Citrix Cloud

Contents

Citrix Cloud

July 2, 2024

> **Remarque :**
>
> Citrix Virtual Apps Essentials et Citrix Virtual Desktops Essentials ont atteint leur fin de vente et leur fin de vie. Pour plus d'informations, veuillez consulter l'article CTX583004.

Citrix Cloud est une plate-forme qui héberge et gère les services cloud 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.

Nouveautés

Visitez Mises à jour de Citrix Cloud pour être tenu informé des fonctionnalités nouvelles et à venir de Citrix Cloud et pour accéder aux services suivants :

- Citrix Analytics
- Citrix DaaS
- Citrix Workspace

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 de plus amples informations, consultez la section Évaluations de services Citrix Cloud.

Documentation sur les services Citrix Cloud

Vous recherchez des informations sur la configuration ou la gestion des services Citrix Cloud ? Accédez à Citrix Cloud Services pour trouver des liens vers la documentation Produit pour tous les services cloud.

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.

Pour en savoir plus sur les composants de service clés dans Citrix Cloud, consultez les ressources suivantes :

- 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 Citrix DaaS : fournit des conseils détaillés sur le déploiement de Citrix DaaS (anciennement 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.

Accord de niveau de service

July 2, 2024

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 d'utilisateur final de Cloud Software Group (EULA) 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 ou comportement abusif ou saisie incorrecte.
- Utilisation par le client d'un Service après que Citrix a conseillé au client de modifier l'utilisation du Service, si le client n'a pas modifié l'utilisation.
- Composant non géré par Citrix, y compris, mais sans s'y limiter, les composants suivants : machines physiques et virtuelles contrôlées par le Client, systèmes d'exploitation installés et entretenus par le Client, logiciels installés et contrôlés par le client, équipement réseau ou autre matériel installé ; paramètres de sécurité, stratégies de groupe et autres stratégies de configuration définis et contrôlés par le Client ; défaillances du fournisseur de cloud public, défaillances du fournisseur de services Internet ou autres facteurs de soutien du Client externes au contrôle de Citrix.
- Les employés, agents, sous-traitants ou fournisseurs du Client, ou toute personne ayant accès aux mots de passe ou à l'équipement du client, ou résultant du manquement du Client à suivre les pratiques de sécurité appropriées.
- Les tentatives du client d'effectuer des opérations dépassant les droits du Service.
- Interruption de service due à un cas de force majeure, y compris, mais sans s'y limiter, les catastrophes naturelles, les guerres, les actes de terrorisme, ou les actions du gouvernement.

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

Citrix offre des engagements de Service aux clients qui :

- Ont acheté les Services en utilisant un abonnement basé sur une durée (période d'abonnement minimum d'1 an).
- Disposent d'au moins un abonnement de 100 unités (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.
Service NetScaler Console	Durée moyenne de disponibilité du Service pour tous les POP.
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.
NetScaler 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.
NetScaler SD-WAN Orchestrator	Les utilisateurs peuvent accéder à leur compte SD-WAN Orchestrator et gérer leur réseau SD-WAN via le service.
Citrix Secure Private Access	Durée pendant laquelle les utilisateurs peuvent accéder à leur application Web interne ou SaaS via le Service.
Citrix DaaS	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.

> **Remarque :**
>
> Citrix DaaS est le nouveau nom de Citrix Virtual Apps Service, Citrix Virtual Desktops Service et Citrix Virtual Apps and Desktops Service.

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 au CLUF 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.

Avis de tiers

November 6, 2023

- Citrix Cloud - Avis de tiers (PDF)
- Citrix Analytics Service - Avis de tiers (PDF)
- Citrix DaaS - Avis de tiers (PDF)
- Citrix DaaS Standard pour Azure - Avis de tiers (PDF)
- Remote Browser Isolation (anciennement Secure Browser) (PDF)
- Citrix Endpoint Management - Avis de tiers (PDF)
- Citrix Cloud Linux VDA Image Service - Avis de tiers (PDF)
- Connector Appliance pour Cloud Services - Avis de tiers (PDF)
- Citrix Gateway Service - Avis de tiers (PDF)
- Citrix Device Posture Service - Avis de tiers (PDF)

> **Remarque :**
>
> Citrix DaaS était auparavant Citrix Virtual Apps and Desktops Service. Citrix DaaS Standard pour Azure était auparavant Citrix Virtual Apps and Desktops Standard pour Azure.

Comment obtenir de l'aide

July 2, 2024

Cet article explique comment résoudre les problèmes et obtenir de l'aide en cas de problème lors de la création d'un compte ou de la connexion à Citrix Cloud ou à un autre site Web Citrix. Cet article inclut également d'autres ressources d'auto-assistance ainsi que des options d'assistance guidée.

> **Important :**
>
> Si vous rencontrez un problème lors de la connexion à un site Web Citrix ou lors de l'inscription à l'authentification multifacteur (MFA), consultez d'abord cet article pour accéder aux ressources de dépannage. Si ces ressources ne vous aident pas à résoudre votre problème, contactez le service client Citrix à l'adresse https://www.citrix.com/contact/customer-service.html.

Création d'un compte

Un compte Citrix est requis pour accéder à certaines ressources du site Web de Citrix, telles que les forums de discussion Citrix, les cours de formation, certains téléchargements de produits et le support technique Citrix.

Pour créer un nouveau compte Citrix pour votre entreprise, contactez Citrix en utilisant l'une des méthodes suivantes :

- Contactez le service client Citrix.
- Contactez un partenaire Citrix ou un commercial Citrix de votre région.

Si vous disposez déjà d'un compte Citrix, vous pouvez créer un compte Citrix Cloud et terminer le processus d'intégration en effectuant les tâches décrites dans la section Créer un compte Citrix Cloud.

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

Connexion aux sites Web de Citrix et à Citrix Cloud

Si vous ne parvenez pas à vous connecter à un site Web Citrix avec votre compte Citrix, utilisez les ressources suivantes pour résoudre les problèmes :

- CTX228792: Troubleshooting login issues on Citrix websites
- CTX283814: Sign in issue after setting up Citrix account

Je n'arrive pas à configurer l'authentification multifacteur (MFA) ou je n'arrive pas à m'authentifier avec l'authentification multifacteur lorsque je me connecte à mon compte Citrix

Consultez les articles suivants pour obtenir des informations de dépannage :

- CTX461297: How to Enroll into Multi Factor Authentication (MFA)
- CIX463758: How to recover access to your account

Si vous n'arrivez toujours pas à vous connecter avec l'authentification multifacteur, contactez le service client Citrix en accédant à https://www.citrix.com/contact/customer-service.html.

Comment trouver le nom d'utilisateur de mon compte Citrix ou réinitialiser mon mot de passe Citrix ?

Suivez les étapes ci-dessous pour vérifier le nom d'utilisateur de votre compte Citrix et réinitialiser votre mot de passe.

1. Accédez à https://www.citrix.com/welcome/request-password.html.
2. Pour vérifier le nom d'utilisateur de votre compte Citrix :
    a) Sous **Rechercher mon compte par**, sélectionnez **E-mail**.
    b) Entrez l'adresse e-mail associée à votre compte Citrix.

3. Pour réinitialiser le mot de passe de votre compte Citrix :
    a) Sous **Rechercher mon compte par**, sélectionnez **Nom d'utilisateur**.
    b) Entrez le nom d'utilisateur de votre compte Citrix.
4. Cliquez sur **Rechercher mon compte**.

Si Citrix trouve votre compte à l'aide de votre adresse e-mail, vous recevrez un e-mail contenant les noms d'utilisateur et les noms d'entreprise associés à votre adresse e-mail. Si Citrix trouve votre compte à l'aide de votre nom d'utilisateur Citrix, vous recevrez un e-mail contenant des instructions pour réinitialiser votre mot de passe.

Si vous ne recevez aucun e-mail au bout de quelques minutes, consultez la section Les e-mails de Citrix n'apparaissent pas dans ma boîte de réception dans cet article.

Je n'arrive pas à me connecter à Citrix Cloud

- Assurez-vous de vous connecter avec les informations d'identification de compte correctes. Pour vérifier le nom d'utilisateur de votre compte, accédez à https://citrix.cloud.com/, sélectionnez **Nom d'utilisateur oublié ?** et entrez votre adresse e-mail. Vous recevrez un e-mail contenant le nom d'utilisateur de votre compte.
- Il se peut que vous deviez réinitialiser votre mot de passe. Citrix Cloud vous invite à modifier votre mot de passe si vous ne vous êtes pas connecté récemment ou si votre mot de passe n'est pas suffisamment sécurisé. Pour plus d'informations, consultez la section Modification de votre mot de passe dans cet article.
- Vous devrez peut-être vous connecter à l'aide d'une URL de connexion personnalisée. Si votre compte Citrix Cloud utilise Azure AD, Google Cloud Identity ou SAML pour authentifier les administrateurs, 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.

Si vous n'arrivez toujours pas à vous connecter à Citrix Cloud, contactez le service client Citrix.

Les e-mails Citrix n'apparaissent pas dans ma boîte de réception

Lorsque Citrix vous envoie des e-mails pour vérifier votre identité pour l'authentification multifacteur, lorsque vous recherchez votre compte Citrix ou lorsque vous modifiez votre mot de passe, l'e-mail arrive généralement en quelques minutes. Si vous ne recevez pas ces e-mails :

- Vérifiez l'adresse e-mail enregistrée pour votre compte Citrix et assurez-vous qu'elle est correcte. Si vous avez récemment changé d'adresse e-mail, l'e-mail de vérification peut être envoyé à votre ancienne adresse.
- L'e-mail a peut-être été filtré accidentellement. Vérifiez les dossiers Spam et Corbeille de votre client de messagerie. Vous pouvez également rechercher dans votre compte de messagerie des e-mails provenant de `donotreplynotifications@citrix.com` ou `cloud@citrix.com`.
- Votre pare-feu a peut-être bloqué l'e-mail. Assurez-vous que les adresses suivantes figurent dans la liste des expéditeurs approuvés :
  - `donotreplynotifications@citrix.com`
  - `cloud@citrix.com`
  - `CustomerService@citrix.com`

Si vous n'avez pas reçu l'e-mail après quelques minutes ou si vous rencontrez un autre problème lors de la connexion, contactez le service client Citrix.

Authentification multifacteur pour les comptes Citrix et Citrix Cloud

Les clients Citrix doivent se connecter à leur compte Citrix et à Citrix Cloud à l'aide de l'authentification multifacteur. L'inscription à l'authentification multifacteur a lieu dans les cas suivants :

- Un nouveau client se connecte à son compte Citrix pour la première fois.
- Un client Citrix intègre un nouveau compte Citrix Cloud mais ne s'est pas encore inscrit à l'authentification multifacteur.
- Un nouvel administrateur rejoint un compte Citrix Cloud existant.

Si vous êtes invité à vous inscrire à l'authentification multifacteur lorsque vous vous connectez à votre compte Citrix ou à Citrix Cloud, suivez les étapes décrites dans CTX461297: How to Enroll into Multi Factor Authentication (MFA).

Pour plus d'informations sur l'authentification multifacteur (MFA) pour les comptes Citrix, consultez CTX463482: Frequently asked questions when setting up Multi-Factor Authentication (MFA) on Citrix properties.

Récupération de compte

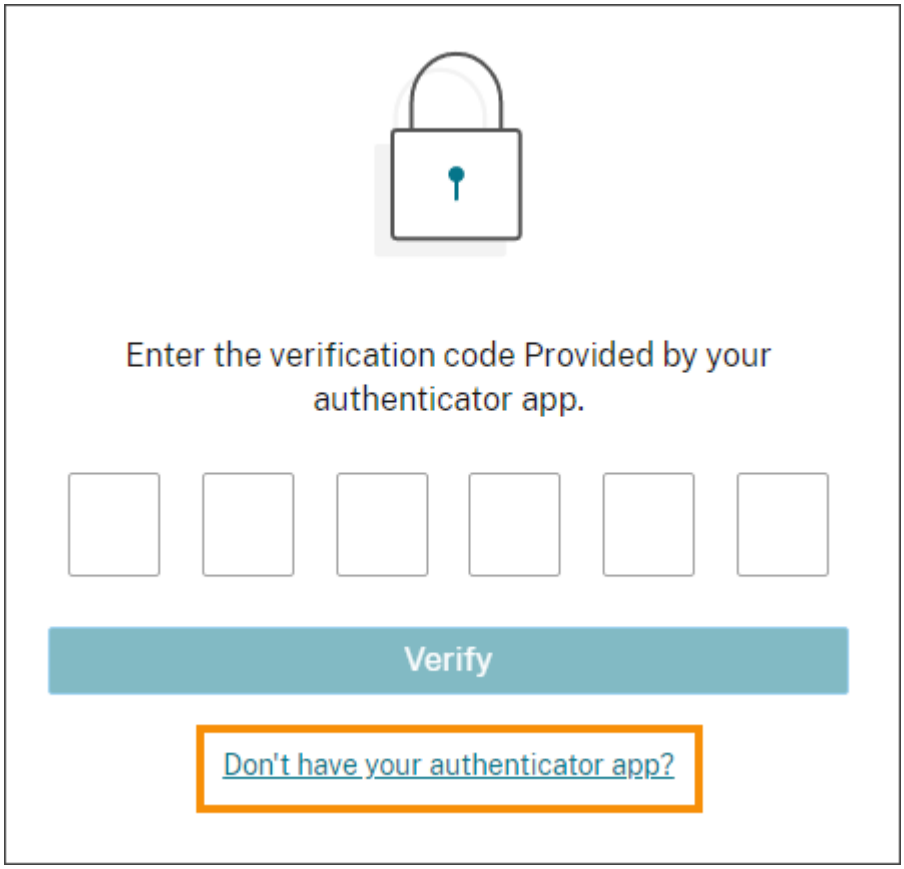
Si vous avez besoin d'aide pour récupérer les informations d'identification de votre compte Citrix, consultez la section Comment trouver le nom d'utilisateur de mon compte Citrix ou réinitialiser mon mot de passe Citrix ? dans cet article.

Si vous avez besoin d'aide pour récupérer l'accès à votre compte Citrix Cloud, vous pouvez utiliser les méthodes de récupération que vous avez configurées lors de votre inscription à l'authentification multifacteur. Ces méthodes de récupération incluent :

- Un code à usage unique que Citrix envoie à votre adresse e-mail de récupération
- Un code de sauvegarde issu de la liste que vous avez générée lors de l'inscription à l'authentification multifacteur
- Un appel du support Citrix à votre numéro de téléphone de récupération pour vérifier votre identité et vous aider à accéder à votre compte La configuration d'un numéro de téléphone de récupération est requise lors de l'inscription à MFA.

Pour vous connecter à l'aide d'une méthode de récupération :

1. À partir du compte Citrix ou de la page de connexion de Citrix Cloud, entrez votre nom d'utilisateur et votre mot de passe, puis sélectionnez **Connexion**.
2. Lorsque vous êtes invité à saisir le code de votre méthode d'authentification multifacteur principale, sélectionnez **Utiliser une méthode de récupération**.



3. Sélectionnez la méthode de récupération que vous souhaitez utiliser, le cas échéant. Si vous n'avez configuré qu'une seule autre méthode de récupération, en plus d'un numéro de téléphone de récupération, Citrix vous invite à utiliser cette méthode automatiquement.

4. Si vous utilisez votre adresse e-mail de récupération, saisissez le code à usage unique envoyé par Citrix et sélectionnez **Vérifier**. Si vous ne recevez pas le code pendant un certain temps, sélectionnez **Renvoyer e-mail**. Après vérification, Citrix Cloud vous connecte.
5. Si vous utilisez un code de secours, saisissez-le lorsque vous y êtes invité et sélectionnez **Vérifier et continuer**. Citrix Cloud vous connecte et vous envoie un e-mail pour vous informer qu'un code de secours a été utilisé et vous indique le nombre de codes de secours valides restants. Notez ou supprimez le code de secours utilisé pour vous assurer de ne pas le réutiliser.
6. Si vous ne parvenez pas à utiliser votre e-mail de récupération ou vos codes de secours :

    a) Sélectionnez **Contacter le support Citrix**.
    b) Remplissez le formulaire avec les détails de votre problème. Un représentant du support Citrix vous contactera à l'aide de votre numéro de téléphone de récupération pour vérifier votre identité. Ensuite, le représentant vous envoie un code de récupération que vous pouvez utiliser pour vous connecter.
    c) Revenez à la page de connexion de Citrix Cloud et connectez-vous à l'aide de vos informations d'identification Citrix Cloud.
    d) Lorsque vous êtes invité à entrer un code, saisissez le code de récupération que vous avez reçu du support Citrix et sélectionnez **Vérifier**.

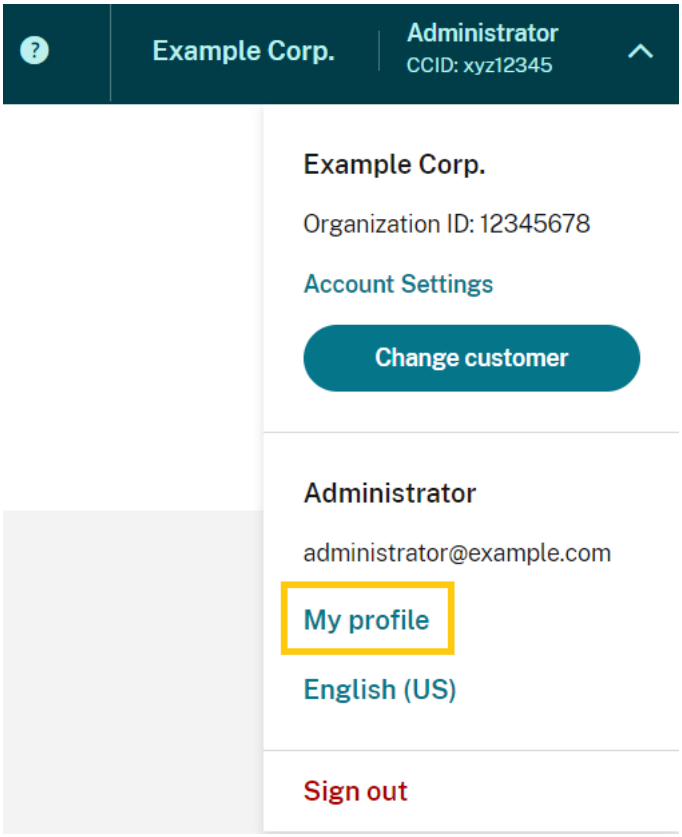
Une fois connecté, assurez-vous de mettre à jour les méthodes de récupération de compte afin d'éviter de futurs problèmes de connexion.

Mettre à jour vos paramètres d'authentification multifacteur

Vous pouvez mettre à jour vos paramètres d'accès via l'authentification multifacteur et vos paramètres de récupération via votre page **Mes paramètres**. Vous pouvez accéder à cette page via votre compte Citrix ou via Citrix Cloud.

Pour accéder à votre page **Mes paramètres** :

1. Connectez-vous à votre compte Citrix ou à Citrix Cloud.
2. Depuis votre compte Citrix, visitez https://accounts.cloud.com/core/profile.
3. Dans Citrix Cloud, sélectionnez **Mes paramètres** dans le menu en haut à droite.



Pour modifier vos paramètres d'authentification multifacteur, consultez les sections suivantes :

- Gérer votre méthode de MFA principale
- Gérer vos méthodes de récupération de MFA

Modification de votre mot de passe

Si vous avez oublié le mot de passe de votre compte, sélectionnez **Mot de passe oublié ?** et entrez le nom d'utilisateur de votre compte lorsque vous y êtes invité. Citrix envoie un e-mail à l'adresse e-mail associée à votre compte contenant un lien permettant de définir un nouveau mot de passe. Si vous ne recevez pas cet e-mail au bout de quelques minutes, ou si vous avez besoin d'une assistance supplémentaire, contactez le service client Citrix.

Citrix Cloud peut vous demander de 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.
- 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 60 derniers jours.

Les mots de passe doivent comporter entre 8 et 128 caractères et inclure :

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

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

État des services cloud

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.

Pour plus d'informations sur Cloud Health Dashboard, consultez la section État du service.

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.

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.

Centre de connaissances du support Citrix

Le Centre de connaissances fournit du contenu de dépannage ainsi que des bulletins de sécurité et des avis de mise à jour des logiciels pour tous les produits Citrix. Entrez simplement un critère de recherche pour trouver du contenu pertinent. Vous pouvez filtrer les résultats en fonction du produit et du type d'article.

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 déploiement des technologies Citrix.

Centre d'aide utilisateur

Le Centre d'aide utilisateur Citrix fournit une documentation sur les produits Citrix destinée uniquement aux utilisateurs finaux de votre organisation. Le Centre d'aide utilisateur fournit des instructions dans un format facile à lire pour les produits destinés aux utilisateurs finaux tels que l'application Citrix Workspace et Citrix SSO. Pour obtenir la documentation utilisateur pour ShareFile, consultez Applications Citrix Files sur le site Web de documentation du produit ShareFile.

Support technique

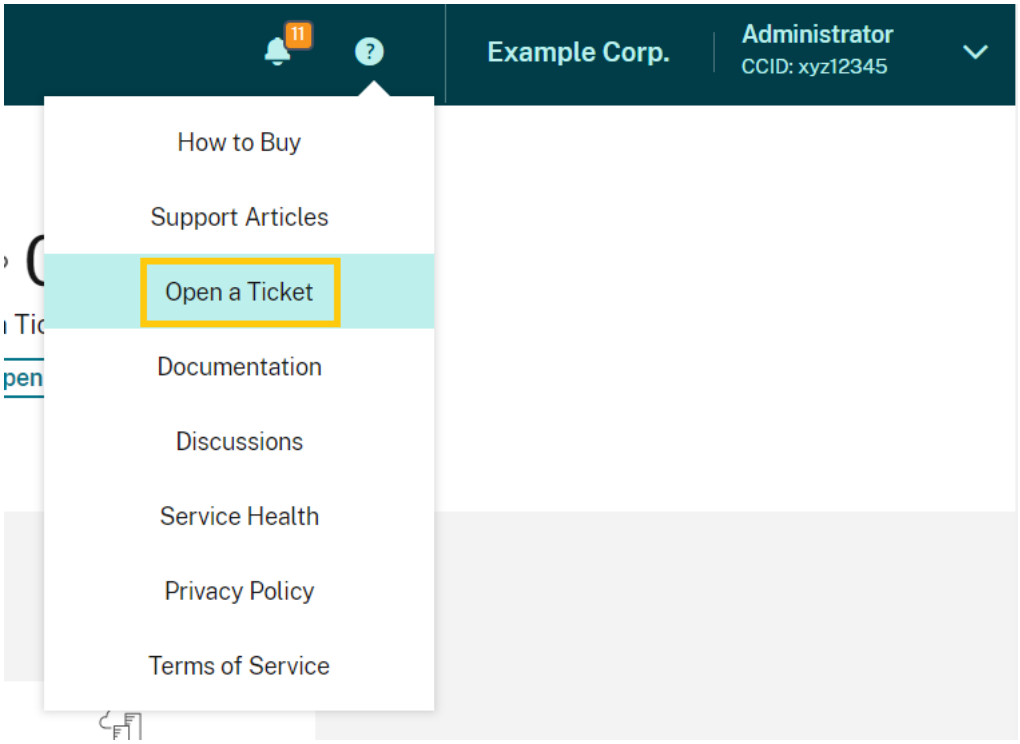
Si vous rencontrez un problème nécessitant une aide technique, vous pouvez accéder au Portail My Support pour ouvrir un ticket de support ou discuter avec un représentant du support technique Citrix.

Pour accéder au portail My Support, visitez https://support.citrix.com/case/manage.

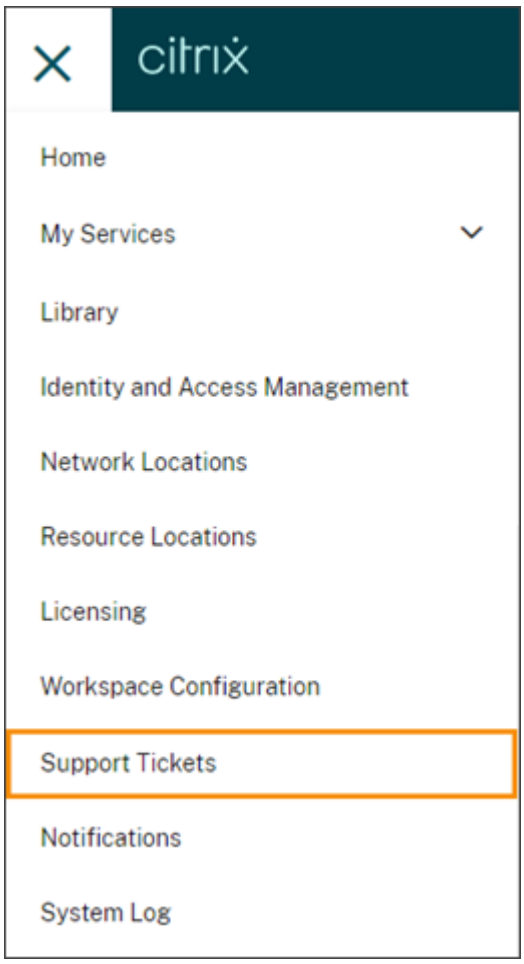
Pour accéder au portail depuis Citrix Cloud, vous devez disposer de l'autorisation **Tickets de support**. Pour plus d'informations sur les autorisations d'administrateur, consultez la section Modifier les autorisations d'administrateur.

Depuis la console de gestion Citrix Cloud, vous pouvez accéder à My Support en utilisant les méthodes suivantes :

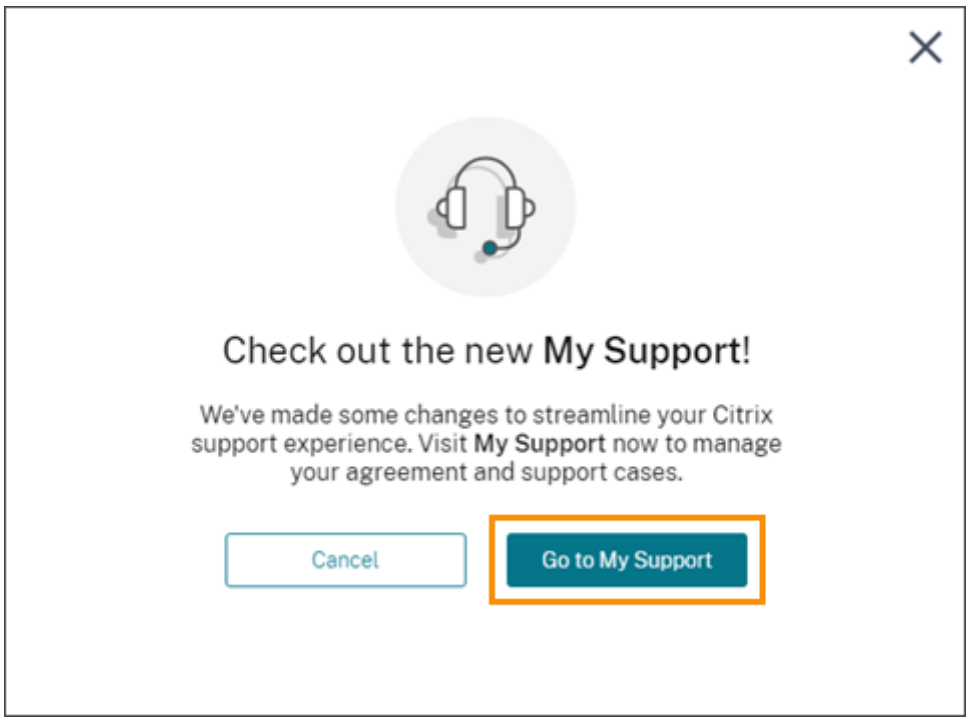
- Sur l'icône d'**aide** en haut à droite de l'écran, sélectionnez **Ouvrir un ticket**.



- Dans le menu Citrix Cloud en haut à gauche de l'écran, sélectionnez **Tickets de supports**.

