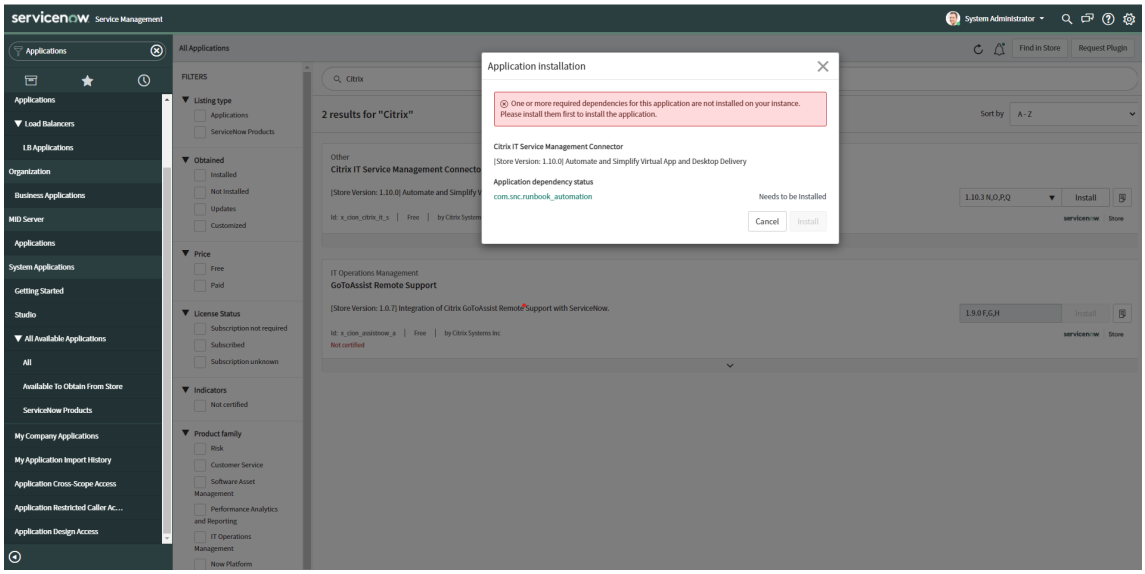
Étape 2 : Configurer le connecteur Citrix ITSM pour ServiceNow

1. Accédez à Citrix Cloud et créez un client sécurisé pour intégrer le service ITSM Adapter dans Citrix Cloud. Conservez un enregistrement de l'ID et de la clé secrète du client sécurisé. Pour plus d'informations, consultez Get started with Citrix Cloud APIs.

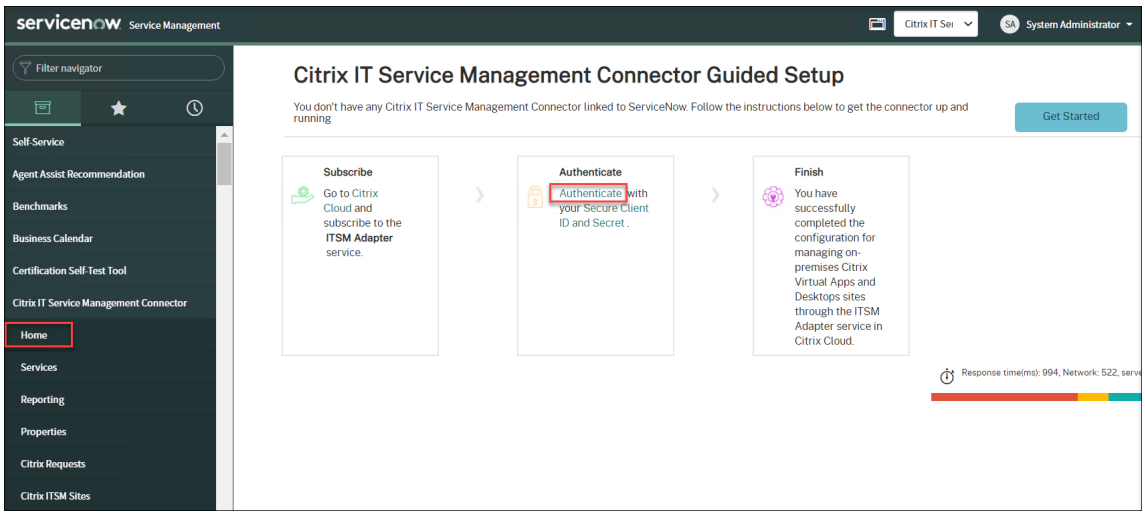


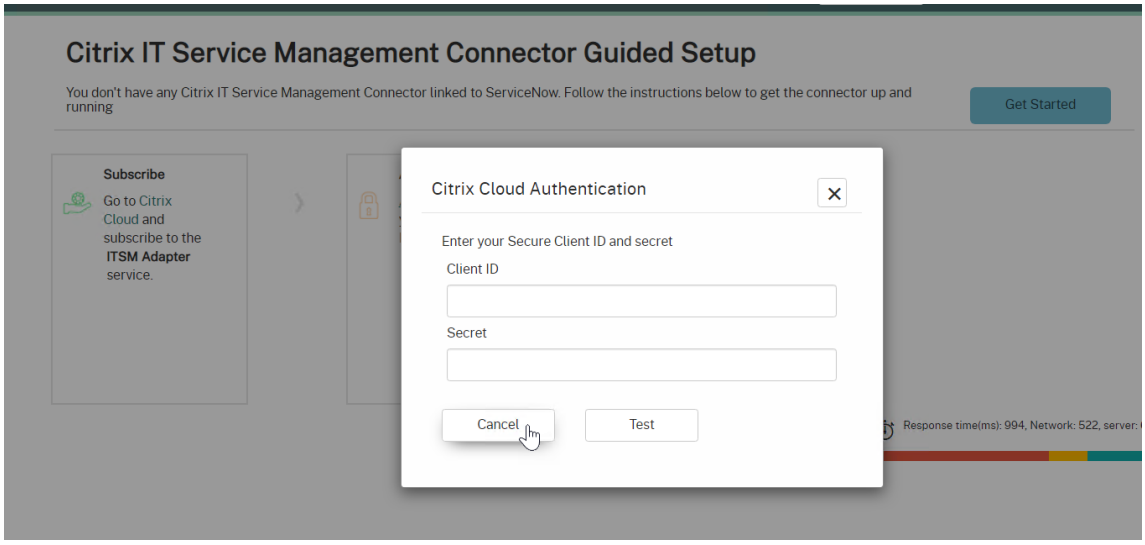
2. Assurez-vous que vous disposez d'un compte ServiceNow HI Portal et que vous disposez des privilèges d'administrateur ServiceNow.
3. Vérifiez que vous avez activé le plug-in ServiceNow Orchestration.

   Si les dépendances nécessaires sont manquantes sur votre instance ServiceNow, vous êtes invité à les installer.

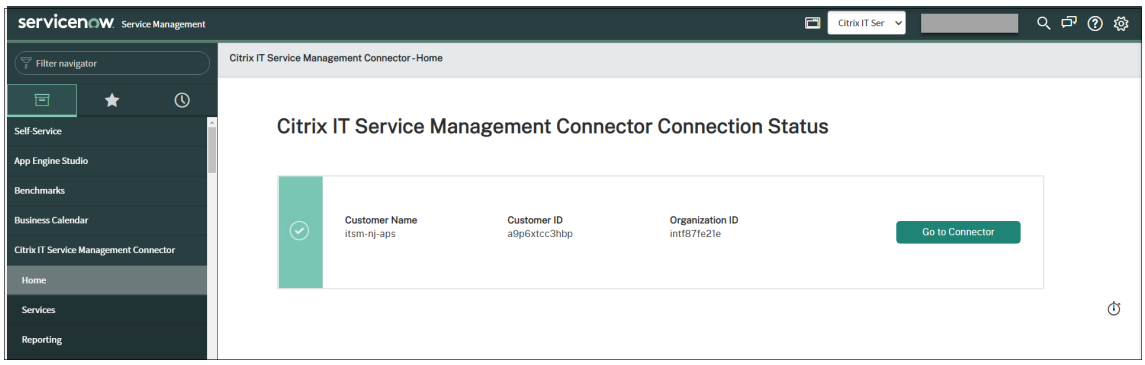


4. Téléchargez et installez le connecteur Citrix ITSM à partir du magasin ServiceNow.
5. Dans le volet **Citrix IT Service Management Connector**, sélectionnez **Home**, puis cliquez sur **Authenticate**. Saisissez votre ID et votre clé secrète de client sécurisé (informations d'identification proxy générées à partir de Citrix Cloud).



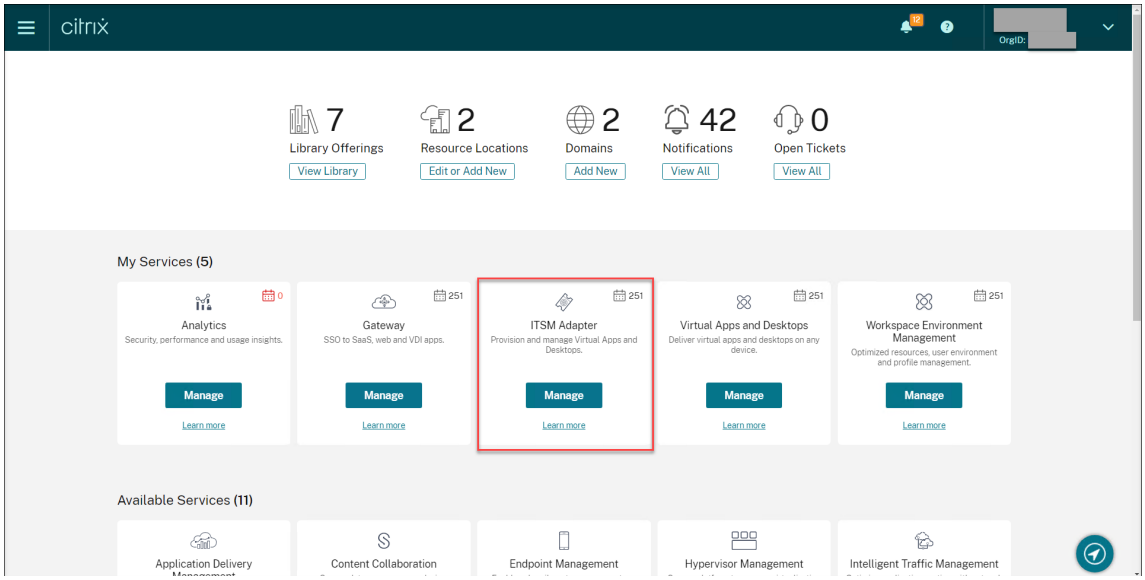


6. Testez la connexion.
7. Enregistrez la configuration. Un accusé de réception provenant de ServiceNow apparaît indiquant que la connexion est en cours.

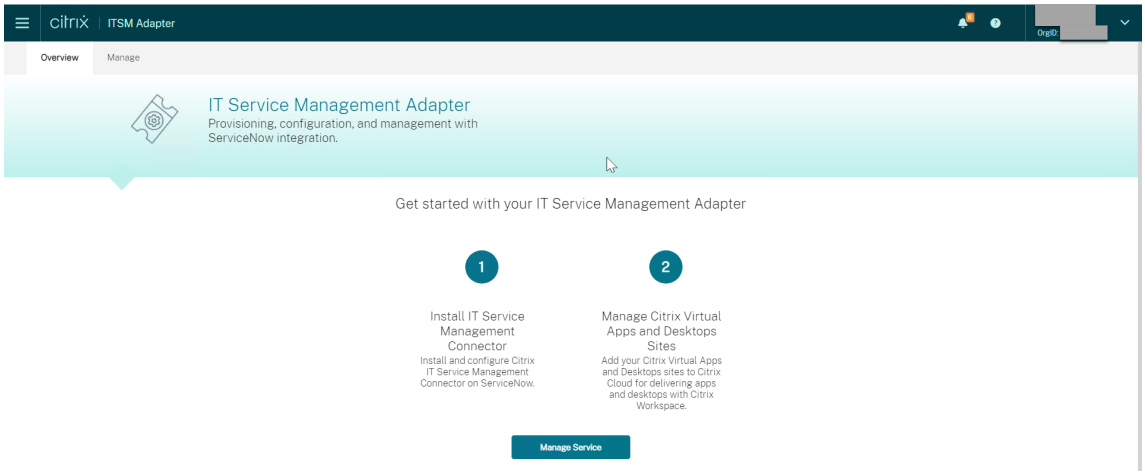


(Facultatif) Étape 3 : Ajouter des sites locaux à Citrix Cloud via l'agrégation de sites

1. Accédez à Citrix Cloud et accédez au service ITSM Adapter.



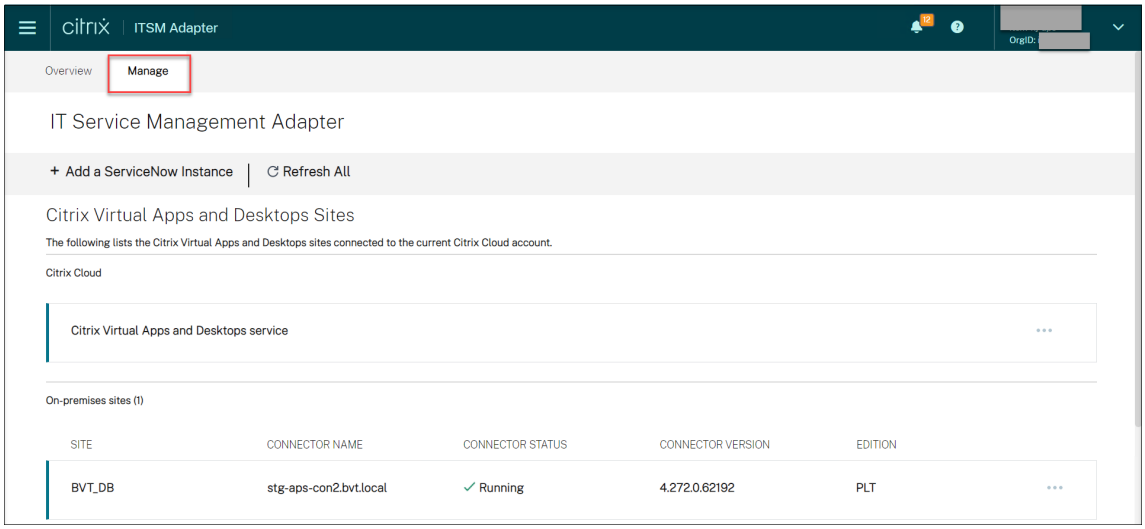
2. Cliquez sur le bouton bleu **Manage**. L'onglet **Overview** s'affiche.



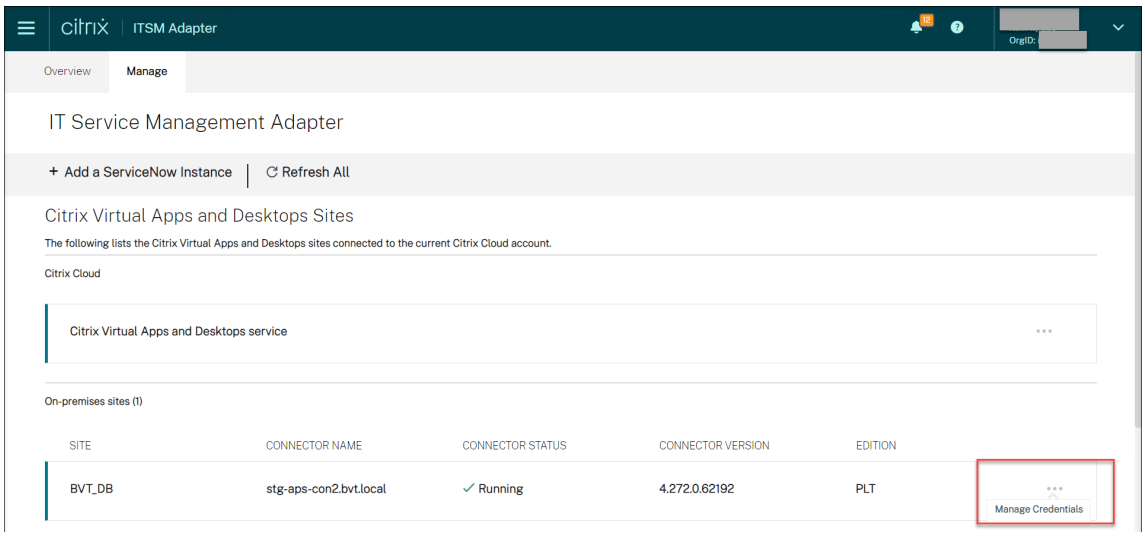
3. Cliquez sur l'onglet **Manage**. L'onglet **Manage** présente les instances ServiceNow et les sites Citrix Virtual Apps and Desktops connectés au compte Citrix Cloud actuel.

   Si vous êtes déjà abonné à Citrix Virtual Apps and Desktops Service, le site du service est automatiquement répertorié. Vous pouvez cliquer sur le menu à points en regard du site de service et choisir **Enable Integration** ou **Disable Integration** pour activer ou désactiver l'intégration, respectivement.

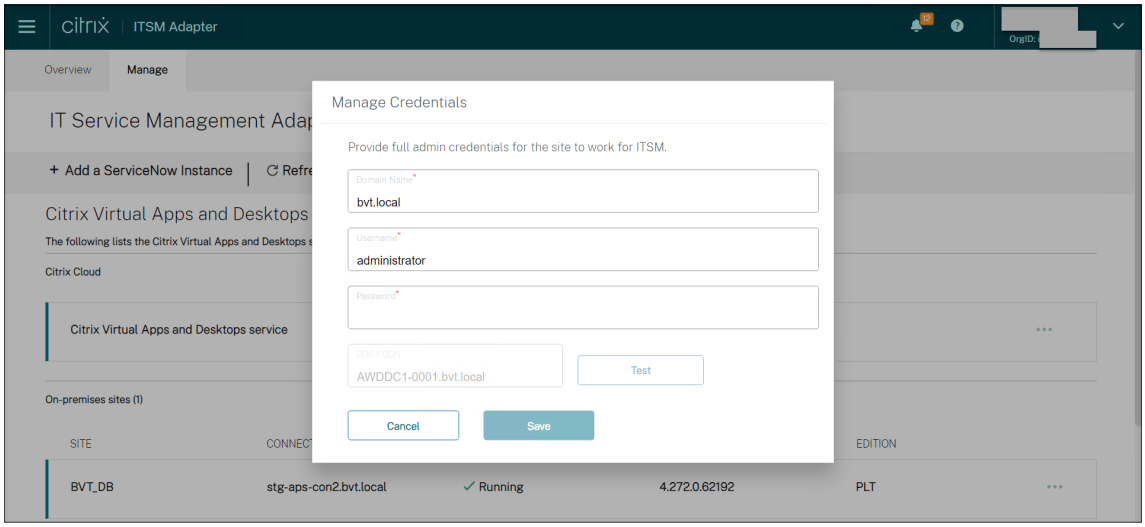
   Si le site local que vous souhaitez gérer n'est pas répertorié, vous devez l'ajouter via l'agrégation de sites.



4. Ajoutez un site local via l'agrégation de sites.
5. Pour un site local récemment ajouté, sélectionnez **Manage Credentials** dans le menu à points.



6. Fournissez les informations d'identification complètes de l'administrateur pour le site.



7. Cliquez sur **Test** pour vérifier la connexion.

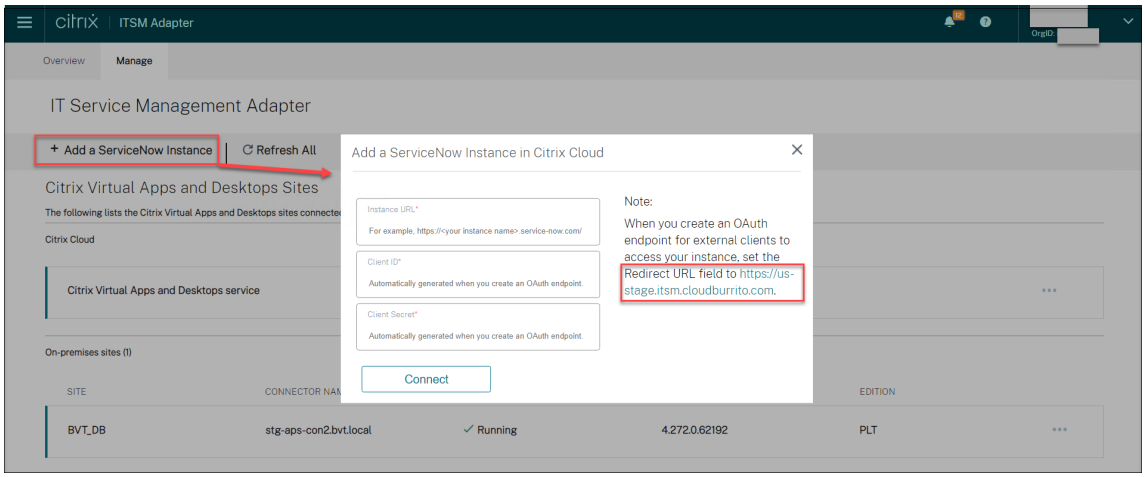
   Le site est maintenant en cours d'exécution et connecté au service ITSM Adapter.

8. Cliquez sur **Save**.

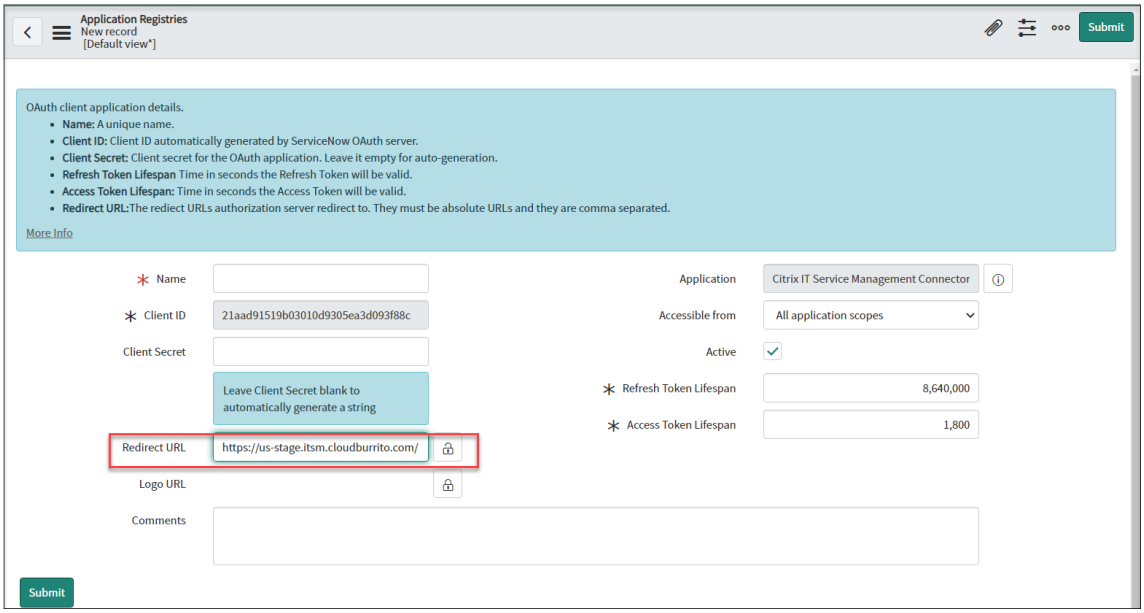
Étape 4 : Ajouter une instance ServiceNow dans Citrix Cloud

> **Remarque :**
>
> Cette étape est nécessaire pour ajouter Citrix Cloud en tant que point de terminaison ServiceNow afin que Citrix Cloud puisse envoyer des messages tels que des alertes et des notifications à ServiceNow.

1. Cliquez sur **Ajouter une instance ServiceNow** et suivez l'assistant pour terminer les paramètres.

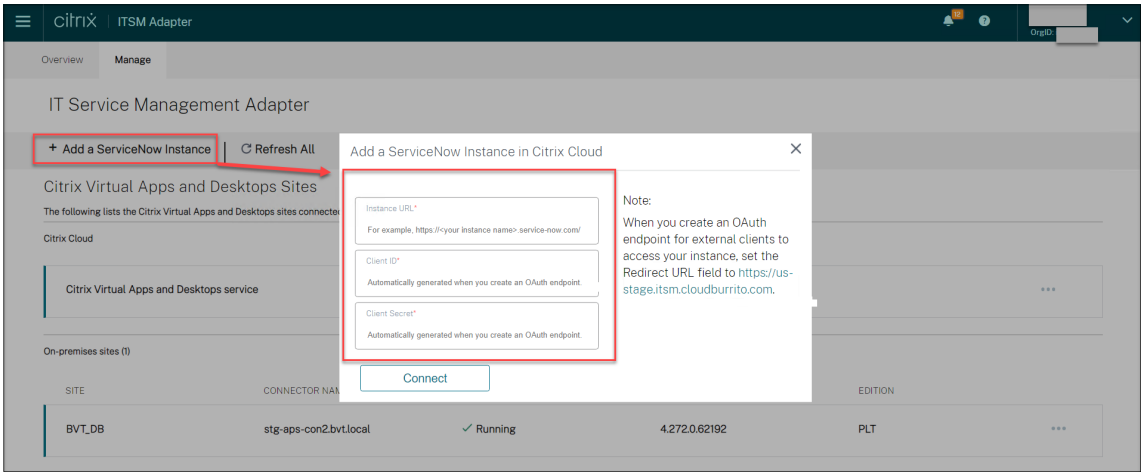


2. Créez un point de terminaison OAuth dans ServiceNow. Conservez un enregistrement de l'URL de l'instance ServiceNow, de l'ID client et de la clé secrète client.

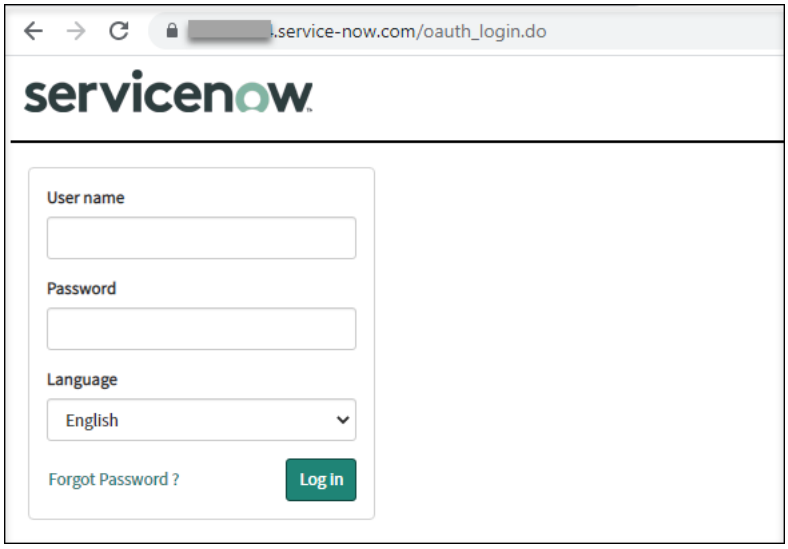


> **Remarque :**
>
> Lorsque vous créez un point de terminaison OAuth dans ServiceNow pour Citrix Cloud, définissez le champ **Redirect URL** sur la valeur demandée sur la page **Add a ServiceNow Instance in Citrix Cloud** . Dans cet exemple, https://us-stage.itsm.cloudburrito.com/.

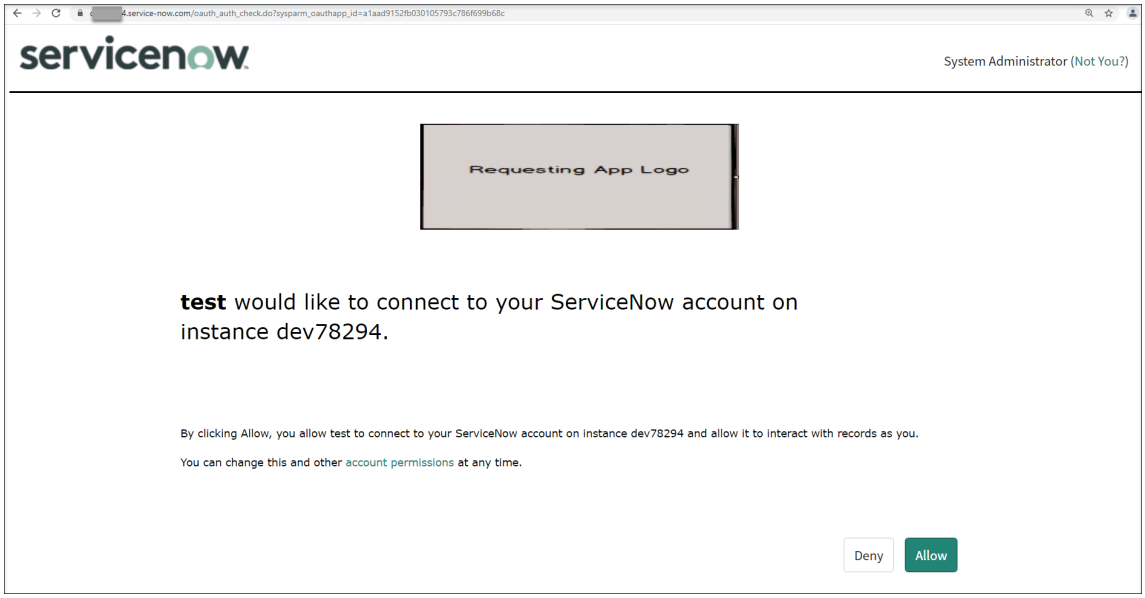
3. Remplissez les valeurs de champ que vous avez enregistrées à l'étape précédente.



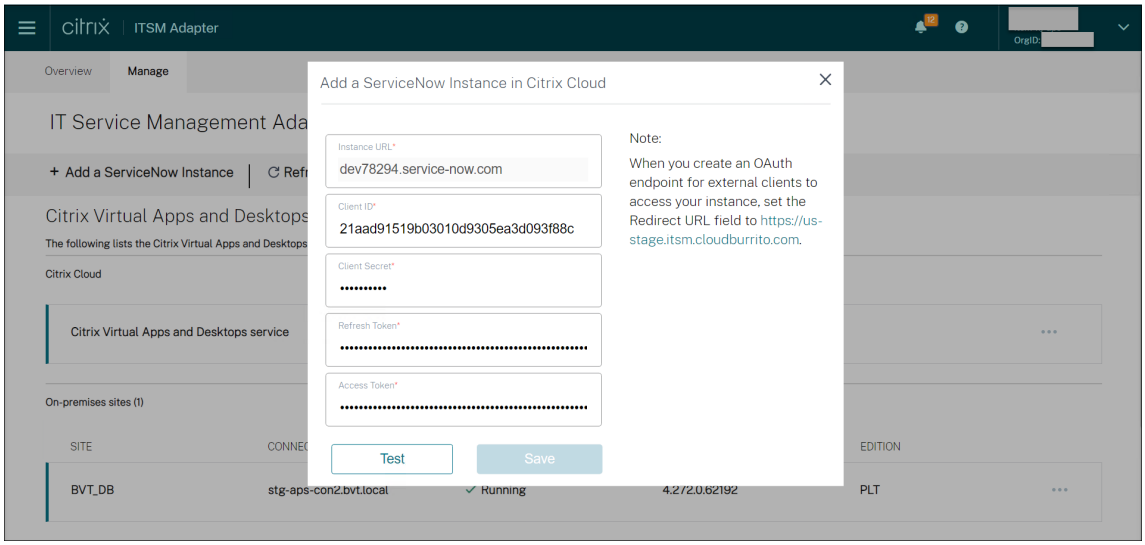
4. Cliquez sur **Connect**. La page de connexion de l'instance s'affiche.