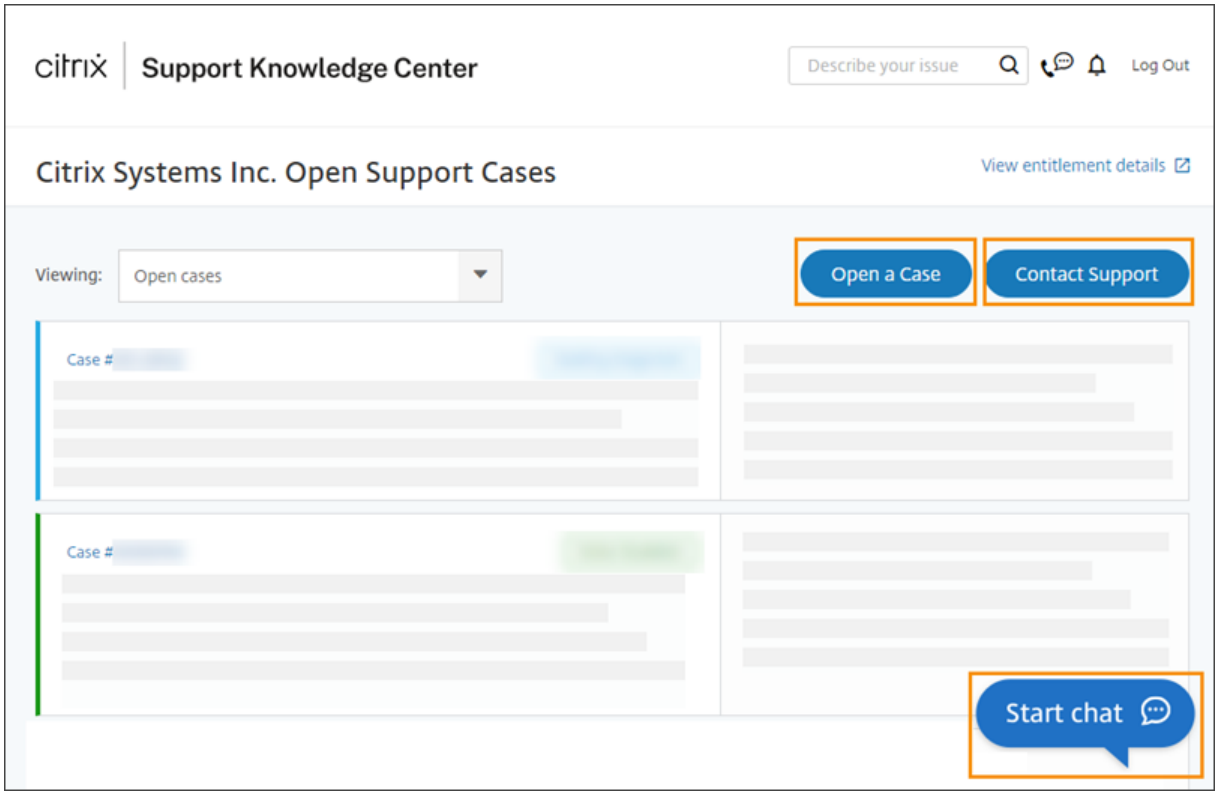


Après avoir sélectionné l'une de ces options, sélectionnez **Accéder à My support**, puis connectez-vous à l'aide des informations d'identification de votre compte Citrix.



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

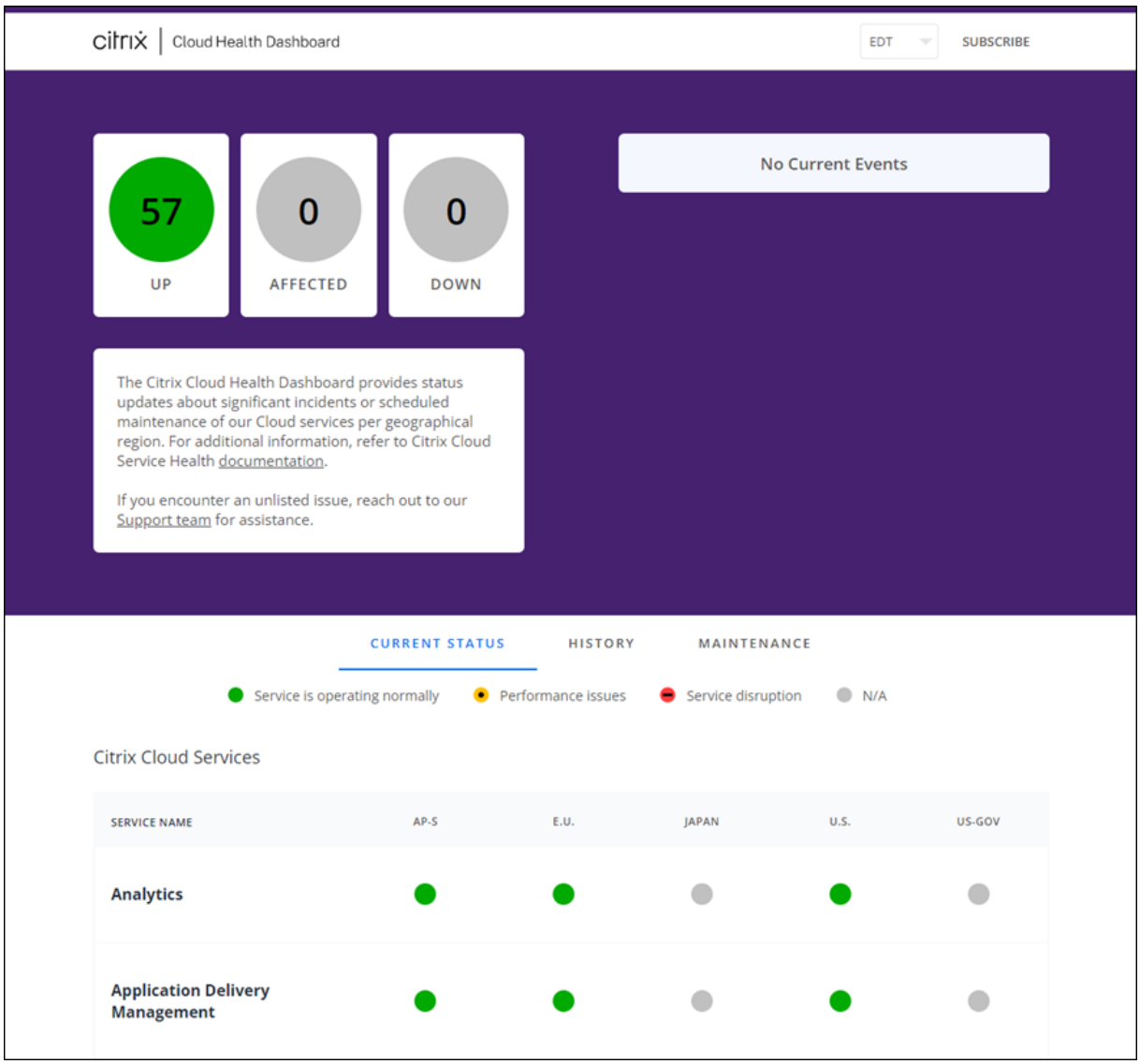
- Ouverture d'un ticket de support : sélectionnez **Open a Case**, puis fournissez les détails du problème que vous rencontrez.
- Par téléphone : sélectionnez **Contact Support** pour afficher la liste des numéros de téléphone locaux que vous pouvez utiliser pour appeler le support technique Citrix.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



État du service Citrix Cloud

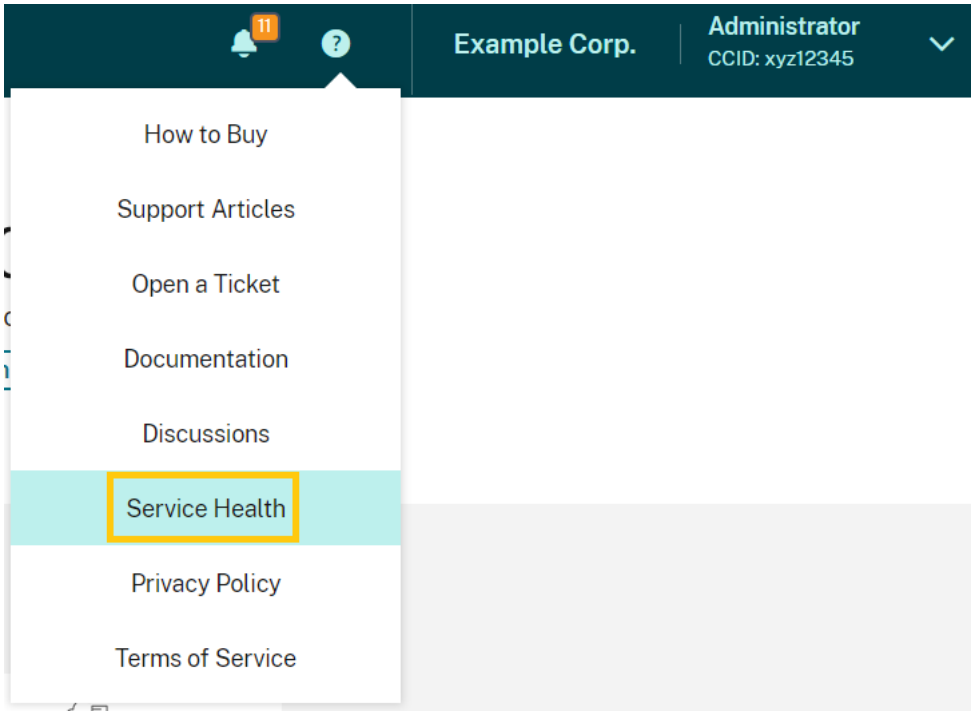
November 29, 2023

Citrix Cloud Health Dashboard 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.



Vous pouvez accéder au Cloud Health Dashboard en utilisant les méthodes suivantes :

- Accédez à https://status.cloud.com via votre navigateur Web.
- Sélectionnez **État du service** dans le menu Aide de Citrix Cloud.



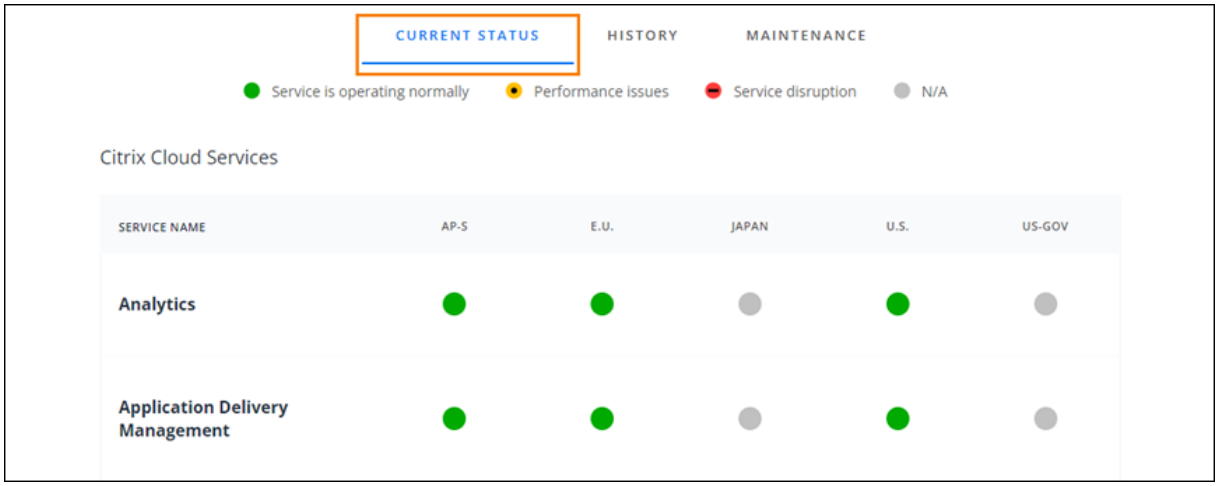
Utilisez le tableau de bord pour en savoir plus sur les conditions suivantes :

- 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

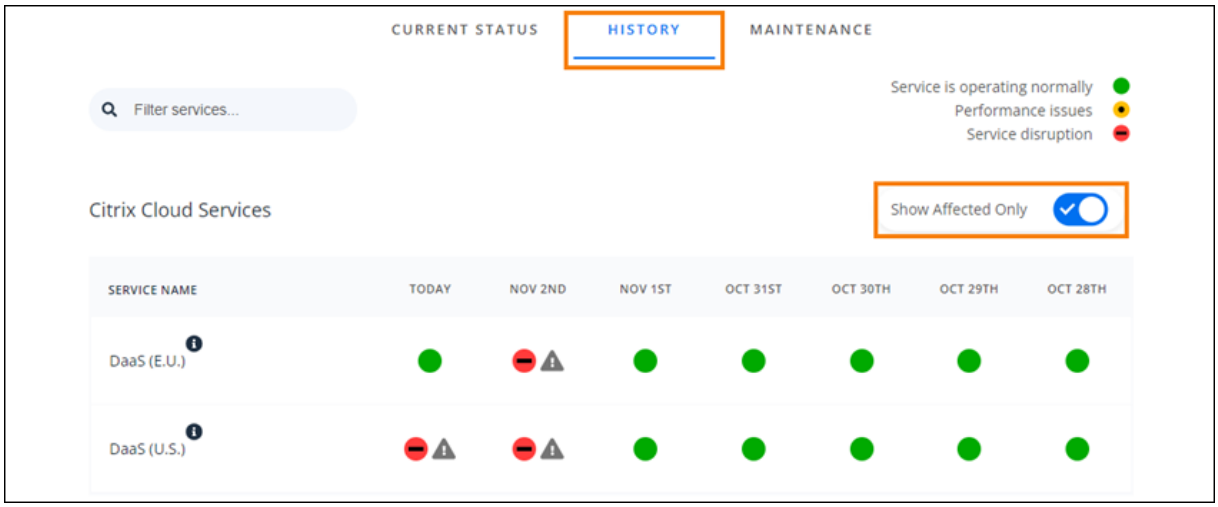
Vous pouvez également vous abonner à des notifications concernant des événements tels que les fenêtres de maintenance et les incidents de service.

Afficher l'état de santé et de maintenance

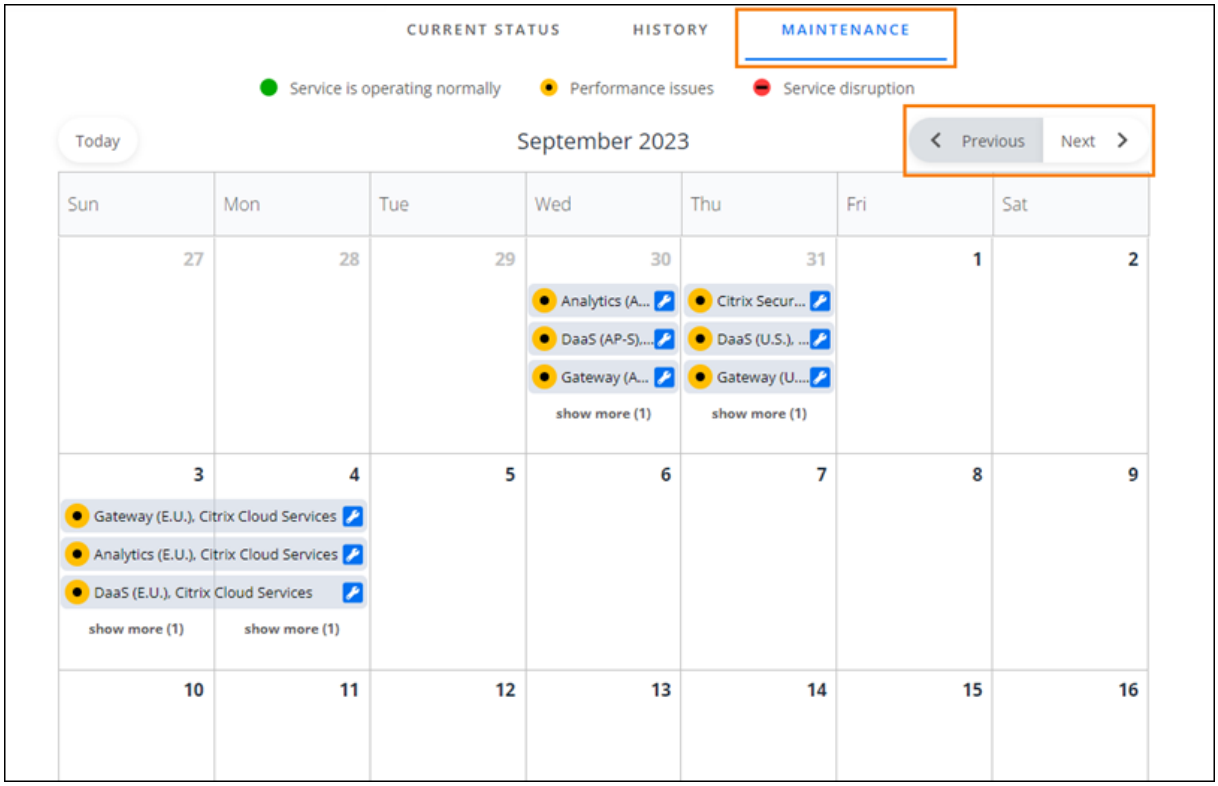
Sélectionnez **Current Status** pour afficher l'état de santé actuel de tous les services et composants de plate-forme Citrix Cloud dans chaque région géographique.



Sélectionnez **History** 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.



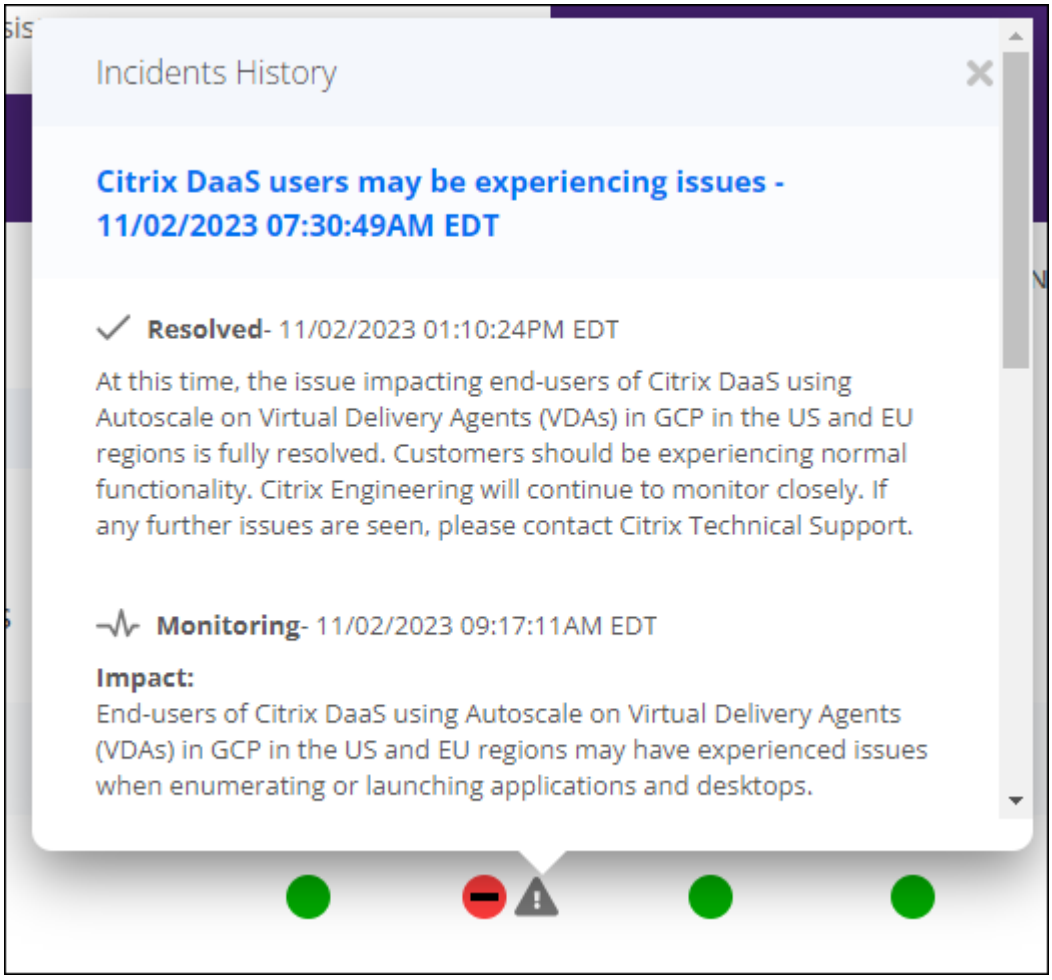
Sélectionnez **Maintenance** pour afficher une vue du calendrier des fenêtres de maintenance du service. Sélectionnez **Next** pour afficher les événements de maintenance prévus pour les mois à venir. Sélectionnez **Previous** pour revenir aux événements du mois en cours.



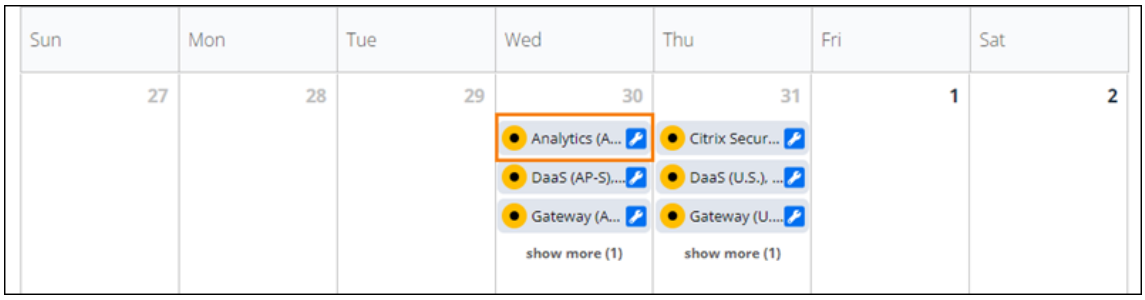
Afficher les détails des incidents d'un service

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

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



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



Fréquence des notifications d'incidents

En cas d'incident lié à l'état du service, Citrix prend en compte les caractéristiques suivantes lors de la publication sur status.cloud.com :

- Durée de l'impact
- Fréquence de l'impact

Au fur et à mesure de la résolution de l'incident, Citrix publie les types de notifications suivants sur le Tableau de bord Cloud Health Dashboard :

- **Investigating :** cette notification indique que Citrix a identifié le problème comme urgent et que ce dernier fait l'objet d'une enquête.
- **Monitoring :** cette notification indique que Citrix a identifié la cause du problème et que ce dernier est en train d'être résolu.
- **Resolved :** cette notification indique que Citrix a résolu le problème et que le service a été restauré à un état normal.

Lors de l'enquête et de la surveillance d'un incident, Citrix publie des mises à jour toutes les 60 à 120 minutes. Ces mises à jour peuvent inclure des informations telles que :

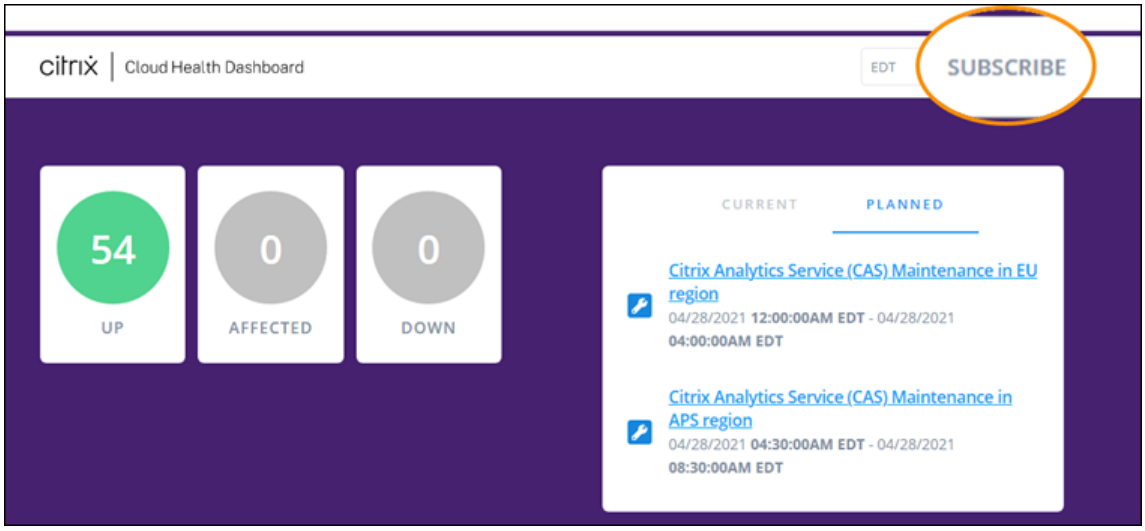
- Détails supplémentaires sur l'incident
- Description des mesures prises par Citrix pour résoudre l'incident
- Indication qu'aucune nouvelle modification n'a été apportée depuis la dernière mise à jour

Lorsqu'un incident est résolu, Citrix publie une dernière mise à jour. Cette mise à jour peut indiquer que l'incident a été résolu et que le service a été restauré à un état normal.

S'abonner aux notifications

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

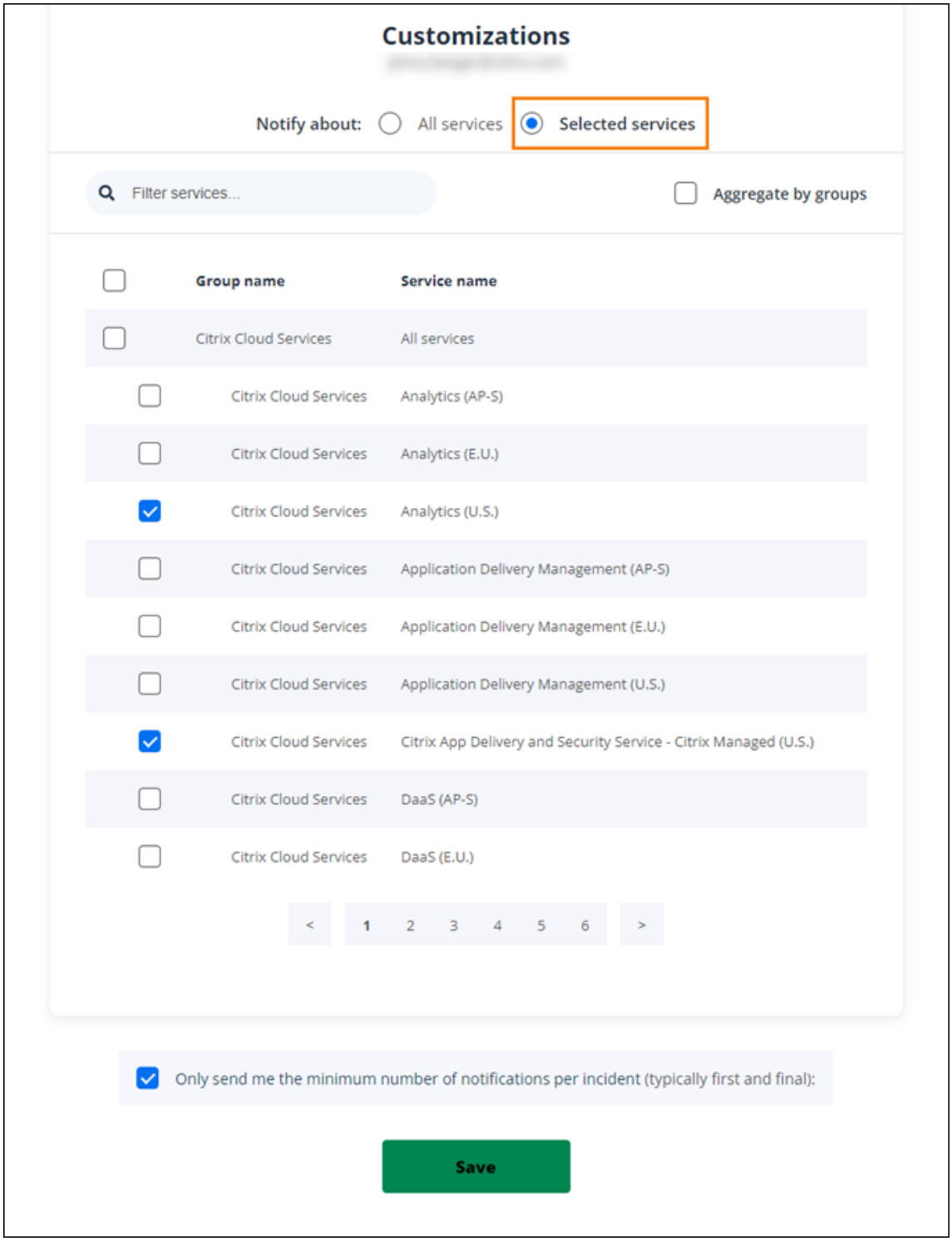
- Sélectionnez **Subscribe** en haut à droite du tableau de bord et sélectionnez la méthode de notification que vous souhaitez utiliser. Vous pouvez choisir parmi plusieurs méthodes, y compris l'e-mail et le téléphone (via SMS).



- 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`.

S'abonner à des services spécifiques dans une région

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 et sélectionnez **I accept terms & services**. Sélectionnez **Next**. La page **Customizations** s'affiche avec la section sélectionnée par défaut **Selected services**.
3. Sur la page **Customizations**, sélectionnez les services dans les régions que vous souhaitez dans la liste de plusieurs pages.