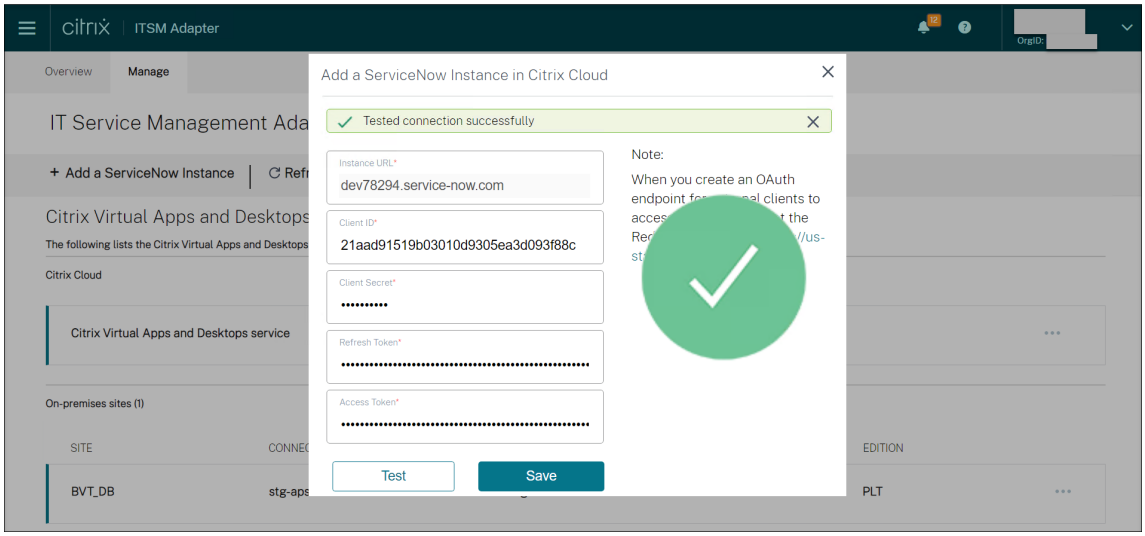
5. Tapez les informations d'identification de votre instance ServiceNow et cliquez sur **Connect**. Une page s'affiche, demandant l'autorisation au point de terminaison OAuth de se connecter à votre compte ServiceNow sur l'instance ServiceNow spécifiée.



6. Cliquez sur **Allow**. Vous revenez à l'onglet **Manage**.
7. Cliquez à nouveau sur **Add a ServiceNow Instance**. Les champs de jeton d'actualisation et de jeton d'accès sont automatiquement remplis.



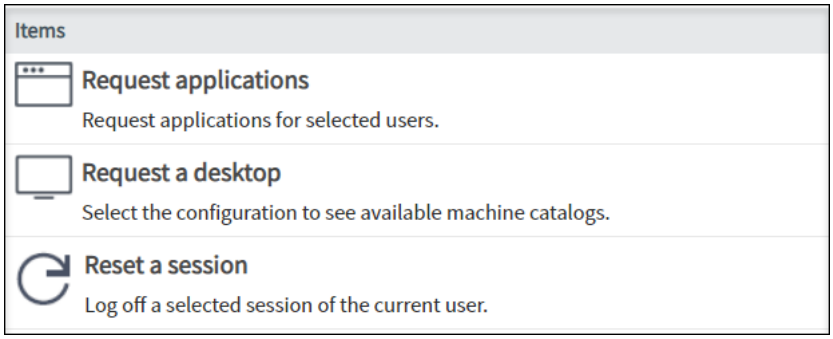
8. Cliquez sur **Test**. Le service ITSM Adapter commence à tester les connexions avec le connecteur ITSM. Le bouton Save est disponible une fois le test terminé avec succès.



9. Cliquez sur **Save** pour enregistrer l'instance dans Citrix Cloud.

Étape 5 : Publier le service ITSM Adapter dans ServiceNow

Une fois que vous avez terminé les étapes 1 à 4, vous et vos utilisateurs pouvez effectuer une recherche en utilisant **Citrix** pour localiser le service ITSM Adapter dans ServiceNow et envoyer des demandes. Pour une meilleure expérience utilisateur, nous vous recommandons de publier les éléments de service choisis sur un tableau de bord ServiceNow pour un accès facile. Par exemple :

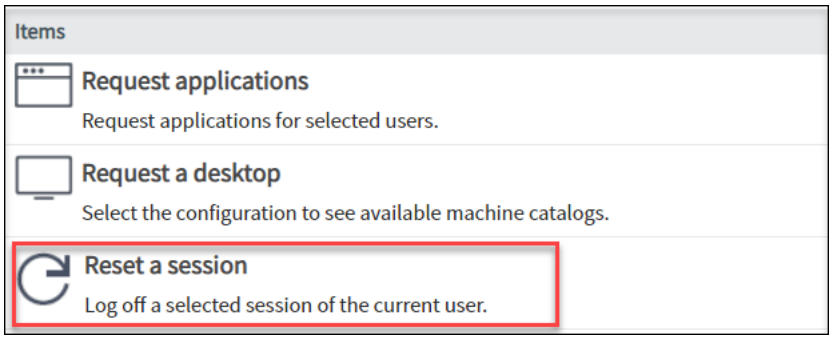


Exemples de scénarios

Reset a session (Réinitialiser une session)

Actions de l'utilisateur

1. Connectez-vous à votre instance de ServiceNow.
2. Recherchez l'entrée **Reset a session**. Par exemple :



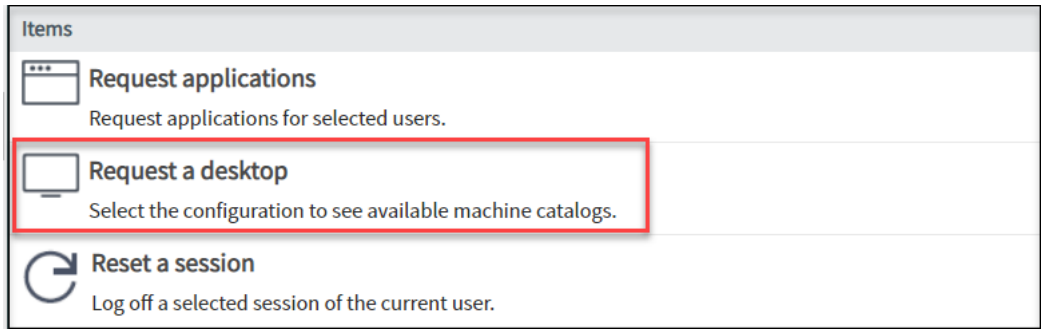
3. Sur la page **Reset a session**, sélectionnez une session de bureau ou d'application liée à l'utilisateur actuel et cliquez sur **Order Now** pour vous déconnecter de la session.

> **Remarque :**
>
> Qu'elles soient provisionnées par un administrateur ou par un utilisateur, toutes les applications exécutées sur la session sont réinitialisées.

Request a Desktop (Demander un bureau)

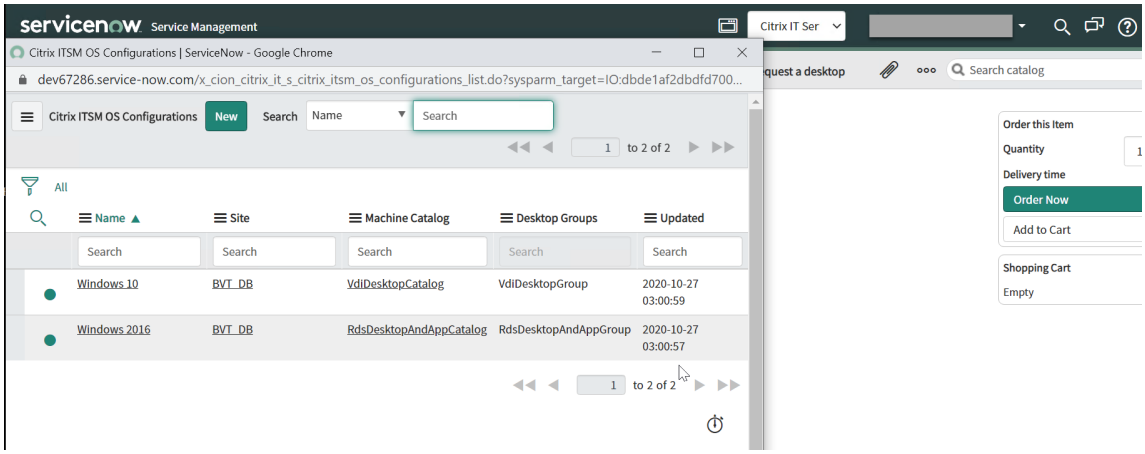
Actions de l'utilisateur

1. Connectez-vous à votre instance de ServiceNow.
2. Recherchez l'entrée **Request a desktop**. Par exemple :



3. Sur la page **Request a Desktop**, utilisez l'outil de recherche de la zone **Configuration** pour rechercher les catalogues de machines disponibles.

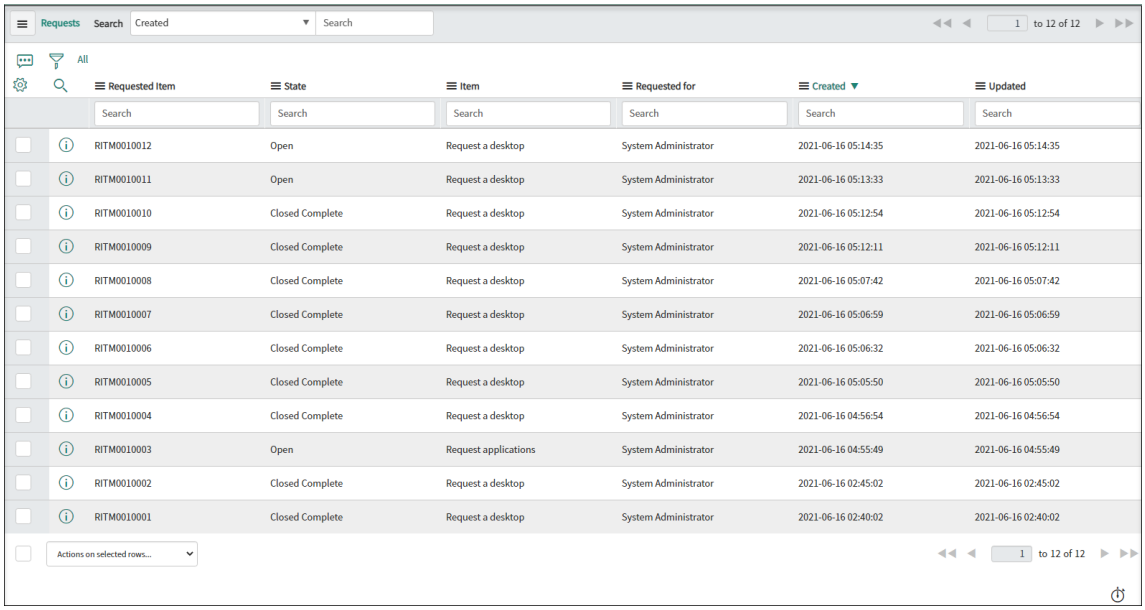
4. Sélectionnez un système d'exploitation cible et définissez la valeur **Quantity**. Cliquez sur **Order Now**.



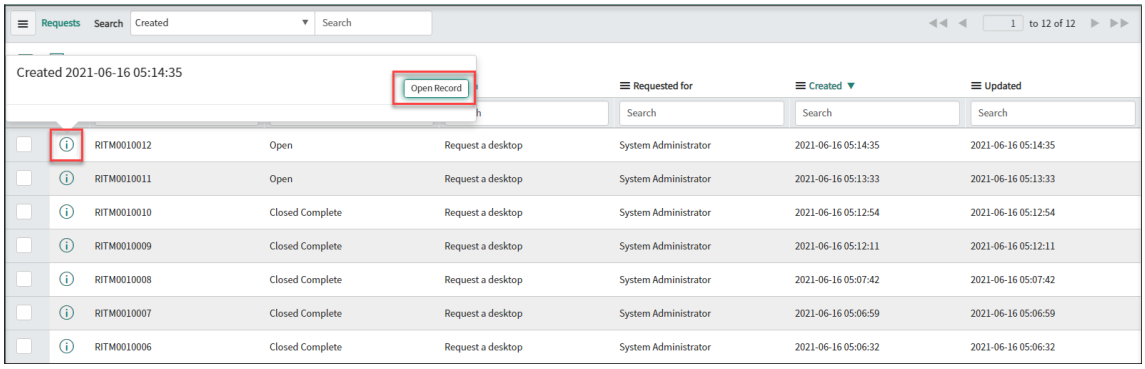
Actions administrateur

1. Connectez-vous au portail ServiceNow, dans le volet gauche, accédez à **Citrix IT Service Management Connector** et choisissez **Requests**.

   La page **Requests** affiche la liste des requêtes.

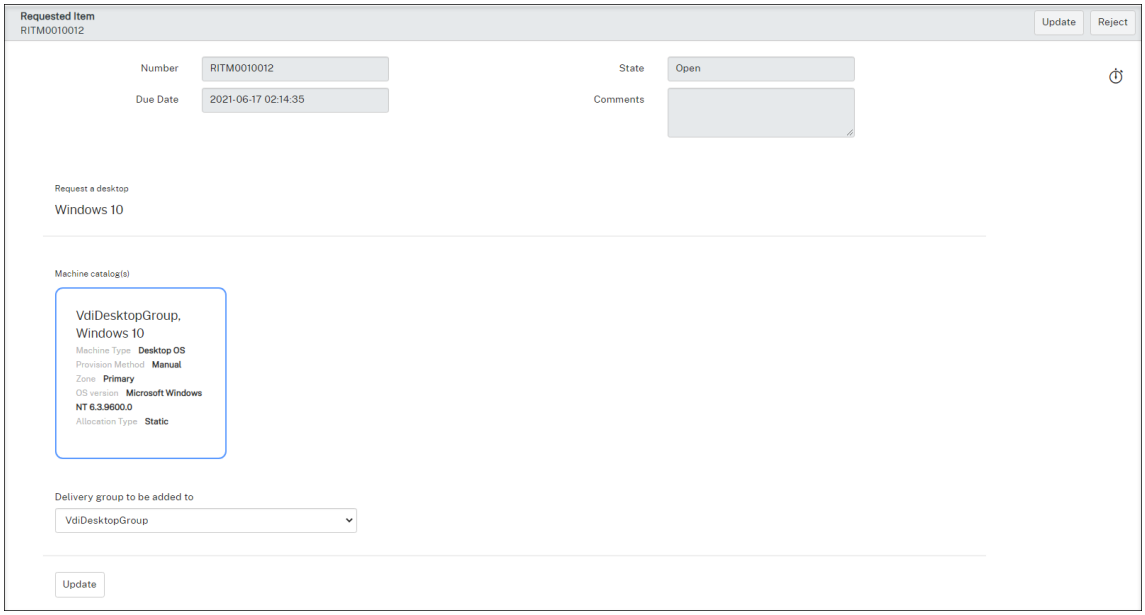


2. Cliquez sur l'icône en regard de l'ID de la requête, puis **Open Record**. Les détails de la demande apparaissent.



3. Choisissez d'abord le catalogue de machines, puis le groupe de mise à disposition dans la liste.

   Si le catalogue de machines demandé manque de machines, vous êtes invité à ajouter des machines au catalogue via MCS. Vous pouvez cliquer sur le lien hypertexte pour créer immédiatement une demande de création de machine ou lancer une demande de création de machine plus tard après la fermeture de la demande de bureau actuelle.



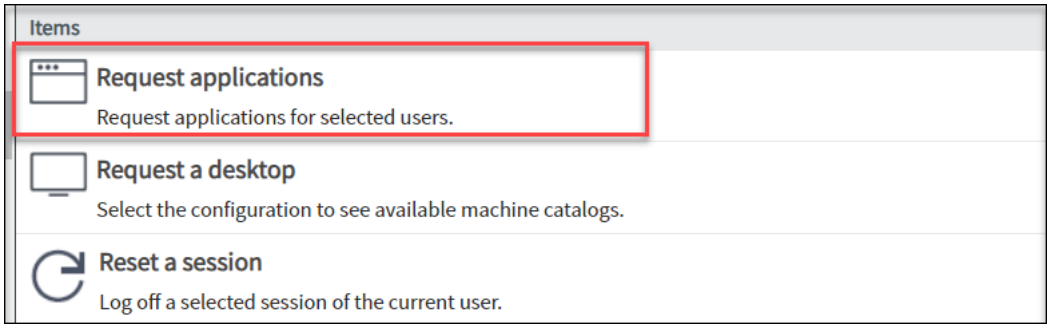
4. Cliquez sur **Update**.

Le bureau demandé est désormais provisionné et affecté à l'utilisateur.

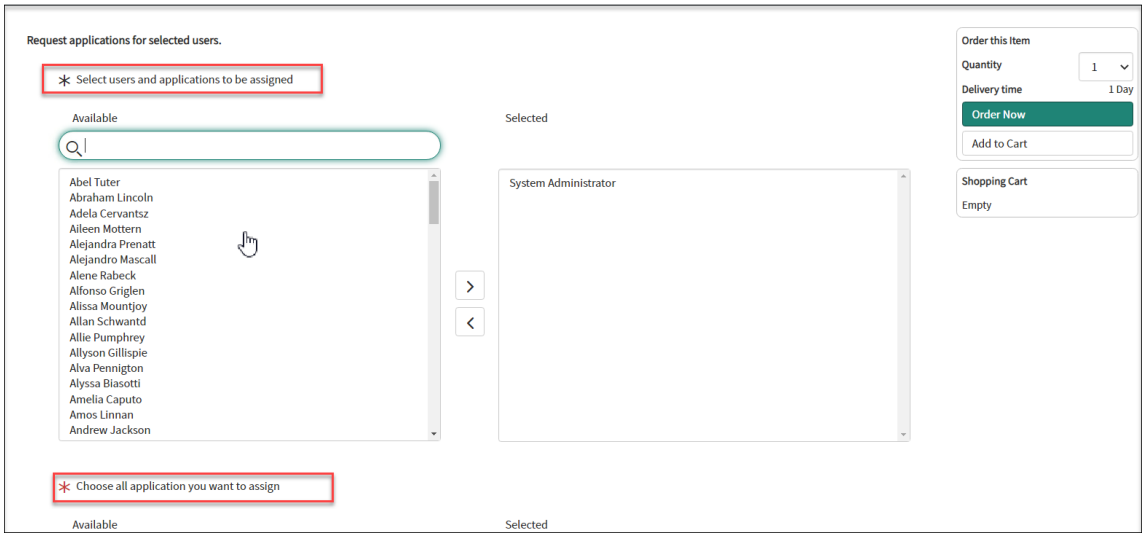
Request applications (Demander des applications)

Actions de l'utilisateur

1. Connectez-vous à votre instance de ServiceNow.
2. Recherchez l'entrée **Request applications**. Par exemple :

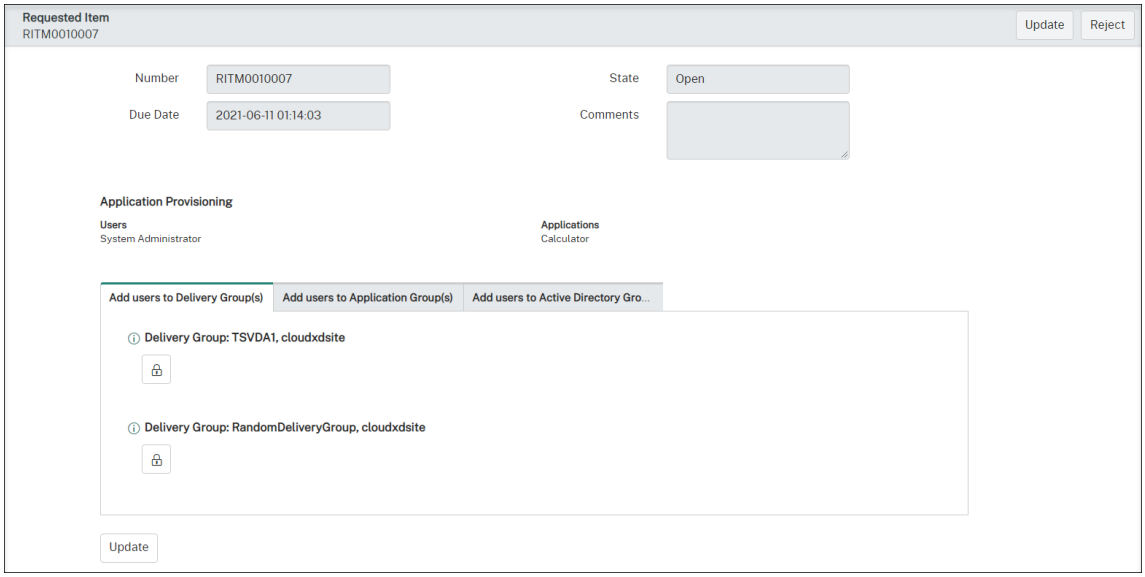


3. Sur la page **Request applications**, les utilisateurs et les applications disponibles sont répertoriés. Faites votre choix et cliquez sur **Request applications**.



Actions administrateur

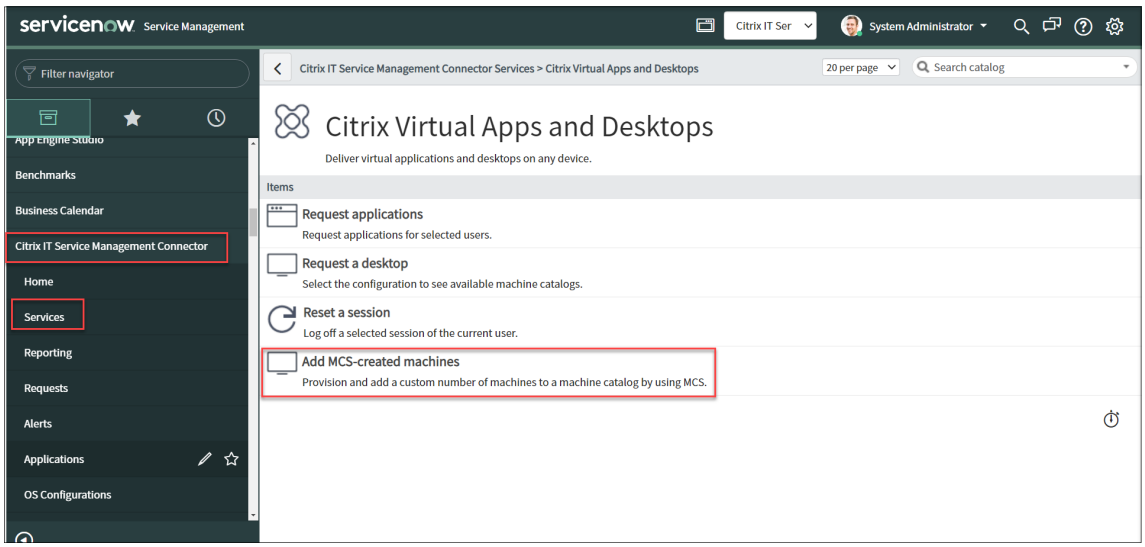
1. La page **Requests** affiche la liste des requêtes. Cliquez sur l'icône en regard de l'ID de la requête de l'application, puis sur **Open Record**. Les détails de la demande apparaissent.
2. Il existe trois options pour effectuer le provisioning d'application :
   - **Add users to Delivery Group(s)** : cliquez sur l'icône de verrouillage pour ajouter des utilisateurs au groupe de mise à disposition spécifique, puis cliquez sur **Update**.
   - **Add users to Application Group(s)** : cliquez sur l'icône de verrouillage pour ajouter des utilisateurs au groupe d'applications spécifique, puis cliquez sur **Update**.
   - **Add users to Active Directory Group(s)** : cliquez sur l'icône de verrouillage pour ajouter des utilisateurs au groupe Active Directory spécifique, puis cliquez sur **Update**.



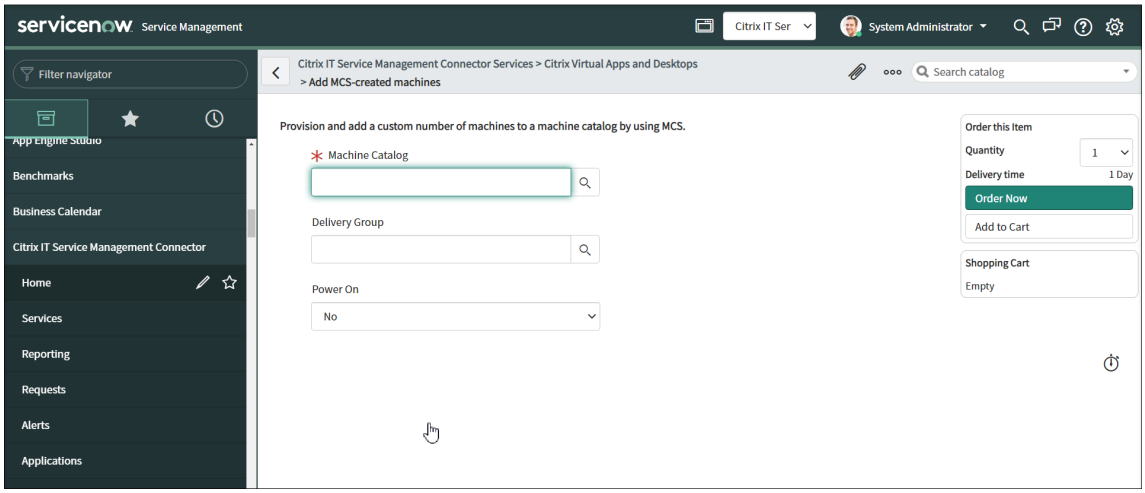
> **Remarque :**
>
> - Le connecteur ITSM synchronise périodiquement les configurations à partir de Citrix Cloud. Actuellement, le cycle de synchronisation est d'une heure. Le contenu de chaque onglet reflète les paramètres spécifiques à l'application demandée dans Citrix Virtual Apps and Desktops. Par exemple, l'onglet **Add users to Active Directory Group(s)** affiche tous les groupes AD associés à l'application demandée.
> - Pour vous assurer que l'onglet **Add users to Active Directory Group(s)** fonctionne comme prévu, activez la solution **Active Directory Automation** dans ServiceNow afin que le connecteur Citrix ITSM puisse multiplier le canal d'automatisation AD pour définir les utilisateurs dans AD ou Azure AD.

Ajouter des machines créées par MCS

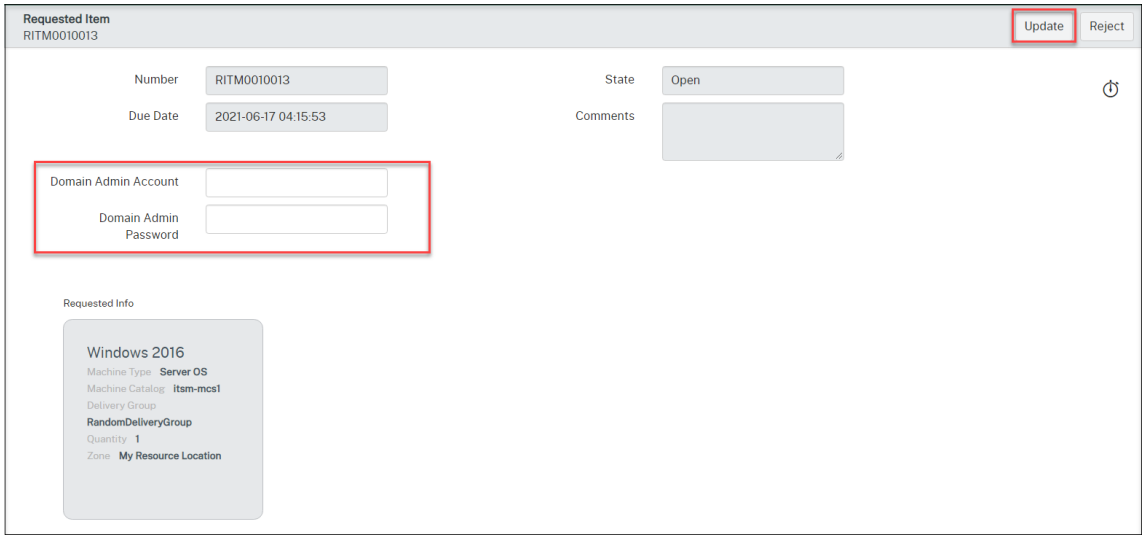
1. Connectez-vous à votre instance de ServiceNow.
2. Dans le volet gauche, accédez à **Citrix IT Service Management Connector** et choisissez **Services**.
3. Sur la page **Citrix IT Service Management Connector Services**, cliquez sur **Citrix Virtual Apps and Desktops**. Les services suivants s'affichent :
   - Request applications (Demander des applications)
   - Request a Desktop (Demander un bureau)
   - Reset a session (Réinitialiser une session)
   - Ajouter des machines créées par MCS



4. Choisissez **Add MCS-created machines**.

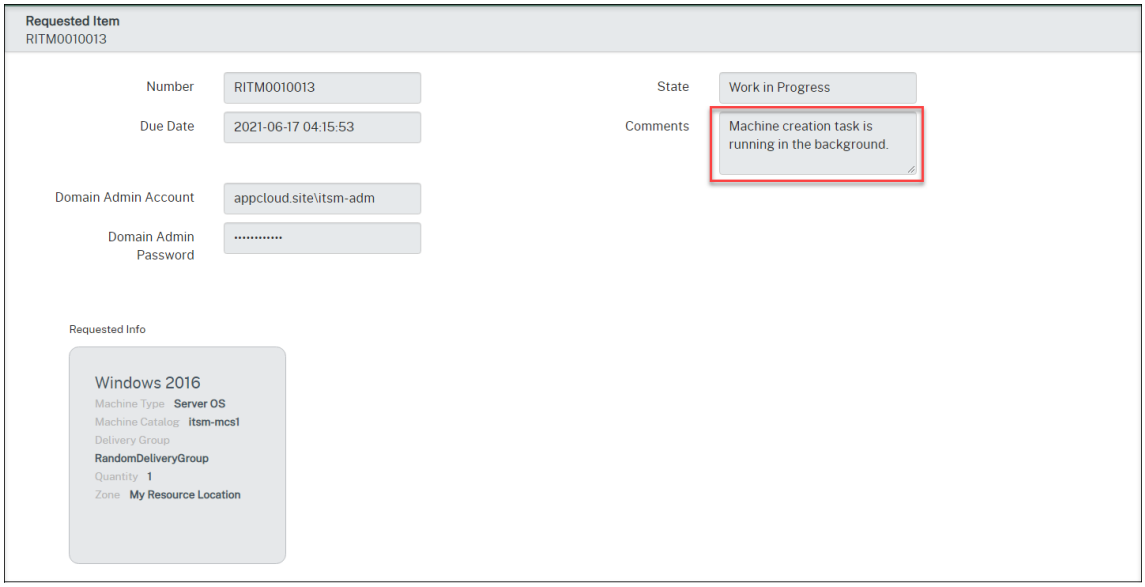


5. Définissez les champs et spécifiez le nombre (Quantity) de machines que vous souhaitez créer.
6. Cliquez sur **Order Now**.
7. Accédez à la page **Requests**.
8. Ouvrez l'enregistrement de la demande de création de machine.