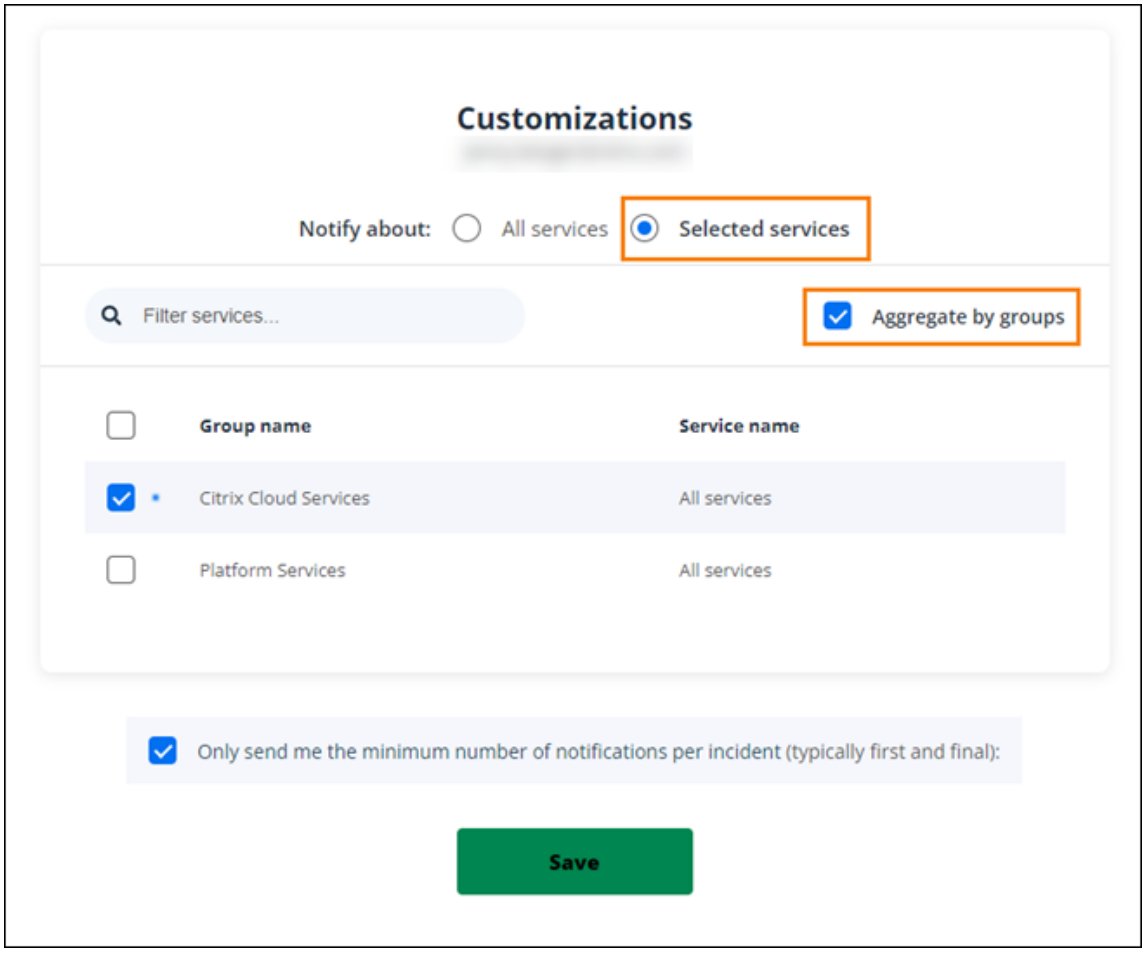


4. Pour ne recevoir que les première et dernière notifications pour chaque incident, sélectionnez **Only send me the minimum number of notifications per incident**.
5. Cliquez sur **Save**.

S'abonner à des groupes de services spécifiques

Vous pouvez vous abonner aux notifications pour tous les services cloud (par exemple, Analytics et DAaS) ou pour tous les services de plate-forme (par exemple, plan de contrôle et API cloud) dans toutes les régions.

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 et sélectionnez **I accept terms & services**. Sélectionnez **Next**. La page **Customizations** s'affiche avec la section sélectionnée par défaut **Selected services**.
3. Sur la page **Customizations**, sélectionnez **Aggregate by groups**.
4. Sélectionnez **Citrix Cloud Services** ou **Platform Services**.

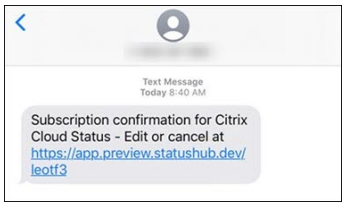


5. Pour ne recevoir que les première et dernière notifications pour chaque incident, sélectionnez **Only send me the minimum number of notifications per incident**.
6. Cliquez sur **Save**.

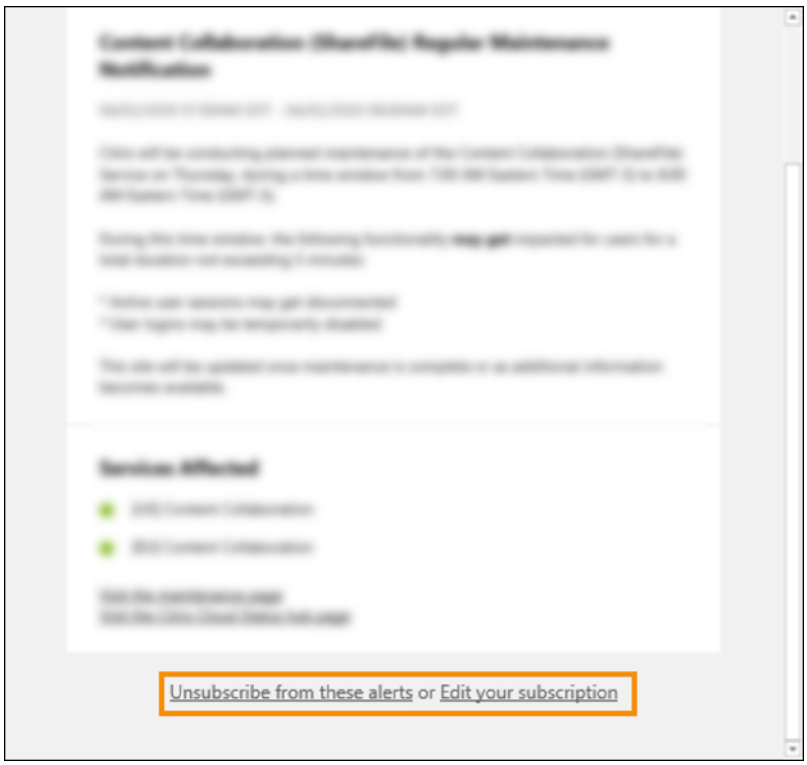
Se désabonner des notifications

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 **Save**.

Configuration requise pour le système et la connectivité

July 2, 2024

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 plus d'informations, consultez la section Détails techniques de Citrix Cloud Connector.
- Des machines physiques ou virtuelles, appartenant à votre domaine, pour l'hébergement des charges de travail et d'autres composants tels que StoreFront. Pour plus d'informations 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
- Dernière version de Apple Safari

Exigences Transport Layer Security

Citrix Cloud prend en charge Transport Layer Security (TLS) 1.2 pour les connexions TCP entre les composants. Citrix Cloud n'autorise pas les communications via TLS 1.0 ou TLS 1.1.

Pour accéder à Citrix Cloud, vous devez utiliser un navigateur compatible TLS 1.2 et avoir configuré des suites de chiffrement acceptées. Pour plus d'informations, consultez Cryptage et gestion des clés.

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. Pour plus d'informations sur les ports requis, consultez la section Configuration des ports entrants et sortants.

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 :

- Citrix Analytics
- Citrix DaaS
- Citrix Workspace

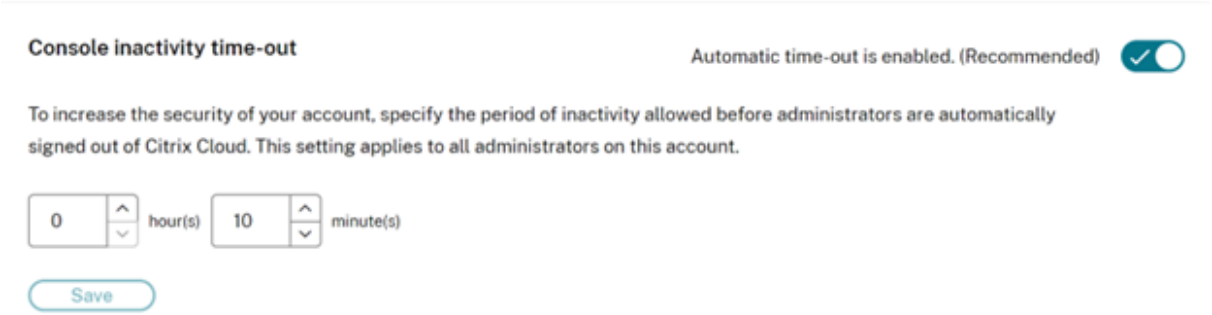
Pendo est un sous-traitant tiers utilisé par Citrix pour fournir des services de cloud et de support aux clients Citrix. Pour obtenir la liste complète de ces sous-traitants, accédez à la page Sub-Processors for Citrix Cloud & Support Services and Citrix Affiliates.

Délais d'expiration de la session

Une fois qu'un administrateur se connecte à Citrix Cloud, la session de la console de gestion expire après 72 heures. Ce délai d'expiration se produit indépendamment de l'activité de la console.

Délai d'inactivité configurable pour la console

En tant qu'administrateur à accès complet, vous pouvez configurer la durée d'inactivité sur la console Citrix Cloud avant que les administrateurs ne soient automatiquement déconnectés. Une fois configuré, le délai d'expiration spécifié sera appliqué à tous les administrateurs du compte Citrix Cloud.



Lorsque la fonctionnalité est activée, les administrateurs sont déconnectés après la période d'inactivité configurée et le délai d'expiration de la session est réinitialisé à chaque nouvelle connexion.

Lorsque la fonctionnalité est désactivée, il n'y a pas d'horloge d'inactivité et les administrateurs ne seront déconnectés que lorsque la limite de session de 72 heures sera atteinte.

> **Remarque :**
>
> - Cette fonctionnalité est désactivée par défaut.
> - Le délai d'inactivité configurable est compris entre 10 minutes et 12 heures.
> - Par défaut, la valeur du délai d'inactivité est de 60 minutes.

Enregistrement du serveur de licences auprès de Citrix Cloud

Si vous enregistrez votre serveur de licences Citrix local auprès de Citrix Cloud pour surveiller l'utilisation des déploiements locaux, assurez-vous que les adresses suivantes sont joignables :

- `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.

La machine hébergeant le Cloud Connector doit disposer d'une connectivité réseau stable avec Citrix Cloud. Les composants réseau doivent prendre en charge HTTPS et les sockets Web sécurisés de longue durée. Si un délai d'expiration est configuré dans les composants réseau, il doit être supérieur à 2 minutes.

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. 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 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 la section 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 :

- `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)
- `https://*.servicebus.windows.net` (fournit un accès à Azure Service Bus, qui est utilisé pour la journalisation et l'agent Active Directory)

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.

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, consultez Enregistrement du serveur de licences auprès de Citrix Cloud dans cet article pour obtenir les adresses contactables requises supplémentaires.

Noms de domaine complets (FQDN) autorisés pour Cloud Connector

Pour vous aider à garantir que tous les noms de domaine complets (FQDN) requis sont autorisés à passer par votre pare-feu, Citrix fournit les ressources suivantes :

- allowlist.json
- CTX270584: Citrix Gateway Service –Points of Presence (PoPs)

Lorsque vous configurez votre pare-feu, consultez ces deux ressources pour vérifier que les noms de domaine complets requis par le déploiement de votre service sont autorisés.

Cache d'hôte local (service de haute disponibilité) Lorsque vous utilisez le cache d'hôte local (LHC, Local Host Cache) dans les connecteurs, assurez-vous que les connecteurs peuvent atteindre le point de terminaison de sélection de tous les autres connecteurs de l'emplacement des ressources. Le point de terminaison de sélection se trouve sur le port 80 et est accessible via l'URL suivante : `http://<FQDN_OR_IP_OF_PEER_CONNECTOR>/Citrix/CdsController/ISecondaryBrokerElection`.

Si les connecteurs ne peuvent pas communiquer à cette adresse, plusieurs brokers sont sélectionnés lors d'un événement LHC, ce qui peut entraîner des échecs intermittents lors du lancement des applications et des bureaux virtuels. Pour plus d'informations, consultez la section Emplacements de ressources avec plusieurs Cloud Connector.

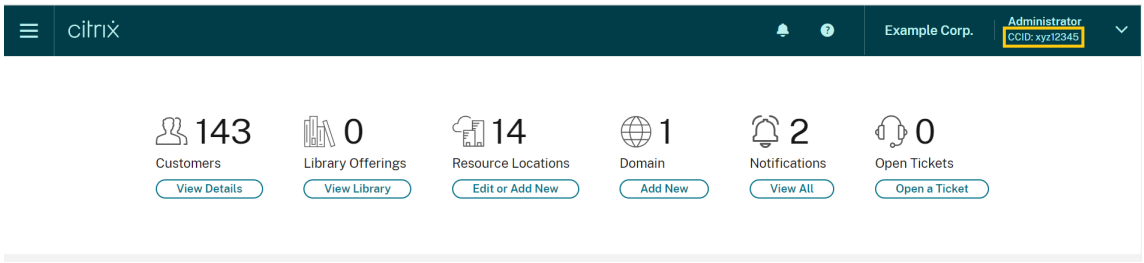
Authentification adaptative Lorsque vous utilisez le Cloud Connector pour vous connecter à un service d'authentification adaptative, vous devez autoriser votre entité Citrix Cloud Connector à accéder au domaine ou à l'URL que vous avez réservé à l'instance d'authentification adaptative. Par exemple, autorisez `https://aauth.xyz.com`. Pour plus d'informations, consultez Authentification adaptative.

Allowlist.json Le fichier allowlist.json se trouve sur https://fqdnallowlistsa.blob.core.windows.net/fqdnallowlist-commercial/allowlist.json et répertorie les noms de domaine complets auxquels le

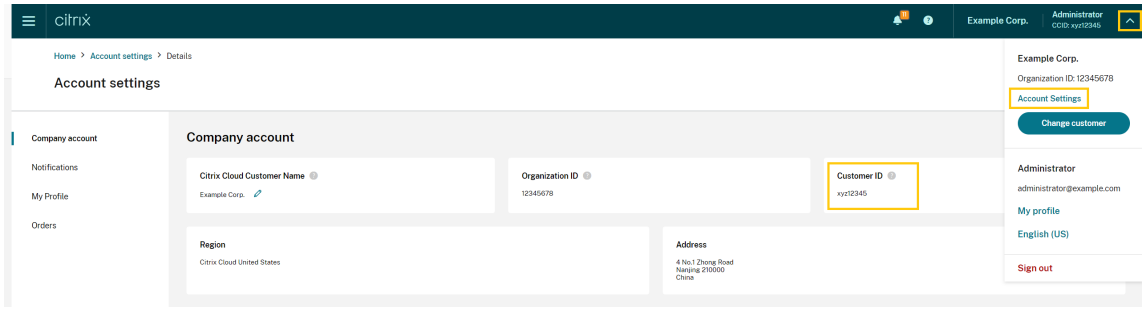
Cloud Connector accède. Cette liste est regroupée par produit et inclut un journal des modifications pour chaque groupe de noms de domaine complets.

Certains de ces noms de domaine complets sont spécifiques à un client et incluent des sections basées sur un modèle entre crochets. Ces sections basées sur un modèle doivent être remplacées par les valeurs réelles avant utilisation. Par exemple, pour <CUSTOMER_ID>.xendesktop.net, vous remplacez <CUSTOMER_ID> par l'ID client réel de votre compte Citrix Cloud. Vous pouvez trouver l'ID client dans les emplacements de console suivants :

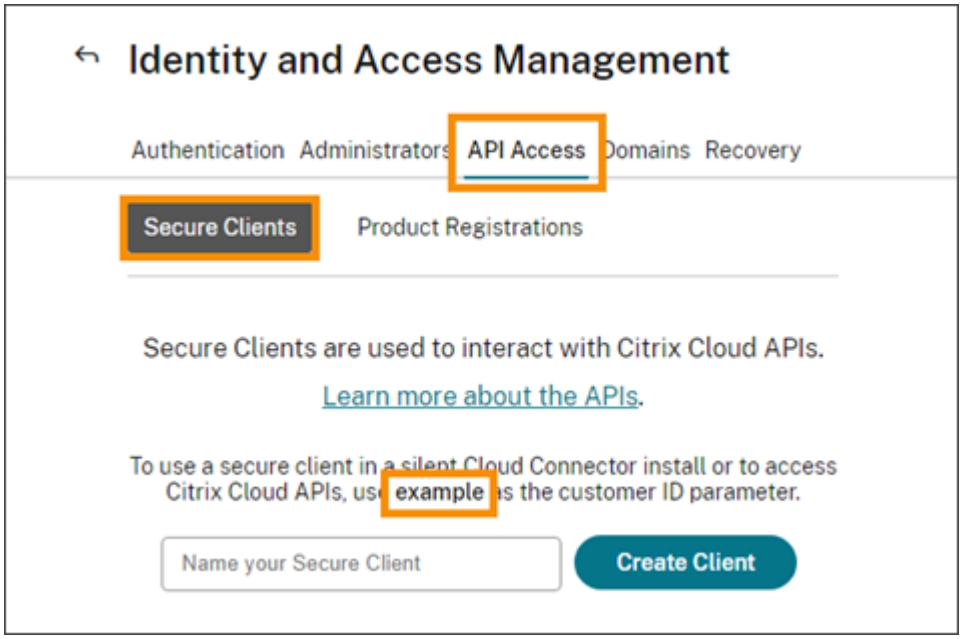
- Dans le coin supérieur droit de l'écran, sous le nom du client associé à votre compte Citrix Cloud



- Sur la page Paramètres du compte, sous **ID client de Citrix Cloud (CCID)**



- Dans l'onglet **Clients sécurisés** (**Gestion des identités et des accès > Accès aux API > Clients sécurisés**).



Points de présence Gateway Service Certains des noms de domaine complets inclus dans le fichier allowlist.json sont également inclus dans CTX270584 : Citrix Gateway Service –Points of Presence (PoPs). Toutefois, l'article CTX270584 inclut également des noms de domaine complets auxquels les clients accèdent, tels que :

- global-s.g.nssvc.net
- azure-s.g.nssvc.net

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 certaines exigences : Pour obtenir la liste complète de ces exigences, consultez Exigences relatives à la validation des certificats.

Décryptage SSL

L'activation du décryptage SSL sur certains proxys 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.

Citrix Connector Appliance pour les services cloud

Connector Appliance est une appliance que vous pouvez déployer dans votre hyperviseur. L'hyperviseur hébergeant Connector Appliance se trouve dans le réseau sur lequel résident les ressources que vous utilisez avec Citrix Cloud. Connector Appliance 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 Connector Appliance, consultez la section Configuration système requise.

Connector Appliance 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`

Configuration réseau requise

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

- Le réseau peut autoriser Connector Appliance à utiliser DHCP pour obtenir des serveurs DNS et NTP, une adresse IP, un nom d'hôte et un nom de domaine, ou vous pouvez définir manuellement les paramètres réseau dans la console de Connector Appliance.
- 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 Connector Appliance.

- Soit l'horloge de l'hyperviseur est réglée sur le temps universel coordonné (UTC) et synchronisée avec un serveur de temps, soit DHCP fournit des informations de serveur NTP à Connector Appliance.
- Si vous utilisez un proxy avec Connector Appliance, le proxy doit être non authentifié ou utiliser une authentification de base.

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 Sources de données prises en charge.

Connectivité du service de console

Pour connaître les exigences complètes en matière de connectivité Internet, consultez la section Ports pris en charge dans la documentation du produit NetScaler.

Connectivité du service Citrix DaaS

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.
- Les clients qui utilisent Déploiement rapide pour installer Citrix DaaS doivent rendre ces adresses supplémentaires joignables :
  - `https://*.apps.cloud.com`
  - Le `AzureCloud` numéro du service
- `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 Citrix DaaS sur le site Web Citrix Tech Zone.

Console d'administration :

- https://*.citrixworkspacesapi.net (Non requis pour le protocole Rendezvous)
- https://*.citrixnetworkapi.net (Non requis pour le protocole Rendezvous)
- https://*.cloud.com (Non requis pour le protocole Rendezvous)
- 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 Citrix DaaS 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/

Protocole Rendezvous

Lors de l'utilisation du service Citrix Gateway, le protocole Rendezvous permet de contourner les Citrix Cloud Connector pour se connecter directement et en toute sécurité au plan de contrôle Citrix Cloud.

Quelle que soit la version du protocole que vous utilisez, les VDA doivent être en mesure de contacter les adresses de la console d'administration répertoriées ci-dessus, sauf indication contraire. Pour obtenir la liste complète des exigences relatives au protocole Rendezvous, consultez les sections suivantes de la documentation du produit Citrix DaaS :

- Rendezvous V1
- Rendezvous V2

Exigences relatives au cache d'hôte local

Si votre pare-feu effectue une inspection des paquets et que vous souhaitez utiliser la fonctionnalité de cache d'hôte local, assurez-vous que votre pare-feu accepte le trafic XML et SOAP. Cette fonctionnalité nécessite la possibilité de télécharger des fichiers MDF, ce qui se produit lorsque Cloud Connector synchronise les données de configuration avec Citrix Cloud. Ces fichiers sont transmis au Cloud Connector via le trafic XML et SOAP. Si le pare-feu bloque ce trafic, la synchronisation entre Cloud Connector et Citrix Cloud échoue. En cas de panne, les utilisateurs ne peuvent pas continuer à travailler car les données de configuration résidant sur le Cloud Connector sont obsolètes.

Pour plus d'informations sur cette fonctionnalité, consultez la section Cache d'hôte local dans la documentation du produit Citrix DaaS.

Exigence de mise à niveau du VDA

À l'aide de l'interface Configuration complète de Citrix DaaS, vous pouvez mettre à niveau les VDA par catalogue ou par machine. Vous pouvez les mettre à niveau immédiatement ou à une heure planifiée. Pour plus d'informations sur la fonctionnalité de mise à niveau des VDA, consultez la section Mettre à niveau les VDA à l'aide de l'interface Configuration complète.

Lorsque vous utilisez cette fonctionnalité, assurez-vous de répondre aux exigences de connectivité suivantes :

- Les URL de Azure CDN suivantes ont été ajoutées à la liste d'autorisation. La fonctionnalité télécharge les programmes d'installation de VDA à partir des points de terminaison Azure CDN.
  - Production - États-Unis (US) : `https://prod-us-vus-storage-endpoint.azureedge.net/*`
  - Production - Union européenne (UE) : `https://prod-eu-vus-storage-endpoint.azureedge.net/*`
  - Production - Asie-Pacifique Sud (APS) : `https://prod-aps-vus-storage-endpoint.azureedge.net/*`
  - Production - Japon (JP) : `https://prod-jp-vus-storage-endpoint.azureedge.net/*`
- La fonctionnalité vérifie que le programme d'installation du VDA est signé par un certificat valide. Assurez-vous que les URL suivantes ont été ajoutées à la liste d'autorisation pour la vérification de la validité et de la révocation des certificats :
  - `http://crl3.digicert.com/*`
  - `http://crl4.digicert.com/*`
  - `http://ocsp.digicert.com/*`
  - `http://cacerts.digicert.com/*`

- La fonctionnalité nécessite VDA Upgrade Agent pour fonctionner. Le VDA Upgrade Agent qui s'exécute sur le VDA communique avec Citrix DaaS. Assurez-vous que les URL suivantes ont été ajoutées à la liste d'autorisation :
  - `https://[customerId].xendesktop.net/citrix/VdaUpdateService/*`, 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.
  - `http://xendesktop.net/citrix/VdaUpdateService/*`

Connectivité du service Endpoint Management

Emplacements des ressources/Cloud Connector Citrix :

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

Console d'administration :

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

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`

> **Important :**
>
> L'interception SSL ne peut pas être effectuée sur des adresses Citrix Gateway. L'activation de l'interception SSL sur certains proxys peut empêcher le Cloud Connector de se connecter à Citrix Cloud.

Connectivité de NetScaler Intelligent Traffic Management Service

- https://*.cedexis-test.com
- https://*.citm-test.com
- https://cedexis.com
- https://cedexis-radar.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 de Citrix SD-WAN Orchestrator.

Connectivité de Remote Browser Isolation Service (anciennement Secure Browser)

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 Private 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 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/

Connectivité à Global App Configuration Service

`https://discovery.cem.cloud.us`

Pour plus d'informations sur ce service, consultez les ressources suivantes :

- Personnaliser les paramètres de l'application Workspace - Documentation produit de Citrix Workspace
- Global App Configuration Service - Documentation Citrix Developer

Connectivité de l'application Citrix Workspace

Ajoutez les URL suivantes à votre liste d'autorisation :

- `https://*.cloud.com`
- Adresse du fournisseur d'identité. Reportez-vous aux instructions de la documentation du fournisseur d'identité correspondante.
- `https://*.wsp.cloud.com`

Pour des URL spécifiques, autorisez l'accès aux adresses suivantes :

- `<yourcustomer>.cloud.com`

Citrix Secure Private Access

- `ngspolicy.netscalergateway.net`
- `config.netscalergateway.net`
- `app.netscalergateway.net`
- `http://tunnel.netscalergateway.net/`

Global App Configuration Service

Reportez-vous à la section Connectivité à Global App Configuration Service dans cet article.

Authentification

- `accounts.cloud.com`
- `accounts-dsauthweb.cloud.com`

Assurez-vous que les URL de votre fournisseur d'identité sont également accessibles depuis les appareils de vos utilisateurs finaux.

Citrix Analytics Service

- locus.analytics.cloud.com

Activez l'accès à l'URL appropriée dans la liste suivante, en fonction de votre localisation :

- États-Unis : citrixanalyticseh.servicebus.windows.net
- Union Européenne : citrixanalyticseheu.servicebus.windows.net
- Asie-Pacifique Sud : citrixanalyticsehaps.servicebus.windows.net

Ressources de l'interface graphique de Workspace

- ctx-ws-assets.cloud.com

Personnalisation, notifications et déploiement de fonctionnalités

- customer-**interface**-personalization.us.wsp.cloud.com
- user-personalization.us.wsp.cloud.com
- admin-notification.us.wsp.cloud.com
- customer-**interface**-personalization.eu.wsp.cloud.com
- user-personalization.eu.wsp.cloud.com
- admin-notification.eu.wsp.cloud.com
- customer-**interface**-personalization.ap-s.wsp.cloud.com
- user-personalization.ap-s.wsp.cloud.com
- admin-notification.ap-s.wsp.cloud.com
- feature-rollout.us.wsp.cloud.com
- feature-rollout.eu.wsp.cloud.com
- feature-rollout.ap-s.wsp.cloud.com

Service d'enregistrement d'appareils

- device-registration.us.wsp.cloud.com
- device-registration.eu.wsp.cloud.com
- device-registration.ap-s.wsp.cloud.com

Service de notification push

- push-events-signalr.us.wsp.cloud.com
- push-events-signalr.eu.wsp.cloud.com
- push-events-signalr.ap-s.wsp.cloud.com

Citrix Gateway Service

- https://*.g.nssvc.net

Authentification unique pour Workspace avec le Service d'authentification fédérée (FAS) 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 :
  - https://*.cloud.com
  - https://*.citrixworkspacesapi.net
  - https://*.citrixnetworkapi.net/
  - Adresses requises par un fournisseur d'identité tiers, si elles sont utilisées dans votre environnement
- Service FAS, sous le compte de service réseau :
  - https://*.citrixworkspacesapi.net
  - https://*.citrixnetworkapi.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.

Si vous utilisez Active Directory ou Active Directory avec un mot de passe à usage unique (TOTP) comme fournisseur d'identité pour l'application Citrix Workspace, vous devez également ajouter login.cloud.com à la liste d'autorisation. Si vous utilisez d'autres fournisseurs d'identité, autorisez les URL des fournisseurs d'identité séparément.

Les URL du hub d'événements CAS sont également spécifiques à la zone géographique. citrixanalyticsehalias.servicebus.windows.net

Connectivité de Workspace Environment Management Service

Emplacements des ressources Citrix/Cloud Connector/Agent :

https://*.wem.cloud.com

Pour connaître les exigences complètes, reportez-vous à la section Exigences de connectivité dans la documentation de Workspace Environment Management Service.

Planifier votre déploiement

July 2, 2024

Pour un aperçu de l'expérience du client, accédez au Citrix Success Center. Le Success Center fournit des conseils sur les cinq étapes clés de votre expérience avec Citrix : planifier, créer, déployer, gérer et optimiser. Les articles et guides du Success Center complètent cette documentation et offrent une perspective globale basée sur les solutions.

Versions d'évaluation de service et abonnements

Citrix Cloud propose des versions d'évaluation pour la plupart des services cloud. Les versions d'évaluation présentent les mêmes caractéristiques et fonctions que les services payants. Elles peuvent donc être utilisées dans le cadre d'une preuve de concept ou d'un déploiement pilote. Pour de plus amples informations, consultez la section Évaluations de services Citrix Cloud.

En général, les droits d'accès aux services payants peuvent avoir une durée mensuelle, annuelle ou à durée déterminée. Lorsque l'autorisation touche à sa fin, Citrix Cloud envoie des rappels et fournit un délai de grâce afin que vous puissiez renouveler vos droits sans interruption de service excessive. Pour plus d'informations sur le renouvellement de vos droits, consultez la section Prolonger les abonnements aux services de Citrix Cloud.

Régions des services

Citrix Cloud fournit des services dans trois régions : États-Unis, Union européenne et Asie-Pacifique Sud. Lorsque vous vous inscrivez à Citrix Cloud, vous devez choisir la région qui correspond le mieux aux besoins de votre entreprise en terme de performance.

Pour en savoir plus sur la sélection d'une région et les services disponibles dans chaque région, consultez Considérations géographiques.