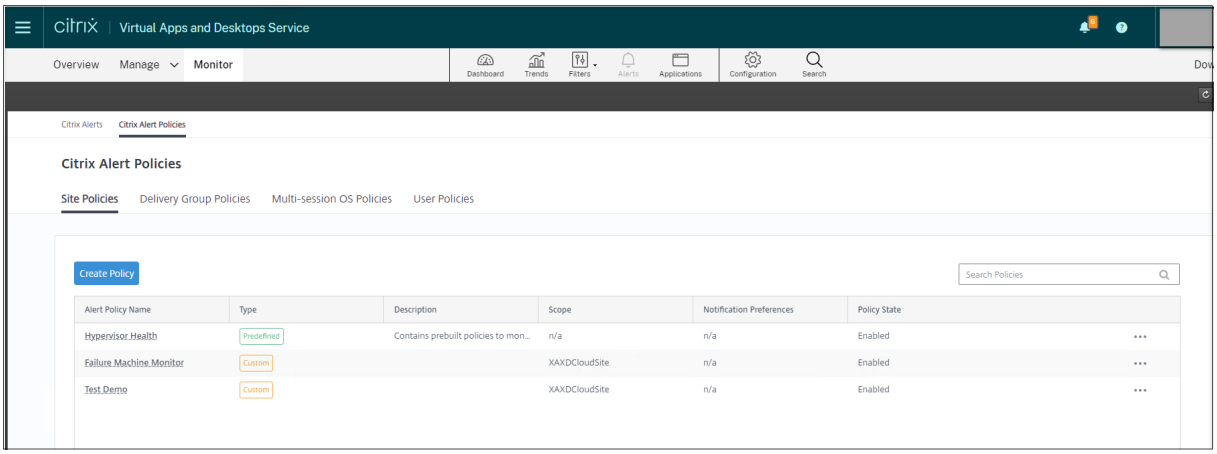
9. Saisissez vos informations d'identification de domaine, puis cliquez sur **Update**. La création d'une machine s'exécute en arrière-plan. Attendez que la création de la machine soit terminée.

   Les informations d'identification de domaine que vous fournissez sont destinées à une utilisation unique. Elles ne seront ni stockées ni mises en cache.

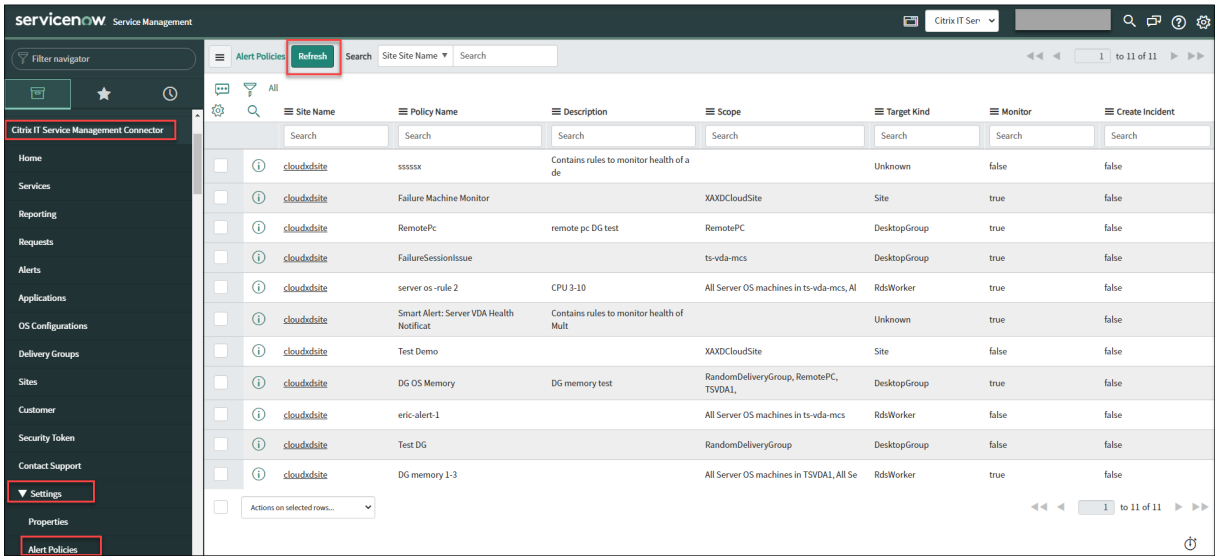


Accéder aux alertes Citrix depuis ServiceNow

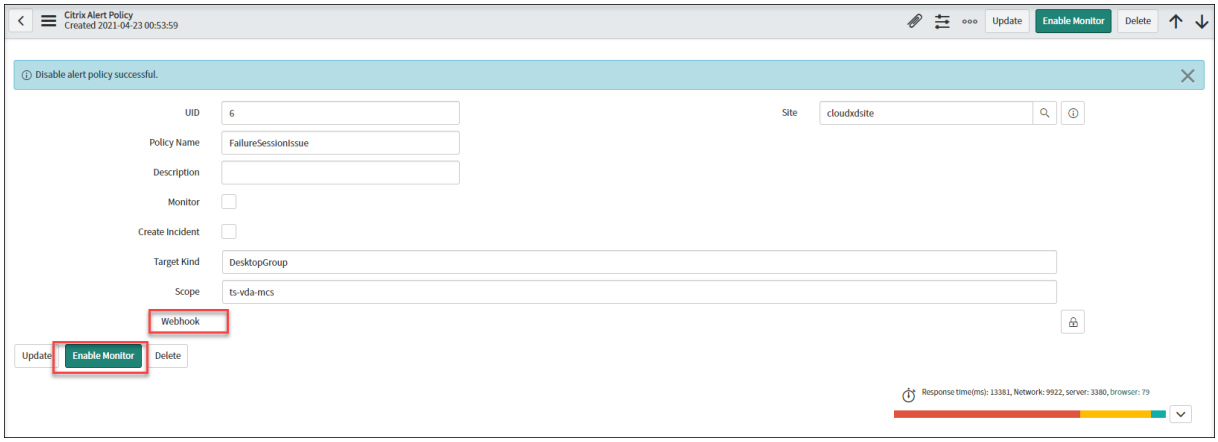
Sous l'onglet **Surveiller** du portail Citrix Virtual Apps and Desktops Service, vous pouvez définir des stratégies d'alerte pour surveiller l'état de fonctionnement de votre environnement.



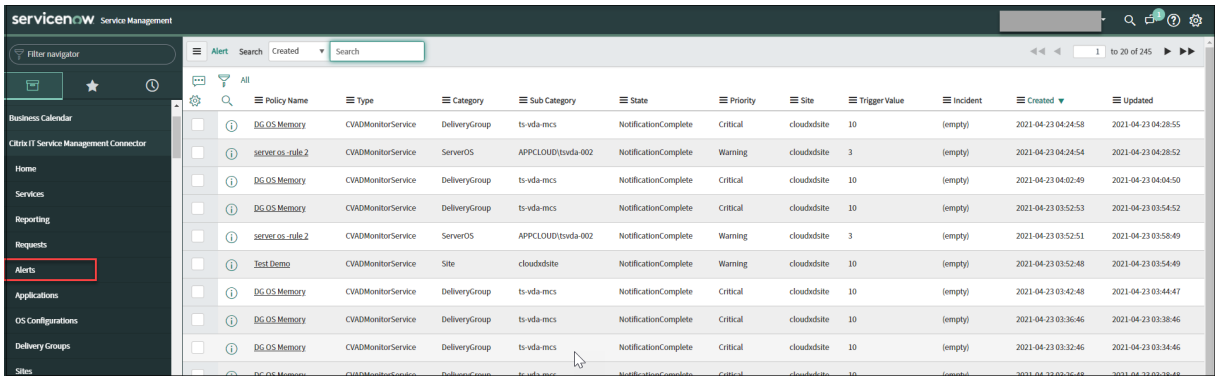
Les stratégies d'alerte sont périodiquement synchronisées avec le portail ServiceNow, sous **Citrix IT Service Management Connector > Settings > Alert Policies**. Actuellement, le cycle de synchronisation est d'une heure. Pour synchroniser immédiatement les stratégies d'alerte, cliquez sur **Refresh**.



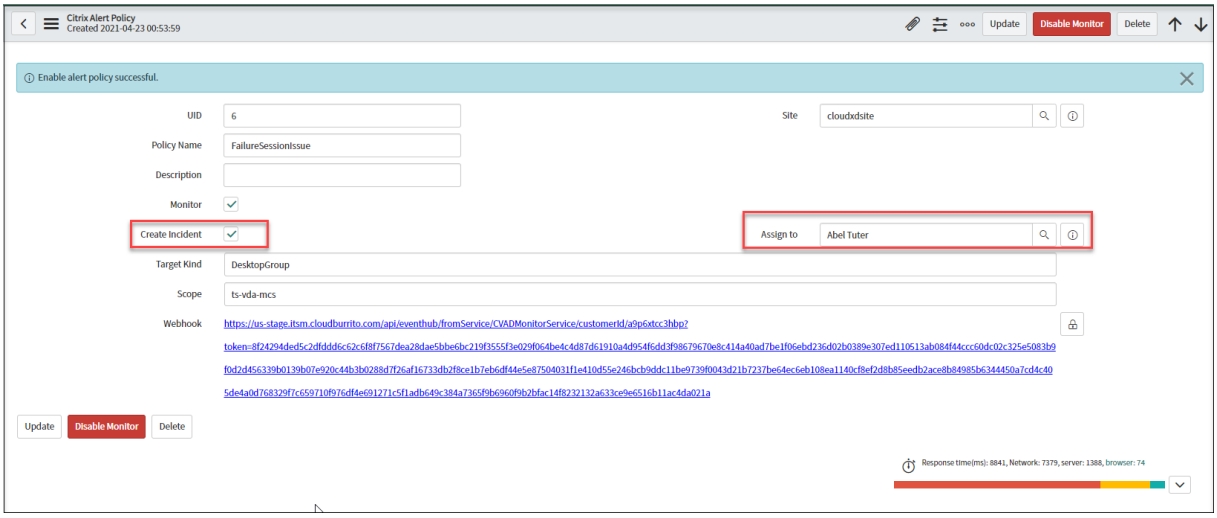
Vous pouvez ouvrir une stratégie d'alerte de votre choix et cliquer sur **Enable Monitor**. Ensuite, les alertes répondant à la stratégie peuvent être répertoriées dans ServiceNow sous **Citrix IT Service Management Connector > Alerts**.



La capture d'écran suivante affiche les alertes présentées dans ServiceNow.



Vous pouvez également créer des incidents et les affecter à des personnes spécifiques qui gèrent les alertes.



Si le moniteur est désactivé, les alertes répondant à la stratégie ne sont pas synchronisées avec ServiceNow.

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

January 22, 2021

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 de plus amples informations, consultez la section CTX220717.

Prise en main du License Usage Insights Service

July 21, 2021

Étape 1 : Mettre à jour le serveur de licences Citrix

Le License Usage Insights Service requiert le serveur de licences Citrix 11.16.3.0 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 sur 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 de votre mot de passe.

Étape 3 : Enregistrer le serveur de licences Citrix avec Citrix Cloud

Pour afficher les détails des licences pour différents produits dans Informations sur l'utilisation des licences, enregistrez votre serveur de licences auprès de Citrix Cloud. Pour plus d'informations sur l'enregistrement de votre serveur de licences avec Citrix Cloud, reportez-vous à la section Enregistrer et supprimer l'enregistrement de votre serveur de licences Citrix.

Étape 4 : Utiliser le License Usage Insights Service

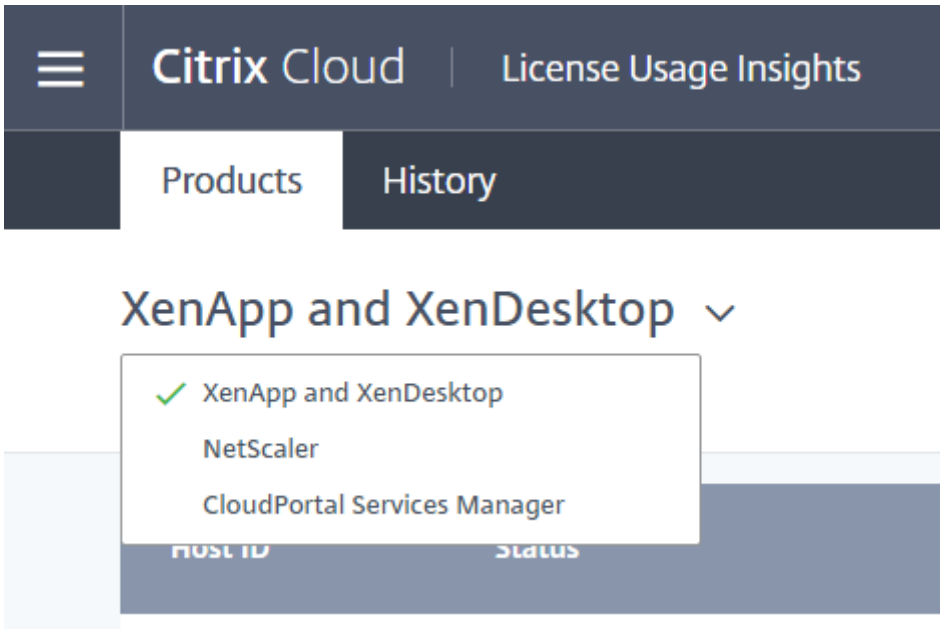
À partir de la console Citrix Cloud, recherchez le License Usage Insights Service et cliquez sur **Gérer**. Pour obtenir un aperçu des fonctionnalités principales du service, consultez la section Utiliser le License Usage Insights Service.

Utiliser le License Usage Insights Service

November 10, 2020

Sélection du produit

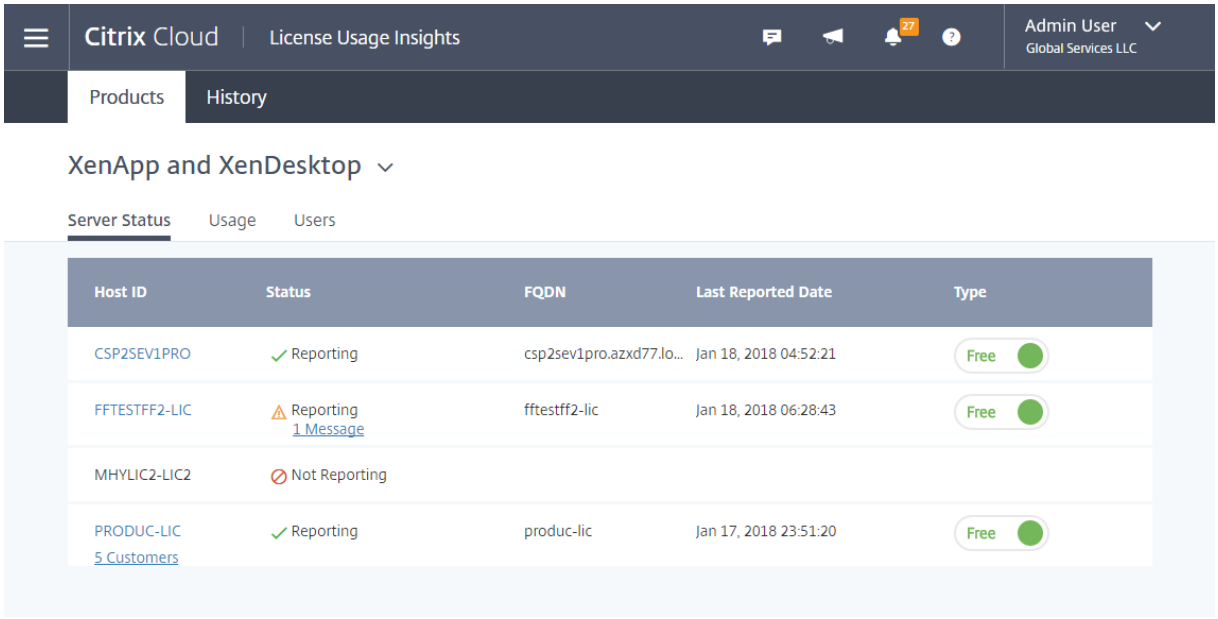
Pour afficher les détails de licence d'un produit différent, cliquez sur la flèche en regard du nom du produit et sélectionnez le produit que vous souhaitez afficher.



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.

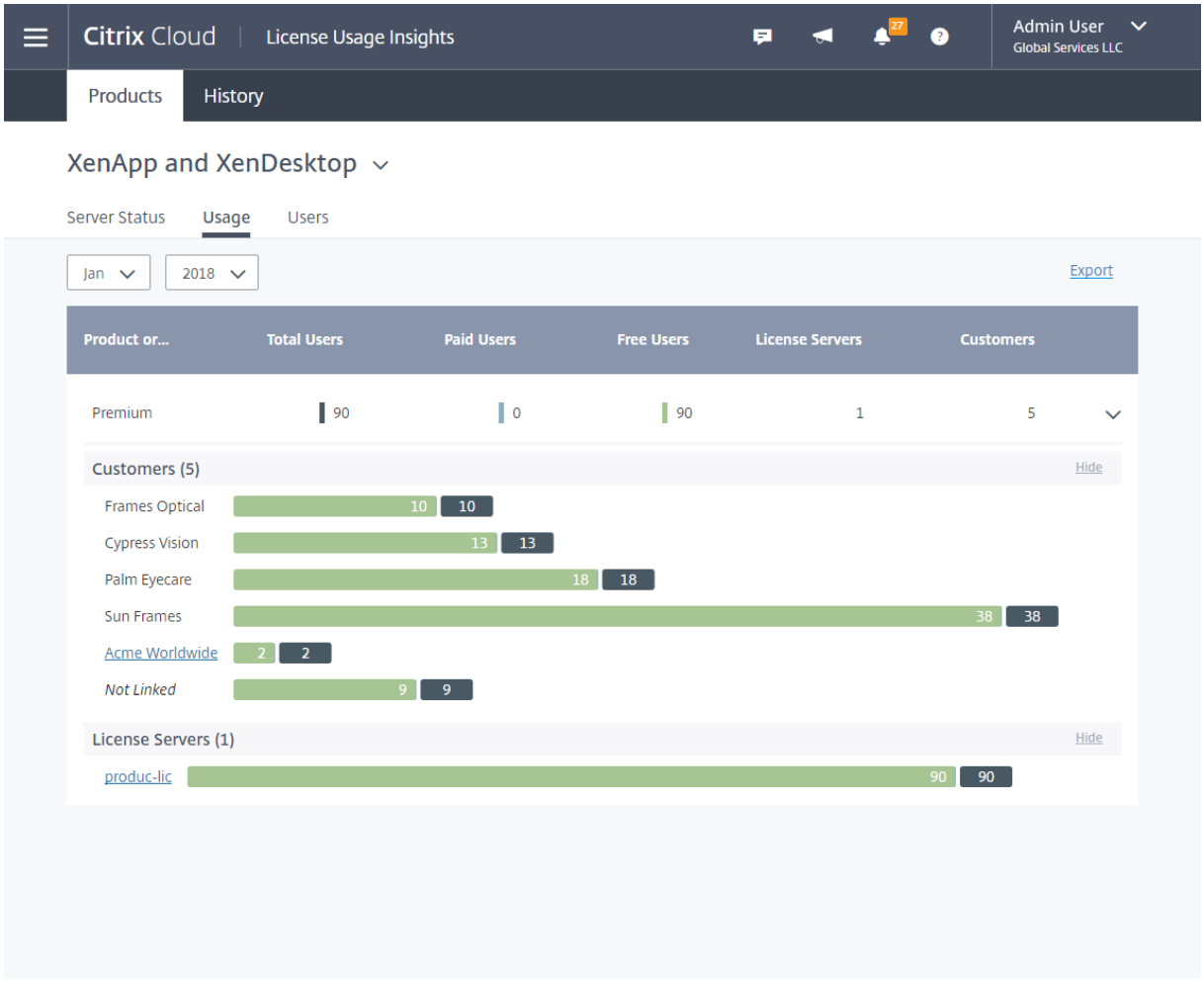


Collecte des données d'utilisation

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.

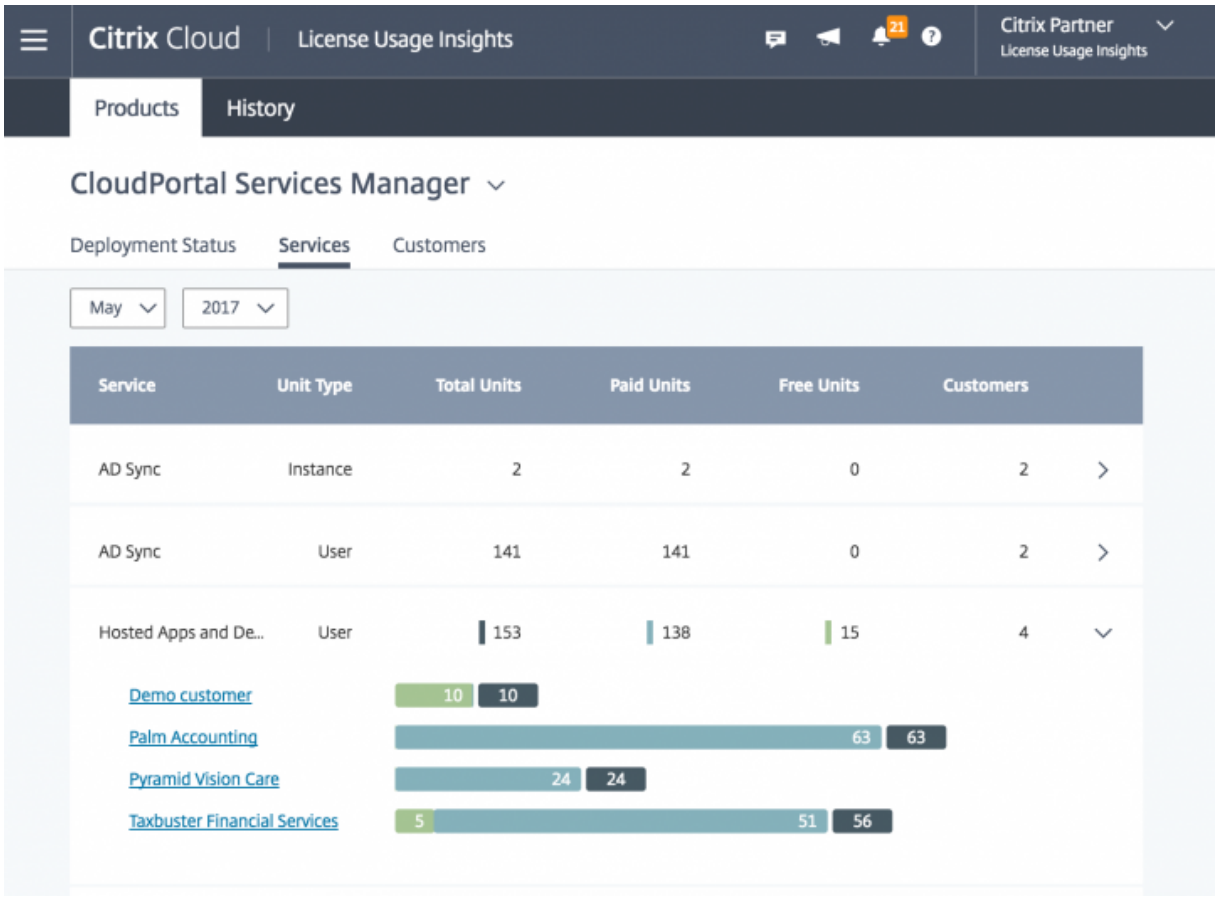
1. Le cas échéant, ajoutez des clients au tableau de bord Clients : dans la page d'accueil de la console de gestion Citrix Cloud, cliquez sur **Clients**, sur **Ajouter ou Inviter**, puis suivez les instructions à l'écran.
2. Cliquez sur le bouton de menu, puis sélectionnez **Mes services > License Usage 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**.

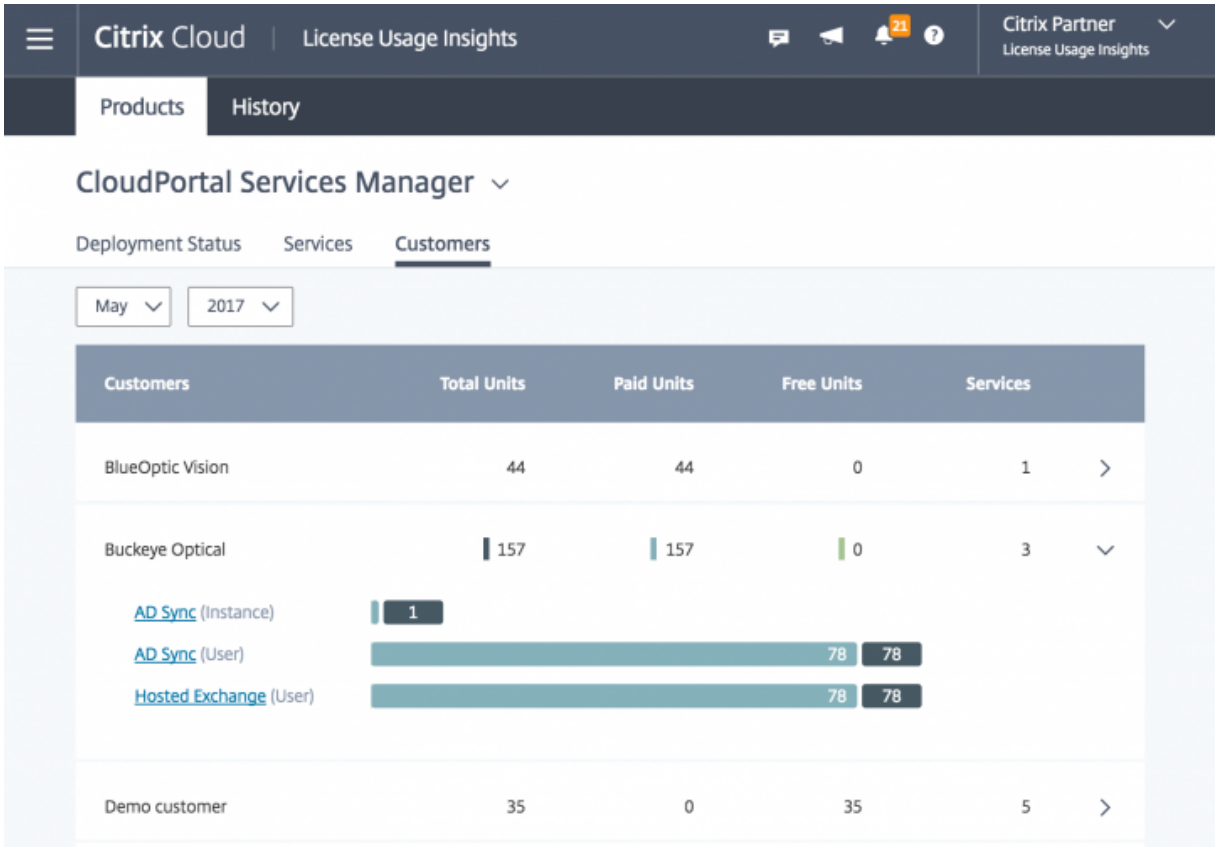
Rapports d'utilisation pour CloudPortal Services Manager

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.

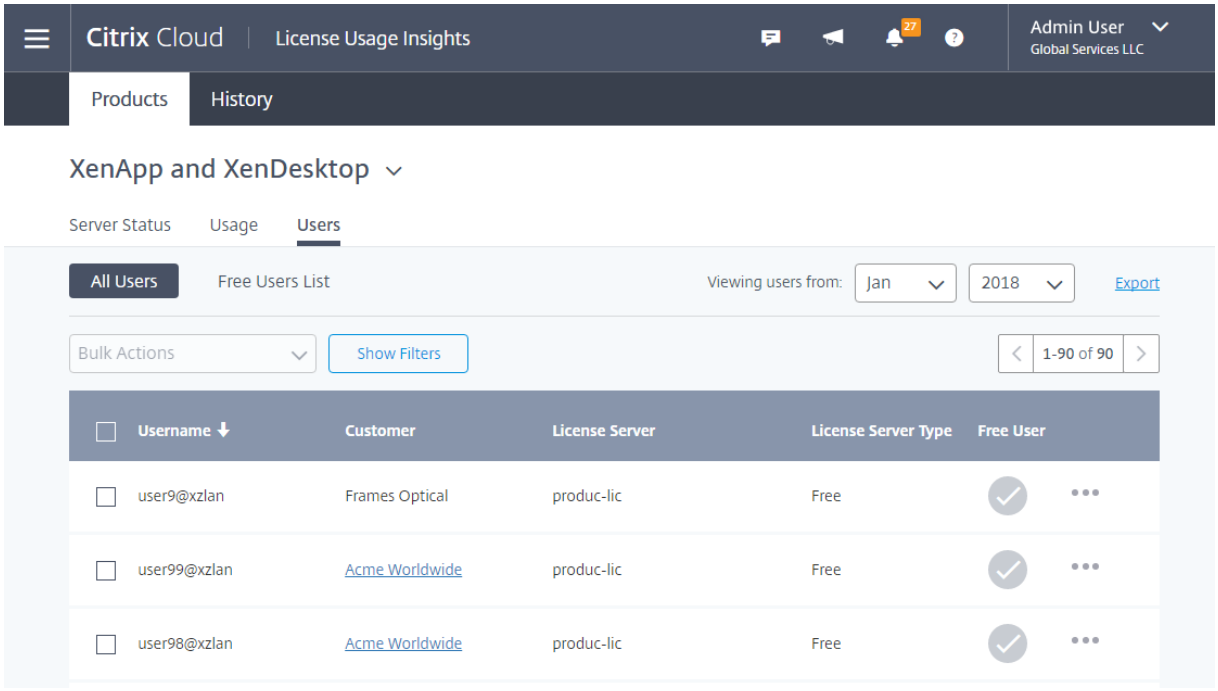


La vue Clients présente des données similaires à la vue Services, mais dans un format différent. Cette vue vous aide à comprendre les services qu'un client spécifique utilise ou consomme. Lorsque vous sélectionnez un client spécifique, vous pouvez explorer plus en détail les services CPSM que ce client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

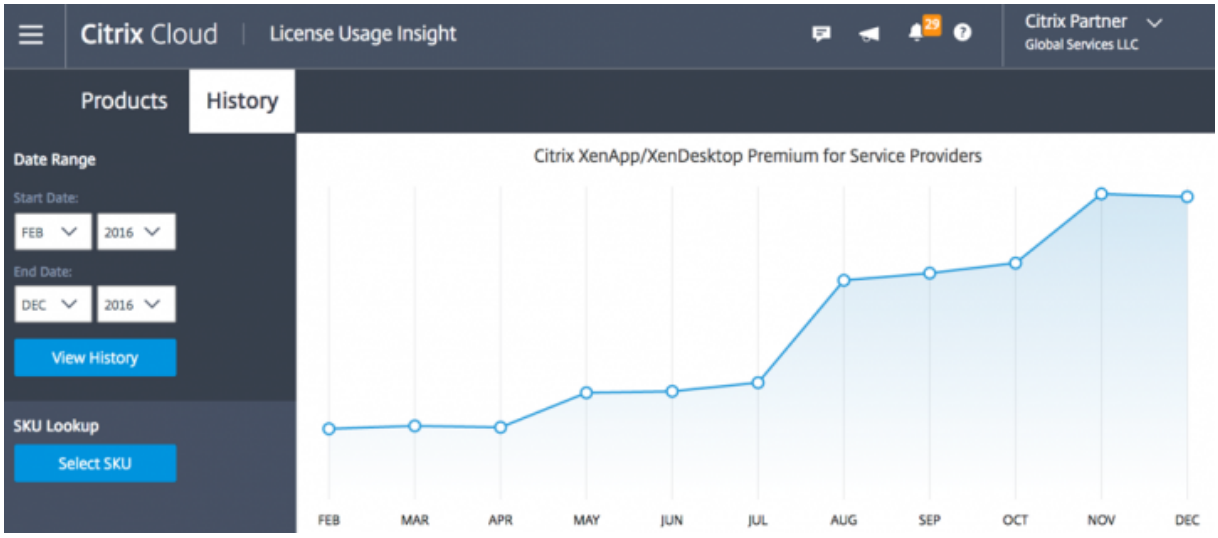


> **Remarque :**
>
> Les utilisateurs gratuits de CloudPortal Services Manager (CPSM) ne sont visibles que dans le service LUI. La gestion des utilisateurs CPSM gratuits se produit dans la console CPSM.

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

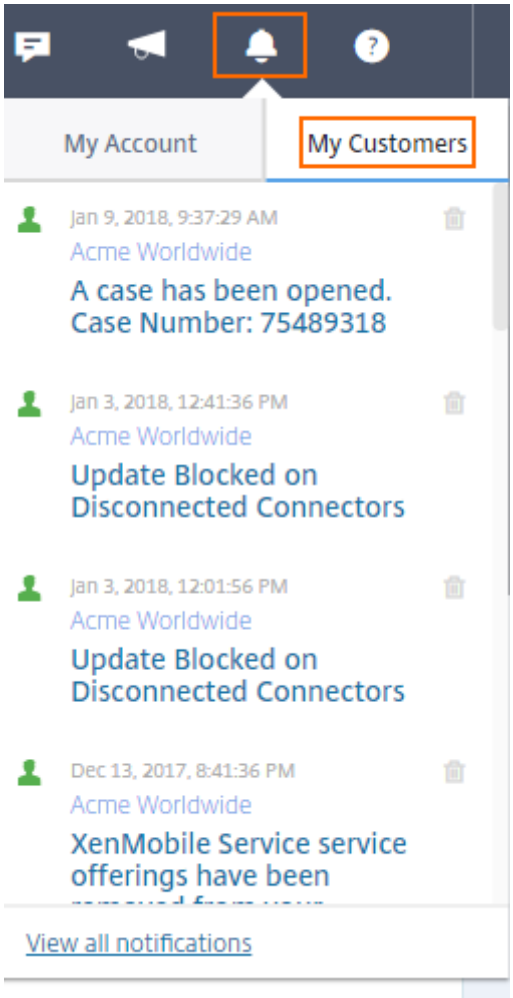
Vous pouvez exporter les types de données suivants en tant que fichier CSV à partir du service LUI :

- 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

June 10, 2021

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 11.16.3.0 ou une version ultérieure.

À propos du serveur de licences Citrix

Le serveur de licences Citrix 11.16.3.0 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. Mise 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**, ajoutez le paramètre **UsageBasedBillingScramble** :

```
<?xml version="1.0" encoding="utf-8"?>
<Configurations>
<EncoreConfiguration>
<SamplingPeriod>15</SamplingPeriod>
<RetentionTime>180</RetentionTime>
<Enabled>true</Enabled>
</EncoreConfiguration>
<SARenewalConfigOptions>Notify</SARenewalConfigOptions>
<UsageBasedBillingScramble>1</UsageBasedBillingScramble>
</Configurations>
```

3. 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.

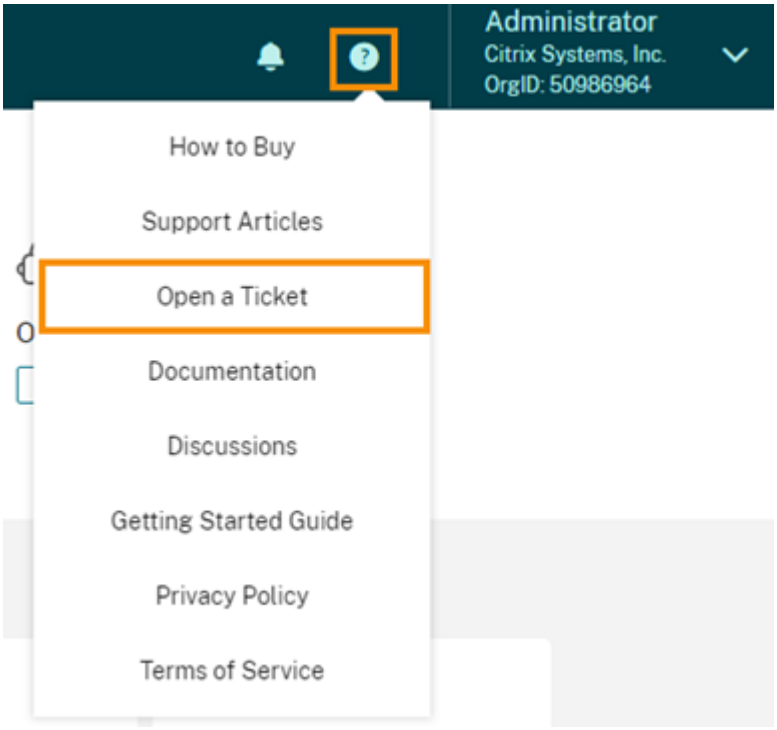
Questions fréquemment posées

January 22, 2021

- **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 plus de détails, consultez la section Utiliser le 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 plus de détails, 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 de plus amples informations, consultez la section 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.

MDX Service

July 21, 2021

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. MDX Service permet d'encapsuler les applications créées dans votre organisation. Vous pouvez ensuite gérer les applications avec Citrix Endpoint Management.

MDX Service peut utiliser MDX version 21.6.0 pour encapsuler des applications tierces.

Annonces

- **Problèmes WKWebView et Citrix SSO**

  Citrix a commencé à prendre en charge WKWebView pour les applications de productivité mobiles à partir de la version 20.11.x, après qu'Apple ait mis fin à la prise en charge des applications utilisant UIWebView. WKWebView est un framework Apple qui a remplacé le framework UIWebView précédemment utilisé. En raison des limitations techniques et de la complexité de WKWebView, certains problèmes de tunneling peuvent survenir avec certains sites Web.

  Citrix peut être en mesure de fournir des analyses et suggérer des modifications à la façon dont vous affichez votre site Web. Cependant, si vous rencontrez des problèmes, nous vous recommandons d'utiliser l'application Citrix SSO pour le tunnel VPN.

  Pour plus d'informations sur Citrix SSO, reportez-vous à la section Clients Citrix Gateway.

- Un SDK MAM (Mobile Application Management ou Gestion d'applications mobiles) est disponible pour remplacer les zones de fonctionnalités MDX qui ne sont pas couvertes par les plates-formes iOS et Android. Pour plus d'informations sur le SDK MAM (préversion), consultez la section Citrix Developer sur SDK pour la gestion des applications mobiles (SDK MAM). Vous pouvez trouver plus d'informations dans cet article de blog Citrix.

  Le SDK peut être téléchargé lorsque vous vous connectez à Téléchargements de Citrix.

- La technologie d'encapsulation MDX devrait atteindre la fin de son cycle de vie en septembre 2021. Pour continuer à gérer vos applications d'entreprise, vous devez incorporer le SDK MAM.

Pour de plus amples informations sur l'encapsulation d'applications iOS, consultez la section Pour encapsuler une application iOS.

Pour de plus amples informations sur l'encapsulation d'applications Android, consultez la section Pour encapsuler une application Android.

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

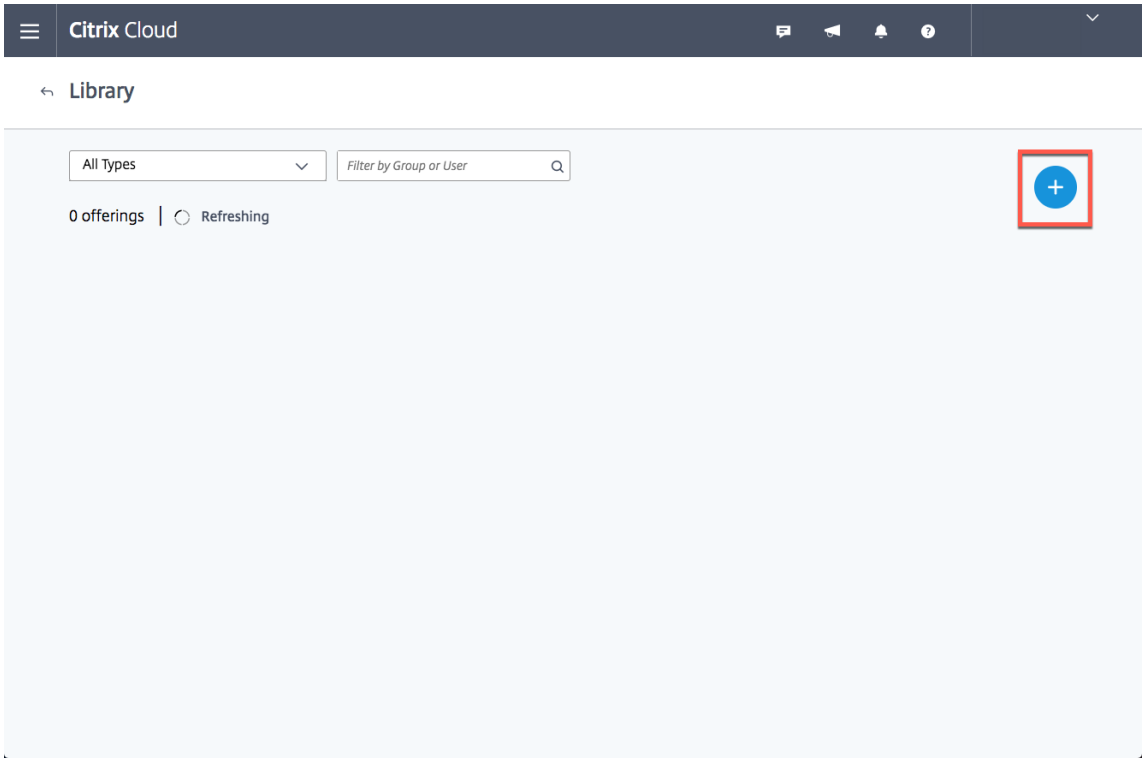
La stratégie de rétention des données pour MDX Service est la suivante :

- **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.

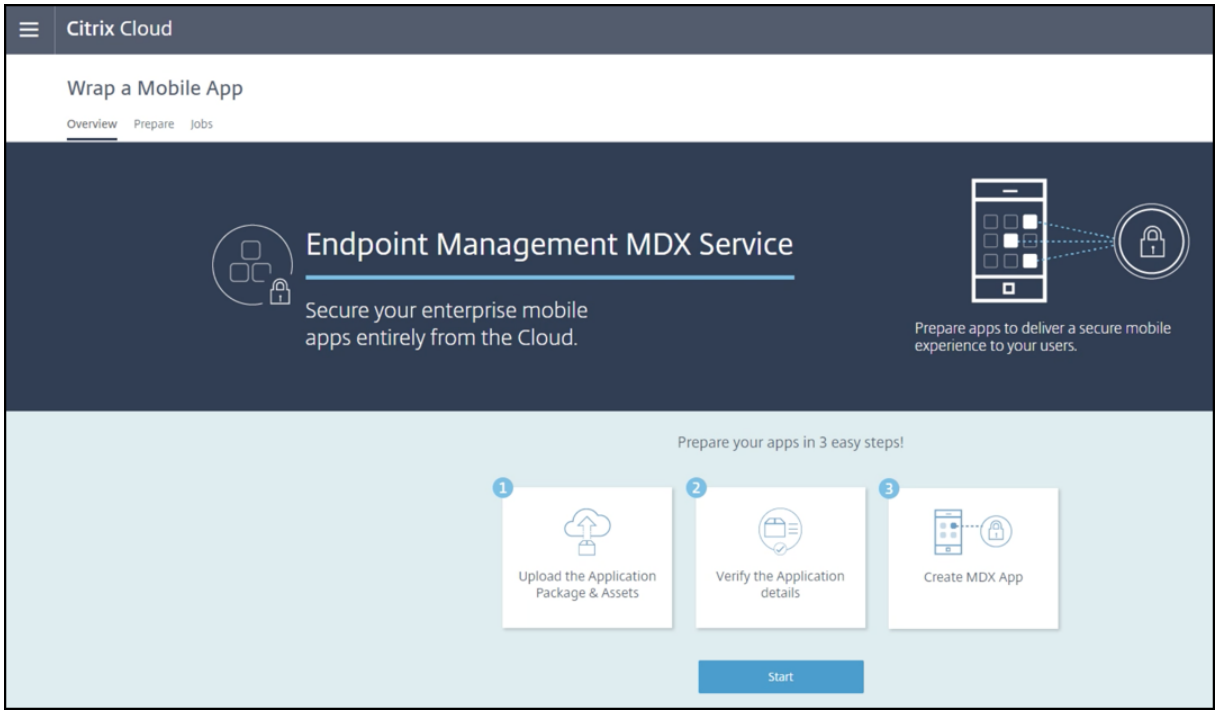
1. Inscrivez-vous à Citrix Cloud en demandant une version d'évaluation si vous ne disposez pas déjà d'un compte Citrix Cloud. Pour de plus amples informations sur l'inscription, consultez la section Ouvrir un compte sur Citrix Cloud.
2. Cliquez sur le menu hamburger dans le coin supérieur droit de la page, puis cliquez sur **Bibliothèque**.
3. 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.

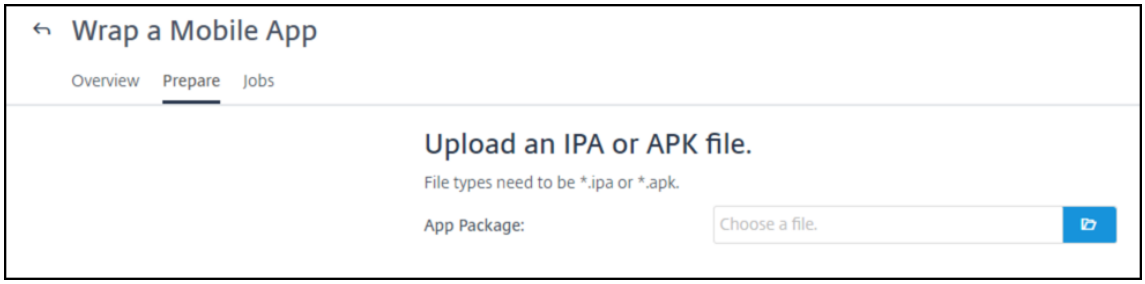
Pour démarrer, dans la page de présentation de MDX Service, en bas de l'écran, cliquez sur **Démarrer**.



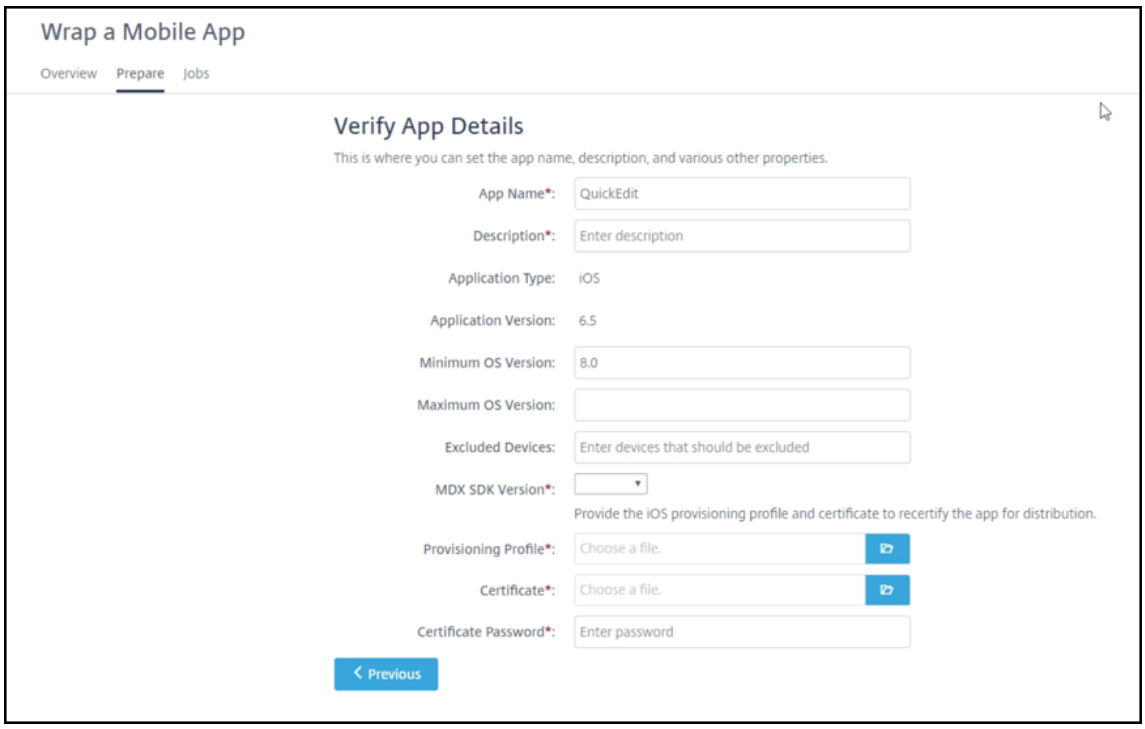
Suivez ensuite les étapes pour encapsuler une application iOS ou Android.

Pour encapsuler une application iOS

1. Chargez le fichier .ipa pour l'application. Le temps nécessaire au chargement dépend de la taille du fichier. La limite de taille de fichier autorisée pour le fichier .ipa est de 209 Mo. Si vous avez une application qui dépasse cette limite, utilisez le MDX Toolkit.



   Une fois le fichier .ipa chargé et traité avec succès, l'écran **Verify App Details** s'affiche.



2. 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).

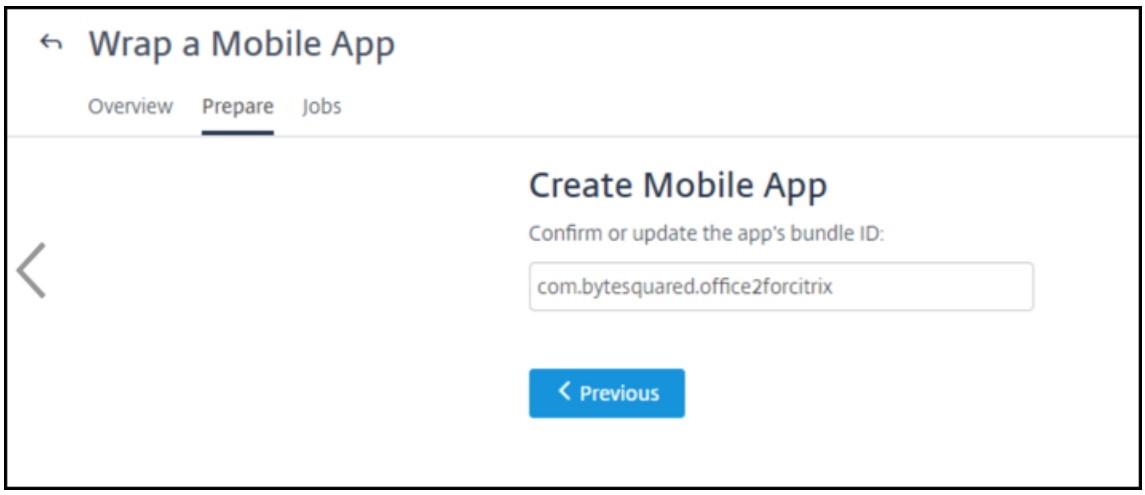
   c) Sélectionnez une version du SDK MDX avec laquelle encapsuler l'application.

   d) Chargez les ressources de signature iOS suivantes :

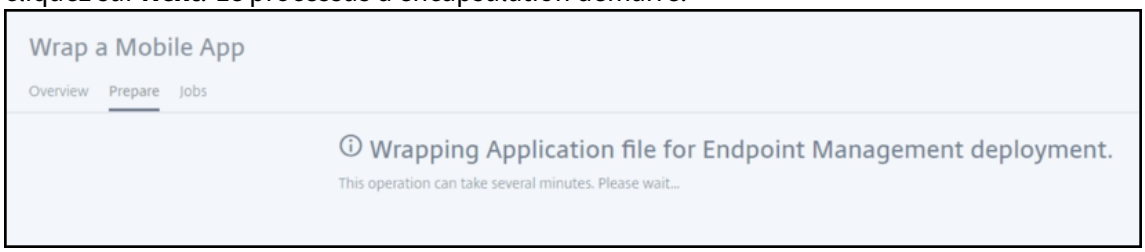
      - **Profil de provisioning**
      - **Certificat**
      - **Mot de passe du certificat**

      Pour collecter les informations sur le certificat et le profil de provisioning iOS, reportez-vous à la section « MDX Service ou MDX Toolkit » de l'article Certificats Endpoint Management sur Gestion des certificats Endpoint Management.

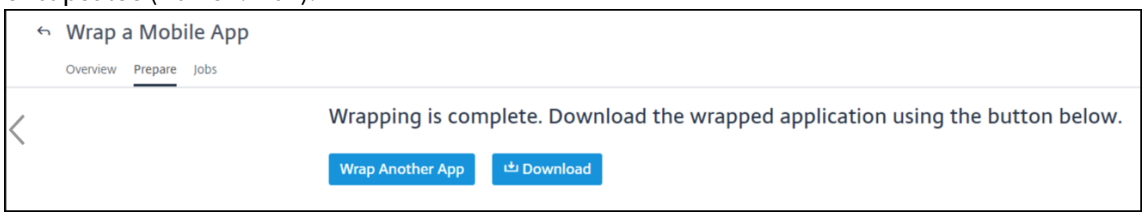
Une fois que MDX Service utilise les ressources de signature pour modifier l'application, l'écran **Create Mobile App** s'affiche.



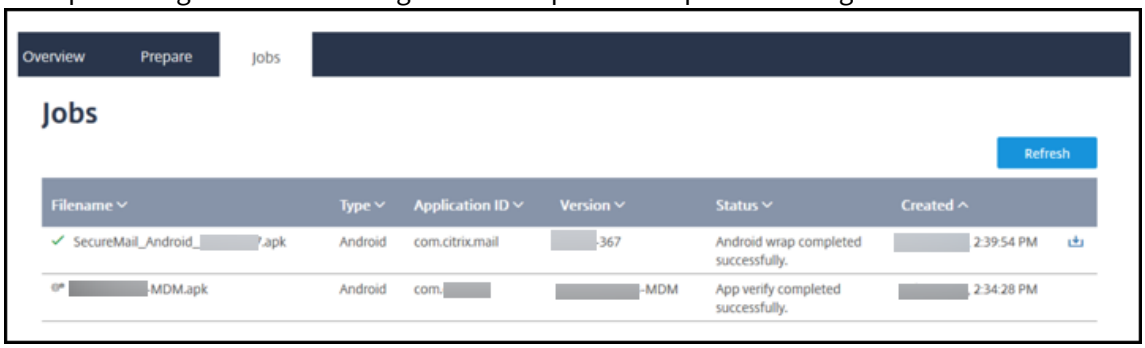
3. (Facultatif) Sur l'écran **Create Mobile App**, modifiez le bundle ID de l'application mobile, puis cliquez sur **Next**. Le processus d'encapsulation démarre.



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

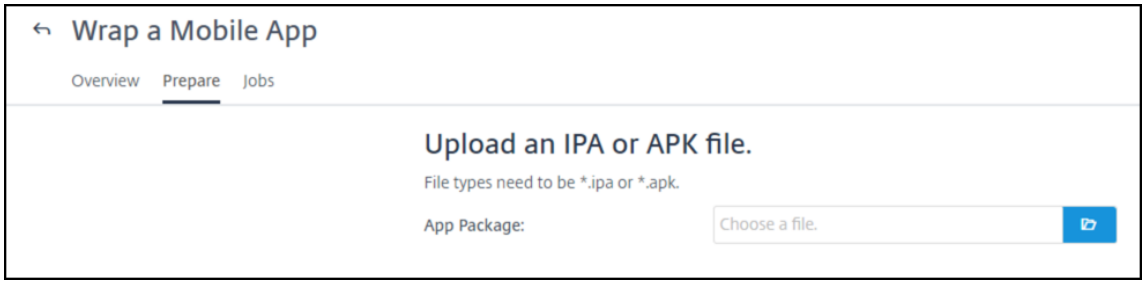


Vous pouvez également télécharger le fichier plus tard à partir de l'onglet **Jobs**.

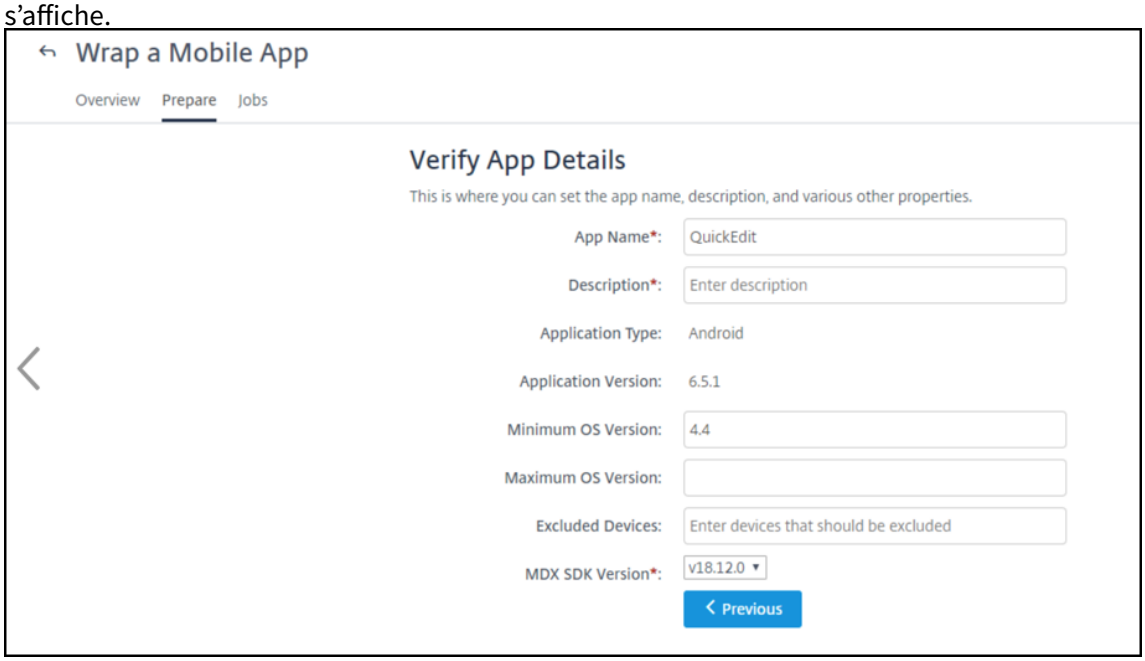


Pour encapsuler une application Android

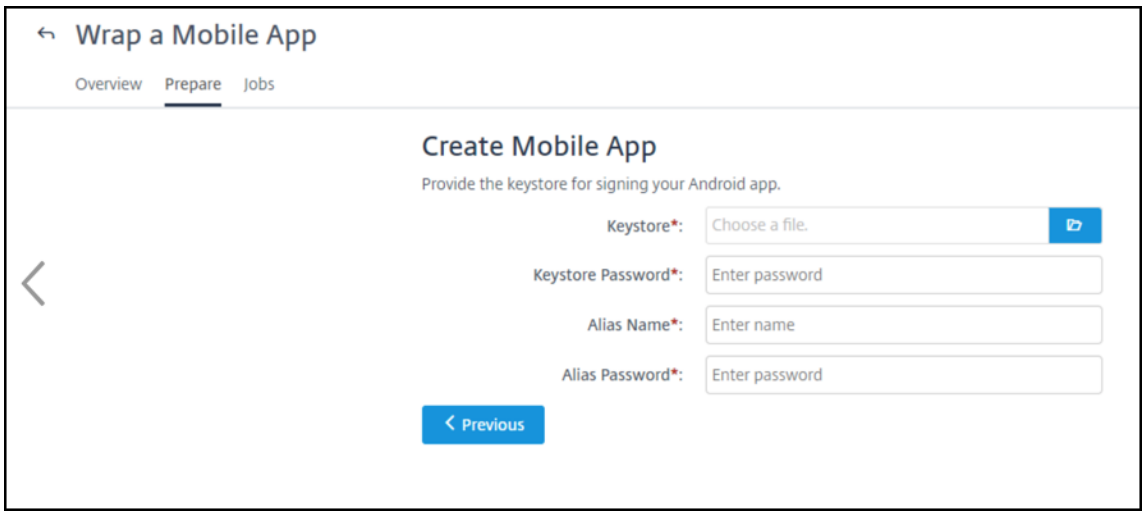
1. Chargez le fichier .apk pour l'application. Le temps nécessaire au chargement dépend de la taille du fichier. La limite de taille de fichier autorisée pour le fichier .ipa est de 209 Mo. Si vous avez une application qui dépasse cette limite, utilisez le MDX Toolkit.