Ressources de déploiement

- Citrix Cloud Resiliency
- Guides de validation de concept de Tech Zone
- Architectures de référence de Tech Zone
- Considérations sur le dimensionnement et la scalabilité des Cloud Connector
- Considérations sur le dimensionnement et la scalabilité du cache d'hôte local
- Architectures de référence de l'authentification d'un magasin StoreFront local pour Citrix DaaS

Ressources de migration

- Preuve de concept : Outil de configuration automatisée
- Migration de Citrix Virtual Apps and Desktops sur site vers Citrix Cloud
- Migration de Citrix Virtual Apps and Desktops de VMware vSphere vers Citrix DaaS sur Microsoft Azure
- Migration from Android Device Administrator to Android Enterprise with Citrix Endpoint Management

Informations supplémentaires

- Citrix Discussions : Citrix Cloud : forums d'assistance communautaire pour Citrix Cloud et les services cloud Citrix
- Citrix Training :
  - Fundamentals of Citrix Cloud
  - Introduction to Citrix Identity and Authentication

Évaluations de services Citrix Cloud

July 2, 2024

Les évaluations de services Citrix Cloud individuels sont fournies via la console de gestion 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 ou un projet pilote de déploiement.

Lorsque vous êtes prêt à acheter les services Citrix Cloud, votre version d'évaluation est convertie en service de production. Il n'est pas nécessaire de reconfigurer quoi que ce soit ni de créer un compte de production distinct.

Présentation des évaluations de service

Les informations de cette section s'appliquent à la plupart des évaluations de service Citrix Cloud. Les services ayant des conditions d'évaluation différentes sont décrits dans des sections distinctes.

	Évaluation de Citrix Cloud
Nombre d'abonnés autorisés	25

		Évaluation de Citrix Cloud
	Durée maximale de l'évaluation	60 jours
	Période de grâce	14 jours après l'expiration de l'évaluation
	Période de rétention des données	90 jours après l'expiration de l'évaluation
	Disponibilité	Disponibilité restreinte
	Emplacement de ressources	Fourni et configuré par le client
	Durée des sessions utilisateur	Illimité
	Intégration locale à Microsoft Active Directory	Oui
	Choix d'emplacements des ressources	Oui
	Déploiement sur site	Oui
	Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service)	Ensemble complet de fonctionnalités
	Endpoint Management	Ensemble complet de fonctionnalités
	Personnalisable	Oui

Demander une version d'évaluation de service

L'accès à l'évaluation Citrix Cloud est géré par service. Pour certains services, vous pouvez demander une évaluation comme décrit dans la section Demander une version d'évaluation de service de cet article. Pour les autres services, vous devez demander une démonstration avant de bénéficier d'un accès à l'évaluation, comme décrit dans la section Demander une démo de service de cet article.

Période de l'évaluation du service

Pour la plupart des services, vous disposez de 60 jours pour essayer le service après l'approbation de votre demande d'évaluation. Vous ne pouvez demander une évaluation du service qu'une seule fois.

Acheter des abonnements à des services

Vous pouvez acheter un abonnement au service à tout moment pendant votre période d'évaluation ou pendant la période de rétention des données. Pour plus d'informations, consultez la section Acheter les services Citrix Cloud.

Une fois que vous avez acheté un abonnement, votre évaluation est convertie en service de production. Les administrateurs et les utilisateurs peuvent accéder au service et toutes les données que vous avez ajoutées pendant la période d'évaluation restent intactes.

Citrix DaaS Standard pour Azure

Cette section décrit les types d'évaluation suivants pour Citrix DaaS Standard pour Azure (anciennement Citrix Virtual Apps and Desktops Standard pour Azure) :

- **Évaluation auto-approuvée :** après avoir demandé la version d'évaluation via la console de gestion Citrix Cloud, l'évaluation est approuvée automatiquement et prête à être utilisée.
- **Évaluation approuvée par l'équipe de vente :** après avoir contacté un représentant commercial Citrix pour demander une version d'évaluation, le représentant commercial approuve l'évaluation. Une fois l'évaluation approuvée, elle est prête à être utilisée.

		Évaluation auto-approuvée	Évaluation approuvée par l'équipe de vente
	Durée maximale de l'évaluation	7 jours	14 jours
	Période de grâce	1 jour après l'expiration de l'évaluation	14 jours après l'expiration de l'évaluation
	Période de rétention des données	30 jours après l'expiration de l'évaluation	90 jours après l'expiration de l'évaluation

Selon le type d'évaluation, vous disposez de sept ou 14 jours pour utiliser le service. Vous ne pouvez demander une évaluation du service qu'une seule fois.

Les évaluations incluent un délai de grâce pour l'accès au service après l'expiration de la période d'évaluation. Ce délai de grâce vous permet d'acheter un abonnement au service ou de supprimer toutes les données que vous avez ajoutées. Après la fin de la période de grâce, Citrix bloque l'accès au service pour les administrateurs et les utilisateurs.

Selon le type d'évaluation, Citrix conserve toutes les données que vous ajoutez au service pendant 30 jours ou 90 jours après l'expiration de la période d'évaluation. Si vous achetez un abonnement au

service pendant cette période de rétention, les administrateurs et les utilisateurs peuvent accéder au service avec vos données intactes.

Vous pouvez acheter un abonnement au service via Azure Marketplace ou en contactant votre représentant commercial Citrix.

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. En outre, le représentant s'assure que vous disposez de toutes les informations nécessaires pour utiliser le service avec succès.

1. Connectez-vous à votre compte Citrix Cloud.
2. À partir de la console de gestion, sélectionnez **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

1. Connectez-vous à votre compte Citrix Cloud.
2. À partir de la console de gestion, sélectionnez **Demander version d'évaluation** pour le service que vous souhaitez tester.

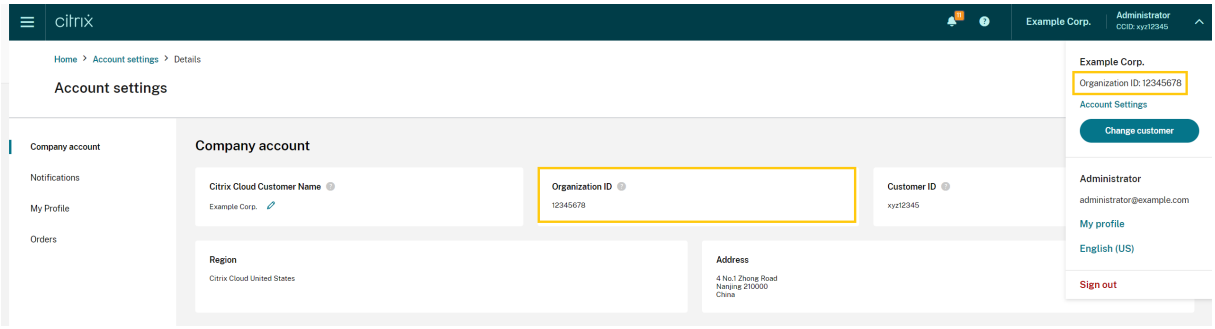
Lorsque votre version d'évaluation est approuvée et prête à être utilisée, Citrix vous envoie une notification par e-mail.

> **Remarque :**
>
> Pour offrir la meilleure expérience client possible, Citrix se réserve le droit d'approuver des évaluations pour un nombre limité de participants à tout moment.

Acheter les services Citrix Cloud

Lorsque vous êtes prêt à convertir votre version d'évaluation en service de production, visitez https://www.citrix.com/buy/ pour trouver un partenaire Citrix local.

Pour acheter le service, vous avez besoin de votre identifiant d'organisation (OrgID). Votre OrgID apparaît dans le menu client dans le coin supérieur droit de la console de gestion Citrix Cloud. Votre OrgID apparaît également sur la page **Paramètres du compte**.



Informations supplémentaires

- Conditions d'utilisation des services Citrix Cloud
- Le cours Fundamentals of Citrix Cloud fournit une courte vidéo qui vous guide tout au long de la demande d'évaluation. Le cours complet couvre également les composants de la plate-forme Citrix Cloud et de ses services.

Prolonger les abonnements aux services de Citrix Cloud

July 2, 2024

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

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 *abonnements pluriannuels* font référence aux services achetés sur une base pluriannuelle.

> **Remarque :**
>
> Les Citrix Service Provider (CSP) peuvent prolonger leurs abonnements en soumettant un bon de commande d'une valeur nulle à leur distributeur CSP. Pour plus d'informations sur les renouvellements et les licences des produits CSP, consultez *Citrix Service Provider Licensing Guide for Citrix Cloud*, disponible sur le site Web de Citrix Partner Central.

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 : 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 90 jours après la date d'expiration du service. Si vous prolongez votre abonnement avant la fin de la période de rétention de 90 jours, vos administrateurs et vos utilisateurs peuvent accéder au service et les données sont préservées. 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 jour de chaque mois.
- Pour les abonnements annuels et pluriannuels, la date de début de votre abonnement prolongé est le jour qui suit immédiatement la date d'expiration. Par exemple, si votre abonnement ex-

pire le 30 septembre et que vous le prolongez le 23 octobre, la date de début de l'abonnement prolongé est le 1er octobre.

Si vous ne prolongez pas votre abonnement avant la fin de la période de rétention de 90 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 Citrix DaaS), Citrix effectue les actions suivantes après la fin de la période de rétention de 90 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 90 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

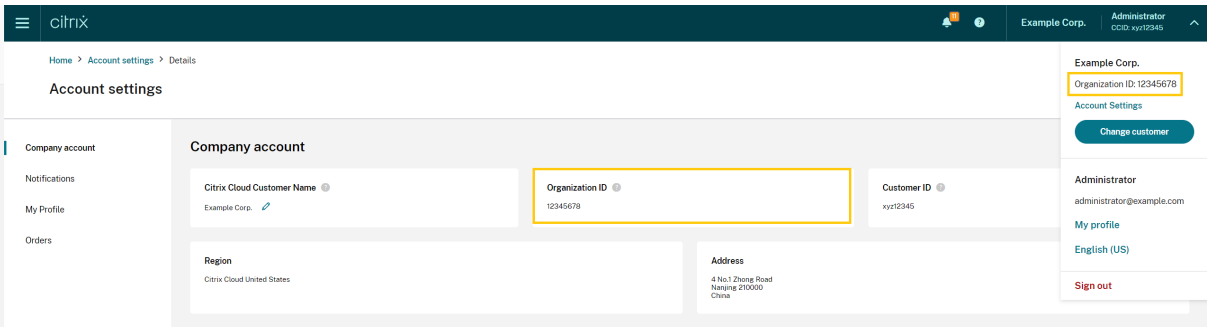
Pour prolonger votre abonnement aux services Citrix Cloud, contactez votre représentant commercial Citrix. Pour trouver votre représentant commercial, procédez comme suit :

1. Connectez-vous à votre compte Citrix.
2. Sélectionnez **Quoting (DOTI)**, puis **Transactions**. Votre représentant commercial et son adresse e-mail sont affichés en haut de cette vue.

Vous pouvez également consulter la page Citrix Customer Service pour obtenir les informations de contact dans votre région géographique.

Pour finaliser l'achat, votre représentant commercial a besoin de l'identifiant d'organisation de votre compte Citrix Cloud. Pour trouver votre identifiant d'organisation, connectez-vous à votre compte Citrix Cloud. L'identifiant de votre organisation est affiché aux endroits suivants :

- Dans le menu client, dans le coin supérieur droit de la console Citrix Cloud.
- Sur la page **Paramètres de compte**.



Considérations géographiques

July 2, 2024

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

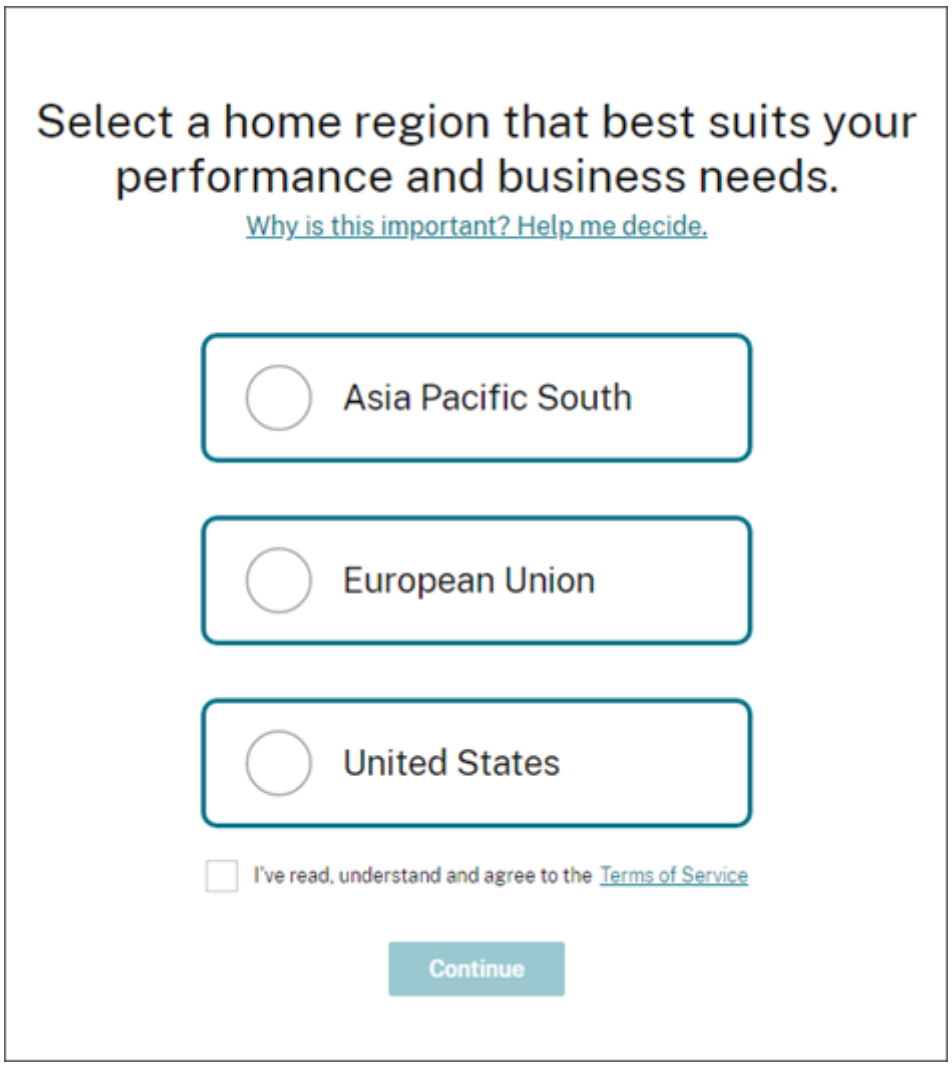
Pour plus d'informations sur les régions géographiques et la présence de services pour les plates-formes cloud du secteur public et dédiées de Citrix, consultez Autres plates-formes cloud de Citrix.

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

Lorsque vous sélectionnez une région, les services hébergés dans cette région géographique sont utilisés pour les actions associées à l'organisation dans la mesure du possible. 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 Citrix Cloud n'est pas pris en charge dans votre région, choisissez la région la plus proche de celle où se trouvent la plupart de vos utilisateurs et ressources.

Disponibilité du service dans chaque région

La plupart des services Citrix Cloud sont répliqués dans le monde entier. La région que vous sélectionnez indique une préférence quant à l'endroit où les connexions doivent être établies. Cependant, des

connexions peuvent toujours être établies avec d'autres régions géographiques. Lorsqu'un service est répliqué globalement, toutes les données de ce service sont stockées dans toutes les régions.

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

Certains services disposent d'instances régionales dédiées. Certains services disposent uniquement d'instances basées aux États-Unis. Dans ces cas, les connexions et les données sont contenues dans la région géographique.

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.

Service	États-Unis	UE	Asie Pacifique Sud	Remarques
Plan de contrôle Citrix Cloud	Oui	Oui	Oui	
Citrix Analytics for Security	Oui	Oui	Oui	
Citrix Analytics for Performance	Oui	Oui	Oui	
NetScaler Console (anciennement Application Delivery Management)	Oui	Oui	Oui	Consultez la section Intégration simplifiée des instances NetScaler à l'aide de Console Advisory Connect dans cet article. Pour le programme de télémétrie sur site de la console, cliquez ici.
Citrix DaaS (anciennement Virtual Apps and Desktops Service)	Oui	Oui	Oui	Le service utilise la région Citrix Cloud.

Service	États-Unis	UE	Asie Pacifique Sud	Remarques
Citrix DaaS Standard pour Azure (anciennement Virtual Apps and Desktops Standard pour Azure)	Oui	Oui	Oui	Le service utilise la région Citrix Cloud.
Citrix DaaS Standard pour Google Cloud (anciennement Virtual Apps and Desktops Standard pour Google Cloud)	Oui	Non (Utilise la région États-Unis)	Non (Utilise la région États-Unis)	
Citrix DaaS Premium pour Google Cloud (anciennement Virtual Apps and Desktops Premium pour Google Cloud)	Oui	Non (Utilise la région États-Unis)	Non (Utilise la région États-Unis)	
Citrix Endpoint Management	Oui	Oui	Oui	Sélectionnez parmi plusieurs emplacements dans plusieurs régions. Consultez la section Emplacements de Endpoint Management Service dans cet article.

Service	États-Unis	UE	Asie Pacifique Sud	Remarques
Remote Browser Isolation Service	Oui	Oui	Oui	Le service utilise la région Citrix Cloud.
SD-WAN Orchestrator	Oui	Oui	Oui	
Nœuds/POP pour Citrix Secure Internet Access	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	Consultez la section Emplacements pour Secure Internet Access Service dans cet article.
Citrix Secure Private Access	Réplication globale	Réplication globale	Réplication globale	Consultez la section Points de présence (PoP) de Secure Private Access dans cet article.
Service d' enregistrement de session	Oui	Oui	Oui	
Citrix Virtual Apps Essentials	Oui	Oui	Oui	Le service utilise la région Citrix Cloud.
Citrix Virtual Desktops Essentials	Oui	Oui	Oui	Le service utilise la région Citrix Cloud.
Web App Firewall	Oui	Oui	Non (Utilise la région États-Unis)	
Workspace Environment Management ; Citrix Optimization Pack	Oui	Oui	Oui	
Services de réseau	Oui	Non (Utilise la région États-Unis)	Non (Utilise la région États-Unis)	

Service	États-Unis	UE	Asie Pacifique Sud	Remarques
License Usage Insights (CSP uniquement)	Réplication globale	Réplication globale	Réplication globale	
Nœuds d'accès Citrix Gateway Service/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	Vous pouvez configurer les emplacements de ressources de façon à autoriser le routage du trafic utilisateur vers des régions spécifiques. Pour plus d'informations, consultez Routage par géolocalisation - Technical Preview

> **Remarque :**
>
> Certains services régionaux peuvent inclure des droits à des services de composants non régionaux, tels que définis ailleurs dans le tableau ci-dessus, et peuvent être utilisés au choix du client.
>
> Les services Citrix Cloud utilisent la région désignée par le client pour stocker le contenu et les journaux du client, à l'exception de certains journaux collectés par les sous-processeurs Citrix ou pour lesquels un stockage non régional est nécessaire aux performances du service, notamment pour le support ou le dépannage, la surveillance des performances, la sécurité, l'audit et pour permettre l'authentification entre régions (par exemple lorsqu'un ingénieur de support basé dans l'UE doit accéder à un environnement basé aux États-Unis). Le contenu et les journaux des clients peuvent être consultés à l'échelle mondiale si cela est nécessaire pour fournir les services.

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.

Intégration simplifiée des instances NetScaler Console à l'aide de Console Advisory Connect

Lors de l'intégration simplifiée des instances Console basée sur Console Advisory Connect:

- Si vous êtes déjà client Citrix Cloud, le locataire du service Console est créé dans la même région géographique que celle que vous avez sélectionnée lors de la création de votre compte Citrix Cloud.
- Si vous n'êtes pas déjà client Citrix Cloud, l'adresse mentionnée pour le client sur le portail Citrix.com est référencée. Un espace réservé de locataire de service Console est créé dans la région géographique qui correspond à la région de l'adresse référencée. Si vous choisissez d'intégrer Citrix Cloud à l'avenir, un nouveau locataire de service Console est créé dans la même région que celle que vous avez sélectionnée lorsque vous avez créé votre compte Citrix Cloud. En outre, les données sont migrées de l'espace réservé du locataire de service Console vers le nouveau locataire de service Console.

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 Ouest
- Asie du Sud-Est
- Sydney

Emplacements pour Secure Internet Access Service

Le trafic est acheminé vers les emplacements de Secure Internet Access Service 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

Points de présence (PoP) de Secure Private Access

Pour obtenir la liste des points de présence (POP) utilisés par Secure Private Access pour garantir la continuité et la qualité de service aux clients, consultez Quels sont les emplacements PoP de Secure Private Access ? dans la documentation de Secure Private Access Service.

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 certains services Citrix Cloud dans un environnement dédié géré par Citrix. Citrix Cloud Japan et les services proposés ne sont disponibles qu'au Japon.

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

Guide de déploiement sécurisé pour la plate-forme Citrix Cloud

July 2, 2024

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.

Vues d'ensemble de la sécurité technique pour les différents services

Consultez les articles suivants pour plus d'informations sur la sécurité des données au sein des services 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 Remote Browser Isolation
- Vue d'ensemble de la sécurité technique Citrix DaaS
- Vue d'ensemble de la sécurité technique de Citrix DaaS Standard pour Azure

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 de Citrix Cloud est réalisée à l'aide du fournisseur d'identité Citrix par défaut. Lorsque les administrateurs s'inscrivent à Citrix

Cloud ou sont invités à accéder à un compte Citrix Cloud, ils doivent s'inscrire à l'authentification multifacteur (MFA). Si un client utilise Microsoft Azure pour authentifier les administrateurs de Citrix Cloud, l'authentification multifacteur peut être configurée comme décrit dans la section Configurer les paramètres d'authentification multifacteur Azure AD sur le site Web de Microsoft.

- Par défaut, Citrix Cloud met automatiquement fin aux sessions d'administrateur après 24 minutes, quelle que soit l'activité de la console. Ce délai d'expiration ne peut pas être modifié.
- Les comptes d'administrateur peuvent être associés à un maximum de 100 comptes clients. Si un administrateur doit gérer plus de 100 comptes clients, il doit créer un compte administrateur distinct avec une adresse e-mail différente pour gérer les comptes clients supplémentaires. Vous pouvez également supprimer un administrateur des comptes clients qu'il n'a plus besoin de gérer.

Conformité des mots de passe

Citrix Cloud invite les administrateurs à modifier leurs mots de passe si l'une des conditions suivantes existe :

- Le mot de passe actuel n'a pas été utilisé pour se connecter depuis plus de 60 jours.
- Le mot de passe actuel a été répertorié dans une base de données connue de mots de passe compromis.

Les nouveaux mots de passe doivent répondre à tous les critères suivants :

- Au moins 8 caractères (128 caractères maximum)
- 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 :

- Le mot de passe actuel ne peut pas être utilisé comme nouveau mot de passe.
- Les 5 mots de passe précédents ne peuvent pas être réutilisés.
- Le nouveau mot de passe ne peut pas être similaire au nom d'utilisateur du compte.
- Le nouveau mot de passe ne doit pas figurer dans une base de données connue de mots de passe compromis. Citrix Cloud utilise une liste fournie par https://haveibeenpwned.com/ pour déterminer si les nouveaux mots de passe ne respectent pas cette condition.

Cryptage et gestion des clés

Le plan de contrôle Citrix Cloud 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).

Pour les données au repos, le stockage Citrix Cloud est crypté à l'aide de clés AES-256 bits ou supérieures. Ces clés sont gérées par Citrix.

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 vous accédez au plan de contrôle Citrix Cloud à partir de Windows Server 2016, Windows Server 2019 ou Windows Server 2022, les chiffrements forts suivants sont recommandés : TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- Si vous accédez au plan de contrôle Citrix Cloud à partir de Windows Server 2012 R2, les chiffrements forts ne sont pas disponibles ; les chiffrements suivants doivent donc être utilisés : TLS_DHE_RSA_WITH_AES_256_GCM_SHA384, TLS_DHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

Pour savoir comment les données des services Citrix Cloud sont protégées, consultez Citrix Cloud Services Data Protection Overview sur le site Web de Citrix.

Pour plus d'informations sur le chiffrement et la gestion des clés au sein de chaque service cloud, consultez la documentation du service.

Pour plus d'informations sur la configuration de TLS 1.2, consultez les articles suivants :

- Appliquer l'utilisation de TLS 1.2 sur les ordinateurs clients : CTX245765, Erreur : « La connexion sous-jacente a été fermée : une erreur inattendue s'est produite lors d'un envoi. » lors de l'interrogation du point de terminaison OData de Monitoring Service
- Mettre à jour et configurer le .NET Framework pour prendre en charge TLS 1.2 sur le site Web Microsoft Docs.

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.

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 plate-forme 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 DaaS (anciennement Citrix Virtual Apps and Desktops Service)

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

Port client	Port du serveur	Service
49152 -65535/TCP	464/TCP/UDP	Changement de mot de passe Kerberos
49152 -65535/TCP	49152-65535/TCP	RPC pour LSA, SAM, Netlogon (*)
49152 -65535/TCP/UDP	389/TCP/UDP	LDAP
49152 -65535/TCP	3268/TCP	LDAP GC
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

Le Cloud Connector utilise la signature et le scellement LDAP pour sécuriser les connexions au contrôleur de domaine. Cela signifie que LDAP sur SSL (LDAPS) n'est pas nécessaire. Pour plus d'informations sur la signature LDAP, consultez Comment activer la signature LDAP dans Windows Server et Instructions de Microsoft concernant l'activation de la liaison de canaux LDAP et la signature LDAP.

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 terme de connexion Internet pour les services Citrix Cloud
- Exigences relatives aux ports de service de la console
- 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 terme de connexion Internet pour les services Citrix Cloud

Affichage des journaux Cloud Connector

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

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

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

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

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

Configuration de SSL/TLS

Les chiffrements détaillés dans la section Cryptage et gestion des clés doivent être activés sur le serveur Windows Server hébergeant le Cloud Connector.

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 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.

Citrix Connector Appliance pour les services cloud

Installation du Connector Appliance

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

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

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 du Connector Appliance, consultez la section Connector Appliance pour Cloud Services.

Connexion à l'hyperviseur hébergeant un Connector Appliance

Le Connector Appliance 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 le Connector Appliance (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. Le Connector Appliance est auto-géré.

Configuration des ports entrants et sortants

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

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

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

Le Connector Appliance 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 du Connector Appliance	Port externe	Service
Entrante	443/TCP	N'importe lequel	Interface Web locale
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
Sortante	49152 -65535/UDP	123/UDP	W32Time
Sortante	49152 -65535/TCP	464/TCP/UDP	Changement de mot de passe Kerberos
Sortante	49152 -65535/TCP/UDP	389/TCP/UDP	LDAP
Sortante	49152 -65535/TCP	3268/TCP	LDAP GC
Sortante	49152 -65535/TCP/UDP	88/TCP/UDP	Kerberos
Sortante	49152 -65535/TCP/UDP	445/TCP	SMB
Sortante	137/UDP	137/UDP	Service de noms NetBIOS
Sortante	138/UDP	138/UDP	Datagramme NetBIOS
Sortante	139/TCP	139/TCP	Session NetBIOS

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

Le Connector Appliance 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 le Connector Appliance peut contacter au cours de ses opérations normales. En outre, les clients ne peuvent pas contrôler les données que le Connector Appliance 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 du Connector Appliance

Vous pouvez télécharger un rapport de diagnostic pour votre Connector Appliance qui inclut divers fichiers journaux. Pour plus d'informations sur l'obtention de ce rapport, consultez Connector Appliance pour Cloud Services.

Configuration de SSL/TLS

Le Connector Appliance n'a pas besoin de configuration SSL/TLS spéciale.

Le Connector Appliance 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 le Connector Appliance approuve.

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

Conformité aux normes de sécurité

Pour garantir la conformité à la sécurité, le Connector Appliance 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. Le Connector Appliance 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.

Dans votre Active Directory (AD), nous vous recommandons de restreindre l'accès en lecture seule au compte de machine du Connector Appliance. 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 Connector Appliance pour surveiller toute activité d'accès à AD.

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.

Créer un compte Citrix Cloud

December 13, 2023

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

Les clients qui collaborent déjà avec Citrix et qui utilisent les services Citrix Cloud pour la première fois peuvent utiliser les tâches décrites dans cet article pour terminer le processus d'intégration.

Processus d'inscription pour les nouveaux clients Citrix

Si vous utilisez Citrix et Citrix Cloud pour la première fois, vous devez contacter Citrix pour créer un nouveau compte Citrix pour votre entreprise. Utilisez l'une des méthodes de contact suivantes :

- Contactez le service client Citrix.
- Contactez un partenaire Citrix ou un commercial Citrix de votre région.

Lorsque vous contactez Citrix, vous pouvez discuter des besoins de votre entreprise avec un représentant Citrix. Le représentant vous aide à terminer le processus d'inscription et vous fournit vos informations de connexion Citrix.

Après avoir reçu les informations d'identification de votre compte Citrix, vous pouvez utiliser les tâches décrites dans cet article pour vous connecter et commencer à utiliser 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. 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 entreprise. Si vous avez besoin d'aide pour connaître votre OrgID, contactez le service client Citrix via https://www.citrix.com/support/.

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 identifié par un ID client et est associé à un OrgID. Un OrgID peut être associé à plusieurs ID client Citrix Cloud, mais un ID client ne peut être associé qu'à un seul OrgID.

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 entreprise 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 peut s'inscrire auprès de Citrix Cloud sur cet OrgID en utilisant les informations de connexion de leur compte Citrix ou une adresse e-mail associée à cet OrgID. Lorsque l'

entreprise décide d'acheter un abonnement Citrix DaaS, la commande peut être passée correctement en utilisant l'OrgID 1234.

> **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.

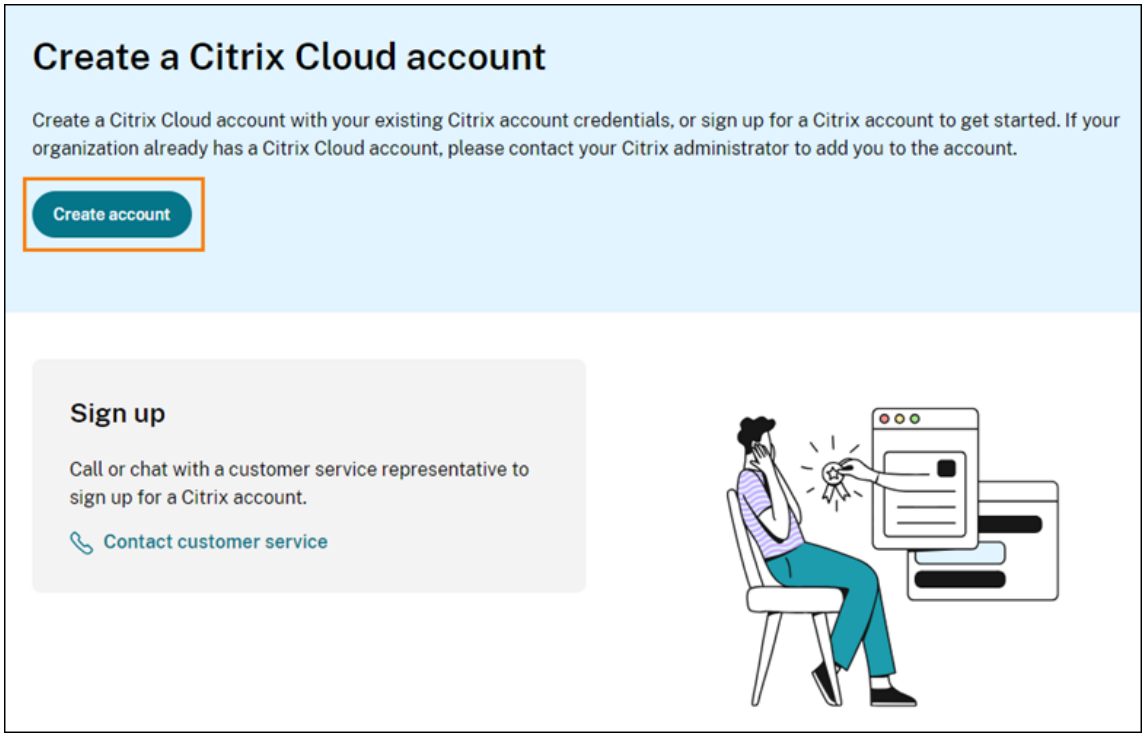
Authentification multifacteur

Pour garantir la sécurité de votre compte Citrix Cloud, Citrix exige que tous les clients s'inscrivent à l'authentification multifacteur (MFA). 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. S'il n'est pas possible d'utiliser un appareil doté d'une application d'authentification, vous pouvez utiliser une adresse e-mail à la place.

Si vous n'êtes pas encore inscrit à l'authentification multifacteur (MFA), Citrix vous invite à le faire lorsque vous vous connectez avec les informations d'identification de votre compte Citrix. Pour connaître les exigences et obtenir les instructions requises, consultez Étape 2 : Configurer l'authentification multifacteur dans cet article.

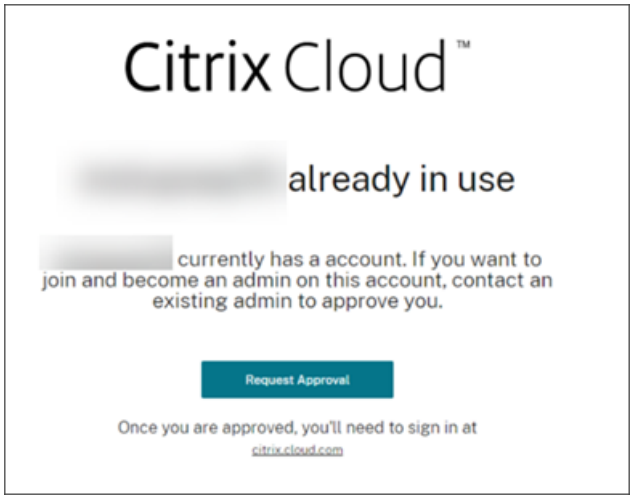
Étape 1 : Accéder au site Web de Citrix Cloud

1. À l'aide d'un navigateur Web, accédez à https://onboarding.cloud.com.
2. Sélectionnez **Créer un compte**.



3. Entrez votre nom d'utilisateur et votre mot de passe ou l'adresse e-mail et le mot de passe associés à votre compte Citrix.com.

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



Si un message indiquant qu'un compte Citrix Cloud est déjà utilisé pour votre organisation s'affiche, cela signifie qu'un autre administrateur de votre compte Citrix a déjà créé le compte Citrix Cloud. Avant de pouvoir accéder au compte, un administrateur existant doit vous inviter à devenir administrateur, même si vous êtes déjà membre du compte Citrix.

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.

Pour demander une invitation à rejoindre le compte Citrix Cloud, sélectionnez **Demander approbation**. Tous les administrateurs existants du compte reçoivent un e-mail les informant de votre demande. Si les administrateurs existants ne font plus partie de votre organisation, contactez le support Citrix.

Lorsqu'un administrateur reçoit votre demande d'approbation, il vous invite à devenir administrateur, comme décrit dans la section Inviter des administrateurs individuels.

Lorsque vous recevez l'e-mail d'invitation, cliquez sur le lien **Connexion** pour accepter l'invitation. Lorsque votre navigateur s'ouvre, Citrix Cloud vous invite à créer un mot de passe et à vous connecter au compte Citrix Cloud.

Étape 2 : Configurer l'authentification multifacteur

Si vous ne vous êtes pas inscrit à l'authentification multifacteur (MFA), Citrix Cloud vous invite à vous inscrire avant de vous connecter. Vous pouvez choisir de vous inscrire à l'authentification multifacteur à l'aide d'une application d'authentification (recommandée) ou de votre adresse e-mail.

> **Remarques :**
>
> - Seuls les administrateurs sous le fournisseur d'identité Citrix peuvent s'inscrire à l'authentification multifacteur (MFA) via Citrix Cloud. Si vous utilisez Azure AD pour gérer les administrateurs Citrix Cloud, vous pouvez configurer l'authentification multifacteur (MFA) à l'aide du portail Azure. Pour plus d'informations, consultez Configurer les paramètres d'authentification multifacteur Azure sur le site Web de Microsoft.
> - Une fois le processus de configuration terminé, l'authentification MFA est utilisée pour toutes les organisations clientes auxquelles vous appartenez dans Citrix Cloud. Vous ne pouvez pas désactiver la MFA une fois le processus de configuration terminé.
> - 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 la section Gérer votre méthode de MFA principale.

E-mail comme méthode d'authentification

Si vous ne pouvez pas utiliser d'application d'authentification pour accéder à Citrix Cloud, l'authentification MFA par e-mail est une alternative pratique. Citrix vous recommande toutefois vivement de prendre des précautions pour garantir la sécurité de l'accès à votre adresse e-mail.

Exigences relatives à la MFA

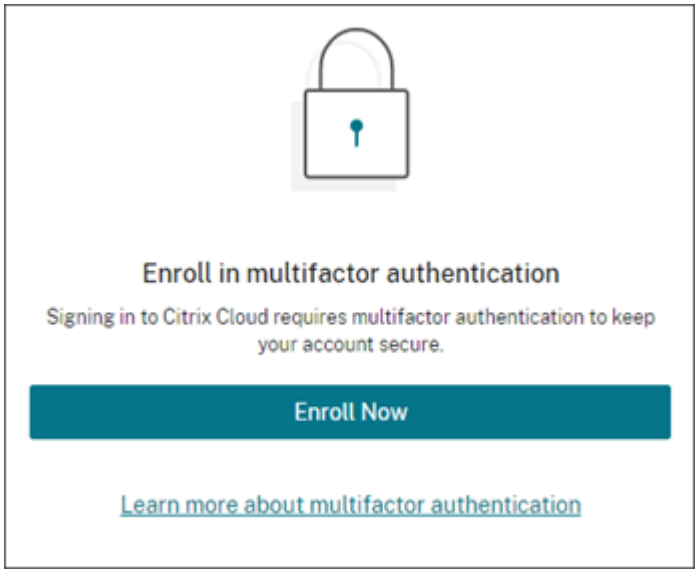
Pour configurer la MFA avec une application d'authentification, vous devez installer une application conforme à la norme TOTP (mot de passe à usage unique temporaire) sur votre appareil, tel qu'un smartphone ou un ordinateur de bureau. Selon l'appareil que vous inscrivez, l'application peut avoir besoin d'accéder à la caméra de votre appareil pour scanner un code QR. Si votre appareil ne possède pas de caméra, vous pouvez saisir une clé fournie par Citrix Cloud.

Pour configurer la MFA avec une adresse e-mail, vous devez utiliser une adresse e-mail répondant aux exigences suivantes :

- L'adresse e-mail est différente de celle que vous utilisez pour votre compte Citrix.
- L'adresse e-mail est une adresse à laquelle vous pouvez accéder pour recevoir des e-mails de vérification de Citrix.

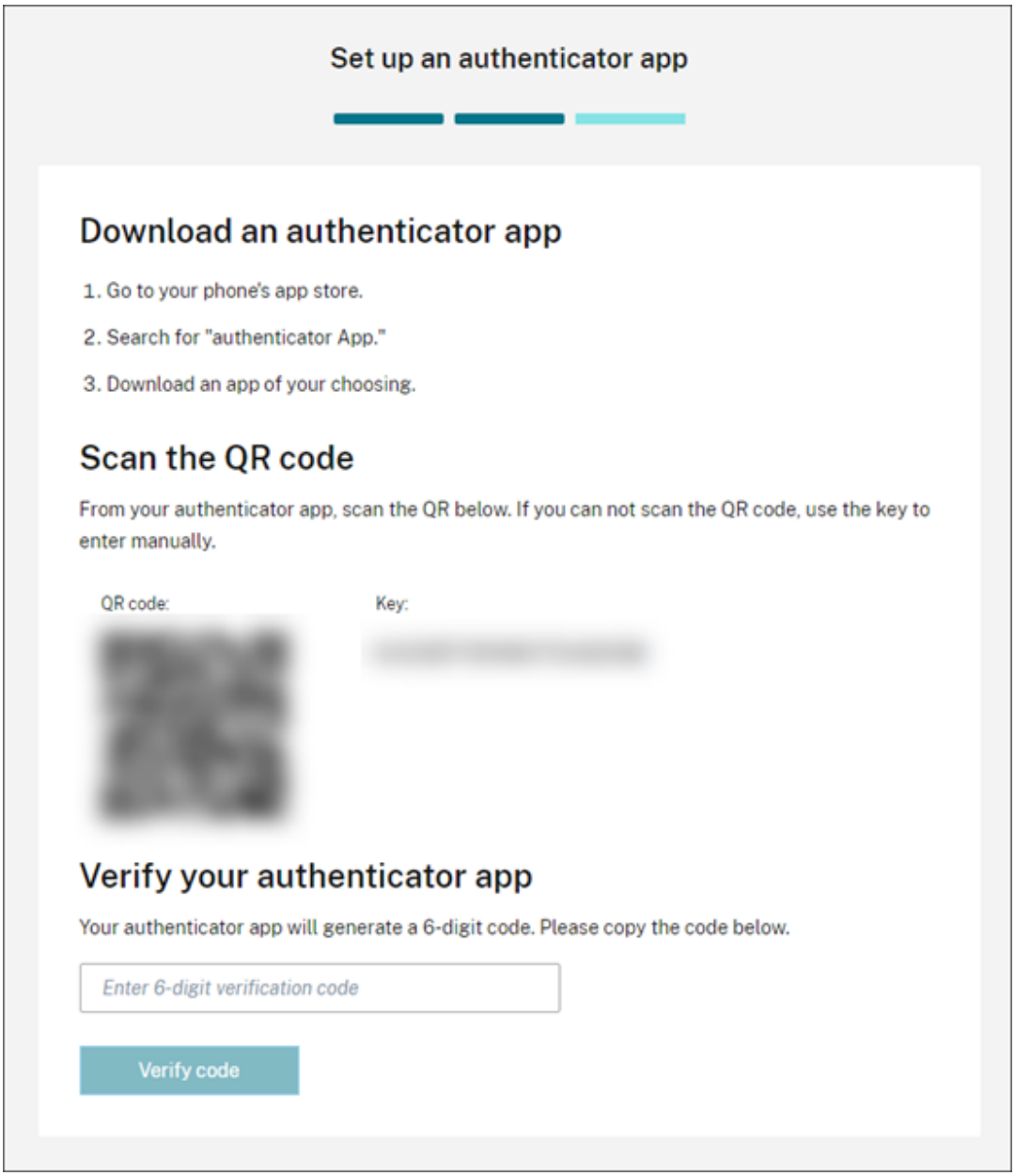
Pour vous inscrire à l'authentification multifacteur

1. Lorsque vous êtes invité à vous inscrire à l'authentification multifacteur (MFA), sélectionnez **S'inscrire maintenant**.



2. Lorsque vous y êtes invité, entrez votre adresse e-mail et sélectionnez **Envoyer e-mail**. Citrix Cloud vous envoie un e-mail avec un code de vérification.
3. Entrez le code de vérification indiqué dans l'e-mail et le mot de passe de votre compte Citrix. Cliquez sur **Vérifier et continuer**.
4. Sélectionnez la méthode d'authentification que vous souhaitez utiliser, qu'il s'agisse d'une application d'authentification ou d'un e-mail.
5. Si vous avez sélectionné **Application d'authentification**, effectuez les actions suivantes :

a) À partir de votre 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.



b) Sous **Vérifier votre application d'authentification**, entrez le code de votre application d'authentification et sélectionnez **Vérifier le code**.

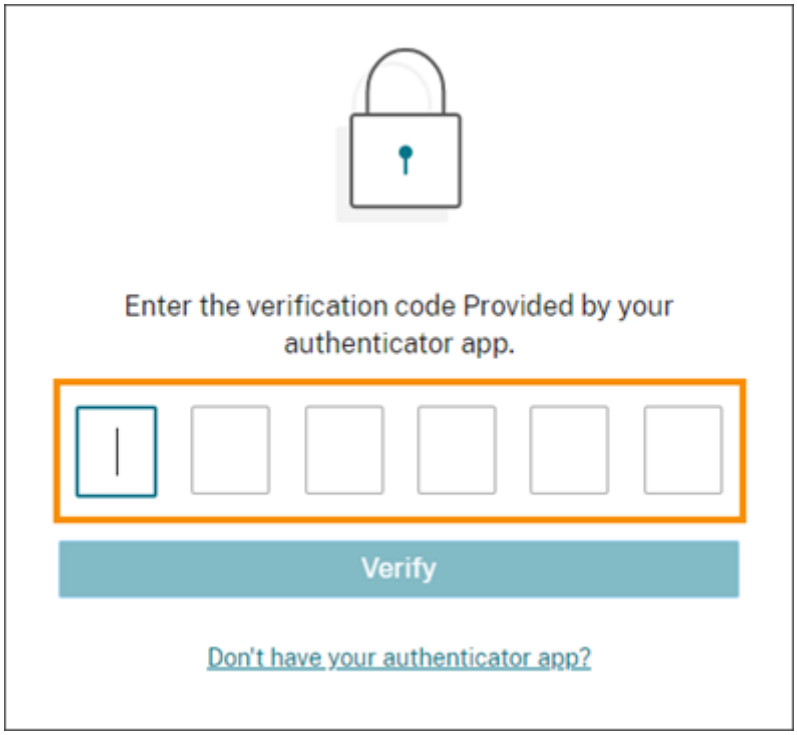
6. Cliquez sur **Étape suivante : Méthodes de récupération**.
7. Sélectionnez **Ajouter un n° de téléphone de récupération** et entrez un numéro de téléphone de récupération que le support Citrix pourra utiliser pour vous appeler et vérifier votre identité. Citrix recommande d'utiliser un numéro de téléphone fixe. Lorsque vous avez terminé, cliquez

sur **Enregistrer le numéro de téléphone de récupération**.

8. Sélectionnez **Suivant**.
9. Sélectionnez **Ajouter un e-mail de récupération** et entrez une adresse e-mail à laquelle vous pouvez accéder et qui est différente de celle que vous utilisez avec Citrix Cloud. Citrix utilise cette adresse pour vous envoyer un code de vérification afin de vérifier votre identité.

   Si vous ne disposez pas d'une autre adresse e-mail, sélectionnez **Vous n'avez pas d'e-mail de récupération ?** pour générer une liste de codes de secours à la place. Les codes de secours ne sont pas recommandés car ils peuvent être facilement perdus. Si vous choisissez cette option, téléchargez les codes et conservez-les dans un endroit où vous pourrez y accéder en cas de besoin.
10. 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 fourni par la méthode de MFA choisie.



Gérer votre inscription à MFA

Pour changer d'appareil, passer à une autre méthode d'authentification multifacteur ou mettre à jour vos méthodes de récupération, consultez les articles suivants :

- Gérer votre méthode de MFA principale

- Gérer vos méthodes de récupération de MFA

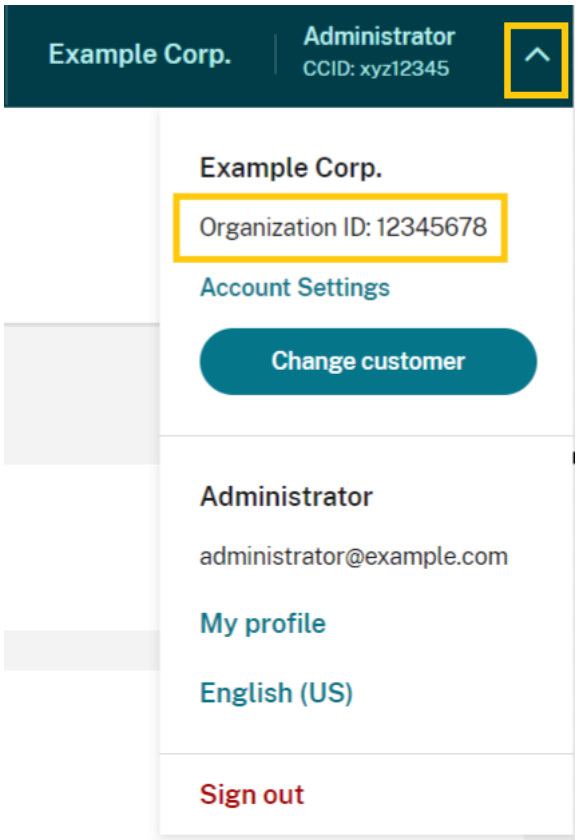
Étape 3 : Vérifier votre OrgID

Avant de commencer à utiliser Citrix Cloud, prenez le temps de vérifier votre OrgID.

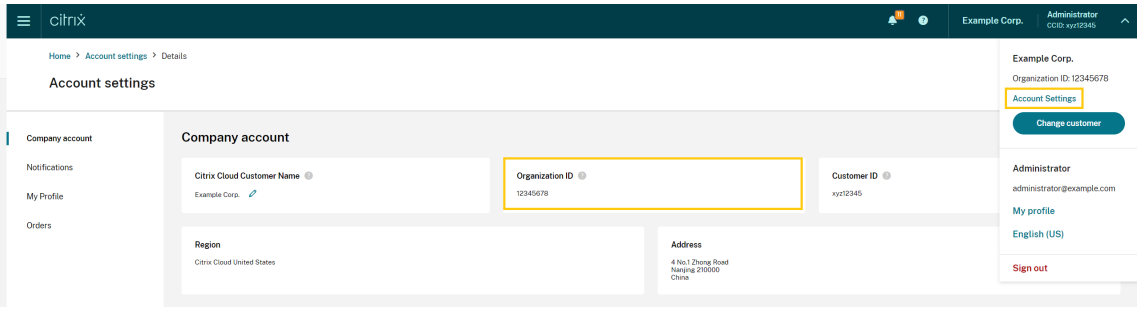
Assurez-vous que l'OrgID de votre compte correspond à l'OrgID que vous utilisez pour passer des commandes. L'un des avantages de Citrix Cloud est que si vous testez un service et décidez de l'acheter, toutes les configurations que vous avez effectuées dans la version d'évaluation sont conservées dans 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 aux emplacements suivants de la console de gestion :

- Dans le menu situé sous le nom de votre client. Cliquez sur le nom de votre client dans le coin supérieur droit pour afficher le menu.



- Sur votre page **Paramètres du compte**. Sélectionnez **Paramètres du compte** dans le menu client.



Étapes suivantes

Après l'intégration, vous pouvez passer aux tâches suivantes :

- Ajoutez un fournisseur d'identité pour authentifier les administrateurs ou les utilisateurs de l'espace de travail.
- Ajoutez des administrateurs à votre compte Citrix Cloud. Même si vos autres administrateurs ont accès à votre compte Citrix sur Citrix.com, vous devez quand même les ajouter à votre compte Citrix Cloud.
- Demandez une version d'évaluation de service. 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.

Informations supplémentaires

- Citrix Training : Fundamentals of Citrix Cloud
- Chaîne Citrix sur YouTube: Citrix Cloud Master Class

Vérifier votre adresse e-mail pour Citrix Cloud

October 19, 2023

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.
- En raison de mises à jour du système de sécurité de Citrix Cloud, vous devez revérifier 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 de vérification. Que dois-je faire ?

Procédez comme suit :

1. Recherchez dans votre boîte de réception un e-mail de vérification provenant de « Citrix ». L'e-mail de vérification expire au bout de 24 heures. Pour déclencher un nouvel e-mail de vérification, reconnectez-vous à Citrix Cloud. Il s'agit d'un processus unique pour chaque connexion Web.
2. Si l'e-mail de vérification ne figure 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 de courrier indésirable. Vérifiez tous les pare-feu.
3. 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.
4. Vérifiez que l'adresse e-mail enregistrée est valide en vous connectant à votre compte Citrix à l'adresse https://www.citrix.com/account. Si l'e-mail n'est pas valide, mettez à jour votre adresse e-mail et reconnectez-vous à Citrix Cloud pour déclencher un nouvel e-mail de vérification. Pour plus d'informations, consultez les sections CTX126336 ou CTX130452 dans le Centre de connaissances Citrix.
5. Si vous n'avez toujours pas reçu d'e-mail de vérification, contactez le support Citrix pour ouvrir un ticket de support. Pour les sites de formation (voir **Partner Services Delivery > eLearning > Citrix Training**), ouvrez un ticket auprès de l'équipe Education pour une enquête plus approfondie. Pour ouvrir un ticket, faites une demande à l'aide de **General Support** sur la page Contact Us.

Si vous avez correctement vérifié votre adresse e-mail mais que vous ne parvenez toujours pas à vous connecter à Citrix Cloud, consultez Troubleshooting login issues on Citrix websites.

Contactez le support Citrix

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

Se connecter à Citrix Cloud

April 5, 2024

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 connecteurs dans votre domaine. Selon les services cloud que vous utilisez, des Cloud Connector ou des appliances Connector sont nécessaires pour permettre la communication entre Citrix Cloud et vos ressources. Pour plus d'informations sur le déploiement de connecteurs, consultez les articles suivants :

- Détails techniques sur Cloud Connector
- Connector Appliance pour Cloud Services

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 un Connector Appliance.

Services qui utilisent Citrix Cloud Connector

- **Citrix DaaS** (anciennement Citrix Virtual Apps and Desktops Service) nécessite le Cloud Connector pour publier des applications et des bureaux et provisionner des catalogues de machines

dans vos emplacements de ressources. Pour obtenir une vue d'ensemble qui explique la façon dont le Cloud Connector communique avec ce service, consultez le diagramme Citrix DaaS) dans Citrix Tech Zone.

- **Citrix DaaS Standard pour Azure** (anciennement Citrix Virtual Apps and Desktops Standard pour Azure) nécessite le Cloud Connector pour fournir des applications et des bureaux virtuels Azure hébergés par Citrix à partir de machines multi-sessions.
- **Endpoint Management** nécessite le Cloud Connector pour gérer les stratégies des applications et des appareils et fournir des applications aux utilisateurs.

Services qui utilisent un Connector Appliance

- Le **service de portabilité des images** simplifie la gestion des images sur toutes les plateformes. Cette fonctionnalité est utile pour gérer les images entre un emplacement de ressources sur site et un emplacement de cloud public. Les API REST Citrix Virtual Apps and Desktops peuvent être utilisées pour automatiser l'administration des ressources au sein d'un site Citrix Virtual Apps and Desktops.

  Le flux de travail de portabilité des images commence lorsque vous utilisez Citrix Cloud pour initier la migration d'une image de votre emplacement sur site vers votre abonnement à un cloud public. Après avoir préparé votre image, le service de portabilité des images vous aide à transférer l'image vers votre abonnement cloud et à la préparer à l'exécution. Enfin, Citrix Provisioning ou Machine Creation Services provisionne l'image dans votre abonnement au cloud public.

  Pour plus d'informations, consultez la section Service de portabilité des images.

- **Citrix Secure Private Access** permet aux administrateurs d'offrir une expérience homogène, intégrant Single Sign-on, accès distant et inspection du contenu dans une solution unique pour un contrôle d'accès de bout en bout. Pour plus d'informations, consultez Secure Private Access avec Connector Appliance.

Il peut y avoir d'autres services dans la version préliminaire qui dépendent également de Connector Appliance.

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

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.

Limites d'emplacement des ressources

Vous pouvez disposer d'un maximum de 50 emplacements de ressources sur votre compte Citrix Cloud.

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 plus d'informations, consultez la section [Sélectionner un emplacement de ressources principal].(/en-us/citrix-cloud/citrix-cloud-management/identity-access-management/primary-resource-locations.html)

Citrix Cloud Connector

April 5, 2024

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.

> **Remarque :**
>
> N'installez pas le SDK PowerShell Remote sur une machine Citrix Cloud Connector. Il peut être installé sur n'importe quelle machine appartenant au domaine dans le même emplacement de ressources.
>
> Citrix recommande de ne pas exécuter les applets de commande de ce SDK sur les Cloud Connector. Le fonctionnement du SDK n'implique pas les Cloud Connector.

Services qui requièrent le Cloud Connector

Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) nécessite le Cloud Connector. Pour obtenir une vue d'ensemble qui explique la façon dont le Cloud Connector communique avec le service, consultez le diagramme Citrix DaaS) dans Citrix Tech Zone.

Citrix Endpoint Management requiert le Cloud Connector pour la connectivité d'entreprise au Endpoint Management Service. Remote Browser Isolation 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 Citrix DaaS 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. Au moins deux Cloud Connector dans chaque emplacement de ressources sont nécessaires pour garantir une connexion haute disponibilité avec Citrix Cloud. 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**.

De combien de Cloud Connector ai-je besoin ?

Au moins deux (2) Cloud Connector sont nécessaires pour créer une connexion haute disponibilité entre Citrix Cloud et votre emplacement de ressources. Selon votre environnement et les charges de travail, vous aurez peut-être besoin d'un plus grand nombre de Cloud Connector pour garantir la meilleure expérience à vos utilisateurs.

Citrix recommande d'utiliser le modèle de redondance N+1 pour déterminer le nombre de Cloud Connector que vous devez déployer. Déterminez le nombre de Cloud Connector dont vous avez besoin dans un emplacement de ressources en fonction de votre environnement, de vos charges de travail, de votre configuration Active Directory et de vos services. À ce nombre, ajoutez au moins un Cloud Connector supplémentaire pour garantir la résilience. Par exemple, si vous déterminez que vous avez besoin de cinq Cloud Connector, ajoutez-en un supplémentaire à ce total et installez six Cloud Connector dans votre emplacement de ressources.

Vous trouverez des consignes liées au dimensionnement et à la scalabilité dans la section Considérations sur le dimensionnement et la scalabilité des Cloud Connector.

Où dois-je installer le Cloud Connector ?

Consultez 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 2016, Windows Server 2019 ou Windows Server 2022. 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 sur site).

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 2, 2024

Citrix Cloud Connector est un composant qui établit une connexion entre Citrix Cloud et vos emplacements de ressources. Cet article décrit les exigences et les scénarios de déploiement, la prise en charge d'Active Directory et FIPS, ainsi que les options de dépannage.