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

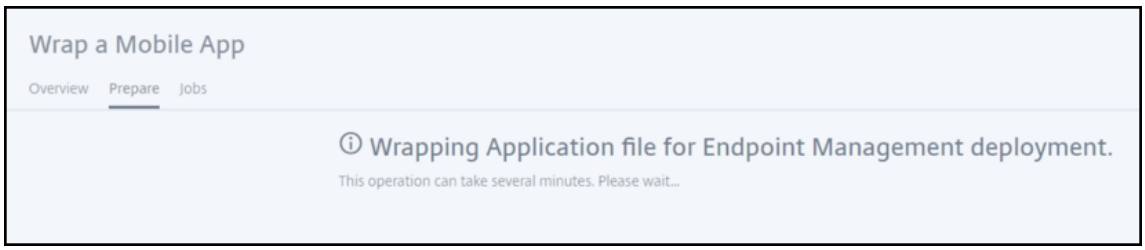


3. Sur l'écran **Verify App Details**, entrez les informations suivantes :
   a) (Facultatif) Modifiez le **nom de l'application**, la **version d'OS minimum** et la **version d'OS maximum**.
   b) Entrez une **description** (obligatoire).
   c) Sélectionnez une version du SDK MDX avec laquelle encapsuler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

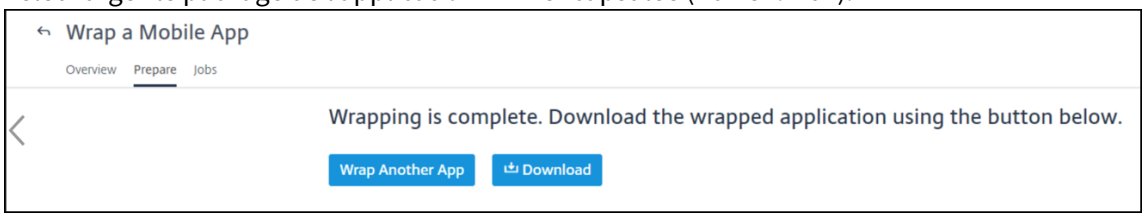


Pour collecter les informations de keystore et de nom d'alias, suivez les étapes de l'article CTX220480.

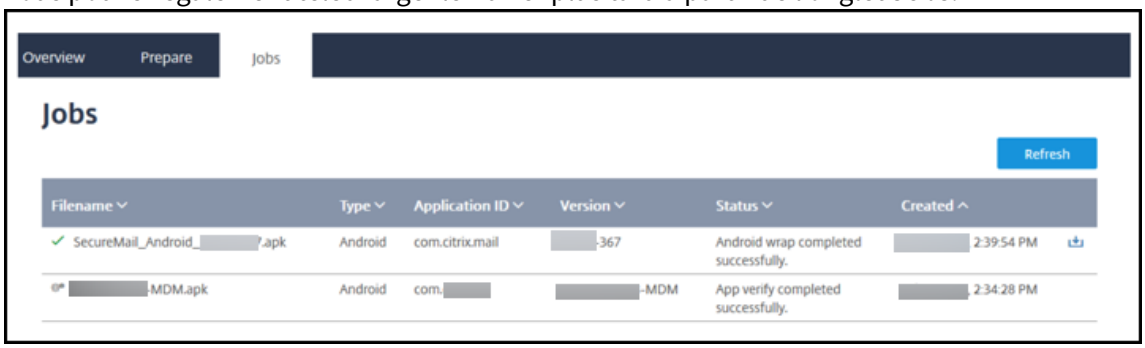
5. Cliquez sur **Next** pour démarrer le processus d'encapsulation.



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**.



Problèmes connus

Problèmes connus dans MDX Service 20.10.5

- Vous ne pouvez pas encapsuler les applications iOS développées sur macOS 10.14 et versions ultérieures à l'aide de MDX Service. Pour ajouter des applications iOS avec le SDK MAM ou la fonctionnalité MDX, préparez l'application avec le SDK MAM ou encapsulez les applications à l'aide du kit MDX Toolkit sur site. [CXM-90666]

Secure Browser Service

June 10, 2021

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. Ce service fournit 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.

Secure Browser Service peut publier des navigateurs sécurisés à utiliser avec :

- **Des applications Web externes authentifiées par code secret partagé.** Si vous publiez un navigateur avec une authentification par code secret partagé, les utilisateurs doivent entrer le code secret pour lancer une application.
- **Des applications Web externes authentifiées.** Lorsque vous publiez des applications Web externes authentifiées et que vous lancez les applications à l'aide de Citrix Workspace, Secure Browser Service nécessite un emplacement de ressources contenant au moins un Cloud Connector (deux ou plus sont recommandés). Pour plus de détails, consultez la section Citrix Cloud Connector. Pour les applications authentifiées, vous devez ajouter des utilisateurs avec la bibliothèque Citrix Cloud.
- **Des applications Web externes non authentifiées.** Lorsque vous publiez des applications Web externes non authentifiées et que vous lancez les applications à l'aide de Citrix Workspace, Secure Browser Service nécessite un emplacement de ressources contenant au moins un Cloud Connector (deux ou plus sont recommandés). Pour plus de détails, consultez la section Citrix Cloud Connector.

Bien que cela ne soit généralement pas recommandé, des applications Web externes non authentifiées peuvent être utilisées pour une preuve de concept simple.

Pour de plus amples informations, consultez Publier un navigateur sécurisé.

Le service propose également :

- Intégration d'applications publiées avec Citrix Workspace
- Intégration d'applications publiées avec StoreFront local
- Liste d'autorisation d'adresses URL simples pour garantir la sécurité
- Surveillance de l'utilisation
- Commandes d'utilisation du presse-papiers, de l'impression, du mode kiosque, du basculement de région et du mappage de lecteurs clients

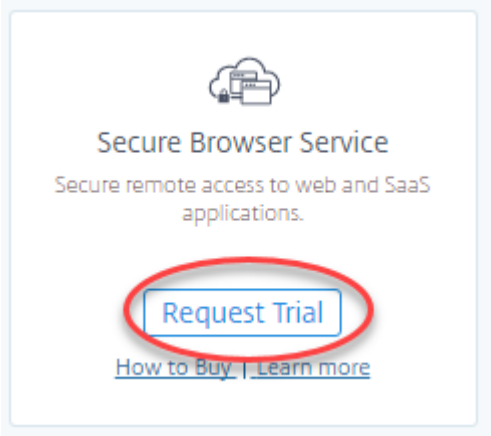
Nouveautés

- Mars 2021 :
  - **Secure Browser prend en charge l'authentification avec Azure Active Directory**. Les utilisateurs peuvent désormais se connecter aux applications Secure Browser à partir de Citrix Workspace à l'aide des informations d'identification Azure Active Directory. Pour de plus amples informations, consultez Intégration avec Citrix Workspace.
  - **Secure Browser vous permet de surveiller et de fermer les sessions actives des utilisateurs**. Secure Browser fournit le nom d'utilisateur, l'ID de session, l'adresse IP du client, le type d'authentification, le nom de l'application, l'heure de début de session et la durée de session associés aux sessions actives des utilisateurs. Vous pouvez afficher des informations de base sur chaque session active et déconnecter la session si nécessaire. Pour de plus amples informations, consultez Surveiller les sessions actives.
- Versions publiées en 2020 : toutes les versions publiées en 2020 contiennent des améliorations au niveau de la stabilité et des performances globales.

Mise en route

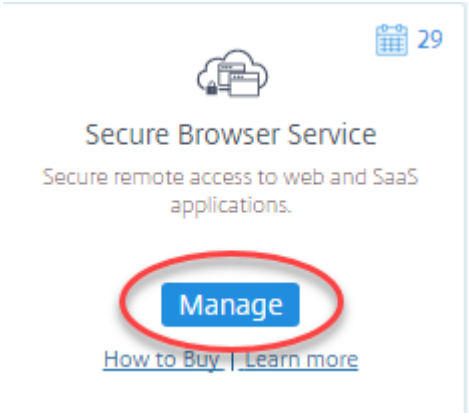
Vous trouverez ci-dessous une vidéo sur la mise en route de Secure Browser.

1. Connectez-vous à Citrix Cloud. Si vous n'avez pas de compte, consultez la section Ouvrir un compte sur Citrix Cloud. Vous pouvez demander une version d'évaluation de Citrix Secure Browser Service de 30 jours.
2. Dans la vignette **Secure Browser Service**, cliquez sur **Demander version d'évaluation**.

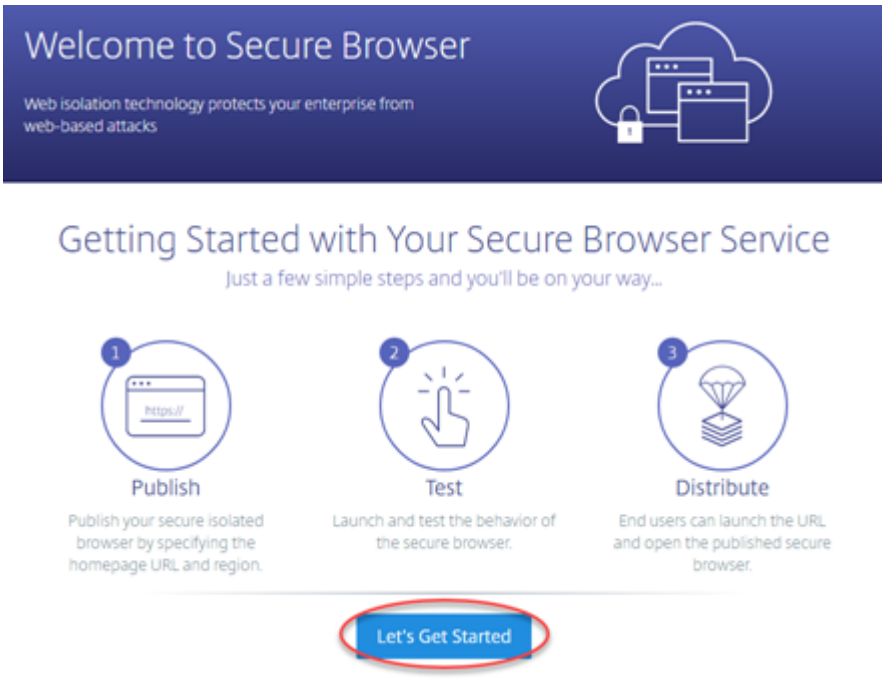


3. Vous allez recevoir un e-mail dans quelques instants (l'e-mail associé à votre compte Citrix Cloud). Cliquez sur le lien **Connexion** de l'e-mail.

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 du service Citrix Secure Browser, accédez à https://www.citrix.com/products/citrix-secure-browser/.

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 Service indique **Activée**. Si ce n'est pas le cas, cliquez sur le menu des points de suspension et sélectionnez **Activer**.

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) composant(s) 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

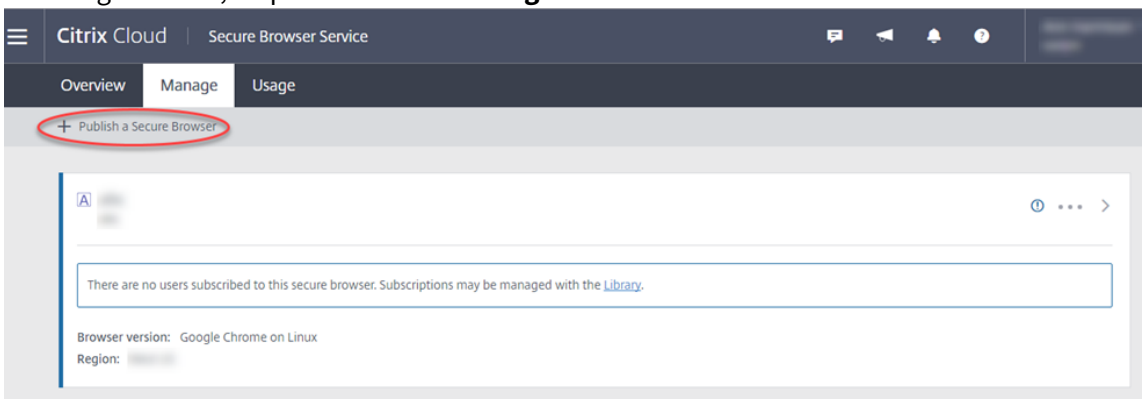
Les clients Citrix Virtual Apps and Desktops disposant d'un StoreFront local peuvent facilement s'intégrer à Secure Browser Service pour offrir les avantages suivants :

- 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.

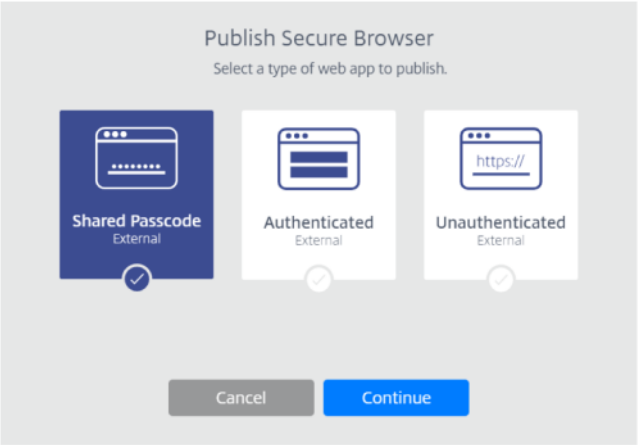
Pour plus de détails, consultez l'article CTX230272 et la documentation sur la configuration de StoreFront.

Publier un navigateur sécurisé

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**.



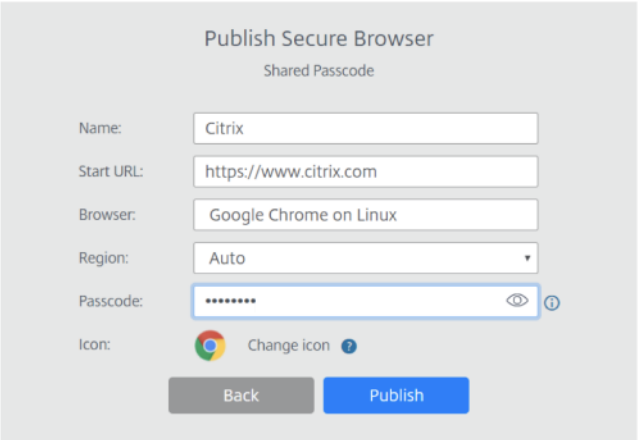
3. Sélectionnez le type de navigateur sécurisé à publier : code secret partagé, authentifié ou non authentifié. Puis cliquez sur **Continuer**.



Par défaut, les utilisateurs doivent lancer des applications avec authentification par code secret partagé à l'aide de launch.cloud.com. Citrix Workspace et la bibliothèque Citrix Cloud ne prennent pas en charge les applications utilisant un code secret partagé.

Pour utiliser Citrix Workspace, vous devez publier des applications authentifiées et attribuer explicitement des abonnés (utilisateurs) ou des groupes dans la bibliothèque Citrix Cloud. Les applications non authentifiées sont disponibles pour tous les abonnés de Workspace sans attribution d'utilisateur.

4. Pour configurer ces paramètres :



- **Nom :** entrez un nom pour l'application que vous créez.
- **URL de démarrage :** spécifiez l'URL qui s'ouvre lorsque les utilisateurs démarrent une application.
- **Région :** choisissez l'emplacement/la région du serveur. Les régions disponibles sont les suivantes : Ouest des États-Unis, Est des États-Unis, Asie du Sud-Est, Est de l'Australie et Europe de l'Ouest.

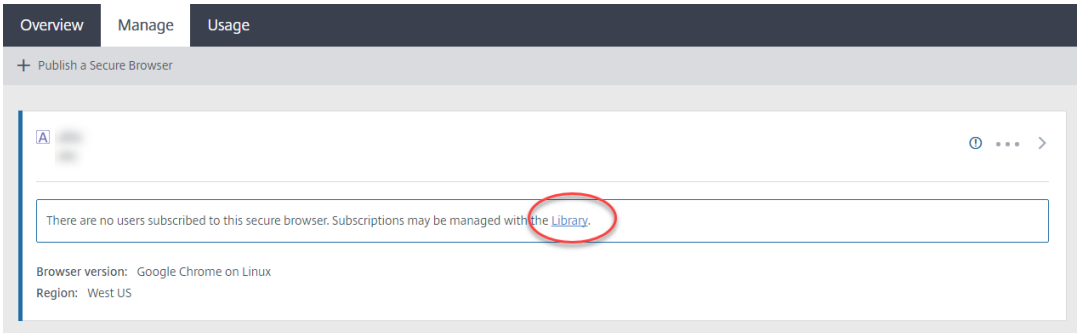
  Si vous sélectionnez **Auto**, votre Secure Browser se connecte à la région la plus proche en fonction de votre géolocalisation.

- **Code secret :** si vous avez sélectionné un navigateur doté d'une authentification par mot de passe partagé, saisissez le code secret pour fournir un accès sécurisé amélioré à votre application. Le code secret doit comporter au moins 8 caractères alphanumériques. Assurez-vous d'enregistrer le code secret et de le partager avec les utilisateurs. Les utilisateurs doivent entrer le code secret lorsqu'ils lancent une application à l'aide de launch.cloud.com.
- **Icône :** par défaut, l'icône de l'exécutable de Google Chrome est utilisée lorsque vous publiez un navigateur sécurisé. Vous pouvez maintenant choisir 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.

5. Une fois terminé, cliquez sur **Publier**. Lorsque la publication est terminée, l'onglet **Gérer** répertorie le navigateur que vous avez publié.

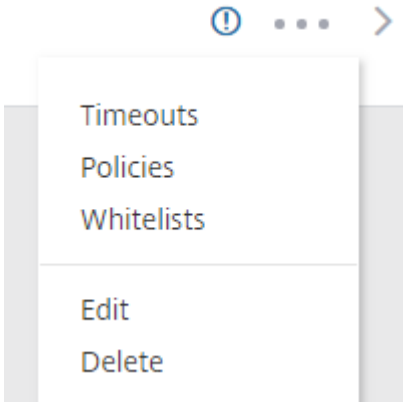
   - Si vous avez publié le navigateur sécurisé authentifié, vous devez utiliser la bibliothèque Citrix Cloud pour ajouter des utilisateurs ou des groupes. Cliquez sur la flèche droite à la fin de la ligne pour développer le volet d'informations contenant un lien vers la bibliothèque.



   Lorsque vous cliquez sur le lien fourni, 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, consultez la section Attribuer des utilisateurs et des groupes à des offres de services à l'aide de la bibliothèque.

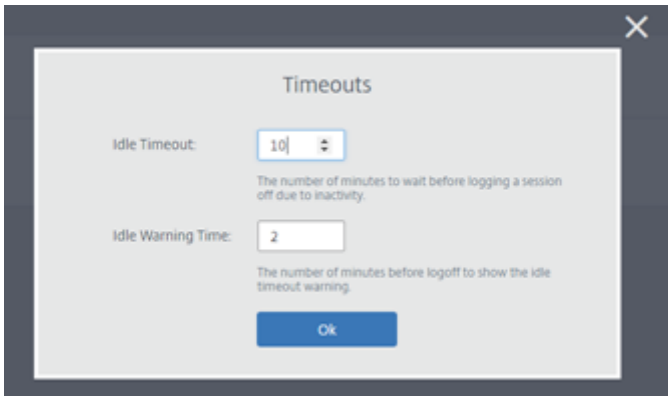
Gérer les navigateurs sécurisés publiés

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



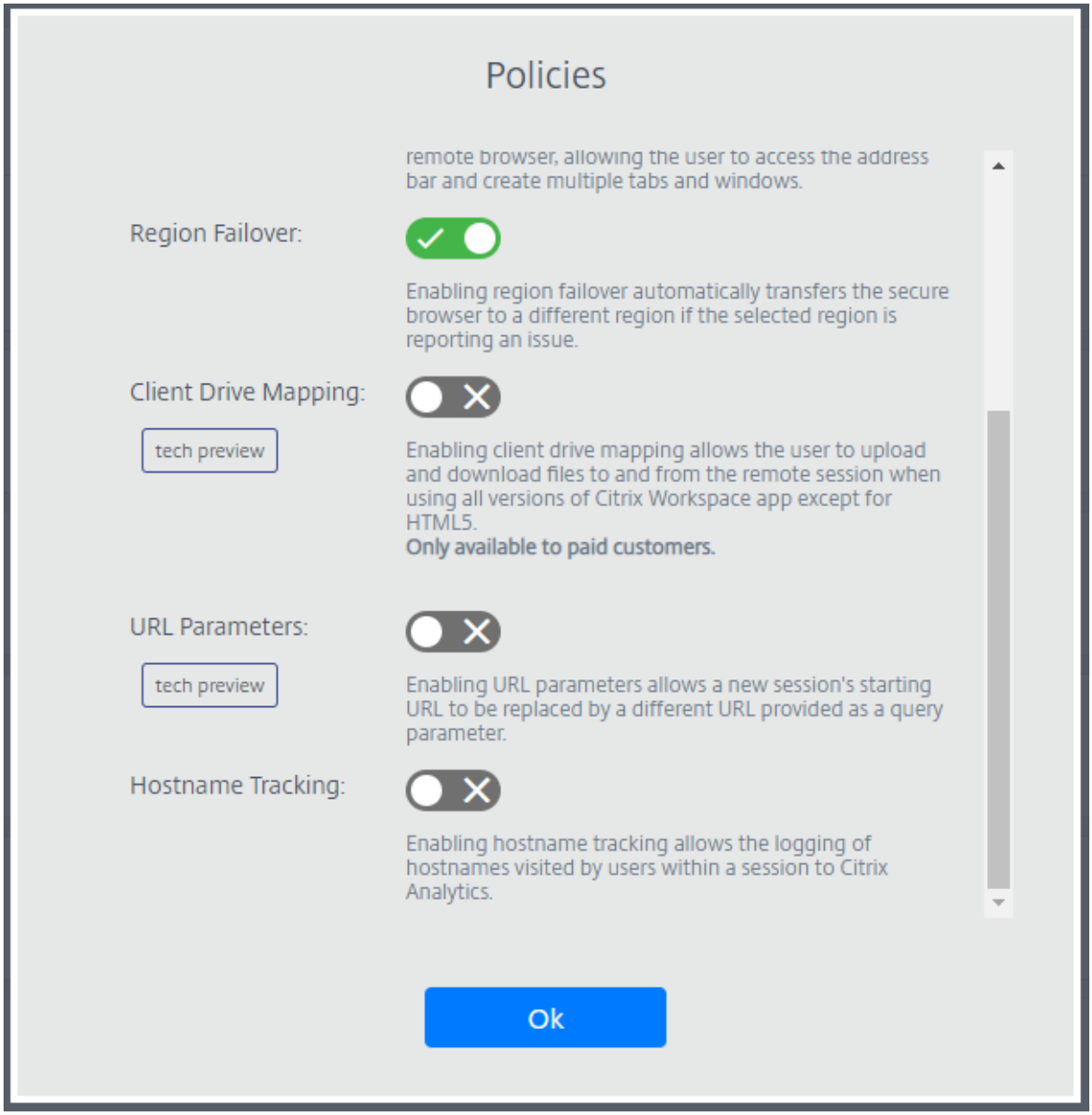
Les paramètres de délai d'expiration incluent :

- 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.

Si vous définissez un délai d'inactivité de 20 et un délai d'avertissement d'inactivité de 5, un message sera affiché 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

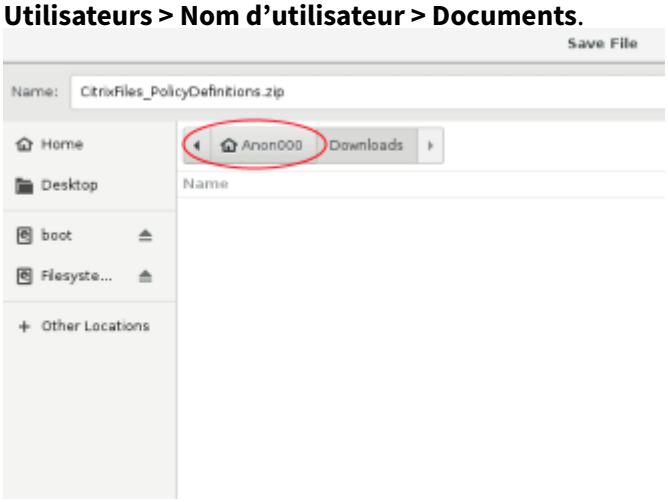


Les paramètres de la page des stratégies contrôlent ce qui suit :

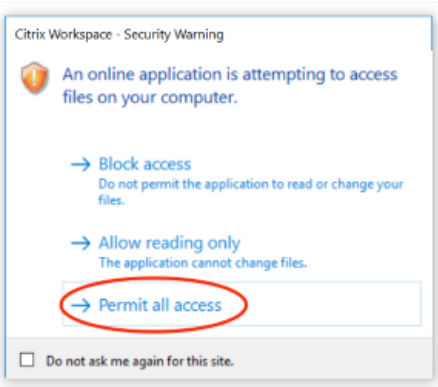
- **Presse-papiers :** lorsque la stratégie Presse-papiers est activée, les opérations de copier-coller vers et depuis la session distante sont autorisées. (Le bouton Presse-papiers est supprimé de la

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).
- **Basculement de région :** la stratégie de basculement de région permet de transférer automatiquement votre navigateur publié vers une autre région si votre région actuelle signale un problème. Si vous ne souhaitez pas utiliser cette fonctionnalité, désactivez la stratégie de basculement de région. Si vous avez publié le navigateur à l'aide de la sélection de région **Auto**, votre navigateur sécurisé reste inscrit à la stratégie. Ce paramètre est activé par défaut.
- **Mappage des lecteurs clients :** l'activation de la stratégie de mappage des lecteurs clients permet à l'utilisateur de charger et télécharger des fichiers vers et depuis la session distante. Cette fonctionnalité est disponible uniquement pour les sessions lancées avec l'application Citrix Workspace. Par défaut, cette stratégie est désactivée.
  - Les utilisateurs doivent enregistrer les fichiers téléchargés uniquement sur le disque `ctxmnt` du répertoire `Anonxxx`. Pour ce faire, les utilisateurs doivent naviguer jusqu'à l'emplacement souhaité pour stocker le fichier. Par exemple, **Anonxxx > ctxmnt > C > Utilisateurs > Nom d'utilisateur > Documents**.



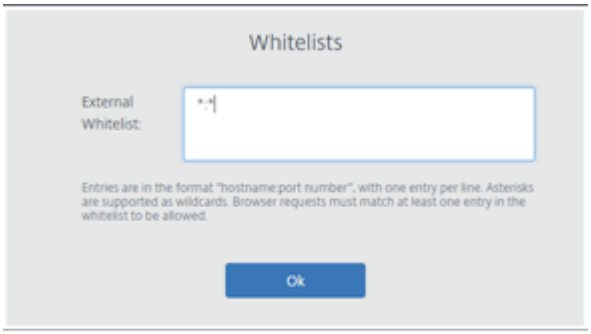
  - La boîte de dialogue peut inviter l'utilisateur à accepter les autorisations **Permit all access** ou **Read and Write** pour accéder au dossier `ctxmnt`.



- **Paramètres d'URL :** l'activation des paramètres d'URL vous permet de modifier l'URL de démarrage d'une nouvelle session lorsque les utilisateurs lancent une application. Pour que cette stratégie prenne effet, configurez un serveur proxy local pour identifier les sites Web suspects et les rediriger vers Secure Browser. Par défaut, ce paramètre est désactivé. Pour de plus amples informations, consultez Guide de preuve de concept : Redirection d'URL vers Secure Browser avec Citrix ADC dans Azure.
- **Suivi des noms d'hôte :** utilisez le suivi des noms d'hôte pour permettre à Secure Browser de consigner les noms d'hôte pendant la session d'un utilisateur. La stratégie est désactivée par défaut. Ces informations sont partagées avec Citrix Analytics. Pour de plus amples informations, consultez Citrix Analytics.

Lorsque vous avez terminé, cliquez sur **OK**.

Listes d'autorisation



Utilisez la tâche **Listes blanches** pour limiter l'accès des utilisateurs uniquement aux URL autorisées dans leur session Secure Browser publiée. Cette fonctionnalité est disponible pour les applications Web authentifiées externes.

Saisissez les entrées de liste autorisée au format `hostname:port number`. 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 d'autorisation.

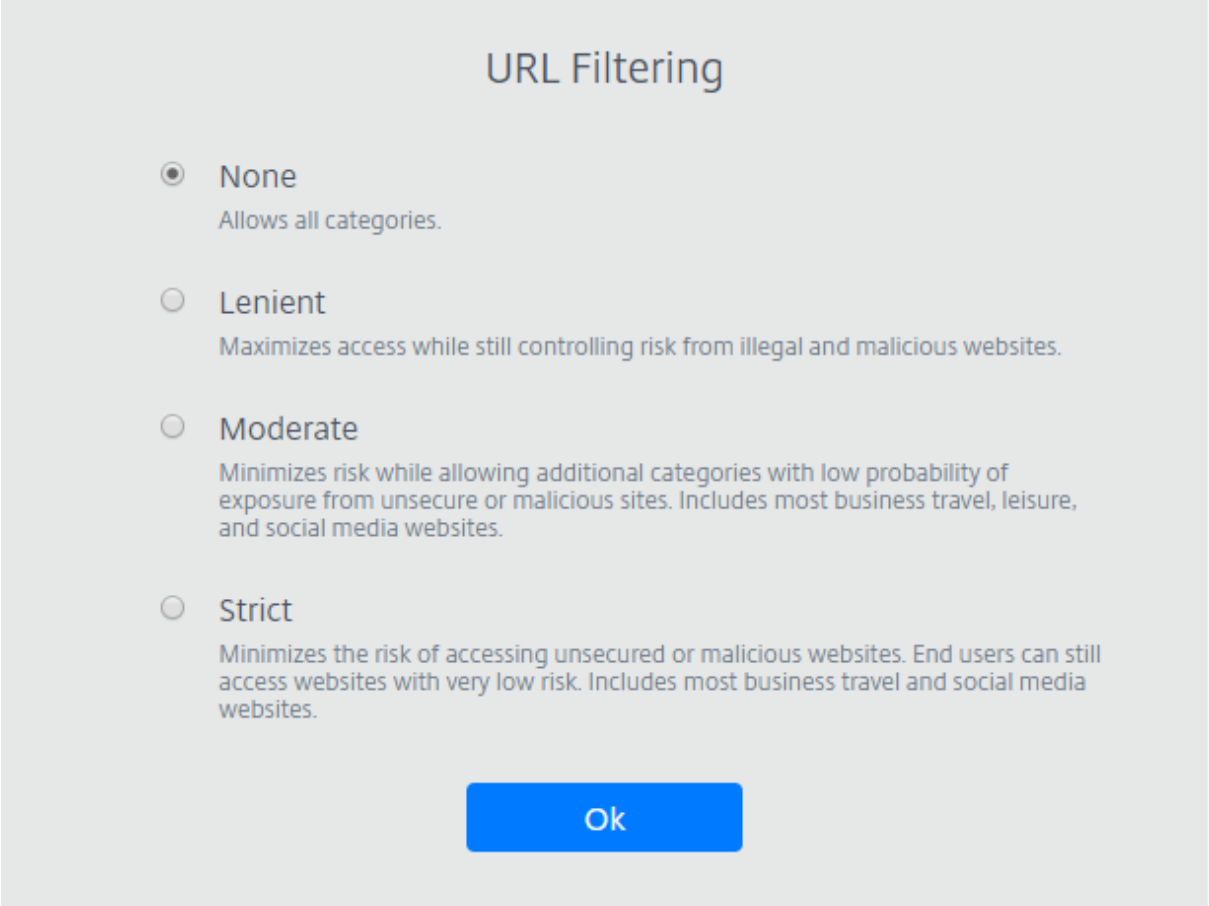
Par exemple, pour définir `https://example.com` comme URL autorisée, procédez comme suit :

- `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 **Liste blanche externe** des applications Web.