Configuration système requise

Les machines hébergeant Cloud Connector doivent satisfaire aux exigences suivantes : Au moins deux Cloud Connector dans chaque emplacement de ressources sont nécessaires pour garantir une haute disponibilité. Citrix recommande d'utiliser le modèle de redondance N+1 lors du déploiement de Cloud Connector afin de maintenir une connexion haute disponibilité avec Citrix Cloud.

Configuration matérielle requise

Chaque Cloud Connector requiert la configuration système minimale suivante :

- 2 processeurs virtuels
- Mémoire de 4 Go
- 20 Go d'espace disque

L'augmentation de la mémoire du processeur virtuel permet à un Cloud Connector de s'adapter à de plus grands sites. Pour connaître les configurations recommandées, consultez la section Considérations sur le dimensionnement et la scalabilité des Cloud Connector.

Systèmes d'exploitation

Les systèmes d'exploitation suivants sont pris en charge :

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

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 sur le 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 Citrix DaaS (anciennement 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.
- Si vous utilisez le programme d'installation graphique, un navigateur doit être installé et le navigateur système par défaut doit être configuré.

Instructions pour Windows Update

Citrix recommande vivement d'activer Windows Update sur toutes les machines hébergeant le composant Citrix Cloud Connector. Le composant Citrix Cloud Connector vérifie régulièrement

les redémarrages en attente pouvant être déclenchés par divers facteurs, notamment Windows Updates, toutes les cinq minutes. Tout redémarrage détecté est exécuté rapidement, quel que soit le calendrier journalier préféré qui a été défini sur l'emplacement des ressources. Cette approche proactive évite de laisser le composant Citrix Cloud Connector en attente de mise à jour pendant une période prolongée, préservant ainsi la stabilité du système.

La plateforme Citrix Cloud gère les redémarrages de façon à maintenir la disponibilité en n'autorisant qu'un seul composant Citrix Cloud Connector à redémarrer à la fois. Lorsque vous configurez Windows Update, veillez à configurer Windows de façon à télécharger et installer automatiquement les mises à jour en dehors des heures de bureau. Cependant, les redémarrages automatiques ne sont pas autorisés pendant au moins quatre heures afin de laisser au composant Citrix Cloud Connector suffisamment de temps pour gérer le processus de redémarrage. Par ailleurs, vous avez également la possibilité d'établir un mécanisme de redémarrage de secours à l'aide de la stratégie de groupe ou d'un outil de gestion du système dans les cas où une machine doit être redémarrée après une mise à jour. Pour plus d'informations, consultez Gérer les redémarrages des appareils après les mises à jour.

> **Remarque :**
>
> - Si le client ne souhaite pas que son composant Citrix Cloud Connector redémarre pendant les heures de bureau, nous lui suggérons de programmer les mises à jour Windows en conséquence en dehors de ces horaires.
> - Le redémarrage de chaque composant Citrix Cloud Connector nécessite environ 10 minutes, y compris le temps nécessaire à la synchronisation avec la plate-forme Citrix Cloud permettant de garantir qu'un seul composant Citrix Cloud Connector redémarre à un moment donné. Ainsi, le délai minimum recommandé de quatre heures pour les redémarrages automatiques, comme indiqué précédemment, peut être réglé en conséquence sur une durée plus ou moins longue en fonction du nombre de composants Citrix Cloud Connector dans le locataire.

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 peut 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 racines utilisées par Azure, consultez https://docs.microsoft.com/en-us/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 CRL et OCSP, consultez https://www.digicert.com/kb/util/utility-test-ocsp-and-crl-access-from-a-server.htm sur le site Web de DigiCert.
  - http://cacerts.digicert.com/
  - http://dl.cacerts.digicert.com/
  - 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 racine suivants sont installés :
  - https://cacerts.digicert.com/DigiCertAssuredIDRootCA.crt
  - https://cacerts.digicert.com/DigiCertGlobalRootG2.crt
  - https://cacerts.digicert.com/DigiCertGlobalRootCA.crt
  - https://cacerts.digicert.com/DigiCertTrustedRootG4.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
  - https://www.microsoft.com/pkiops/certs/Microsoft%20ECC%20Root%20Certificate%20Authority%202017.crt

- Les certificats intermédiaires suivants sont installés :
  - https://cacerts.digicert.com/DigiCertTrustedG4CodeSigningRSA4096SHA384.crt
  - https://cacerts.digicert.com/DigiCertSHA2AssuredIDCodeSigningCA.crt

Si un certificat est manquant, le programme d'installation de Cloud Connector le téléchargera à partir de http://cacerts.digicert.com.

Pour obtenir des instructions complètes sur le téléchargement et l'installation des certificats, consultez la section CTX223828.

Citrix DaaS L'utilisation de Cloud Connector pour la connectivité aux ressources DaaS requiert l'installation de certificats supplémentaires et l'octroi d'un accès à une infrastructure PKI étendue. Chaque machine Cloud Connector doit remplir les conditions suivantes :

- Le port HTTP 80 est ouvert aux adresses suivantes :
  - crl.*.amazontrust.com
  - ocsp.*.amazontrust.com
  - *.ss2.us
- La communication avec les adresses suivantes est activée :
  - https://*.amazontrust.com
  - https://*.ss2.us
- Les certificats racine suivants sont installés :
  - https://www.amazontrust.com/repository/AmazonRootCA1.cer
  - https://www.amazontrust.com/repository/AmazonRootCA2.cer
  - https://www.amazontrust.com/repository/AmazonRootCA3.cer
  - https://www.amazontrust.com/repository/AmazonRootCA4.cer
  - https://www.amazontrust.com/repository/SFSRootCAG2.cer
- Les certificats intermédiaires suivants sont installés :
  - https://www.amazontrust.com/repository/G2-RootCA4.orig.cer


```
- https://www.amazontrust.com/repository/R3-ServerCA3A.cer
- https://www.amazontrust.com/repository/SFC2CA-SFSRootCAG2.cer
- https://www.amazontrust.com/repository/SFC2CA-SFSRootCAG2.v2.
  cer
- https://www.amazontrust.com/repository/G2-RootCA1.orig.cer
- https://www.amazontrust.com/repository/R1-ServerCA1A.cer
- https://www.amazontrust.com/repository/G2-RootCA3.cer
- https://www.amazontrust.com/repository/R3-ServerCA3A.orig.cer
- https://www.amazontrust.com/repository/G2-RootCA2.orig.cer
- https://www.amazontrust.com/repository/G2-RootCA4.cer
- https://www.amazontrust.com/repository/R2-ServerCA2A.cer
- https://www.amazontrust.com/repository/R4-ServerCA4A.cer
- https://www.amazontrust.com/repository/R1-ServerCA1A.orig.cer
- https://www.amazontrust.com/repository/G2-RootCA1.cer
- https://www.amazontrust.com/repository/G2-RootCA2.cer
- https://www.amazontrust.com/repository/G2-RootCA3.orig.cer
- https://www.amazontrust.com/repository/R4-ServerCA4A.orig.cer
- https://www.amazontrust.com/repository/G2-ServerCA0A.cer
- https://www.amazontrust.com/repository/G2-ServerCA0A.orig.cer
- https://www.amazontrust.com/repository/SFSRootCA-SFSRootCAG2.
  cer
```

Si un certificat est manquant, Cloud Connector le téléchargera à partir de https://www.amazontrust.com.

Pour obtenir des instructions complètes sur le téléchargement et l'installation des certificats, consultez 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 l'article Vue d'ensemble du service et exigences relatives aux ports réseau pour Windows

- Utilisez des groupes de sécurité universels au lieu de groupes de sécurité globaux. Cette configuration garantit que l'appartenance au groupe d'utilisateurs peut être obtenue auprès de n'importe quel contrôleur de domaine de la forêt.

Configuration réseau requise

- Être connectée à un réseau qui peut contacter les ressources que vous utilisez dans votre emplacement de ressources. Pour de plus amples informations, consultez la section Configuration du pare-feu et du proxy d'un Cloud Connector.
- Être connectés à Internet. Pour plus d'informations, consultez les sections suivantes dans Configuration requise pour le système et la connectivité.
  - Exigences en termes de connectivité des services communs de Cloud Connector
  - Noms de domaine complets (FQDN) autorisés pour Cloud Connector

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

Niveau fonctionnel de la forêt	Niveau fonctionnel du domaine	Contrôleurs de domaine pris en charge
Windows Server 2012	Windows Server 2016	Windows Server 2016
Windows Server 2012 R2	Windows Server 2012 R2	Windows Server 2012 R2, Windows Server 2016
Windows Server 2012 R2	Windows Server 2016	Windows Server 2016
Windows Server 2016	Windows Server 2016	Windows Server 2016, Windows Server 2019, Windows Server 2022

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 CloudGateway	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
Citrix Remote HCL Server	Communications par proxy entre le Delivery Controller et les hyperviseurs.	Service réseau

Nom du service	Description	S'exécute en tant que
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

Vous pouvez utiliser à la fois un Cloud Connector et un Connector Appliance pour vous connecter aux contrôleurs Active Directory. Le type de connecteur à utiliser dépend de votre déploiement.

Pour plus d'informations sur l'utilisation d'appliances Connector avec Active Directory, voir Scénarios de déploiement pour les appliances Connector dans Active Directory

Installez Cloud Connector dans votre réseau interne sécurisé.

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.

Si l'approbation entre les domaines n'est pas parent/enfant, vous devrez peut-être installer des Cloud Connector pour chaque forêt ou domaine distinct. Cette configuration peut être requise pour gérer l'énumération des ressources lors de l'utilisation de groupes de sécurité pour attribuer des ressources ou pour les enregistrements de VDA provenant de l'un ou l'autre domaine.

> **Remarque :**
>
> Les emplacements de ressources ci-dessous constituent un schéma que vous devrez peut-être répéter 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

> **Remarque :**
>
> Si vous avez une instance d'hyperviseur dans un domaine distinct, vous pouvez toujours déployer un seul ensemble de Cloud Connector tant que l'instance de l'hyperviseur et les Cloud Connector sont accessibles via le même réseau. Citrix Cloud utilise la connexion d'hébergement et un réseau disponible pour établir la communication avec l'hyperviseur. Ainsi, même si l'hyperviseur réside dans un domaine différent, vous n'avez pas besoin de déployer un autre ensemble de Cloud Connector dans ce domaine pour vous assurer que Citrix Cloud peut communiquer avec l'hyperviseur.

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 y a approbation unidirectionnelle lorsque la forêt contenant le domaine de ressources fait confiance à la forêt contenant 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 de forêt unidirectionnelle

- 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 et ne peut pas être utilisé par les fonctionnalités côté 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, si vous utilisez les magasins StoreFront, 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.
- La console Monitor dans Citrix DaaS ne peut pas énumérer les utilisateurs du domaine forest2.local.

Pour contourner ces limitations, déployez les Cloud Connector comme décrit dans 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 y a approbation unidirectionnelle lorsque la forêt contenant le domaine de ressources fait confiance à la forêt contenant le domaine utilisateur. 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 unidirectionnelle
- 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

Dans ce scénario, les Connector Appliance peuvent être utilisés à la place des Cloud Connector dans les forêts d'utilisateurs sans ressources afin de réduire les coûts et les frais de gestion, en particulier

s'il existe plusieurs forêts d'utilisateurs. Pour de plus amples informations, consultez Utilisateurs et ressources dans des forêts distinctes (avec approbation) avec un seul groupe de Connector Appliance pour toutes les forêts.

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. Vous pouvez également afficher les données de vérification de l'intégrité avancée pour chaque Cloud Connector individuel. Pour plus d'informations, consultez la section Contrôles d'intégrité avancés de Cloud Connector.

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.

Dépannage

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 fournissent 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 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.

Déploiement de Cloud Connector en tant que serveurs Secure Ticket Authority

Si vous utilisez plusieurs composants Cloud Connector en tant que serveurs Secure Ticket Authority (STA) avec la console NetScaler, l'ID de chaque serveur STA peut être affiché en tant que **CWSSTA** à la fois dans la console de gestion NetScaler et dans le fichier ICA pour les lancements d'applications et de bureaux. Par conséquent, les tickets STA ne sont pas acheminés correctement et le lancement des sessions échoue. Ce problème peut se produire si les Cloud Connector sont déployés sous des comptes Citrix Cloud distincts portant des ID client différents. Dans ce scénario, une incohérence de ticket se produit entre les comptes distincts qui empêche la création de sessions.

Pour résoudre ce problème, assurez-vous que les composants Cloud Connector que vous liez en tant que serveurs STA appartiennent au même compte Citrix Cloud portant le même ID client. Si vous devez prendre en charge plusieurs comptes clients à partir du même déploiement de console NetScaler, créez un serveur virtuel Gateway pour chaque compte. Pour plus d'informations, consultez les articles suivants :

- Création de serveurs virtuels Gateway : Créer des serveurs virtuels
- Configuration de Secure Ticket Authority sur Citrix Gateway
- Guide de déploiement : Migration de Citrix Virtual Apps and Desktops depuis une version locale vers Citrix Cloud
- CTX232640: How do I configure Citrix Gateway to use a Cloud Connector as a STA

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

April 6, 2024

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 matière de connectivité

Utilisez le port 443 pour le trafic HTTP (en sortie uniquement). Pour obtenir la liste des adresses contactables requises, consultez les ressources suivantes :

- Configuration requise pour le système et la connectivité
- Exigences en termes de 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.

Pour obtenir la liste des ports requis, consultez la section Configuration des ports entrants et sortants.

> **Important :**
>
> - L'activation de l'interception SSL sur certains proxys peut empêcher le Cloud Connector de se connecter à Citrix Cloud.
> - L'interception SSL ne peut pas être effectuée sur des adresses Citrix Gateway. Pour de plus amples informations, consultez la section Exigences de connectivité des services Citrix Gateway.
> - L'interception SSL ne doit pas avoir d'impact sur la connectivité ou la stabilité du réseau. Pour plus d'informations, consultez Citrix Cloud Connector.
> - Si vous utilisez un proxy, il est recommandé que les flux de trafic suivants contournent le proxy :
>
> - Communication entre connecteurs (par exemple, lors d'événements LHC).
> - Communication entre les connecteurs et le VDA (connexion WCF).
> - Communication entre les connecteurs et les contrôleurs de domaine (requêtes AD).

En outre, il est important de noter que le connecteur utilise les paramètres de proxy WinHTTP. Pour les paramètres de configuration, reportez-vous à la page CTX222727.

Vérifier la connectivité Cloud Connector

L'utilitaire de vérification de la connectivité Cloud Connector (Cloud Connector Connectivity Check) 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 tunnelisés via le serveur proxy.

> **Remarque :**
>
> L'utilitaire Cloud Connector Connectivity Check est destiné uniquement aux comptes Citrix Cloud commerciaux. Ne l'utilisez pas avec Citrix Cloud Government ou Citrix Cloud Japan.

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

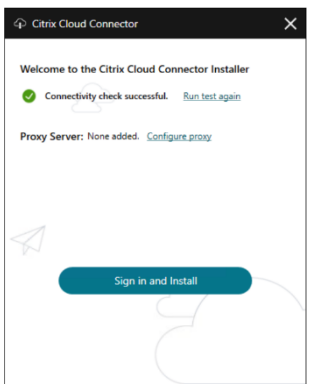
Programme d'installation

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 les paramètres définis pour l'utilisateur (comme décrit ci-dessus).

Vous pouvez configurer les paramètres du proxy pendant le processus d'installation.



Une fois le programme d'installation démarré, avant de vous connecter à Citrix Cloud, cliquez sur **Configurer le proxy**. Vous êtes invité à ajouter les informations et les adresses du proxy pour le contourner. Les noms de domaine complets et les adresses génériques sont pris en charge lors de la spécification d'adresses de contournement.

> **Remarque :**
>
> Si vous utilisez un serveur proxy, vous devez procéder à la configuration manuelle du proxy. La configuration automatique du proxy via la détection automatique ou des scripts PAC/d'installation n'est pas prise en charge.

Installation de Cloud Connector

July 2, 2024

Vous pouvez installer le logiciel Cloud Connector de manière interactive ou à l'aide de 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 à 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 hébergeant 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 mettez pas à niveau les différents composants du Cloud Connector séparément.
- 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 sur site).
- 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.
- Si vous utilisez le programme d'installation graphique, un navigateur doit être installé et le navigateur système par défaut doit être configuré.

Conseils après le déploiement

Une fois l'installation effectuée, conservez tous les Cloud Connector sous tension à tout moment pour garantir une connexion permanente à Citrix Cloud.

Renommer des machines

Après l'installation, ne renommez pas la machine hébergeant le Cloud Connector. Si vous devez modifier le nom du serveur ultérieurement, procédez comme suit :

1. Supprimez la machine de l'emplacement des ressources :
    a) Dans le menu Citrix Cloud, sélectionnez **Emplacements des ressources**.
    b) Localisez l'emplacement de ressources que vous souhaitez gérer et sélectionnez la tuile **Cloud Connector**.
    c) Localisez la machine que vous souhaitez gérer, puis cliquez sur le menu des points de suspension. Sélectionnez **Retirer connecteur**.

2. Désinstallez le logiciel Cloud Connector.
3. Renommez la machine.
4. Installez la dernière version du logiciel Cloud Connector, comme décrit dans cet article.

Déplacement de machines vers un autre domaine

Après l'installation, ne déplacez pas la machine qui héberge le Cloud Connector dans un autre domaine. Si vous devez ultérieurement associer la machine à un autre domaine, procédez comme suit :

1. Supprimez la machine de l'emplacement des ressources.
2. Désinstallez le logiciel Cloud Connector.
3. Dissociez la machine de son domaine actuel et joignez la machine au nouveau domaine.
4. Installez la dernière version du logiciel Cloud Connector, comme décrit dans cet article.

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.

Considérations relatives aux services

Les étapes d'installation décrites dans cet article décrivent le processus de déploiement des Cloud Connector, quel que soit le service pour lequel ils sont utilisés.

Lorsque vous déployez des Cloud Connector pour Citrix DaaS, vérifiez que les domaines AD dans lesquels résident les connecteurs sont actifs et ne sont pas affichés comme « inutilisés » dans la console Citrix Cloud. Si vous spécifiez un domaine inutilisé lors de la création du catalogue de machines dans Citrix DaaS, une erreur peut se produire. Pour plus d'informations, consultez Ajouter un type de

ressource ou activer un domaine inutilisé dans Citrix Cloud dans la documentation du produit Citrix DaaS.

Pour des considérations supplémentaires sur d'autres services, consultez la documentation du service en question.

Emplacement de ressources par défaut

Si vous n'avez aucun emplacement de ressources dans votre compte Citrix Cloud et que vous installez des Cloud Connector dans votre domaine, l'emplacement de ressources créé par Citrix Cloud devient l'emplacement de ressources par défaut. Vous ne pouvez avoir qu'un seul emplacement de ressources par défaut dans votre compte. Si nécessaire, vous pouvez créer des emplacements de ressources supplémentaires dans Citrix Cloud, puis sélectionner celui que vous souhaitez lorsque vous installez des Cloud Connector dans d'autres domaines.

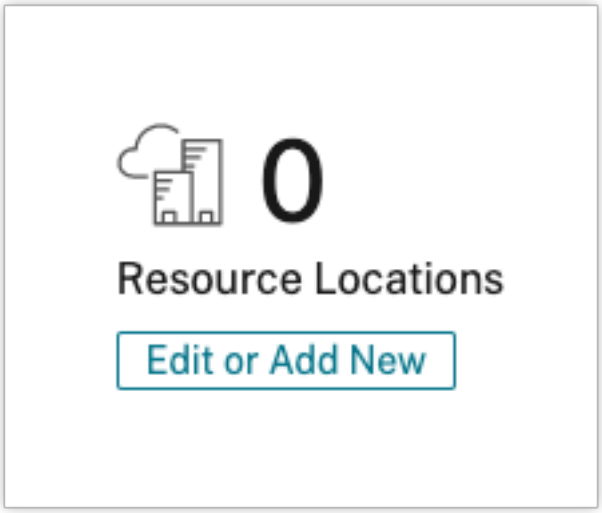
Vous pouvez également créer les emplacements de ressources dont vous avez besoin dans la console, avant d'installer les Cloud Connector dans vos domaines. Le programme d'installation de Cloud Connector vous invite à sélectionner l'emplacement de ressources que vous souhaitez lors de l'installation.

Installation interactive

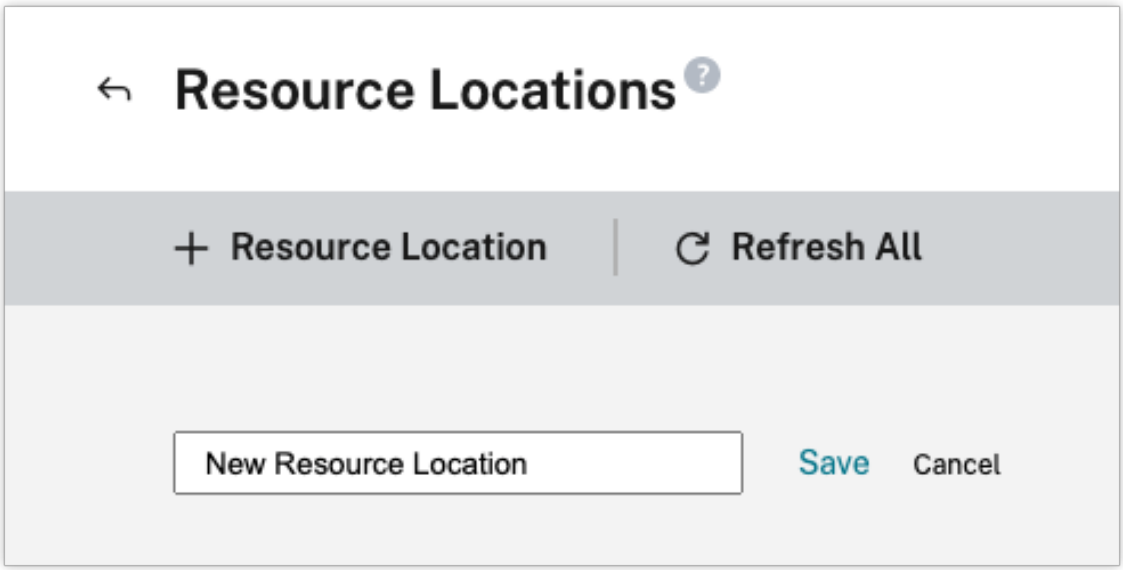
Vous pouvez télécharger et installer les Cloud Connector à l'aide de l'interface graphique du programme d'installation. Avant de procéder, vous devez créer un ou plusieurs emplacements de ressources dans la console de gestion Citrix Cloud sur lesquels déployer les Cloud Connector. Pour plus d'informations sur les emplacements des ressources, consultez la section 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.



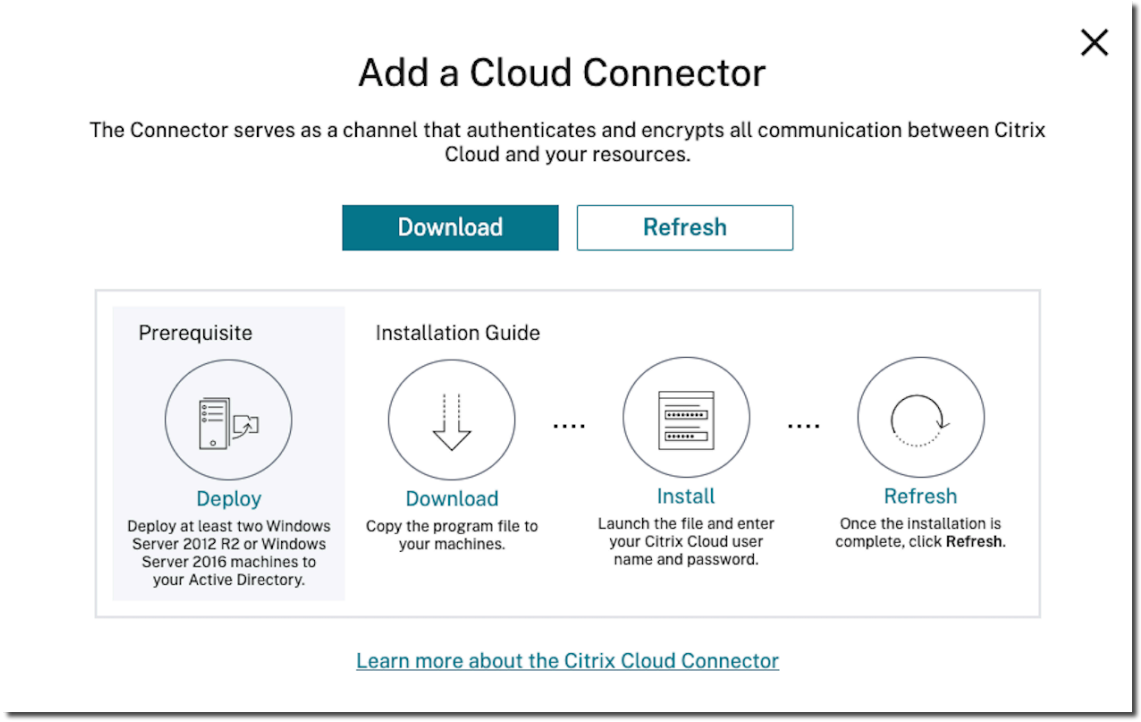
4. Dans Emplacements de ressources, sélectionnez **+ Emplacement de ressources** en haut de la page et enregistrez-le avec un nom unique.



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. (Facultatif) Si nécessaire, cliquez sur **Configurer le proxy** pour ajouter un serveur proxy. Vous êtes invité à ajouter les informations et les adresses du proxy pour le contourner. Les noms de domaine complets et les adresses génériques sont pris en charge lors de la spécification d'adresses de contournement.
3. Cliquez sur **Se connecter et installer** pour vous connecter à Citrix Cloud.
4. 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.

5. 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 de plus amples informations, consultez la section Gestion des identités et des accès.

Activer les domaines inutilisés

Si vous créez des emplacements de ressources et déployez des Cloud Connector pour Citrix DaaS, vérifiez que les domaines AD que vous utilisez avec Citrix DaaS sont actifs et ne sont pas considérés comme inutilisés. Si vous spécifiez un domaine inutilisé lors de la création de catalogues de machines dans Citrix DaaS, une erreur peut se produire.

Pour plus d'informations, consultez Ajouter un type de ressource ou activer un domaine inutilisé dans Citrix Cloud dans la documentation du produit Citrix DaaS.

Créer des emplacements de ressources supplémentaires

1. Dans la console de gestion Citrix Cloud, cliquez sur le bouton de menu et sélectionnez **Emplacements des ressources**.
2. Cliquez sur **+ Emplacement des ressources** et saisissez un nom significatif.

3. Cliquez sur **Enregistrer**. Citrix Cloud affiche une vignette pour le nouvel emplacement des ressources.
4. Cliquez sur **Cloud Connector**, puis sur **Télécharger** pour acquérir le logiciel Cloud Connector.
5. Sur chaque machine préparée, installez le logiciel Cloud Connector à l'aide de l'assistant d'installation ou de l'installation par ligne de commande. Citrix Cloud vous invite à sélectionner l'emplacement de ressources que vous souhaitez associer au Cloud Connector.