Lorsque vous avez terminé, cliquez sur **OK**.

Des fonctionnalités avancées de filtrage Web sont disponibles via l'intégration au service Contrôle d'accès. Pour en savoir plus, consultez la section Cas d'utilisation : Accès sélectif aux applications.

Filtrage d'URL



Vous pouvez configurer le filtrage d'URL pour contrôler les méthodes d'accès basées sur des catégories prédéfinies associées aux modèles de risque. Les options de filtrage d'URL incluent :

- **Aucun** : autorise toutes les catégories.
- **Minimal** : maximise l'accès tout en contrôlant les risques liés aux sites Web illégaux et malveillants. Comprend les catégories suivantes :

  - **Adulte :** contenu grotesque, éducation sexuelle, pornographie, nudité, services sexuels, recherche et liens pour adultes, maillots de bain et lingerie, magazines et actualités pour adultes, expression sexuelle (texte), fétiche et rencontres.
  - **Informatique et Internet :** proxys distants, adresses IP privées, partage de fichiers d'égal à égal et torrents.
  - **Jeux d'argent :** concours, prix, loteries et jeux d'argent en général.
  - **Contenu illégal et nuisible :** terrorisme, extrémisme, haine, diffamation, armes, violence, suicide, drogues illicites, médicaments, activités illégales, marijuana et défense d'intérêts en général.
  - **Malware et spam :** piratage, malware, spam, spyware, botnets, sites infectés, sites de phishing, keyloggers (enregistreurs de frappe), logiciels malware sur mobiles, robots téléphoniques, sites Web malveillants et dangereux.

- **Modéré :** minimise les risques tout en autorisant des catégories supplémentaires affichant une faible probabilité d'exposition à des sites non sécurisés ou malveillants. Comprend les catégories suivantes :

  - **Adulte :** contenu grotesque, éducation sexuelle, pornographie, nudité, services sexuels, recherche et liens pour adultes, maillots de bain et lingerie, magazines et actualités pour adultes, expression sexuelle (texte), fétiche et rencontres.
  - **Commerce et industrie :** enchères.
  - **Informatique et Internet :** publicités, bannières, proxys distants, adresses IP privées, partage de fichiers d'égal à égal et torrents.
  - **Téléchargements :** App Stores pour mobiles, services de stockage, téléchargements et téléchargements de programmes.
  - **E-mail :** messagerie Internet et abonnements par e-mail.
  - **Finance :** crypto-monnaie.
  - **Jeux d'argent :** concours, prix, loteries et jeux d'argent en général.
  - **Malware et spam :** piratage, malware, spam, spyware, botnets, sites infectés, sites de phishing, keyloggers (enregistreurs de frappe), logiciels malware sur mobiles, robots téléphoniques, sites Web malveillants et dangereux.
  - **Messagerie, chat et téléphonie :** messages instantanés et chat sur le Web.
  - **Actualités, divertissement et société :** Wordpress (publication et chargements), URL non prises en charge, occulte, aucun contenu, divers, horoscope, astrologie, divination, alcool, religions, pages Web personnelles, blogs et jeux en ligne.
  - **Réseaux sociaux :** sites de recherche et de partage de photos, bulletins informatiques et bulletins électroniques.

- **Strict :** minimise 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 les catégories suivantes :

- **Adulte :** contenu grotesque, éducation sexuelle, pornographie, nudité, services sexuels, recherche et liens pour adultes, maillots de bain et lingerie, magazines et actualités pour adultes, expression sexuelle (texte), fétiche et rencontres.
- **Commerce et industrie :** enchères.
- **Informatique et Internet :** publicités, bannières, DNS dynamique, applications mobiles, éditeurs, domaines parqués, proxys distants, adresses IP privées, partage de fichiers d'égal à égal et torrents.
- **Téléchargements :** App Stores pour mobiles, services de stockage, téléchargements et téléchargements de programmes.
- **E-mail :** messagerie Internet et abonnements par e-mail.
- **Finance :** crypto-monnaie et produits financiers.
- **Jeux d'argent :** concours, prix, loteries et jeux d'argent en général.
- **Contenu illégal et nuisible :** terrorisme, extrémisme, haine, diffamation, armes, violence, suicide, drogues illicites, médicaments, activités illégales, marijuana et défense d'intérêts en général.
- **Emplois et CV :** emploi, avancement professionnel et LinkedIn (mises à jour, messages, connexions et emplois).
- **Malware et spam :** piratage, malware, spam, spyware, botnets, sites infectés, sites de phishing, keyloggers (enregistreurs de frappe), logiciels malware sur mobiles, robots téléphoniques, sites Web malveillants et dangereux.
- **Messagerie, chat et téléphonie :** messages instantanés et chat sur le Web.
- **Actualités, divertissement et société :** Wordpress (publication et chargements), hébergement, voyage et tourisme, URL non prises en charge, politique, mode et beauté, événements artistiques et culturels, référence, loisirs et hobbies, communautés locales, divers, boissons, sujets populaires, événements spéciaux, actualités, société et culture, magazines en ligne, jeux en ligne, événements de la vie, occulte, aucun contenu, horoscope, astrologie, divination, célébrités, streaming de multimédia, divertissement, lieux, activités, pages Web personnelles et blogs, et religions.
- **Réseaux sociaux :** réseaux sociaux en général, YikYak (publication), Twitter (publication, messages et suivre), Vine (charger, commenter et messages), Google+ (charger des photos et des vidéos, messages, chat vidéo et commenter), Instagram (charger et commenter), YouTube (partages et commenter), Facebook (groupes, jeux, questions, charger des vidéos, charger des photos, événements, chat, applications, publication, commenter et amis), Tumblr (publication, commenter, charger des photos et des vidéos), Pinterest (épingles et commenter), bulletins informatiques et bulletins électroniques.

Lorsque vous avez terminé, cliquez sur **OK**.

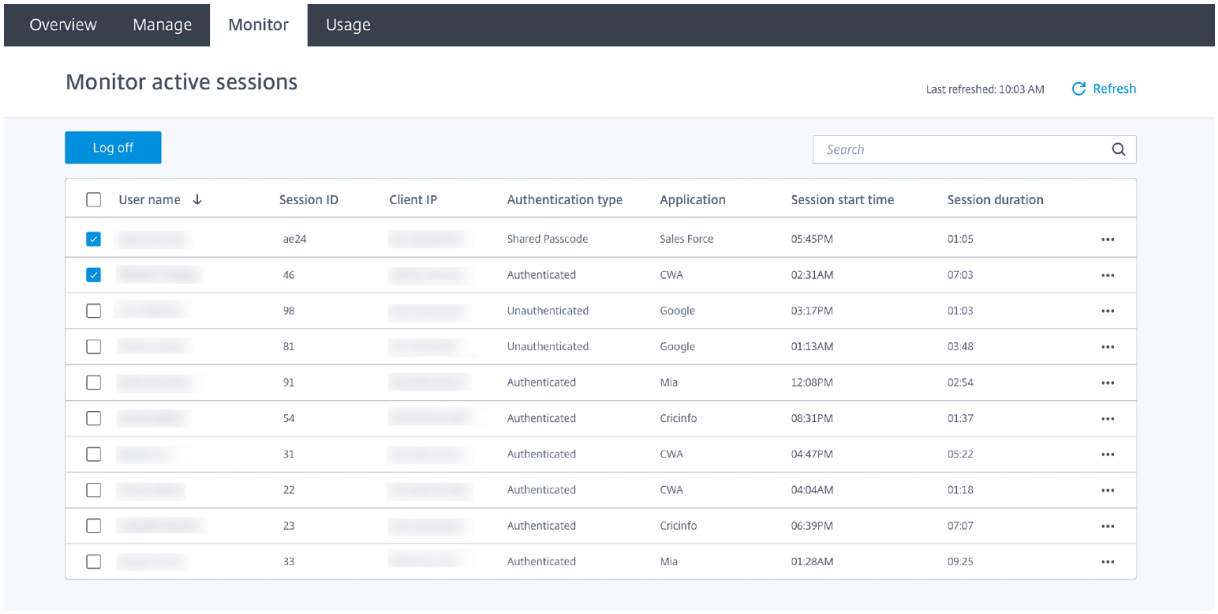
Modifier

Utilisez la tâche **Modifier** pour modifier le nom, l'URL de démarrage, la région d'un navigateur publié ou le code secret. 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 les sessions actives

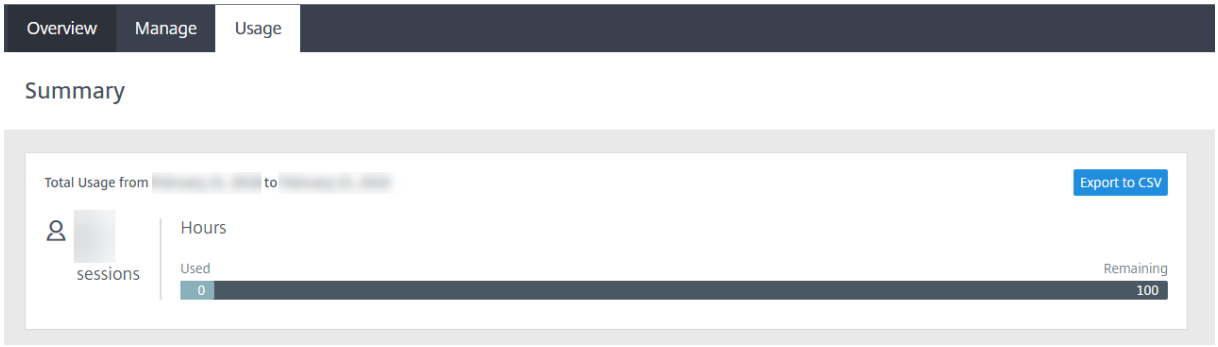


L'onglet **Surveiller** fournit des informations sur les sessions des utilisateurs en temps réel. Vous pouvez surveiller et déconnecter une ou plusieurs sessions actives.

Pour déconnecter une session unique, sélectionnez-la et cliquez sur le menu des points de suspension à la fin de la ligne d'une entrée. Cliquez sur **Fermer session** et confirmez vos modifications.

Pour déconnecter plusieurs sessions, sélectionnez les sessions actives dans la liste et cliquez sur le bouton **Fermer session** en haut de la page. Une fois vos modifications confirmées, Secure Browser déconnecte immédiatement toutes les sessions sélectionnées.

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

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 suivent l'historique de navigation de l'utilisateur et effectuent 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 1.2 uniquement.

Le trafic de sortie pour Secure Browser utilise des adresses IP spécifiques pour protéger le réseau interne. Pour obtenir la liste des adresses IP acceptées, consultez l'article du Centre de connaissances CTX286379.

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 publient 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

June 10, 2021

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.

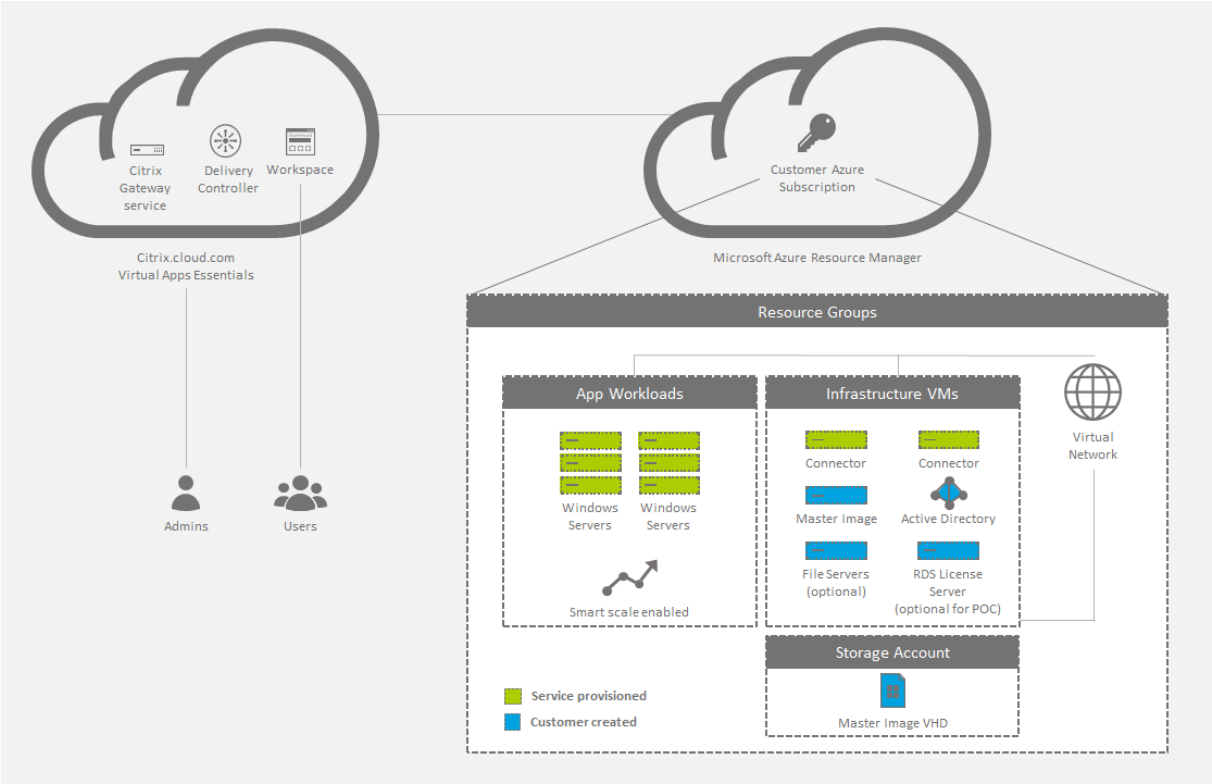
Les machines équipées d'un système d'exploitation serveur exécutent plusieurs sessions à partir d'une seule machine pour mettre à disposition plusieurs applications et bureaux vers de multiples utilisateurs connectés simultanément. Chaque utilisateur requiert une seule session depuis laquelle il peut 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.

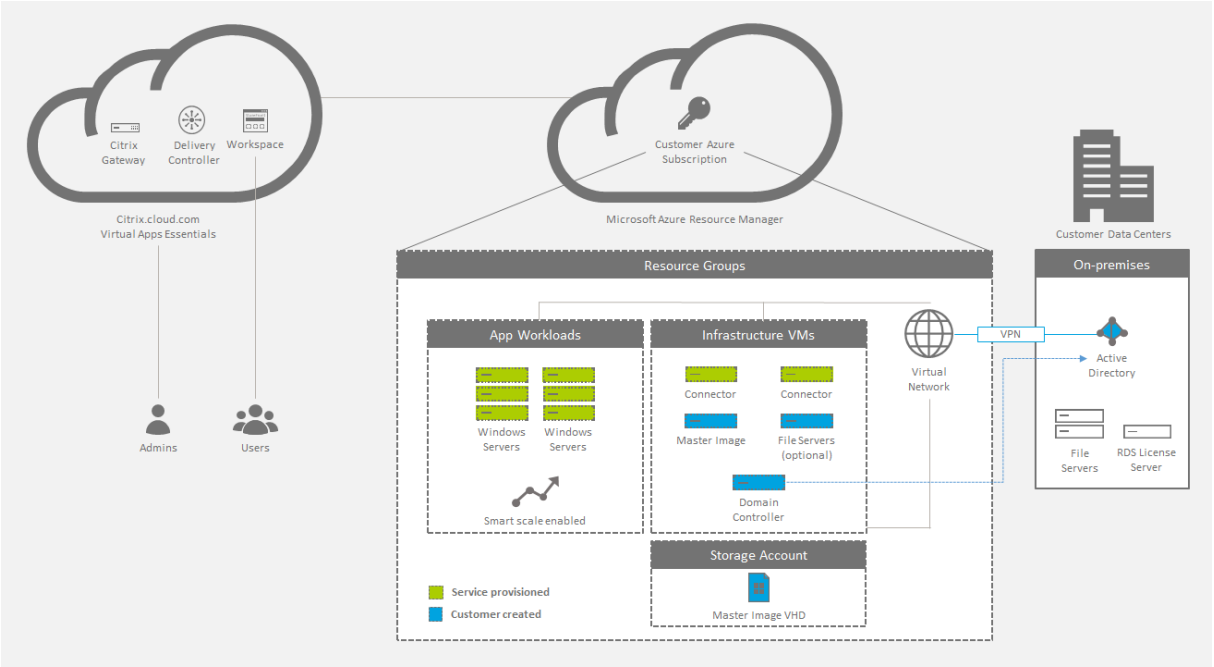
Virtual Apps Essentials inclut l'expérience d'espace de travail et le Service Citrix Gateway, en plus de ses services de gestion de base. Vos charges de travail applicatives s'exécutent dans votre abonnement Azure.

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.
- Déployer un catalogue, publier des applications et des bureaux et affecter des abonnés

Nouveautés

- Décembre 2018 : **Suppression de StoreFront hébergé dans le cloud**

  StoreFront hébergé dans le cloud n'est plus disponible pour une utilisation avec Virtual Desktops Essentials. Les clients qui ont acheté Virtual Desktops Essentials (anciennement XenDesktop Essentials) avant décembre 2017 peuvent utiliser Citrix Workspace comme décrit dans cet article pour fournir aux abonnés un accès aux bureaux.

- 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, reportez-vous à 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, consultez la section 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 plus de détails, consultez la section 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 locataire Azure Active Directory, consultez la section 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 :

- Sur les VDA Windows Server 2019, certaines icônes d'application peuvent ne pas apparaître correctement pendant la configuration et dans l'espace de travail des utilisateurs. Pour résoudre le problème, une fois l'application publiée, utilisez la fonction **Changer icône** pour attribuer une autre icône qui s'affiche correctement.

- Si vous utilisez Azure AD Domain Services : les noms UPN de connexion à Workspace 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. Pour plus d'informations, consultez la section Configuration requise > Citrix Cloud.

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 d'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 contrôleurs 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, consultez l'article Configurer des adresses IP privées pour une machine virtuelle à l'aide du portail Azure dans 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 de plus amples informations, consultez Attacher un disque de données géré à une VM Windows à l'aide du 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 de plus amples informations, consultez 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 de plus amples informations, consultez Installer une nouvelle forêt Active Directory sur un réseau virtuel Azure.

Si vous préférez utiliser Azure Active Directory Domain Services 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, consultez la section Préparer une image principale dans Virtual Apps Essentials.

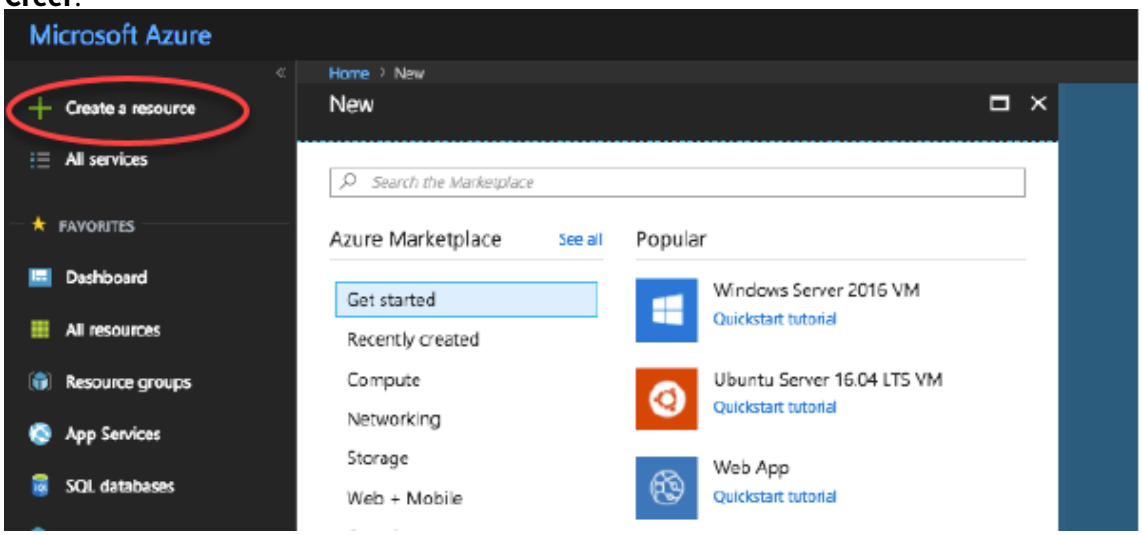
Résumé de la procédure

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. Consultez la page Lifecycle Policy for Citrix Cloud Virtual Apps and Desktops Service pour en savoir plus sur la stratégie de cycle de vie des VDA CR et LTSR.

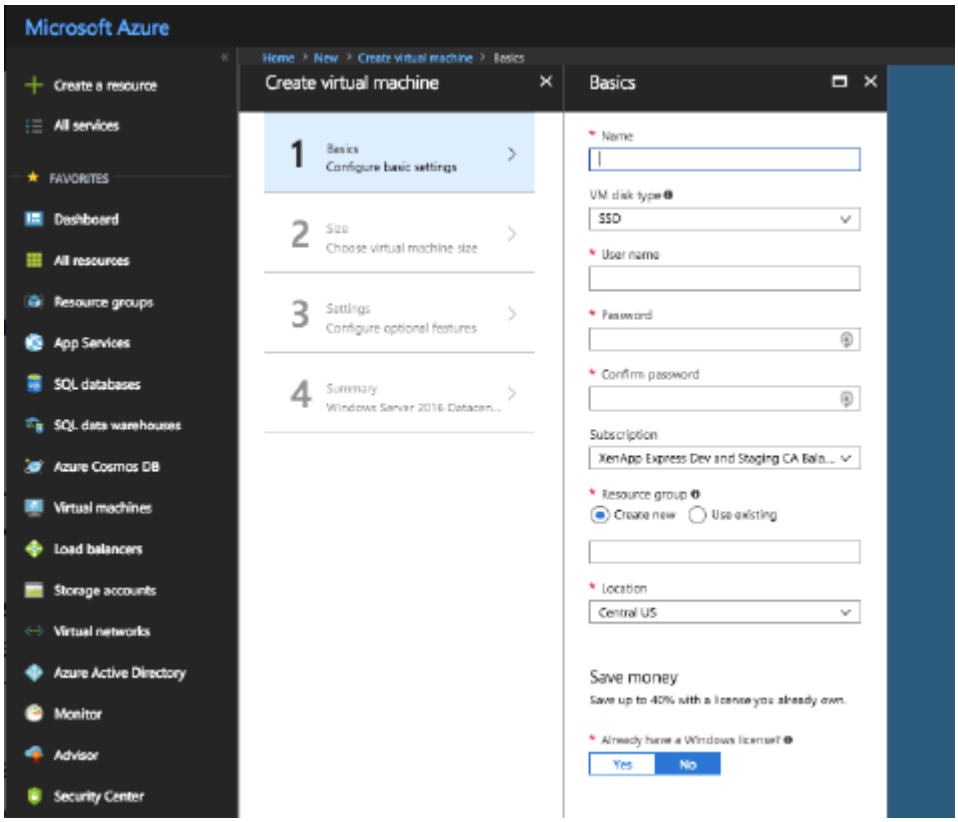
Créer une VM image principale dans Azure

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**.



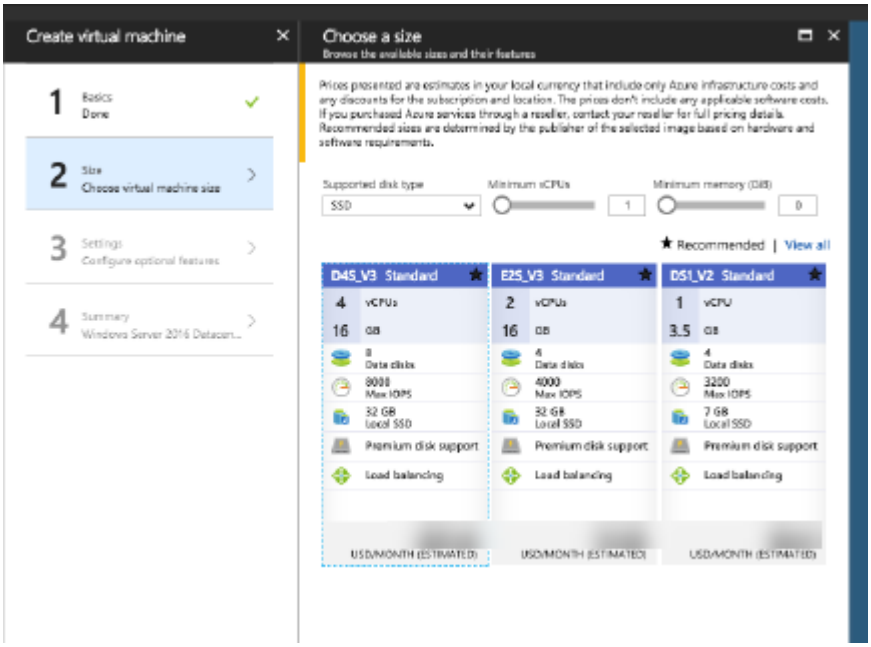
3. Sur la page **Créer une machine virtuelle**, dans le volet 1 De base :
   a) Entrez un nom pour la VM.
   b) Sélectionnez un type de disque de machine virtuelle (facultatif). Créez un disque standard.
   c) Entrez le nom d'utilisateur et le mot de passe locaux et confirmez le mot de passe.
   d) Sélectionnez 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**.



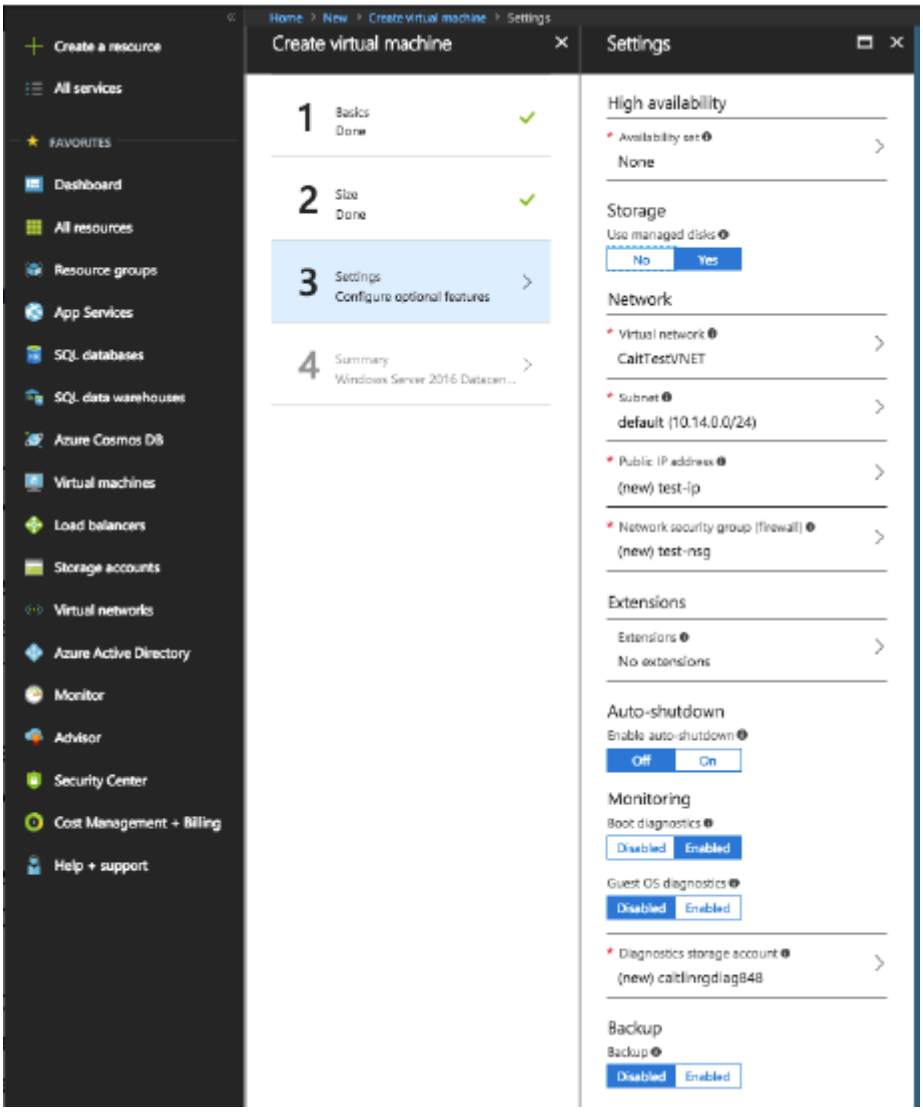
4. Sur la page **Créer une machine virtuelle**, dans le volet 2 Taille, choisissez la taille de la machine virtuelle :

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) Indiquez le nom du réseau virtuel, le sous-réseau, l'adresse IP publique et la sécurité du réseau.
   c) Vous pouvez aussi sélectionner les extensions.
   d) Activez ou désactivez l'arrêt automatique, la surveillance (diagnostics de démarrage, diagnostics de système d'exploitation invité, compte de stockage des diagnostics).
   e) Activez ou désactivez la sauvegarde.
   f) 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. Vous pouvez également utiliser un navigateur pour accéder à la page de téléchargement Citrix Virtual Apps and Desktops Service. 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 sur la page 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**.

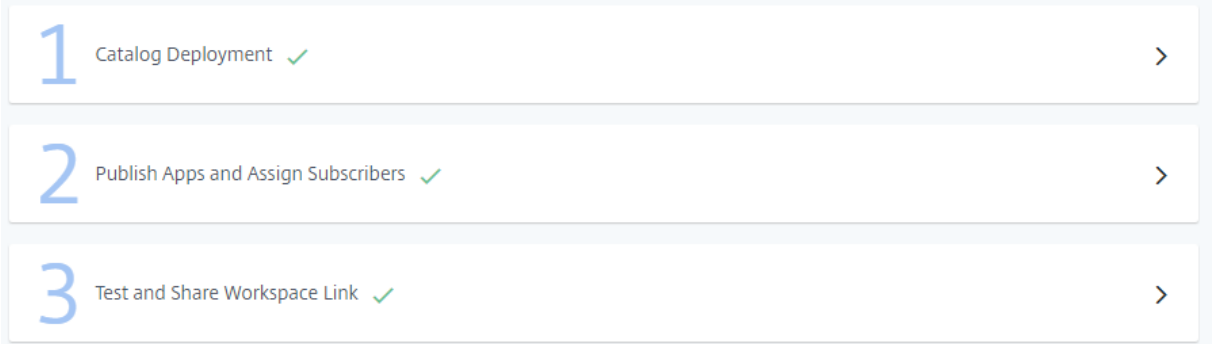
Déployer un catalogue, publier des applications et des bureaux et affecter des abonnés

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



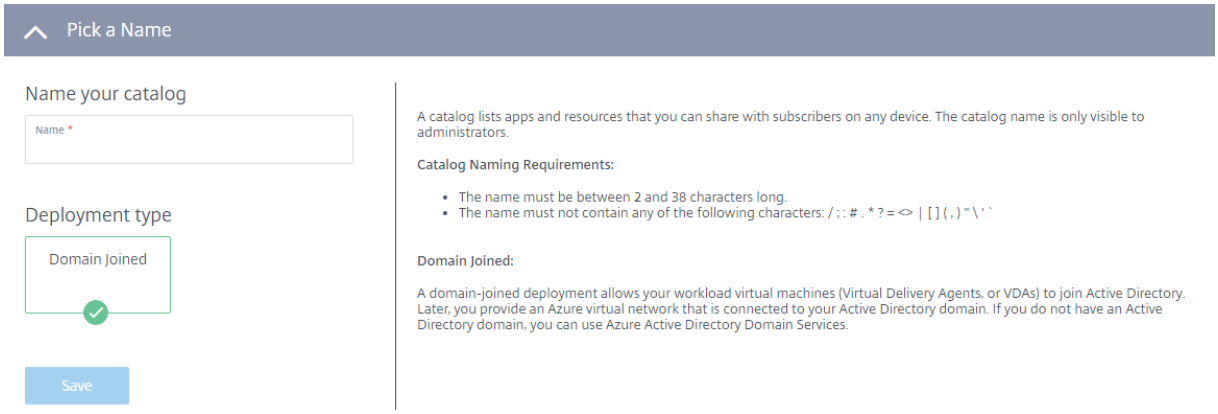
Créer un catalogue

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 sur la page 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 infor-

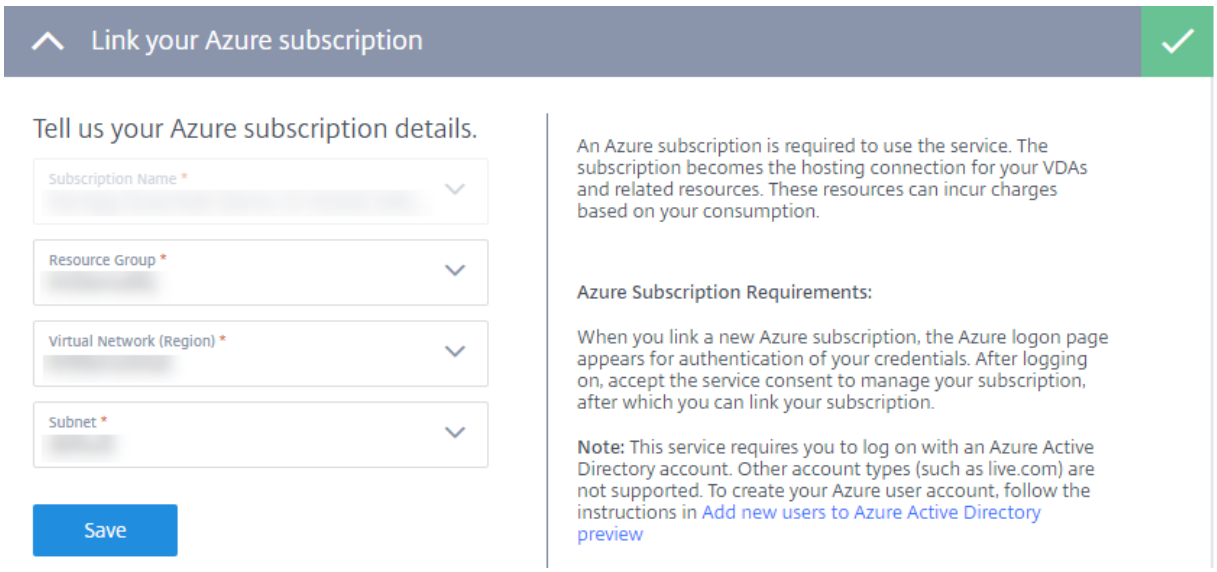
mations requises sont manquantes ou invalides. Une coche indique que l'information est complète.

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

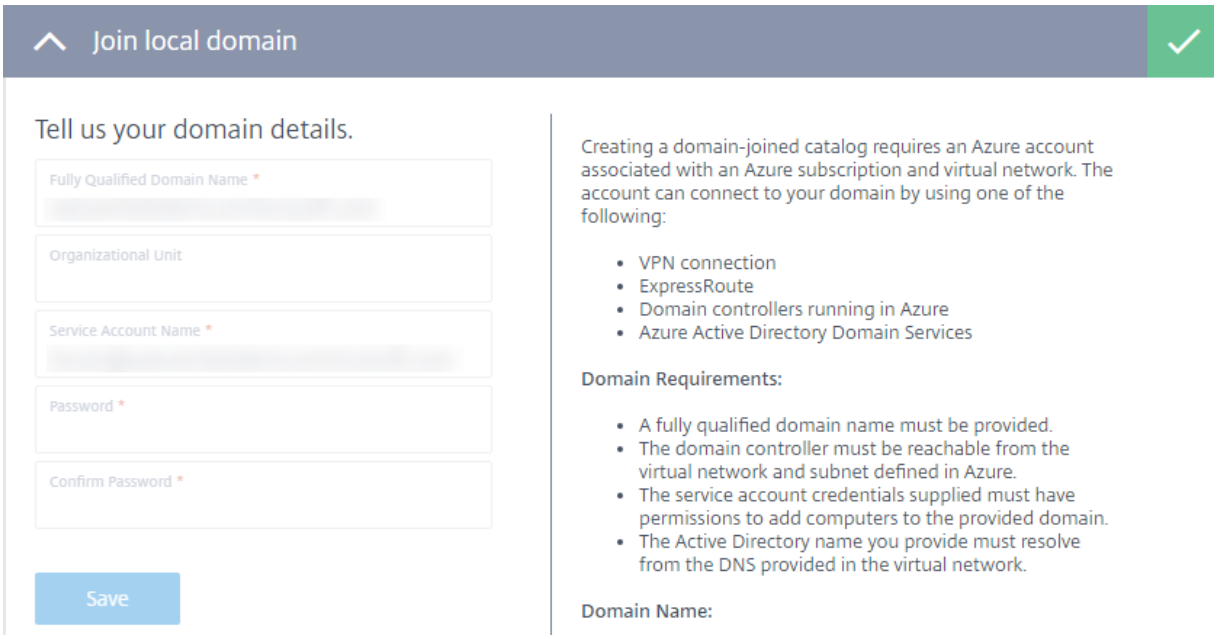


1. Sélectionnez votre abonnement Azure. Lorsque vous liez un nouvel abonnement Azure, la page de connexion Azure apparaît pour l'authentification de vos informations d'identification Azure.

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.

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

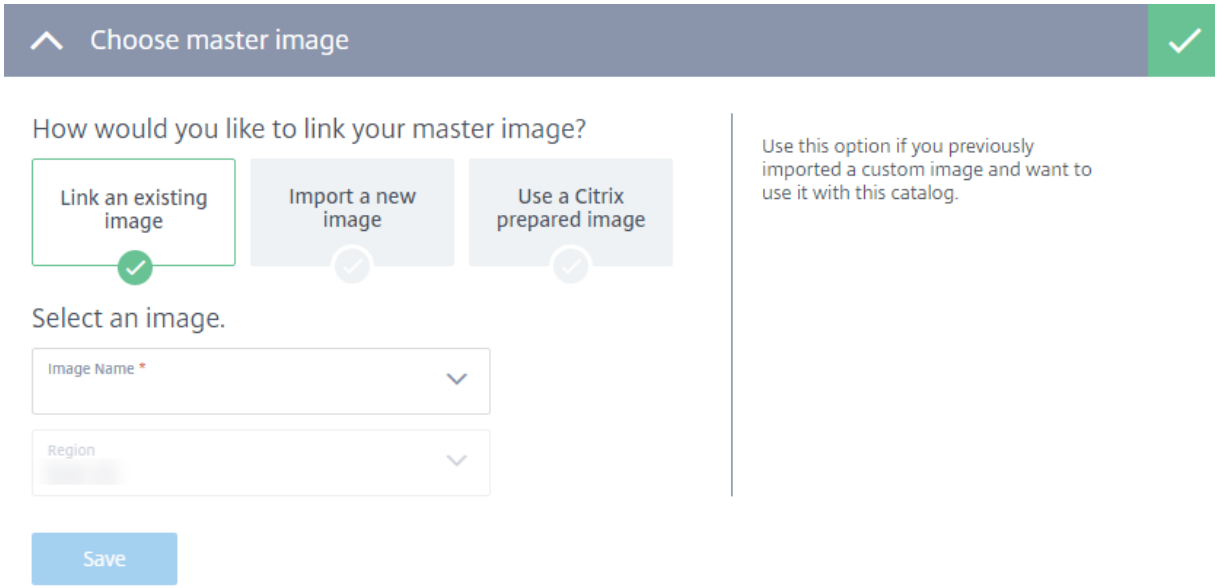
à Internet. Assurez-vous également que vous pouvez accéder au domaine en joignant la VM au domaine. Vous pouvez effectuer un test en utilisant les mêmes informations d'identification que celles utilisées pour déployer ce catalogue.

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

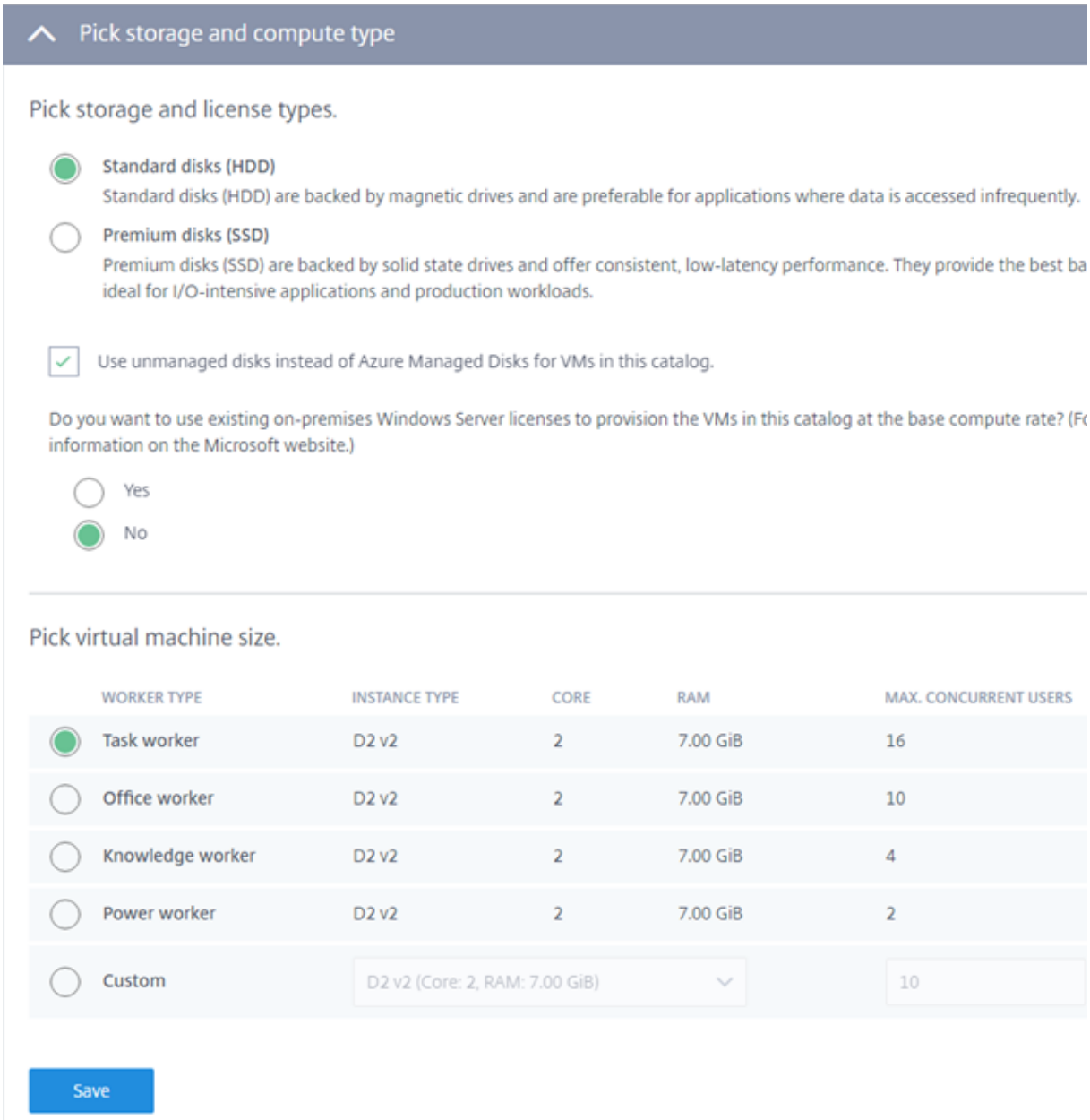


1. Sélectionnez l'une des options suivantes :

- **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 des disques gérés Azure ou des disques non gérés :** Pour en savoir plus sur les disques gérés Azure, consultez 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

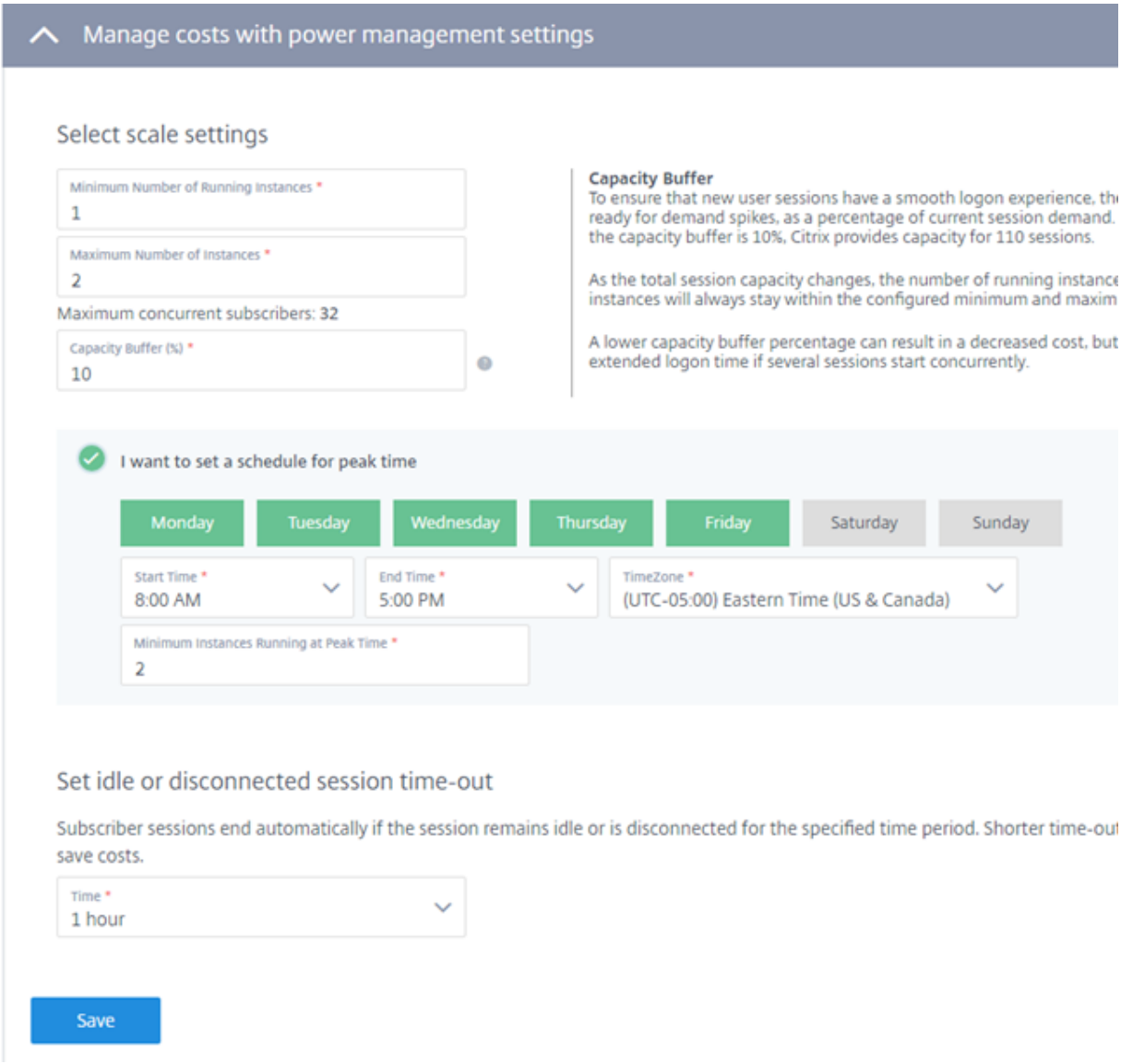
Server locales existantes. Si cette fonction est activée et que vous utilisez les images Windows Server locales existantes, Azure Hybrid Use Benefits (HUB) est utilisé. Pour plus de détails, consultez la section https://azure.microsoft.com/pricing/hybrid-use-benefit/.

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. Consultez Azure Hybrid Benefit pour Windows Serversur le site Web de Microsoft.

- **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, dans 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 :

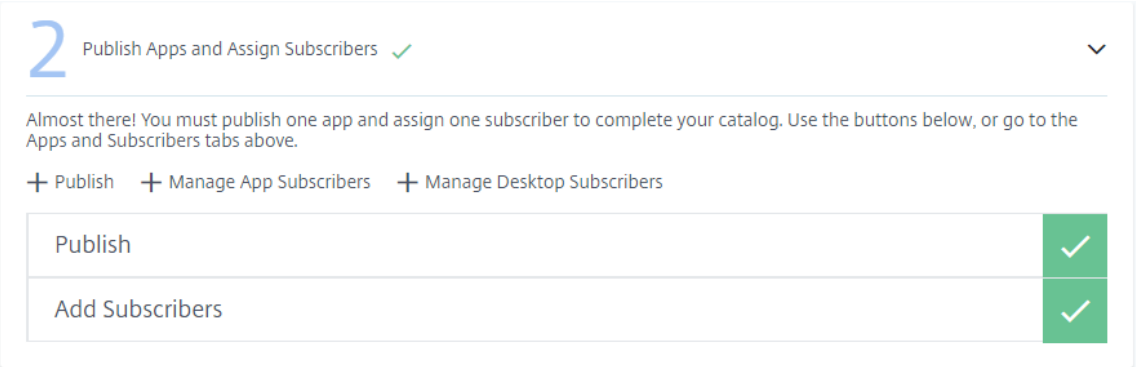
- Un groupe de ressources et un compte de stockage dans ce groupe de ressources pour les machines de charge de travail sont créés automatiquement dans Azure.
- Les VM sont nommées Xenappxx-xx-yyy, où xx est dérivé d'un facteur environnemental et yy est un nombre ordinal.

Publier des applications et affecter des abonnés à un catalogue

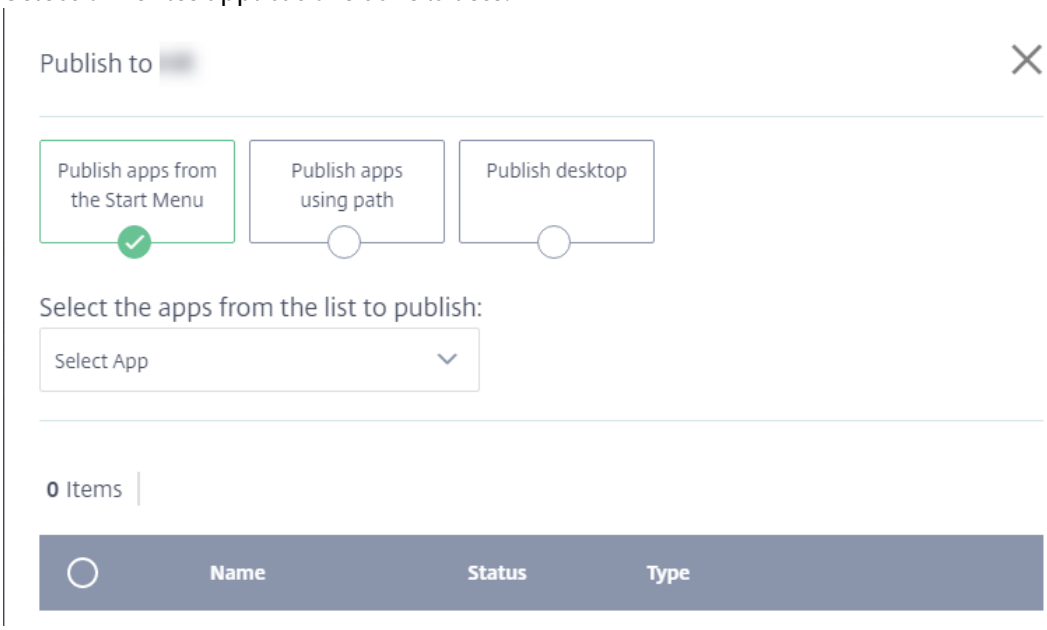
Pour finaliser le catalogue après son déploiement, vous devez publier une application ou un bureau et attribuer au moins un abonné.

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 sur la page 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.



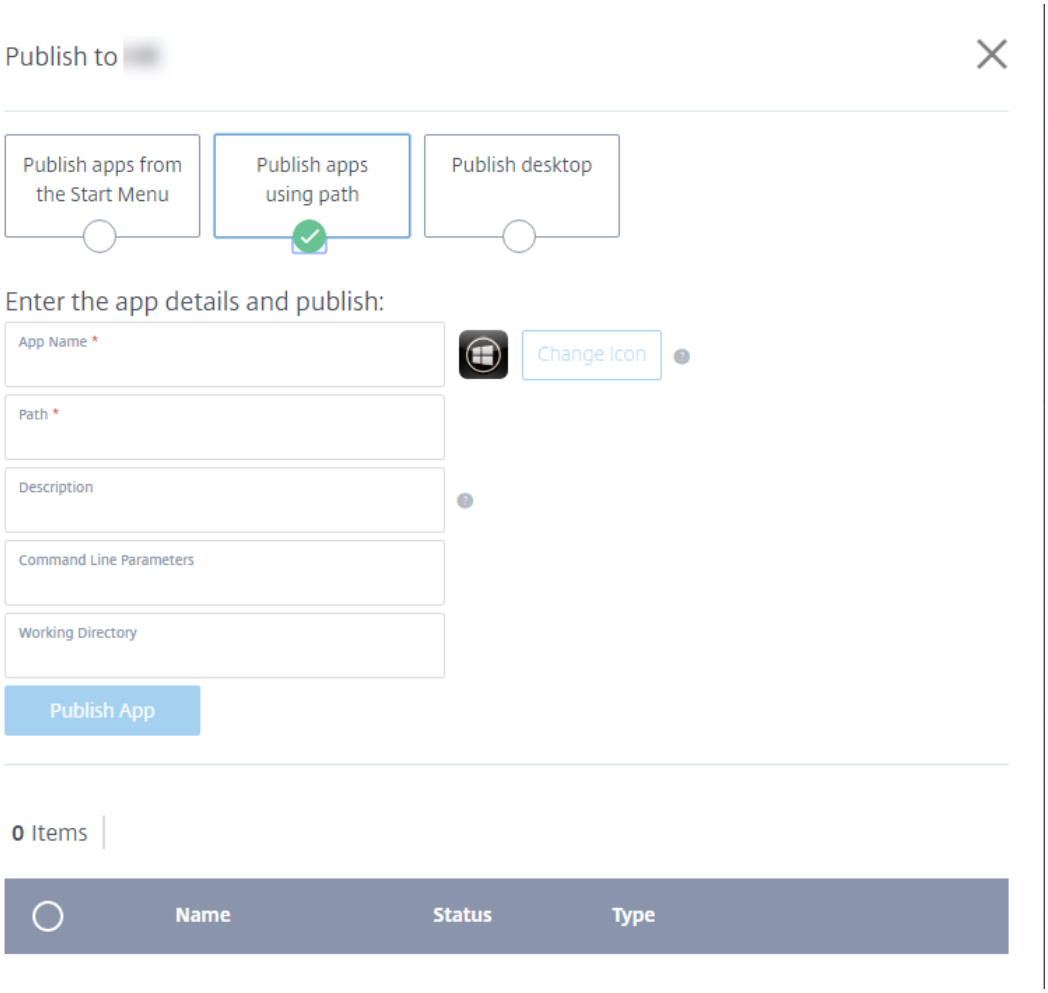
7. Pour publier des applications en spécifiant leur emplacement et d'autres informations :
   a) Sélectionnez **Publier applications à l'aide du chemin**.

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**.



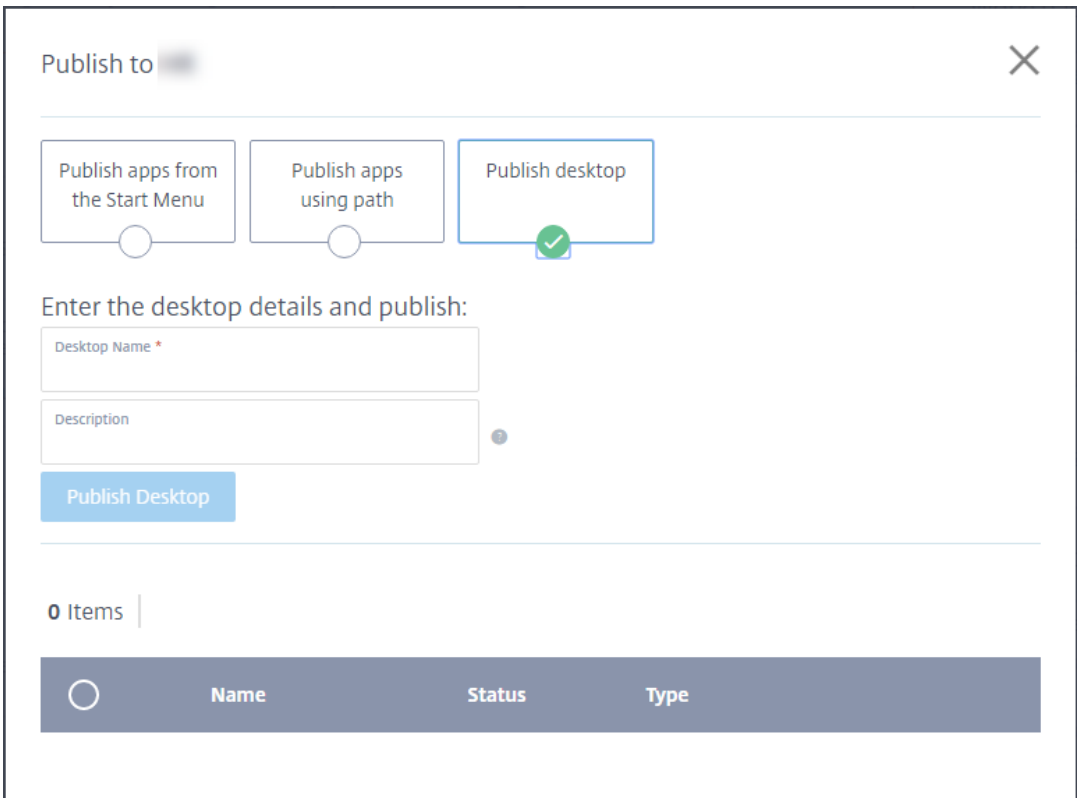
8. Pour publier un bureau :

a) Sélectionnez **Publier le bureau**.

b) Entrez le nom du bureau.

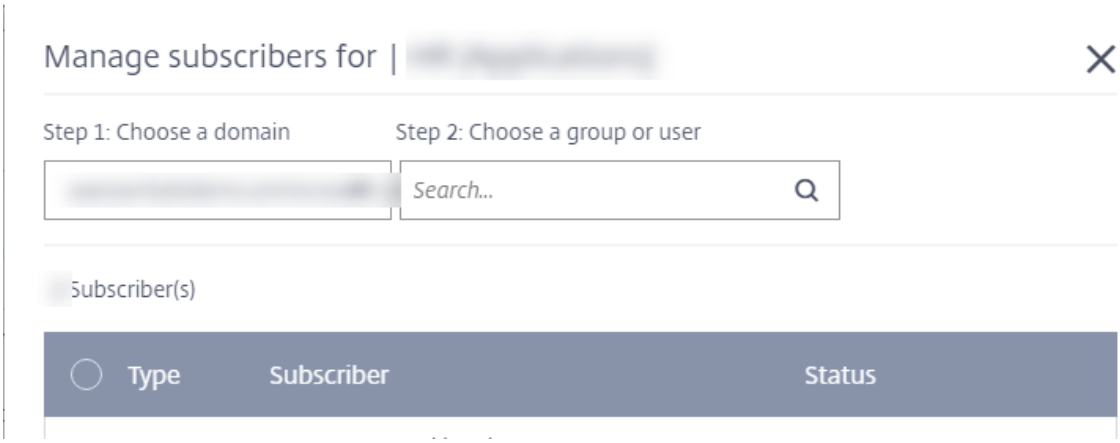
c) Entrez éventuellement une description qui apparaîtra dans l'espace de travail de l'utilisateur.

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**.