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"
 }
```



```
9
10 <!--NeedCopy-->
```

Exemple de commande

La commande suivante installe silencieusement le logiciel Cloud Connector à l'aide d'un fichier de configuration JSON :

```
1 CWCConnector.exe /q /ParametersFilePath:c:\cwcconnector_install_params.
     json
2 <!--NeedCopy-->
```

Utilisez `/q` pour spécifier une installation silencieuse.

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 CloudGateway
- 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 Citrix. Pour plus d'informations, consultez l'article 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.

Contrôles d'intégrité avancés de Cloud Connector

December 13, 2023

Cloud Connector effectue des contrôles de l'intégrité avant et après les mises à jour afin de s'assurer que les mises à jour n'entraînent pas de temps d'arrêt pour les fournisseurs. Vous pouvez voir l'état de la connectivité et de l'intégrité du Connector et de chaque service ou fournisseur sur le Connector.

Afficher les données de contrôle de l'intégrité du Connector

1. Dans le menu Citrix Cloud, sélectionnez **Emplacements des ressources**.
2. Sélectionnez le Connector pour lequel vous souhaitez afficher les données de contrôle de l'intégrité.
3. Sur la page Connecteurs, accédez au menu représentant des points de suspension à côté du connecteur et sélectionnez **Afficher les données du connecteur**.

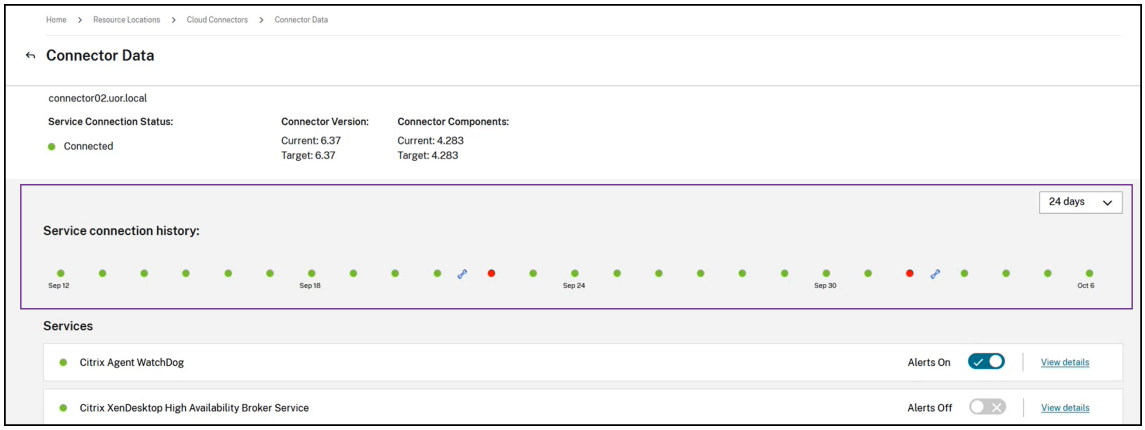
La page Données du connecteur apparaît et contient les informations suivantes.

- **État de la connexion du service**. Cette zone de la page Données du connecteur indique :

  - Si votre Connector est connecté au cloud
  - Pour le Connector et ses composants, la version actuellement installée et la version cible à installer lors de la prochaine mise à jour

- **Historique des connexions du service**. 24 indicateurs d'état indiquent l'état de l'intégrité du Connector au fil du temps. Par défaut, l'historique des connexions du service affiche l'état des 24 heures précédentes, par intervalles d'une heure. Pour voir plus d'historique, sélectionnez **24 jours** dans le menu déroulant. La vue affiche l'état des 24 derniers jours, par intervalles d'un jour.

  - Un point vert indique un état sain pendant l'intervalle de temps.
  - Un point rouge indique un état d'échec ou d'exception pendant l'intervalle de temps. Survolez le point pour plus d'informations.
  - Une icône représentant une clé à molette indique qu'une mise à jour a eu lieu pendant l'intervalle de temps. Survolez l'icône de la clé à molette pour plus d'informations.
  - Un point gris indique qu'aucune information sur l'état de l'intégrité n'a été reçue pendant cet intervalle de temps.



- **Services**. Cette zone répertorie chaque service exécuté sur le Connector.

  - Le point situé à côté de chaque service indique l'état actuel du service.
  - Utilisez **Alertes activées** et **Alertes désactivées** pour contrôler si vous êtes notifié des alertes du service. Si les alertes sont activées, les défaillances du service entraînent une défaillance de l'état global de la connexion du Connector.
  - Sélectionnez **Afficher les détails** pour afficher les détails de l'état de l'intégrité du service au fil du temps.

- **Mesures du connecteur**. Cette zone indique l'utilisation par le Connector de la mémoire, du processeur, des données réseau et de l'espace disque au cours des dernières 24 heures ou derniers 24 jours. Utilisez le menu déroulant de la zone **Historique des connexions du service** pour contrôler la période affichée.

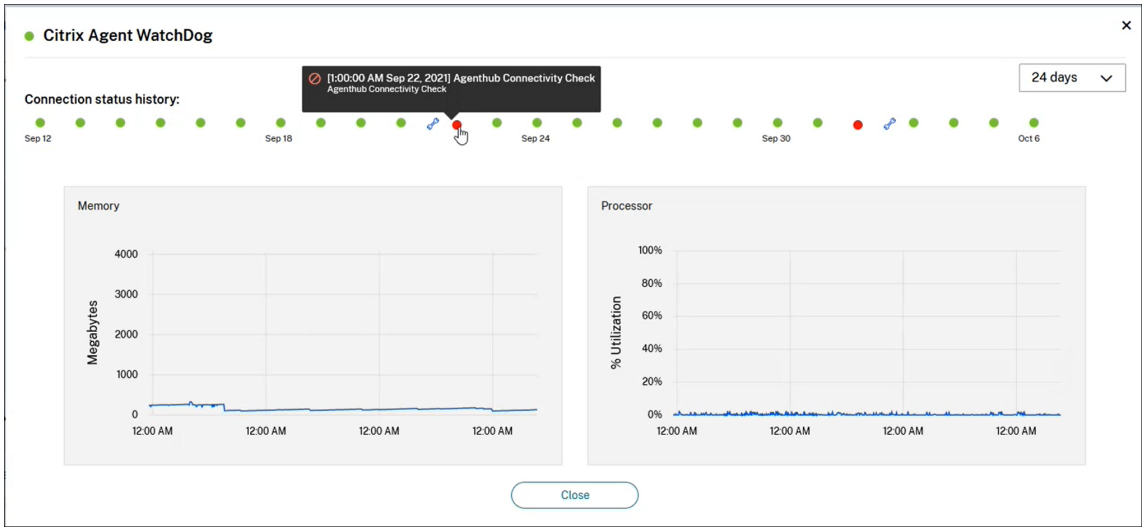
Afficher les détails du service

Pour afficher l'historique de l'état de la connexion et les mesures pour chaque service :

1. Utilisez le menu déroulant de la section **Historique des connexions du service** pour sélectionner la période. Vous pouvez consulter les 24 heures précédentes, par intervalles d'une heure, ou les 24 jours précédents, par intervalles d'un jour.
2. Sur la page Données du connecteur, sélectionnez **Afficher les détails** en regard du service.

La page qui apparaît indique :

- 24 indicateurs d'état qui indiquent l'état de l'intégrité du service au fil du temps.
  - Un point vert indique un état sain pendant l'intervalle de temps.
  - Un point rouge indique un état d'échec ou d'exception pendant l'intervalle de temps. Survolez le point pour plus d'informations.
  - Une icône représentant une clé à molette indique qu'une mise à jour a eu lieu pendant l'intervalle de temps. Survolez l'icône de la clé à molette pour plus d'informations.
  - Un point gris indique qu'aucune information sur l'état de l'intégrité n'a été reçue pendant cet intervalle de temps.
- Graphiques indiquant l'utilisation de la mémoire et du processeur pour le service pendant la période spécifiée.



Notifications de Connector

November 1, 2022

Vos connecteurs génèrent des notifications dans les 2 heures suivant l'apparition d'un avertissement ou d'une erreur. Vous pouvez voir les nouvelles notifications sur l'icône en forme de cloche dans l'en-tête de Citrix Cloud.

Cliquez sur cette icône pour afficher les notifications ou sélectionnez **Notifications** dans le menu de la console.

Pour de plus amples informations, consultez la section Notifications.

Cloud Connector

Le tableau suivant répertorie les notifications que Cloud Connector peut envoyer :

Message d'alerte	Type d'alerte	Détails	Résolution
Le connecteur *CONNECTOR_NAME* est hors connexion et obsolète car aucune tâche de maintenance régulière n'a été effectuée. Les connecteurs obsolètes affecteront la disponibilité du service et empêcheront la maintenance.	Erreur	Si un connecteur est resté hors connexion pendant une longue période et qu'il est ensuite reconnecté, il s'agit peut-être d'une ancienne version qui ne peut pas être mise à jour vers la dernière version. Les connecteurs obsolètes ne peuvent pas effectuer d'opérations de maintenance et peuvent affecter le processus de maintenance des autres connecteurs dans l'environnement.	Comment mettre à jour un Cloud Connector obsolète

Message d'alerte	Type d'alerte	Détails	Résolution
Le connecteur *CONNECTOR_NAME* n'est pas synchronisé avec l'heure UTC. Les connecteurs affichant cet état peuvent affecter la disponibilité, le fonctionnement ou les performances du service.	Erreur		Comment synchroniser l'heure du Cloud Connector
La maintenance du connecteur *CONNECTOR_NAME* a échoué. L'échec de la maintenance de ce connecteur empêchera la maintenance des autres connecteurs de l'environnement. Les connecteurs dont la maintenance a échoué peuvent avoir un impact sur la disponibilité, la fonctionnement ou les performances du service.	Erreur	Une mise à niveau du connecteur ou une autre opération de maintenance a échoué sur ce connecteur.	Comment résoudre une opération de maintenance ayant échoué sur un Cloud Connector

Message d'alerte	Type d'alerte	Détails	Résolution
Le connecteur *CONNECTOR_NAME* est hors connexion depuis *NUMBER* heures ou plus. Les connecteurs hors connexion affecteront la disponibilité du service et empêcheront la maintenance.	Avertissement	Si le connecteur est resté inaccessible pendant un certain nombre d'heures, il est considéré comme étant hors connexion.	Comment restaurer un Cloud Connector hors connexion à un état en ligne
Le connecteur *CONNECTOR_NAME* a échoué lors d'une récente vérification de connectivité. L'échec de vérification de la connectivité peut affecter la disponibilité ou le fonctionnement du service.	Avertissement	Une vérification de connectivité a échoué avec le code d'erreur *HEALTH_CHECK_CODE*. Ce connecteur n'a pas pu contacter certaines adresses Web ou IP répertoriées dans le message de notification.	Échec de la vérification de la connectivité du Cloud Connector
Le connecteur *CONNECTOR_NAME* enregistre une utilisation élevée du processeur. Les connecteurs fonctionnant avec des ressources limitées peuvent avoir un impact sur la disponibilité, les fonctionnement ou les performances des services.	Avertissement	Ce connecteur a dépassé 80% d' utilisation du processeur sur une période d' échantillonnage d'une heure.	Comment résoudre une alerte de disponibilité des ressources des Cloud Connector

Message d'alerte	Type d'alerte	Détails	Résolution
L'espace disque disponible du connecteur *CONNECTOR_NAME* est faible. Les connecteurs fonctionnant avec un espace disque limité peuvent affecter les performances et la maintenance du service.	Avertissement	Ce connecteur dispose de moins de 2 Go d'espace disque libre.	Comment résoudre une alerte de disponibilité des ressources des Cloud Connector
Le connecteur *CONNECTOR_NAME* a détecté qu'un processus ou un service critique n'est plus en cours d'exécution. Cet état peut affecter la disponibilité, le fonctionnement ou les performances du service.	Avertissement		

Collecte de journaux pour Citrix Cloud Connector

October 4, 2023

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 Citrix. Pour plus d'informations sur la collecte de journaux pour l'application Citrix Workspace, consultez 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.

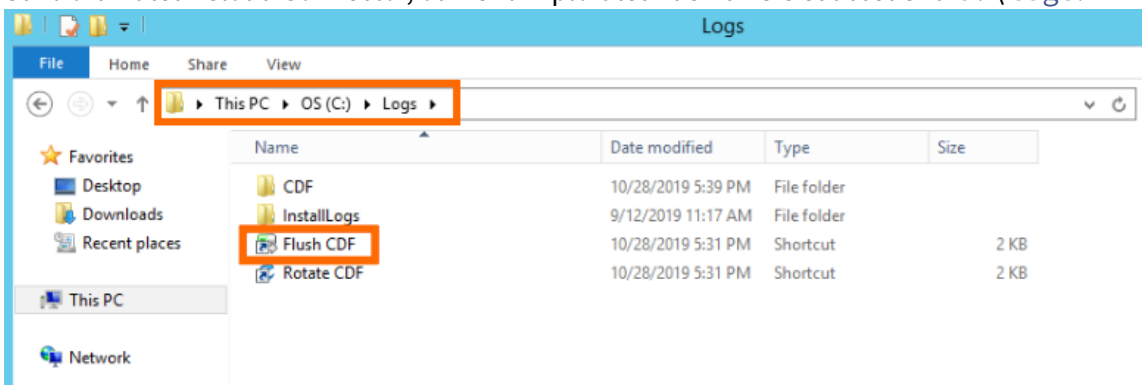
Étape 1 : Recréer le problème

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.

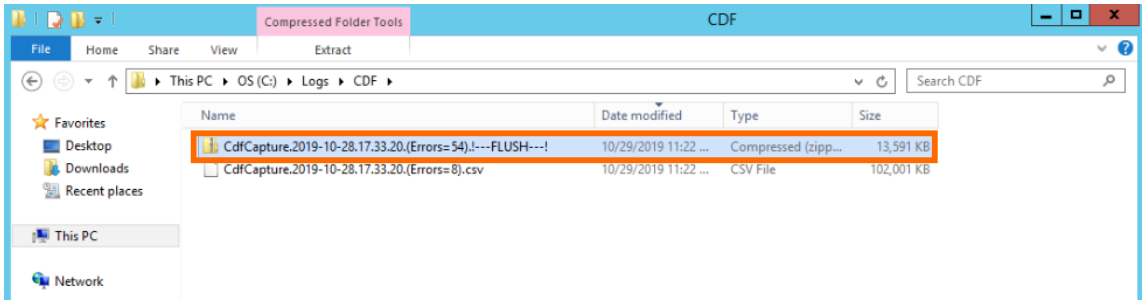
Étape 2 : Recueillir des traces CDF

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—!**.

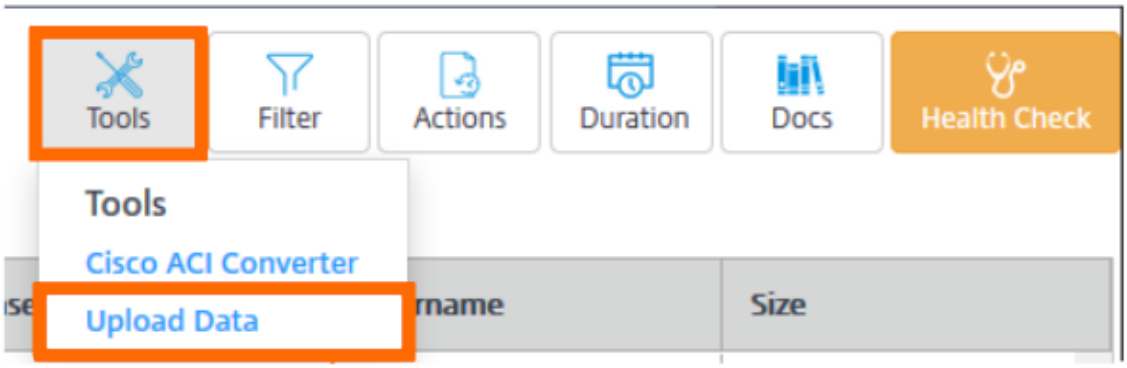


5. Effectuez les étapes 1 à 5 sur chaque machine Cloud Connector de votre emplacement de ressources et combinez toutes les traces de Cloud Connector dans une seule archive ZIP. Si vous ne créez pas d'archive ZIP des traces de purge à partir de toutes vos machines Cloud Connector, vous devrez les soumettre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

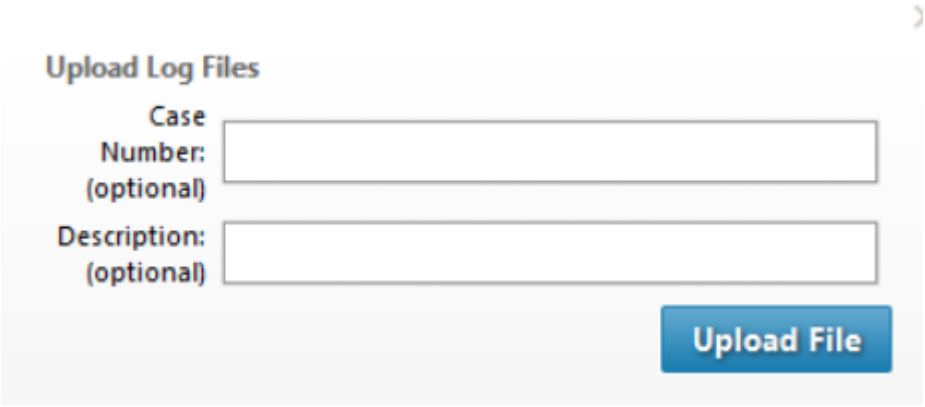
Étape 3 : Soumettre les données à Citrix

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

1. Accédez à 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.

Sélectionner un emplacement de ressources principal

October 4, 2023

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 dans la mesure du possible. 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. Les ouvertures de session utilisant un nom d'utilisateur principal (UPN) peuvent ne pas contenir le nom de domaine et peuvent ne pas utiliser l'emplacement de ressources principal.

> **Remarque :**
>
> Pour garantir que les Cloud Connector sont toujours disponibles dans tous les emplacements de

> ressources, installez au moins deux Cloud Connector dans chaque emplacement de ressources.

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**.

Connector Appliance pour Cloud Services

April 5, 2024

Connector Appliance 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. Connector Appliance vous permet de gérer et d'axer la priorité sur les ressources qui apportent de la valeur à vos utilisateurs.

Connector Appliance fournit les fonctions suivantes :

- **La connexion d'Active Directory à Citrix Cloud** autorise la gestion d'AD, ce qui permet d'utiliser des forêts et des domaines AD au sein de vos emplacements de ressources. Cela supprime le besoin d'ajouter des approbations Active Directory supplémentaires. Pour plus d'informations, voir Active Directory avec Connector Appliance
- Le **service de portabilité des images** simplifie la gestion des images sur toutes les plateformes. Cette fonctionnalité est utile pour gérer les images entre un emplacement de ressources sur site et un emplacement de cloud public. Les API REST Citrix Virtual Apps and Desktops peuvent être utilisées pour automatiser l'administration des ressources au sein d'un site Citrix Virtual Apps and Desktops.

Le flux de travail de portabilité des images commence lorsque vous utilisez Citrix Cloud pour initier la migration d'une image de votre emplacement sur site vers votre abonnement à un cloud public. Après avoir préparé votre image, le service de portabilité des images vous aide à transférer l'image vers votre abonnement cloud et à la préparer à l'exécution. Enfin, Citrix Provisioning ou Machine Creation Services provisionne l'image dans votre abonnement au cloud public.

Pour plus d'informations, consultez la section Service de portabilité des images.

- **Citrix Secure Private Access** permet aux administrateurs d'offrir une expérience homogène, intégrant Single Sign-on, accès distant et inspection du contenu dans une solution unique pour un contrôle d'accès de bout en bout. Pour plus d'informations, consultez Secure Private Access avec Connector Appliance.

Il peut y avoir d'autres services dans la version préliminaire qui dépendent également de Connector Appliance.

La plate-forme Connector Appliance fait partie de Citrix Cloud Platform et Citrix Identity Platform et peut traiter des données, notamment les informations suivantes :

- Adresses IP ou noms de domaine complets
- Identificateurs d'emplacement de ressource, d'appareil et d'utilisateur
- Horodatages
- Données sur les événements
- Détails des utilisateurs et des groupes Active Directory (par exemple, utilisés pour l'authentification et la recherche d'utilisateurs et de groupes)

Les détails des informations spécifiques traitées par Connector Appliance sont disponibles dans le tableau *Données collectées par Citrix Cloud Platform* de la vue d'ensemble de la protection des données Citrix Cloud Services.

Disponibilité et gestion de la charge de Connector Appliance

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 un Connector Appliance n'est pas disponible à un moment donné, les autres appliances Connector peuvent maintenir la connexion. Étant donné que chaque Connector Appliance est sans état, la charge peut être distribuée sur tous les Connector Appliance disponibles. Il n'est pas nécessaire de configurer cette fonction d'équilibrage de charge. Le processus est automatisé. Tant qu'un Connector Appliance 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 de Connector Appliance

Connector Appliance 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 plus d'informations sur la configuration des mises à jour, consultez Mises à jour de Connector.

Dans le cadre de la mise à jour, Connector Appliance devient temporairement indisponible. Les mises à jour ne sont appliquées qu'à un seul Connector Appliance dans un emplacement de ressources à la fois. Pour cette raison, enregistrez au moins deux Connector Appliance dans chaque emplacement de ressources pour vous assurer qu'au moins un Connector Appliance est toujours disponible.

Communication de Connector Appliance

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

Le tableau suivant répertorie les ports auxquels le Connector Appliance doit accéder :

Service	Port	Protocoles de domaine pris en charge	Détails de la configuration
DNS	53	TCP/UDP	Ce port doit être ouvert pour la configuration locale
NTP	123	UDP	Ce port doit être ouvert pour la configuration locale
HTTPS	443	TCP	Le Connector Appliance nécessite un accès sortant à ce port

Pour configurer le Connector Appliance, les administrateurs informatiques doivent pouvoir accéder à l'interface d'administration du port 443 (HTTPS) du Connector Appliance.

> **Remarque :**
>
> vous devez inclure `https://` au début de l'adresse IP.

Connector Appliance 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 de Connector Appliance, seul le trafic entre Connector Appliance et les systèmes externes est acheminé via ce proxy Web. Si votre système local se trouve dans un espace d'adressage privé, le trafic de Connector Appliance vers ce système n'est pas acheminé via le proxy Web.

Connector Appliance 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`
  - 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`

Configuration réseau requise

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

- Le réseau peut autoriser Connector Appliance à utiliser DHCP pour obtenir des serveurs DNS et NTP, une adresse IP, un nom d'hôte et un nom de domaine, ou vous pouvez définir manuellement les paramètres réseau dans la console de Connector Appliance.
- 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 Connector Appliance.
- Soit l'horloge de l'hyperviseur est réglée sur le temps universel coordonné (UTC) et synchronisée avec un serveur de temps, soit DHCP fournit des informations de serveur NTP à Connector Appliance.
- Si vous utilisez un proxy avec Connector Appliance, le proxy doit être non authentifié ou utiliser une authentification de base.

Configuration système requise

Connector Appliance est prise en charge sur les hyperviseurs suivants :

- Citrix Hypervisor 8.2 CU1 LTSR
- VMware ESXi version 7 mise à jour 2
- Hyper-V sur Windows Server 2016, Windows Server 2019 ou Windows Server 2022.
- Nutanix AHV
- Microsoft Azure
- AWS
- Google Cloud Platform

Votre hyperviseur doit fournir les fonctionnalités minimales suivantes :

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

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.

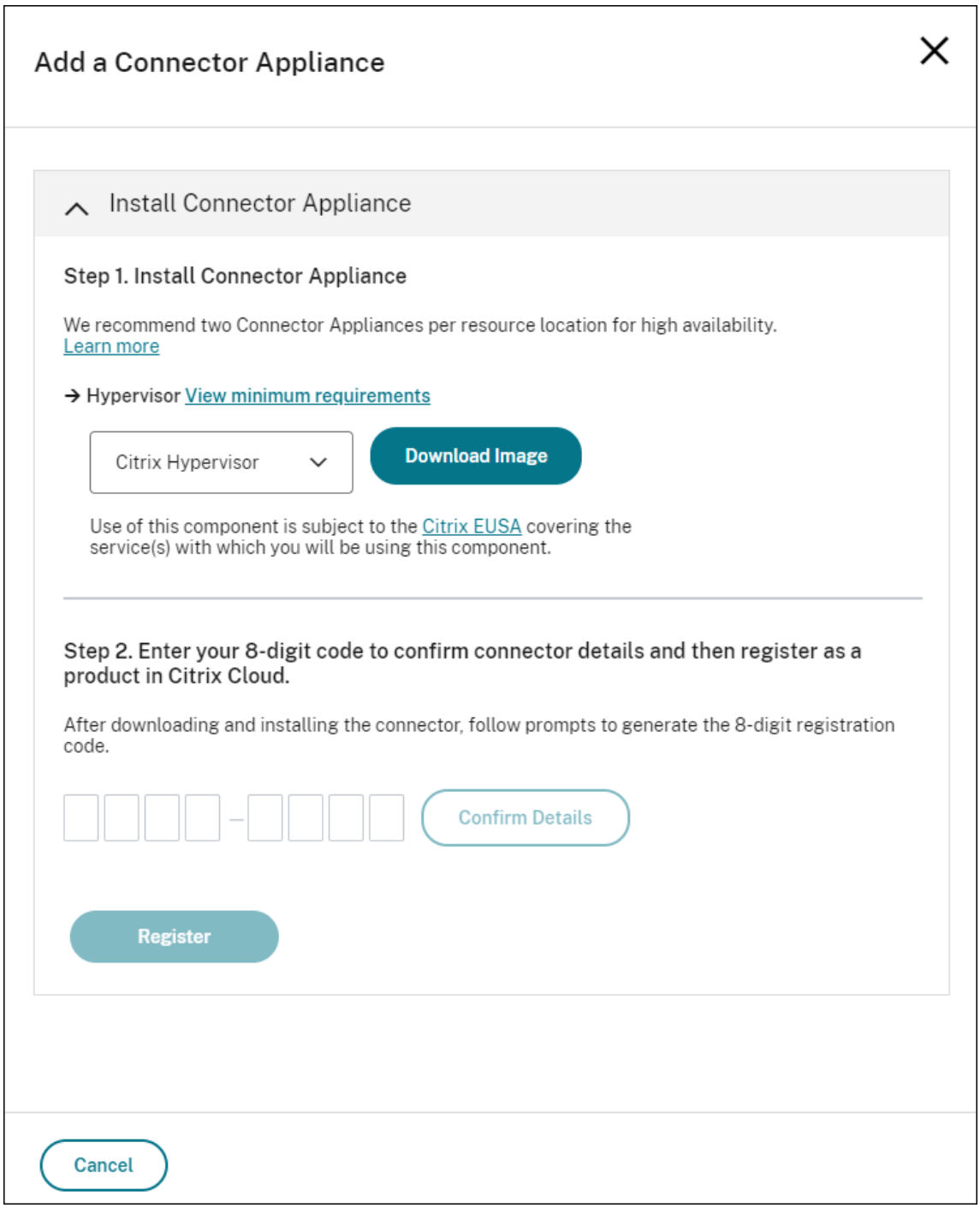
> **Remarque :**
>
> Le clonage, la suspension et la prise d'instantanés de la machine virtuelle de Connector Appliance ne sont pas pris en charge.

Obtenir Connector Appliance

Téléchargez le logiciel Connector Appliance 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 Connector Appliance, cliquez sur l'icône Plus (+) de **Connector Appliance**.

   La tâche **Ajouter un Connector Appliance** s'ouvre.



5. Dans la liste **Hyperviseur** de l'**étape 1**, choisissez le type d'hyperviseur ou de fournisseur de cloud que vous utilisez pour héberger votre Connector Appliance.

   - Pour les hyperviseurs et les environnements cloud locaux, vous pouvez télécharger Connector Appliance depuis Citrix Cloud :

     a) Cliquez sur **Télécharger l'image**.

b) Consultez le contrat de service de l'utilisateur final Citrix et, si vous êtes d'accord, sélectionnez **Accepter et continuer**.

c) Lorsque vous y êtes invité, enregistrez le fichier de Connector Appliance fourni.

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

- Pour certains environnements cloud, vous pouvez obtenir Connector Appliance depuis marketplace :
  - AWS
  - Microsoft Azure
  - Google Cloud

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

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

Installer Connector Appliance sur votre hyperviseur

- Citrix Hypervisor
- VMware ESXi
- Hyper-V
- Nutanix AHV
- Microsoft Azure
- Google Cloud Platform
- AWS

Citrix Hypervisor

Cette section décrit comment importer Connector Appliance 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 de Connector Appliance téléchargé.
2. Sélectionnez **Fichier** > **Importer**.
3. Spécifiez ou accédez au chemin d'accès où se trouve le fichier XVA de Connector Appliance. Cliquez sur **Suivant**.

4. Sélectionnez le serveur Citrix Hypervisor sur lequel vous souhaitez héberger Connector Appliance. Vous pouvez également sélectionner le pool dans lequel héberger Connector Appliance et Citrix Hypervisor choisit un serveur disponible approprié. Cliquez sur **Suivant**.
5. Spécifiez le référentiel de stockage à utiliser pour votre Connector Appliance. Cliquez sur **Importer**.
6. Cliquez sur **Ajouter** pour ajouter une interface réseau virtuelle. Dans la liste **Réseau**, sélectionnez le réseau que Connector Appliance doit utiliser. Cliquez sur **Suivant**.
7. Passez en revue les options à utiliser pour déployer Connector Appliance. 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 Connector Appliance déployée et démarrée avec succès, sa console affiche une page d'accueil contenant l'adresse IP de Connector Appliance. Utilisez cette adresse IP pour vous connecter à la page d'administration de Connector Appliance et compléter le processus d'enregistrement.

Par défaut, Connector Appliance 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 Connector Appliance avant de pouvoir accéder à la console de gestion de Connector Appliance. Pour plus d'informations, consultez Définir la configuration réseau à l'aide de la console de Connector Appliance.

Étape suivante : Enregistrer votre Connector Appliance avec Citrix Cloud

VMware ESXi

Cette section décrit comment déployer un Connector Appliance 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 Connector Appliance téléchargé.
2. Sélectionnez **Fichier** > **Déployer le modèle OVF…**
3. Spécifiez ou accédez au chemin d'accès où se trouve le fichier OVA de Connector Appliance. Cliquez sur **Suivant**.
4. Vérifiez les détails du modèle. Cliquez sur **Suivant**.
5. Vous pouvez spécifier un nom unique pour votre instance de Connector Appliance. Par défaut, le nom est défini sur **Connector Appliance**. Assurez-vous de choisir un nom qui distingue cette instance de Connector Appliance des autres instances hébergées sur cet hôte ESXi. Cliquez sur **Suivant**.
6. Spécifiez le stockage de destination de votre Connector Appliance. 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 Connector Appliance. En cas d'erreur, utilisez **Précédent** pour modifier ces options.
9. Sélectionnez **Mise sous tension après le déploiement**. Cliquez sur **Terminer**.

Une fois Connector Appliance déployée et démarrée avec succès, sa console affiche une page d'accueil contenant l'adresse IP de Connector Appliance. Utilisez cette adresse IP pour vous connecter à la page d'administration de Connector Appliance et compléter le processus d'enregistrement.

Par défaut, Connector Appliance 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 Connector Appliance avant de pouvoir accéder à l'interface utilisateur de Connector Appliance. Pour plus d'informations, consultez Définir la configuration réseau à l'aide de la console de Connector Appliance.

Étape suivante : Enregistrer votre Connector Appliance avec Citrix Cloud

Hyper-V

Cette section décrit comment déployer Connector Appliance 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 Connector Appliance à l'aide du Gestionnaire Hyper-V

1. Connectez-vous à l'hôte Hyper-V.
2. Copiez ou téléchargez le fichier ZIP de Connector Appliance sur l'hôte Hyper-V.
3. Extrayez le contenu du fichier ZIP. Le fichier ZIP contient 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 pour identifier votre Connector Appliance. Cliquez sur **Suivant**.
8. Dans le panneau **Spécifier la génération**, sélectionnez **Génération 1**. Cliquez sur **Suivant**.
9. Dans le panneau **Affecter la mémoire**, configurez les paramètres suivants, puis cliquez sur **Suivant** :

    a) Attribuez 4 Go de RAM.

b) Désactivez la mémoire dynamique.

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 Connector Appliance et sélectionnez **Paramètres**.
15. Dans la fenêtre **Paramètres**, sélectionnez **Matériel > Processeurs** et effectuez les opérations suivantes :

    a) Dans **Nombre de processeurs virtuels**, remplacez la valeur par **2**.
    b) Cliquez sur **Appliquer**.
    c) Cliquez sur **OK**.

16. Dans le panneau **Ordinateurs virtuels**, cliquez avec le bouton droit de la souris sur l'ordinateur virtuel de Connector Appliance et sélectionnez **Démarrer**.
17. Cliquez avec le bouton droit de la souris sur l'ordinateur virtuel de Connector Appliance et sélectionnez **Se connecter** pour ouvrir la console.

Une fois Connector Appliance 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 Connector Appliance. Utilisez cette adresse IP pour vous connecter à la page d'administration de Connector Appliance et compléter le processus d'enregistrement.

Par défaut, Connector Appliance 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 Connector Appliance avant de pouvoir accéder à l'interface utilisateur de Connector Appliance. Pour plus d'informations, consultez Définir la configuration réseau à l'aide de la console de Connector Appliance.

Étape suivante : Enregistrer votre Connector Appliance avec Citrix Cloud

Déployer Connector Appliance 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 en savoir plus, 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 Connector Appliance 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 actuellement le contenu du fichier ZIP et exécutez la commande suivante :