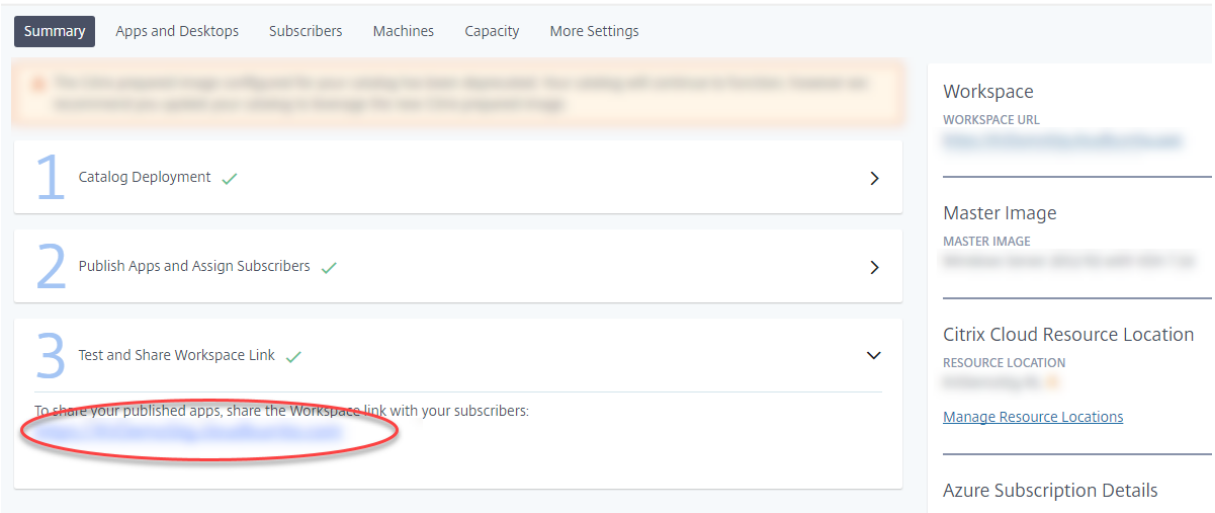
    Une fois que vous avez ajouté un utilisateur ou un groupe, il apparaît dans la liste sous les sélecteurs. Pour supprimer un utilisateur ou un groupe sélectionné, cliquez sur l'icône de la corbeille en regard de l'entrée, puis cliquez sur **Supprimer**. Plus tard, si vous souhaitez supprimer des utilisateurs, 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 sur la page 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.



Consultez Expérience d'espace de travail pour de plus amples 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 sur la page 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 **Update**.

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.

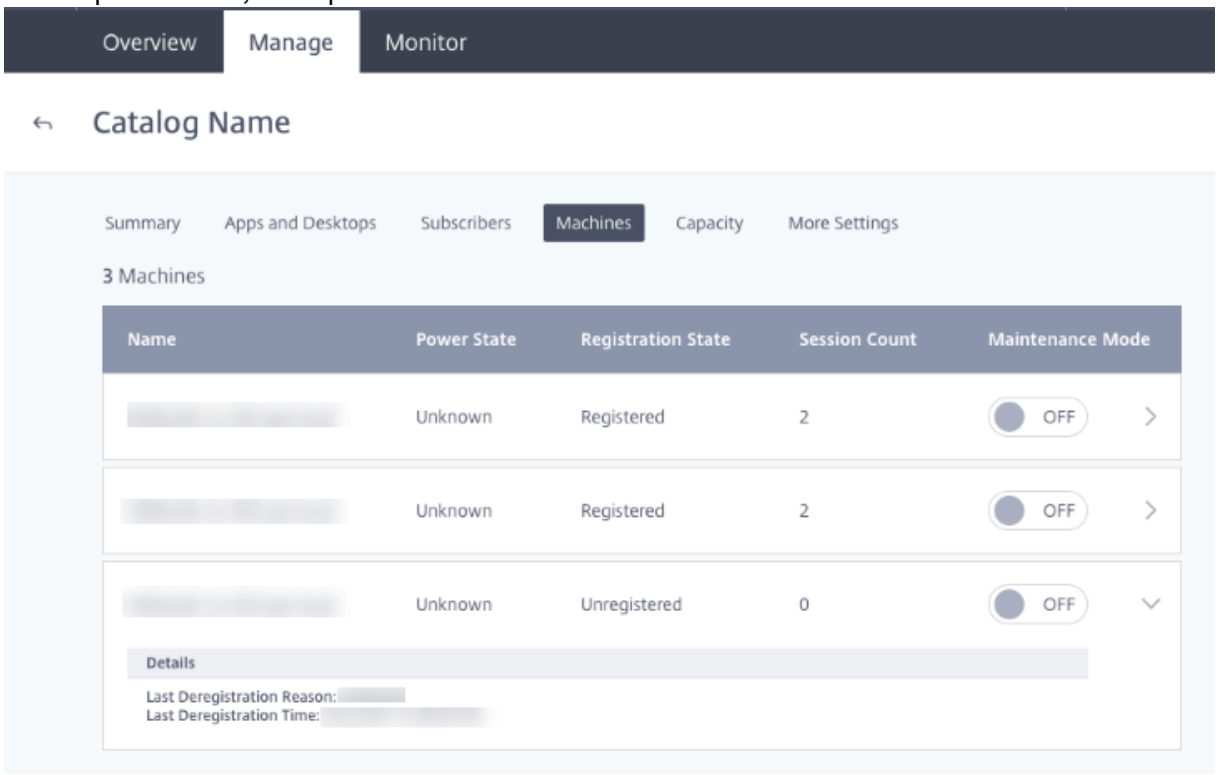
Mettre à jour le nombre de VDA dans un catalogue

1. Si vous n'êtes pas déjà sur la page Citrix Cloud, connectez-vous. Dans le menu en haut à gauche, sélectionnez **Mes services > Virtual Apps and Desktops**.
2. Cliquez sur l'onglet **Manage**.
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

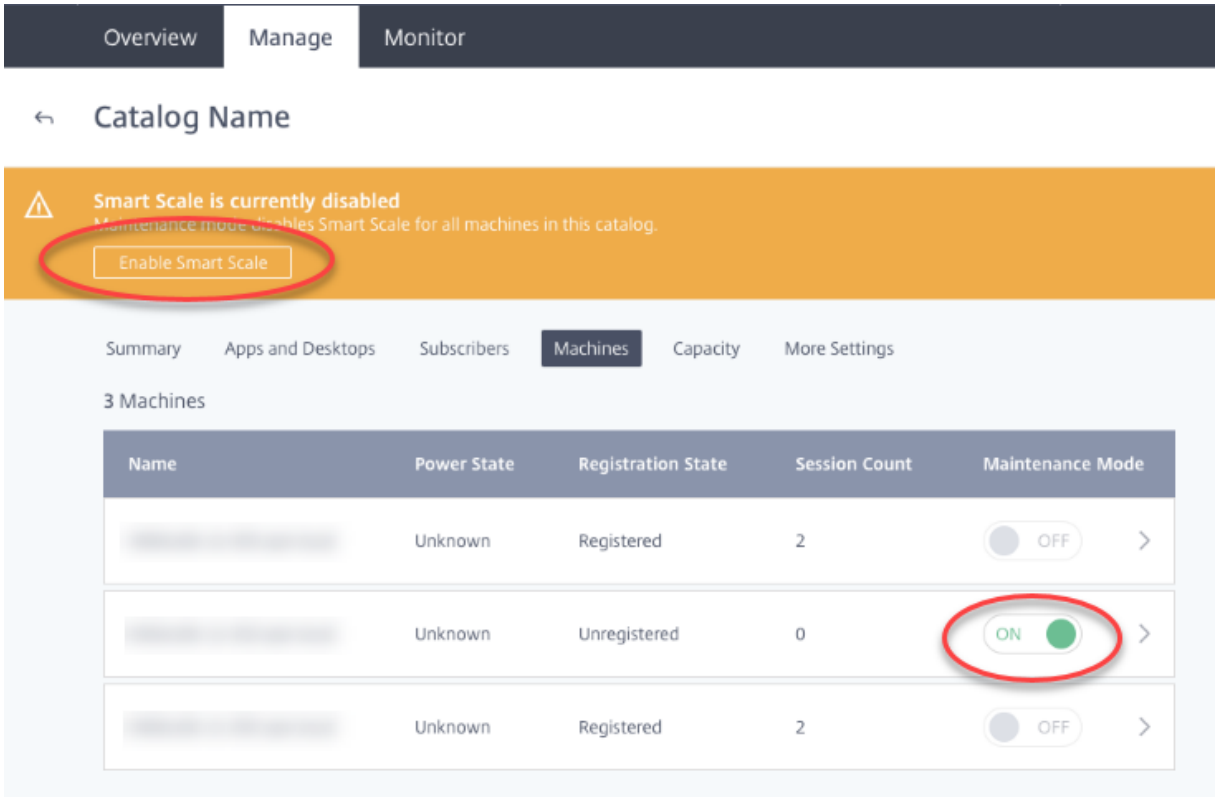
Lorsque vous sélectionnez un catalogue, l'onglet Machines de la page de résumé du catalogue répertorie toutes les machines de ce catalogue. L'affichage inclut les états d'alimentation et d'enregistrement de chaque machine, ainsi que le nombre de sessions en cours.



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 sur la page 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, consultez la section 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 sur la page 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 de plus amples informations, consultez 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 de plus amples informations, consultez 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 de plus amples informations, consultez 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, consultez 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 sur la page 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. 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 Connecter Azure Active Directory à Citrix Cloud.
- Activez Azure AD pour l'authentification auprès de l'expérience Citrix Workspace.

Pour de plus amples informations, consultez 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 Citrix Cloud.

Si vous n'êtes pas déjà sur la page 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, consultez la section 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, consultez l'article CTX220345.
- Pour résoudre les problèmes de création de catalogue, reportez-vous à la section CTX224151.

Mettre à niveau vers Citrix Virtual Apps and Desktops Standard pour Azure

Apprenez comment mettre à niveau Citrix Virtual Apps Essentials vers Citrix Virtual Apps and Desktops Standard pour Azure.

Citrix Virtual Desktops Essentials

June 10, 2021

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.

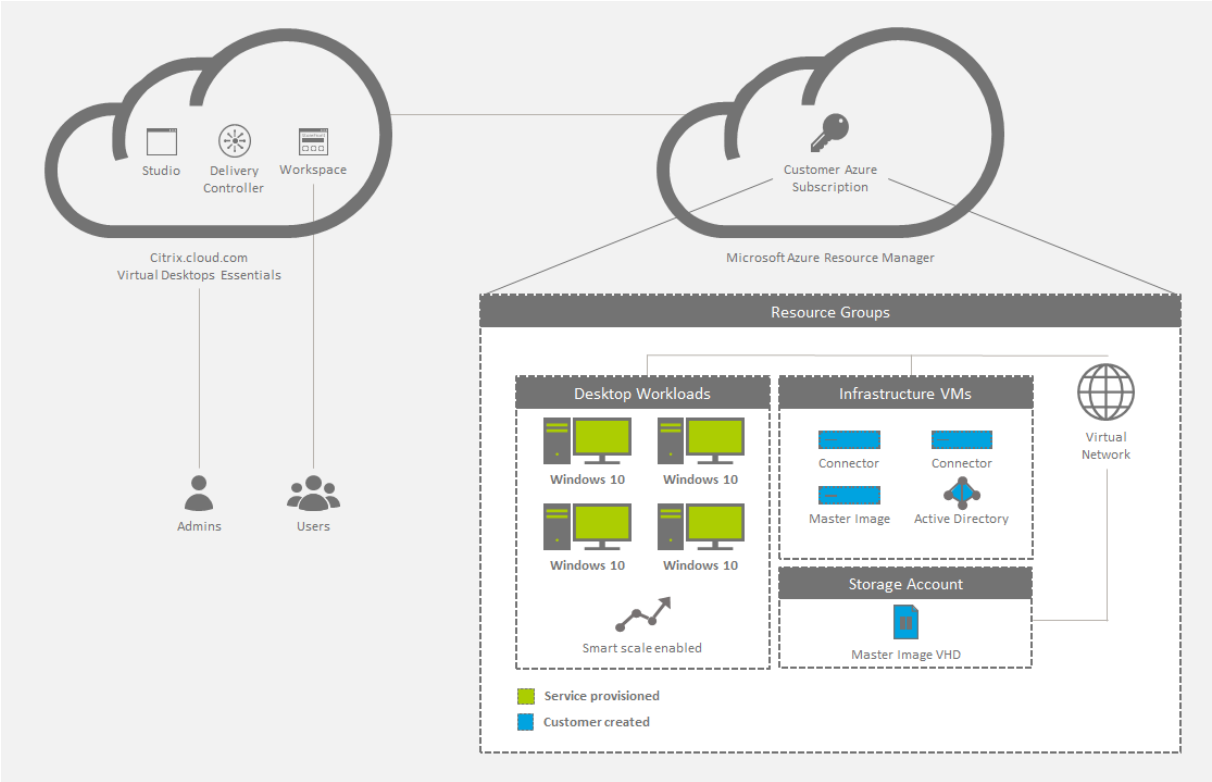
Vous gérez les bureaux Windows 10 à l'aide de Studio et surveillez les sessions à l'aide de Director. Les utilisateurs se connectent à leurs bureaux virtuels Windows 10 en se connectant avec l'application Citrix Workspace.

Après avoir configuré Citrix Virtual Desktops Essentials, vous fournissez à vos utilisateurs une URL vers Citrix Workspace. 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

> **Important :**
>
> 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. Virtual Desktops Essentials ne prend pas en charge StoreFront sur site.

Pour plus d'informations sur l'espace de travail, consultez la section Configuration de l'espace de travail.

Le diagramme présente une vue d'ensemble de l'architecture d'un déploiement de Virtual Desktops Essentials.



Nouveautés

Décembre 2018 : **Suppression de StoreFront hébergé dans le cloud**

StoreFront hébergé dans le cloud n'est plus disponible pour une utilisation avec Virtual Desktops Essentials. Les clients qui ont acheté Virtual Desktops Essentials (anciennement XenDesktop Essentials) avant décembre 2017 peuvent utiliser Citrix Workspace comme décrit dans cet article pour fournir aux abonnés un accès aux bureaux.

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 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, reportez-vous à 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 composants Cloud Connector, consultez la section 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 de Citrix ADC VPX, consultez la section Déploiement de Citrix NetScaler VPX sur Microsoft Azure.

Problèmes connus

- Le rôle d'accès personnalisé Administrateur du service d'assistance Citrix ne fonctionne pas correctement. Pour résoudre le problème, utilisez le rôle Administrateur Cloud ou activez l'accès complet. [BRK-3589]
- Si vous utilisez Azure AD Domain Services : les noms UPN de connexion à Workspace 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.

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 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 **Manage**. 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**, **Chiffrement du stockage** 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 seule 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. Cliquez sur **Créer un catalogue de machines** dans le volet Actions.
5. Sur la page **Système d'exploitation**, OS de bureau est 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 VHD 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 cliquez sur **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 cliquez sur **Modifier le groupe de mise à disposition** dans le volet Actions.
3. Sur la page **Paramètres utilisateur** (ou **Paramètres de base**) :
   a) Dans **Description**, saisissez le texte que l'espace de travail 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 les 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 plus d'informations sur la configuration, consultez la section 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 de plus amples informations, consultez 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, veuillez consulter la section 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 fournit le service aux appareils des utilisateurs. Dans la console Citrix Cloud, sélectionnez **Configuration de l'espace de travail** dans le menu supérieur gauche.

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 de détails, consultez la section 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.

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 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, consultez la section Activation de Microsoft CSP pour Citrix Essentials.

Mettre à niveau vers Citrix Virtual Apps and Desktops Standard pour Azure

Apprenez comment mettre à niveau Citrix Virtual Desktops Essentials vers Citrix Virtual Apps and Desktops Standard pour Azure.

Concepts avancés

June 17, 2019

La section Concepts avancés du site de documentation Citrix Cloud fournit une sélection d'articles techniques provenant des équipes Citrix. Les articles de cette section fournissent des conseils détaillés pour le déploiement de composants clés afin de vous aider à fournir des applications et des données de manière sécurisée et résiliente.

Pour obtenir des articles techniques encore plus détaillés, des architectures de référence et des meilleures pratiques rédigés par des experts en technologie Citrix, visitez le site Citrix Tech Zone.

Pour accéder à des forums de support communautaire pour la plate-forme et les services Citrix Cloud, consultez la section Citrix Discussions.

Architectures de référence de l'authentification d'un magasin StoreFront local pour Citrix Virtual Apps and Desktops Service

January 9, 2020

Il existe plusieurs raisons d'héberger Citrix StoreFront dans un centre de données client plutôt que d'utiliser la plate-forme Citrix Workspace. Compte tenu de la complexité de certains environnements, il est nécessaire de comprendre comment les composants Citrix Cloud interagissent avec StoreFront et Active Directory lorsque StoreFront est l'interface utilisateur principale du service.

Bien que Citrix Workspace puisse répondre aux exigences de la plupart des cas d'utilisation de Citrix Virtual Apps and Desktops, certains cas d'utilisation et exigences nécessitent que StoreFront soit hébergé dans le centre de données ou les emplacements de ressources du client.

Raisons de gérer un magasin StoreFront local

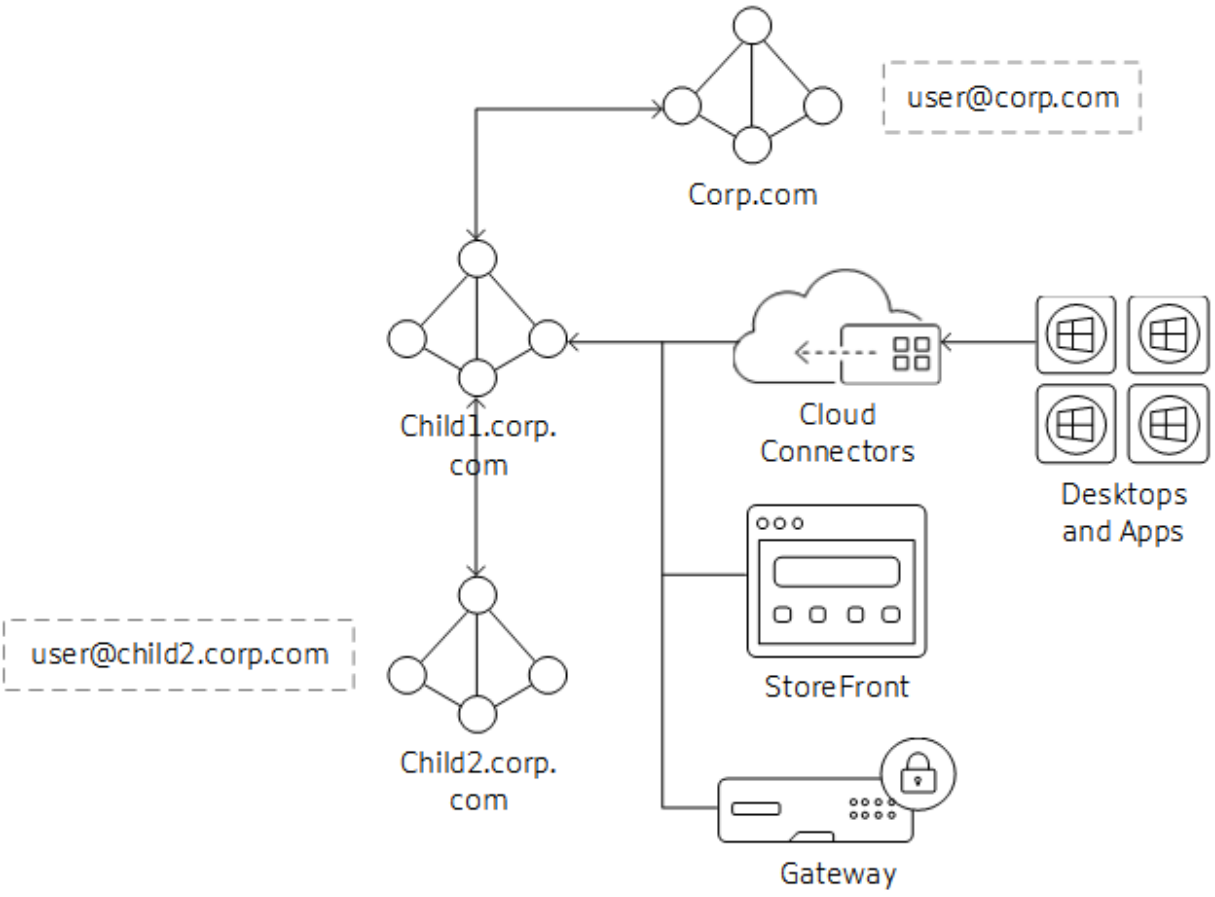
- Prise en charge de la fonctionnalité de cache d'hôte local dans les composants Cloud Connector
- Aucune prise en charge de la méthode d'authentification par carte à puce ou SAML dans Citrix Workspace
- Configurations de magasin autres que celles utilisées par défaut (modifications apportées à web.config)
- Hébergement de plusieurs configurations de magasin pour les utilisateurs internes et externes

Cet article décrit les architectures de haut niveau et la façon dont les composants interagissent avec divers scénarios d'authentification pris en charge par les conceptions Active Directory. Les composants Cloud Connector rejoignent un des domaines et autorisent le service Virtual Apps and

Desktops à attribuer des utilisateurs et des groupes Active Directory du domaine ou des domaines approuvés. Les composants Cloud Connector agissent également en tant que Delivery Controller et serveurs STA pour les composants StoreFront et Citrix Gateway.

Cet article suppose que les composants StoreFront et Gateway sont hébergés ensemble dans chaque centre de données.

Domaines parent-enfant en tant que domaines de ressources



Dans ce scénario, le domaine enfant agit en tant que domaine de ressources pour les agents VDA (Virtual Desktop Agent) et les instances StoreFront. Le domaine parent contient les utilisateurs qui accèdent aux ressources du domaine enfant.

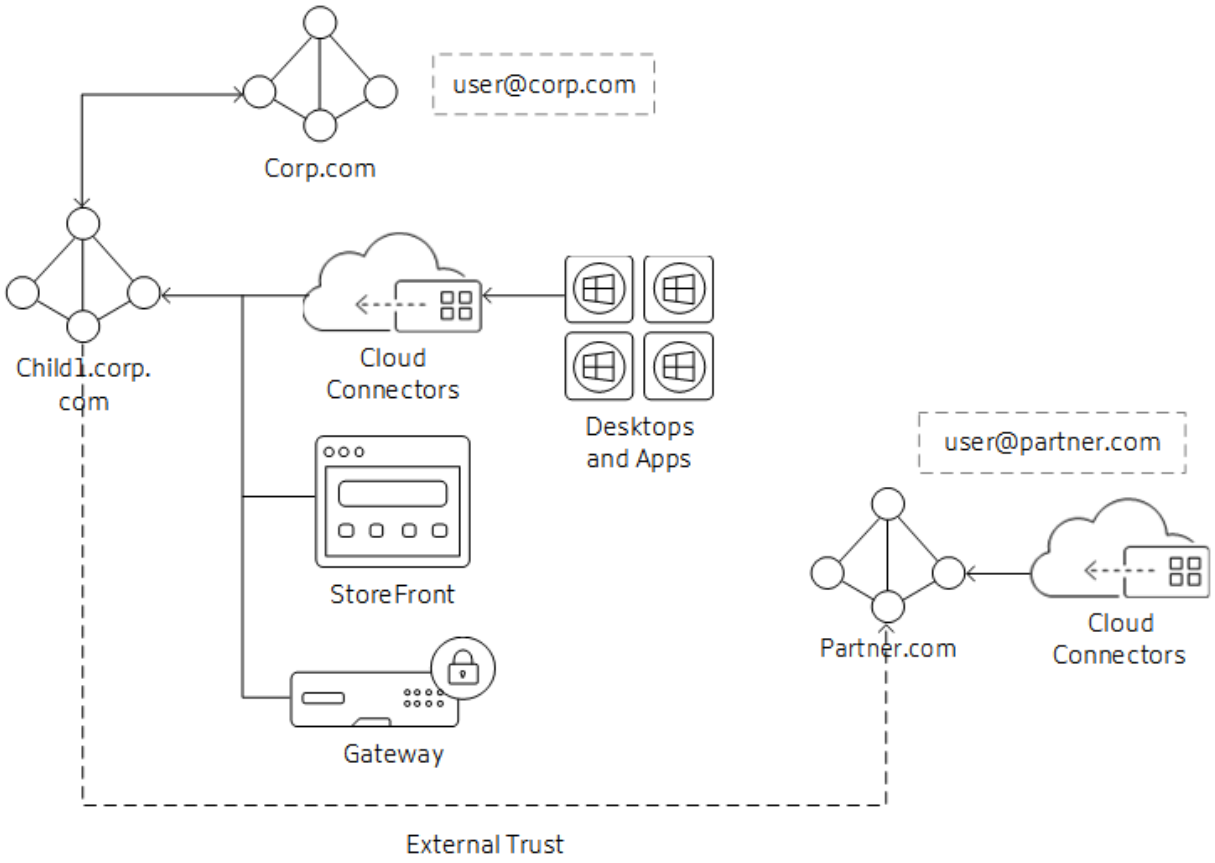
1. Les composants Cloud Connector sont associés au domaine enfant uniquement. L'approbation transitive bidirectionnelle entre le domaine enfant et le domaine parent permet aux composants Cloud Connector de communiquer avec le catalogue global dans le domaine parent.
2. StoreFront est associé au domaine enfant. La configuration du magasin utilise l'authentification par nom d'utilisateur/mot de passe et l'authentification pass-through à partir de Citrix Gateway. L'authentification par nom d'utilisateur/mot de passe est configurée pour faire confiance à n'importe quel domaine.

3. Le profil d'authentification Citrix Gateway est configuré pour que le domaine parent utilise le nom d'utilisateur principal (UPN) comme méthode d'ouverture de session principale. Si des utilisateurs doivent s'authentifier à partir du domaine enfant, le profil et la stratégie d'authentification LDAP pour le domaine enfant doivent également être liés au vServer de Gateway.
4. Modifiez le système d'exploitation de session Citrix Gateway et les profils Web, et laissez les paramètres Published Applications/Single Sign-On Domain vides (il peut être nécessaire de définir le paramètre de remplacement).

Workflow de connexion

1. L'utilisateur user@corp.com se connecte à Citrix Gateway. Gateway recherche l'utilisateur via le profil d'authentification et établit l'action de stratégie correspondante.
2. Les informations d'identification sont transmises à StoreFront. StoreFront accepte les informations d'identification et les transmet aux composants Cloud Connector (agissant en tant que Delivery Controller).
3. Les composants Cloud Connector recherchent les détails de l'objet utilisateur requis par Citrix Cloud.
4. Les composants Cloud Connector transmettent des informations d'identité à Citrix Cloud ; les jetons d'identité authentifient l'utilisateur et énumèrent les ressources attribuées à celui-ci.
5. Les composants Cloud Connector renvoient les ressources attribuées à StoreFront pour l'énumération des utilisateurs.
6. Lorsque l'utilisateur lance une application ou un bureau, Citrix Gateway génère une demande de ticket STA à l'aide des composants Cloud Connector configurés.
7. Les brokers Citrix Cloud gèrent les sessions entre les composants Cloud Connector et les VDA de domaine de ressources enregistrés dans cet emplacement de ressources.
8. La session est établie entre le client, Citrix Gateway et le VDA résolu.

Domaines approuvés externes vers domaines de ressources



Dans ce scénario, le partenaire a besoin d'accéder aux ressources publiées à l'intention des utilisateurs d'entreprise. Le domaine d'entreprise est corp.com et le domaine partenaire est partner.com.

1. Le domaine d'entreprise dispose d'une approbation externe sortante pour le domaine partenaire. Les utilisateurs du domaine partenaire peuvent s'authentifier auprès des ressources associées au domaine d'entreprise.
2. Le client Citrix Cloud a besoin de deux emplacements de ressources : un pour les composants Cloud Connector corp.com et l'autre pour les composants Cloud Connector partner.com. Les composants Cloud Connector partner.com sont nécessaires uniquement pour les appels d'authentification et d'identité vers le domaine ; ils ne sont pas utilisés pour la négociation des VDA ou des sessions.
3. StoreFront est associé au domaine corp.com. Les composants Cloud Connector dans le domaine corp.com sont utilisés comme Delivery Controller dans la configuration du magasin. La configuration du magasin utilise l'authentification par nom d'utilisateur/mot de passe et l'authentification pass-through à partir de Citrix Gateway. L'authentification par nom d'utilisateur/mot de passe est configurée pour faire confiance à n'importe quel domaine.
4. Le profil d'authentification Citrix Gateway est configuré pour que le domaine corp.com utilise le nom d'utilisateur principal (UPN) comme méthode d'ouverture de session principale. Con-

figurez un deuxième profil et une deuxième stratégie pour que le domaine partner.com utilise UPN et liez-le au même vServer de Gateway que le domaine corp.com.

5. Modifiez le système d'exploitation de session Citrix Gateway et les profils Web, et laissez les paramètres Published Applications/Single Sign-On Domain vides (il peut être nécessaire de définir le paramètre de remplacement).

> **Remarque :**
>
> Selon l'emplacement du domaine approuvé externe, les utilisateurs du domaine externe peuvent connaître des délais de lancement plus longs que les utilisateurs du domaine parent ou de ressources.

Workflow de connexion

1. L'utilisateur user@partner.com se connecte à Citrix Gateway. Gateway recherche l'utilisateur via le profil d'authentification qui correspond à la recherche UPN et établit l'action de stratégie correspondante.
2. Les informations d'identification sont transmises à StoreFront. StoreFront accepte les informations d'identification et les transmet aux composants Cloud Connector (agissant en tant que Delivery Controller).
3. Les composants Cloud Connector recherchent les détails de l'objet utilisateur requis par Citrix Cloud.
4. Les composants Cloud Connector transmettent des informations d'identité à Citrix Cloud ; les jetons d'identité authentifient l'utilisateur et énumèrent les ressources attribuées à celui-ci.
5. Les composants Cloud Connector renvoient les ressources attribuées à StoreFront pour l'énumération des utilisateurs.
6. Lorsque l'utilisateur lance une application ou un bureau, Citrix Gateway génère une demande de ticket STA à l'aide des composants Cloud Connector configurés, dans ce cas à partir de child1.corp.com.
7. Les brokers Citrix Cloud gèrent les sessions entre les composants Cloud Connector et les VDA de domaine de ressources enregistrés dans cet emplacement de ressources.
8. La session est établie entre le client, Citrix Gateway et le VDA résolu.

Approbation de forêt/Approbation de raccourci vers domaines de ressources

Les domaines d'approbation de forêt et de raccourcis ne sont pris en charge que s'ils sont traités comme une relation d'approbation de domaine externe avec le domaine de ressources. Pour les approbations de forêt, vous pouvez suivre les mêmes étapes que celles décrites dans la section Domaines approuvés externes vers domaines de ressources. Cette section peut changer à l'avenir en fonction de la prise en charge des approbations de forêts natives entre les domaines/forêts utilisateur et les ressources.

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