```
.\connector-appliance-install.ps1
<!--NeedCopy-->
```

5. Lorsque vous y êtes invité, tapez un nom pour votre machine virtuelle ou appuyez sur **Entrée** pour accepter la valeur par défaut **Connector Appliance**.
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 sélectionnez **Entrée** pour accepter la valeur par défaut de connector-appliance.vhdx.
8. Lorsque vous y êtes invité, sélectionnez le commutateur à utiliser. Sélectionnez **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 Connector Appliance.

Une fois Connector Appliance déployée et démarrée avec succès, sa console affiche une page d'accueil contenant l'adresse IP de Connector Appliance. Utilisez cette adresse IP pour vous connecter au Connector Appliance et compléter le processus d'enregistrement.

Étape suivante : Enregistrer votre Connector Appliance avec Citrix Cloud

Nutanix AHV

Cette section explique comment déployer le Connector Appliance à partir du fichier `connector-appliance.vhdx` sur un hôte Nutanix AHV à l'aide de la console Web Nutanix Prism.

1. Dans le menu principal de la console Web Nutanix Prism, sélectionnez la vue **Storage**.

2. Cliquez sur **+ Storage Container** pour créer un conteneur de stockage destiné à contenir le fichier image de Connector Appliance. Vous pouvez également utiliser un conteneur de stockage existant.
3. Téléchargez le fichier `connector-appliance.vhdx` sur votre conteneur de stockage.
    a) Dans le menu principal de la console Web, sélectionnez **Settings**.
    b) Sélectionnez l'onglet **Image Configuration** et cliquez sur **+ Upload Image**.
    c) Dans **Create Image**, spécifiez un **nom** pour votre image.
    d) Dans la liste **Image Type**, sélectionnez **DISK**.
    e) Dans la liste **Storage Container**, sélectionnez le conteneur de stockage que vous avez créé.
    f) Sélectionnez **Upload a file**.
    g) Cliquez sur **Choose file** et accédez au fichier `connector-appliance.vhdx` sur votre système local.
    h) Cliquez sur **Enregistrer**.
4. Attendez que l'image soit créée et que son état affiche **ACTIVE** sur la page **Image Configuration**.
5. Sélectionnez l'onglet **Network Configuration**.
6. Cliquez sur **+ Create Network** pour créer un réseau à utiliser par le Connector Appliance.
7. Sur la page **Create Network**, spécifiez les informations suivantes :
    - Le nom du réseau.
    - L'ID VLAN du réseau.
8. Dans le menu principal de la console Web, sélectionnez la vue **VM**.
9. Cliquez sur **+ Create VM** pour créer une instance de Connector Appliance.
10. Dans **Create VM**, spécifiez les informations suivantes :
    - Le nom de la machine virtuelle
    - Le nombre de processeurs virtuels
    - La quantité de mémoire en Gio
11. Sélectionnez cette option pour utiliser **Legacy BIOS**.
12. Cliquez sur **+ Add New Disk** pour ajouter un disque à la machine virtuelle.
13. Dans **Add Disk**, renseignez les informations suivantes :
    a) Pour **Type**, sélectionnez **DISK**.
    b) Pour **Operation**, sélectionnez **Clone from Image Service**.
    c) Pour **Bus Type**, sélectionnez **SCSI**.

d) Pour **Image**, sélectionnez l'image que vous avez créée lorsque vous avez chargé le fichier Connector Appliance.

14. Cliquez sur **Add** pour terminer l'ajout du disque.
15. Dans **Create VM**, cliquez sur **+ Add New NIC**.
16. Dans **Create NIC**, sélectionnez le réseau auquel ajouter la machine virtuelle.
17. Pour **Network Connection State**, sélectionnez **Connected**.
18. Cliquez sur **Add** pour terminer l'ajout de la carte réseau.
19. Cliquez sur **Save** pour créer la machine virtuelle.

    Par défaut, la nouvelle machine virtuelle est hors tension.
20. Dans la vue **VM**, sélectionnez la machine virtuelle et cliquez sur **Power on**.
21. Attendez que la machine virtuelle démarre. Ce processus peut prendre plusieurs minutes.

Une fois le Connector Appliance déployé et démarré avec succès, vous trouverez l'adresse IP du Connector Appliance à l'un des emplacements suivants :

- Dans la vue **VM** de la console Web Nutanix Prism.
- Dans la console Connector Appliance.

Utilisez cette adresse IP pour vous connecter à la page d'administration de Connector Appliance et compléter le processus d'enregistrement.

Étape suivante : Enregistrer votre Connector Appliance avec Citrix Cloud

Microsoft Azure

Cette section décrit comment déployer Connector Appliance dans Microsoft Azure. Vous pouvez déployer Connector Appliance à partir d'Azure Marketplace ou de l'image disque téléchargée à l'aide du script PowerShell inclus.

Déployer Connector Appliance depuis Azure Marketplace Pour déployer Connector Appliance à partir d'Azure Marketplace, procédez comme suit :

1. Accédez à Connector Appliance sur Azure Marketplace (Azure Marketplace)

   Vous pouvez également rechercher « Connector Appliance for Cloud Services » dans Marketplace.
2. Cliquez sur **Get It Now**, puis sur **Create**.

3. Sur la page **Create Citrix Connector Appliance for Cloud Services**, renseignez les informations suivantes :

   - Sélectionnez l'**abonnement** à utiliser.
   - Sélectionnez le **groupe de ressources** à utiliser.
   - Sélectionnez la **région** dans laquelle vous se trouve Connector Appliance.
   - Spécifiez un **nom de VM**.
   - Sélectionnez un **réseau virtuel** auquel ajouter Connector Appliance. Ce réseau est utilisé pour accéder à Citrix Cloud, aux ressources locales et à la page d'administration de Connector Appliance. Ce réseau ne peut pas être modifié ultérieurement.
   - Spécifiez une valeur pour le **réseau virtuel**.

   Cliquez sur **Next: Tags >**.

4. Dans l'onglet **Tags**, ajoutez les balises requises si nécessaire.

   Cliquez sur **Next : Review + create >**.

5. Après avoir passé en revue les détails du déploiement, cliquez sur **Create**.

Une fois Connector Appliance déployée et démarrée avec succès, sa console affiche une page d'accueil contenant l'adresse IP de Connector Appliance. Utilisez cette adresse IP pour vous connecter à la page d'administration de Connector Appliance et compléter le processus d'enregistrement.

Étape suivante : Enregistrer votre Connector Appliance avec Citrix Cloud

Déployer la VM de Connector Appliance à l'aide d'un script PowerShell Le fichier `connector-appliance-azure.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.

Effectuez les étapes suivantes :

1. Copiez ou téléchargez le fichier ZIP de Connector Appliance 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 actuellement le contenu du fichier ZIP et exécutez la commande suivante :

```
.\connector-appliance-upload-Azure.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 Connector Appliance déployée et démarrée avec succès, sa console affiche une page d'accueil contenant l'adresse IP de Connector Appliance. Utilisez cette adresse IP pour vous connecter à la page d'administration de Connector Appliance et compléter le processus d'enregistrement.

Étape suivante : Enregistrer votre Connector Appliance avec Citrix Cloud

AWS

Cette section explique comment déployer Connector Appliance dans AWS. Connector Appliance est disponible en tant qu'AMI sur AWS Marketplace et nous vous recommandons de l'installer à partir de l'AMI. Vous pouvez également déployer une image disque téléchargée à l'aide de l'interface utilisateur AWS ou du script PowerShell inclus.

Conditions préalables pour la mise en réseau Pour déployer Connector Appliance sur AWS, assurez-vous d'avoir accès à Citrix Cloud à partir du sous-réseau dans lequel Connector Appliance est créée.

Nous vous recommandons d'utiliser une adresse IP privée pour l'appliance, qui nécessite une configuration spécifique pour fournir un accès à Citrix Cloud. Pour réaliser cette configuration, procédez comme suit dans la **console de gestion AWS** :

1. Créez la passerelle NAT.
    a) Dans la barre de navigation supérieure, sélectionnez **Services > VPC > NAT Gateways**.
    b) Dans l'angle supérieur droit, cliquez sur **Create NAT Gateway**. Entrez les informations suivantes :
        - Renseignez le champ **Name**.
        - Sélectionnez la valeur **Subnet** dans la liste.

- Définissez **Connectivity type** sur **Public**.
- Sélectionnez un identifiant **Elastic IP allocation ID** dans la liste. Si aucune adresse IP Elastic n'est disponible, cliquez sur **Allocate Elastic IP** et suivez les instructions pour en créer une.

c) Cliquez sur **Create NAT Gateway**.

2. Créez une entrée de table de routage comprenant la passerelle NAT.

a) Dans la barre de navigation supérieure, sélectionnez **Services > VPC > Route Tables**.

b) Dans l'angle supérieur droit, cliquez sur **Create route table**. Entrez les informations suivantes :

- Renseignez le champ **Name**.
- Dans la liste, sélectionnez le VPC qui contient le sous-réseau que vous avez sélectionné lors de la création de la passerelle NAT.

c) Cliquez sur **Create route table**.

d) Dans l'onglet **Routes** de la table de routage que vous avez créée, cliquez sur **Edit routes > Add route**.

e) Renseignez les champs **Destination** et **Cible** pour la nouvelle entrée de routage.

- Définissez la destination sur 0.0.0.0/0.
- Pour la cible, sélectionnez la passerelle **NAT Gateway** que vous avez créée dans la liste.

f) Cliquez sur **Save change**.

3. Attachez le sous-réseau à utiliser pour Connector Appliance à cette table de routage.

a) Dans la barre de navigation supérieure, **Select Services > VPC > Route Tables**.
b) Sélectionnez la table de routage qui contient la passerelle NAT.
c) Sur la page d'affichage, accédez à l'onglet **Subnet Associations**.
d) Cliquez sur **Edit subnet associations**.
e) Sélectionnez le ou les sous-réseaux à attacher à la table de routage.
f) Cliquez sur **Save Associations**.

Déployer Connector Appliance depuis AWS Marketplace Avant de commencer, assurez-vous de remplir les conditions préalables suivantes :

- Vous êtes autorisé à exploiter les ressources EC2.
- Vous avez terminé la configuration de l'étape Conditions préalables pour la mise en réseau.

- (Facultatif) Vous pouvez créer un groupe de sécurité qui restreint les adresses IP autorisées à accéder à votre Connector Appliance.

Effectuez les étapes suivantes :

1. Connectez-vous à la **console de gestion AWS**.
2. Trouvez l'AMI de Connector Appliance sur AWS Marketplace. Vous pouvez pour cela procéder de plusieurs façons :
   - Suivez le lien Marketplace fourni dans Citrix Cloud. (AWS Marketplace)
   - Recherchez l'AMI dans la console de gestion AWS :
     a) Accédez à **Services > Calcul > EC2 > AMI**.
     b) Assurez-vous de vous trouver dans la région USA Est (Ohio).
     c) Dans **Images publiques**, recherchez « Citrix Connector Appliance » ou l'ID d'AMI « ami-026eaf9b3b232577f ».
3. Vérifiez que vous disposez de l'AMI correcte en vérifiant l'ID d'AMI (ami-026eaf9b3b232577f) et l'ID du propriétaire (414337923189).
4. Copiez l'AMI dans votre abonnement :
   a) Accédez à **Actions > Copier l'AMI**.
   b) Dans la boîte de dialogue **Copier l'AMI**, vous pouvez sélectionner la **région de destination** dont vous avez besoin.
   c) Cliquez sur **Copier l'AMI**.
5. Sur la page récapitulative de votre AMI copiée, cliquez sur **Lancer une instance à partir d'une AMI**.
6. Dans la boîte de dialogue **Lancer une instance**, procédez comme suit :
   a) Sélectionnez le nombre d'instances à créer. Pour des raisons de résilience, nous vous recommandons de disposer de deux appliances Connector ou plus dans chaque emplacement de ressources.
   b) Spécifiez un nom pour l'instance.
   c) Pour le **type d'instance**, sélectionnez **t2.medium**. Le type d'instance doit comporter au moins 4 Go et 2 processeurs.
   d) Pour **Paire de clés [connexion]**, sélectionnez **Continuer sans paire de clés**. La connexion SSH à Connector Appliance n'est pas autorisée, une paire de clés n'est donc pas nécessaire.
   e) Pour les **paramètres réseau**, dans la section **Pare-feu (groupe de sécurité)**, configurez les paramètres suivants :

i. Choisissez de **créer un groupe de sécurité** ou de **sélectionner un groupe de sécurité existant**.
ii. Désélectionnez **Autoriser le trafic SSH provenant d'Internet**
iii. Sélectionnez **Autoriser le trafic HTTPs provenant d'Internet**
iv. Sélectionnez **Autoriser le trafic HTTP provenant d'Internet**

Cliquez sur **Lancer l'instance**.

7. Une fois l'instance créée, dans la section **Succès**, cliquez sur le lien ID d'instance pour afficher votre instance de Connector Appliance.

   Vous pouvez également cliquer sur le bouton **Afficher toutes les instances** sur cette page ou accéder à **Services > EC2 >Instances** dans la console de gestion AWS pour voir la liste de vos instances.

8. Lorsque **l'état de l'instance** passe à **En cours d'exécution**, accédez aux détails de l'instance et utilisez l'**adresse IPv4 privée** pour vous connecter à la page d'administration du Connector Appliance et compléter le processus d'enregistrement.

Vous devrez peut-être utiliser un hôte bastion pour accéder à la page d'administration de Connector Appliance à l'adresse IP interne de votre navigateur et compléter le processus d'enregistrement.

Par défaut, Connector Appliance utilise DHCP pour définir sa configuration réseau. Vous pouvez modifier cette configuration réseau à l'aide de l'interface Web de Connector Appliance. Pour plus d'informations, consultez la section Configuration des paramètres réseau sur la page d'administration de Connector Appliance.

Étape suivante : Enregistrer votre Connector Appliance avec Citrix Cloud

Déployer Connector Appliance à l'aide de l'interface utilisateur AWS Avant de commencer, assurez-vous de remplir les conditions préalables suivantes :

- Vous êtes autorisé à exploiter les ressources S3 et EC2.
- Vous avez créé un rôle de service et une stratégie qui disposent d'un accès à l'importation de machines virtuelles. Pour en savoir plus, consultez https://docs.aws.amazon.com/vm-import/latest/userguide/required-permissions.html#vmimport-role.

  > **Remarque :**
  >
  > Pour créer un rôle de service, vous devez créer un compartiment S3. Lors de la création de la stratégie, définissez le compartiment S3 que vous avez créé avec l'accès à l'importation de machines virtuelles.

- Vous avez accès à AWS CloudShell. Cet environnement n'est disponible que dans certaines régions. Pour obtenir la liste des régions dans lesquelles AWS CloudShell est pris en charge,

consultez https://docs.aws.amazon.com/cloudshell/latest/userguide/supported-aws-regions.html.

- Vous avez terminé la configuration de l'étape Conditions préalables pour la mise en réseau.

Effectuez les étapes suivantes :

1. Sur votre système local, extrayez le contenu de `connector-appliance-aws.zip`.
2. Connectez-vous à la **console de gestion AWS**.
3. Créez un compartiment de stockage en effectuant les étapes suivantes. (Vous pouvez également ignorer ces étapes et utiliser un compartiment de stockage existant.)
   a) Dans la barre de navigation supérieure, sélectionnez **Services** > **S3** > **Create bucket**.
   b) Entrez un nom unique pour votre compartiment. Pour connaître les conventions de dénomination des compartiments dans Amazon S3, consultez https://docs.aws.amazon.com/AmazonS3/latest/userguide/bucketnamingrules.html.
   c) Sélectionnez la région de votre compartiment. Assurez-vous de choisir la même région que votre région AWS, car vous ne pouvez pas utiliser les fichiers du compartiment si ces régions sont différentes.
   d) Conservez les paramètres par défaut restants, puis cliquez sur **Create bucket**.
4. Cliquez sur le nom du compartiment que vous avez créé. Cliquez sur **Upload** > **Add files**, puis sélectionnez le fichier `connector-appliance.vhd`. Conservez les paramètres par défaut restants, puis cliquez sur **Upload**.
5. Cliquez sur le fichier que vous avez chargé. Cliquez sur **Copy S3 URI**.
6. Cliquez sur l'**icône AWS CloudShell** dans la barre de navigation supérieure et exécutez les commandes suivantes :
   a) Créez une tâche pour convertir votre fichier VHD en instantané :

   ```
   aws ec2 import-snapshot --disk-container Format=VHD,Url="<S3_URI>"
   ```

   Remplacez la valeur de l'espace réservé par votre URI S3 que vous avez copié à l'étape précédente. Par exemple, `aws ec2 import-snapshot --disk-container Format=VHD,Url="s3://my-aws-bucket/connector-appliance.vhd"`.

   Cette commande est terminée lorsque la commande suivante renvoie une chaîne JSON contenant `"Status": "completed"`. Notez la valeur `ImportTaskId` dans la sortie JSON.

   b) Exécutez la commande suivante :

   ```
   aws ec2 describe-import-snapshot-tasks --import-task-ids <ImportTaskId>
   ```


Remplacez la valeur de l'espace réservé par la valeur `ImportTaskId` copiée à l'étape précédente. Par exemple, `aws ec2 describe-import-snapshot-tasks --import-task-ids import-snap-0273h2836153itg5`.

7. Sur la **console AWS Management**, dans la barre de navigation supérieure, sélectionnez **Services** > **EC2**.
8. Dans le menu situé à gauche de l'écran, cliquez sur **Snapshots**.
9. Cliquez avec le bouton droit sur l'instantané que vous avez créé, puis cliquez sur **Create Image**
10. Dans le volet qui s'ouvre, effectuez les étapes suivantes :

    a) Entrez un nom pour votre image AMI.
    b) Sélectionnez **Hardware-assisted virtualization**.

    Cliquez sur **Créer**.

11. Dans le menu situé à gauche de l'écran, cliquez sur **AMI**.
12. Cliquez avec le bouton droit sur l'image AMI que vous avez créée, puis cliquez sur **Launch**.
13. Dans le volet qui s'ouvre, effectuez les étapes suivantes :

    a) Choisissez le type d'instance.
    b) (Facultatif) Personnalisez le réseau dans l'onglet **Configure Instance**.
    c) (Facultatif) Connectez un autre volume dans l'onglet **Add Storage**.
    d) Définissez les règles du groupe de sécurité dans l'onglet **Configure Security Group**.

    Après avoir examiné le lancement de l'instance, cliquez sur **Review and Launch**.

Une fois Connector Appliance déployée et démarrée avec succès, accédez à **Services** > **EC2** > **Instances** et sélectionnez l'instance que vous avez créée. Utilisez l'**adresse IPv4 privée** pour vous connecter à la page d'administration de Connector Appliance et compléter le processus d'enregistrement. Vous devrez peut-être utiliser un hôte bastion pour accéder à la page d'administration de Connector Appliance à l'adresse IP interne de votre navigateur et poursuivre le processus d'installation.

Par défaut, Connector Appliance utilise DHCP pour définir sa configuration réseau. Vous pouvez modifier cette configuration réseau à l'aide de l'interface Web de Connector Appliance. Pour plus d'informations, consultez la section Configuration des paramètres réseau sur la page d'administration de Connector Appliance.

Étape suivante : Enregistrer votre Connector Appliance avec Citrix Cloud

Déployer Connector Appliance à l'aide d'un script PowerShell Le fichier `connector-appliance-aws.zip` contient un script PowerShell qui crée et démarre une nouvelle machine virtuelle. Avant d'exécuter le script, assurez-vous de remplir les conditions préalables suivantes :

- Vous avez installé AWS.Tools, AWSPowerShell.NetCore ou AWSPowerShell sur votre système. Pour en savoir plus, consultez https://docs.aws.amazon.com/powershell/latest/userguide/pstools-getting-set-up.html.
- Vous avez créé un rôle de service et une stratégie qui disposent d'un accès à l'importation de machines virtuelles. Le rôle de service et la stratégie doivent tous deux être nommés `vmimport` pour que ce script PowerShell fonctionne. Pour en savoir plus, consultez https://docs.aws.amazon.com/vm-import/latest/userguide/required-permissions.html#vmimport-role.

  > **Remarque :**
  >
  > Pour créer un rôle de service, vous devez créer un compartiment S3. Lors de la création de la stratégie, définissez le compartiment S3 que vous avez créé avec l'accès à l'importation de machines virtuelles.

- Vous avez créé un groupe de sécurité Amazon EC2.
- Vous disposez d'autorisations S3 et d'un accès à l'API.
- Vous avez terminé la configuration de l'étape Conditions préalables pour la mise en réseau.

Effectuez les étapes suivantes :

1. Sur votre système local, extrayez le contenu de `connector-appliance-aws.zip` dans un dossier.
2. Dans PowerShell, exécutez les commandes suivantes :

   a) Pour pouvoir exécuter une applet de commande AWS dans votre environnement local, exécutez la commande suivante pour ajouter un nouveau profil au magasin AWS SDK :

   ```
   Set-AWSCredential -AccessKey <access_key_ID> -SecretKey <
       secret_key> -StoreAs MyProfile
   ```

   Remplacez les valeurs de l'espace réservé par votre clé d'accès et votre clé secrète. Indiquez un nom de profil unique. Dans l'exemple que nous avons fourni, il s'agit de `MyProfile`.

   b) Définissez le profil sur la valeur par défaut :

   ```
   Initialize-AWSDefaultConfiguration -ProfileName MyProfile
   ```

   c) Accédez au dossier dans lequel se trouvent actuellement les fichiers extraits et exécutez la commande suivante :

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

3. Suivez les instructions du script qui vous guident tout au long de la sélection de la région pour le déploiement de votre Connector Appliance, du téléchargement de l'image dans le compartiment de votre choix et de la saisie d'un nom pour votre machine virtuelle.

- Vous devez utiliser le compartiment disposant d'un accès à l'importation de machines virtuelles que vous avez créé précédemment.
- Lorsque vous êtes invité à sélectionner le VPC à utiliser, sélectionnez le VPC sur lequel la passerelle NAT et les tables de routage sont configurées.
- Lorsque vous êtes invité à sélectionner le sous-réseau à utiliser, sélectionnez le sous-réseau attaché à la table de routage contenant la passerelle NAT.

Pour plus d'informations, consultez Conditions préalables pour la mise en réseau.

Une fois Connector Appliance déployée et démarrée avec succès, le script affiche l'adresse IP privée de Connector Appliance. Vous devrez peut-être utiliser un hôte bastion pour accéder à la page d'administration de Connector Appliance à l'adresse IP interne de votre navigateur et compléter le processus d'enregistrement.

Par défaut, Connector Appliance utilise DHCP pour définir sa configuration réseau. Vous pouvez modifier cette configuration réseau à l'aide de l'interface Web de Connector Appliance. Pour plus d'informations, consultez la section Configuration des paramètres réseau sur la page d'administration de Connector Appliance.

Étape suivante : Enregistrer votre Connector Appliance avec Citrix Cloud

Google Cloud Platform

Cette section décrit comment déployer Connector Appliance sur Google Cloud Platform. Vous pouvez installer le Connector Appliance depuis le Google Cloud Marketplace. Vous pouvez également déployer une image disque téléchargée à l'aide de la console Google Cloud Platform ou du script PowerShell inclus.

Le fichier `connector-appliance-gcp.zip` contient :

- `connector-appliance.tar.gz`, qui est une image disque du Connector Appliance
- `connector-appliance-upload-gcp.ps1`, qui est un script PowerShell qui peut être utilisé pour déployer automatiquement le Connector Appliance

Déployer le Connector Appliance depuis le Google Cloud Marketplace

1. Connectez-vous à votre compte Google.
2. Suivez le lien Marketplace fourni dans Citrix Cloud. (Google Cloud Marketplace)

   Vous pouvez également rechercher « Connector Appliance for Cloud Services » dans Marketplace.
3. Cliquez sur **Lancement**.

4. Sur la page **Nouveau déploiement de Citrix Connector Appliance for Cloud Services**, renseignez les informations suivantes :

   - Spécifiez un **nom de déploiement** pour la tâche de déploiement.
   - Sélectionnez la **zone** dans laquelle se trouve le Connector Appliance.
   - Sélectionnez la **famille de machines**, la **série** et le **type de machine** à utiliser.
   - Sélectionnez le **type de disque de démarrage** et la **taille du disque de démarrage en Go** à utiliser.
   - Dans la section **Réseau**, spécifiez l'interface réseau à utiliser par le Connector Appliance. Si vous souhaitez pouvoir vous connecter à la page d'administration depuis un réseau public, spécifiez une **adresse IP externe**.

   Cliquez sur **Déployer**. Vous êtes redirigé vers la page **Deployment Manager**.

   > **Remarque :**
   >
   > Une fois le Connector Appliance déployé et démarré avec succès, vous recevez un e-mail confirmant que le Connector Appliance est déployé sur Google Cloud Platform.

5. Sur la page **Deployment Manager**, cliquez sur le nom de l'instance. Vous pouvez également rechercher l'instance du Connector Appliance que vous avez créée dans **Compute Engine**.
6. Si vous avez précédemment spécifié une **adresse IP externe** lors de la configuration de l'interface réseau de votre Connector Appliance, copiez l'**adresse IP externe** dans la section **Interfaces réseau** de l'onglet **Détails**. Utilisez cette adresse IP pour vous connecter à la page d'administration de Connector Appliance et compléter le processus d'enregistrement. Vous pouvez également utiliser l'**adresse IP interne principale** pour accéder à la page d'administration du Connector Appliance à partir d'une autre machine se trouvant dans le même sous-réseau que votre Connector Appliance.

Étape suivante : Enregistrer votre Connector Appliance avec Citrix Cloud

Déployer Connector Appliance à l'aide de la console Google Cloud Platform

1. Sur votre système local, extrayez le contenu de `connector-appliance-gcp.zip`.
2. Dans votre projet Google Cloud Platform, créez un compartiment (ou bucket) de stockage. (Vous pouvez également utiliser un compartiment de stockage existant.)

   a) Dans le menu principal, sélectionnez **Cloud Storage**.
   b) Dans le volet principal, sélectionnez **Créer un bucket**.
   c) Spécifiez un nom pour votre compartiment.
   d) Configurez les paramètres de stockage et d'accès des données dont vous avez besoin. Vous pouvez laisser ces paramètres comme valeurs par défaut.

e) Cliquez sur **Créer**.

3. Dans votre compartiment de stockage, sélectionnez **Charger des fichiers** et choisissez le fichier `connector-appliance.tar.gz`. Patientez pendant le chargement du fichier.
4. Sélectionnez le fichier téléchargé pour afficher ses détails. Copiez la valeur de l'**URI gsutil** dans le presse-papiers.
5. Ouvrez Cloud Shell en cliquant sur l'icône **Activer Cloud Shell** dans la barre d'en-tête.
6. Dans votre instance Cloud Shell, exécutez la commande suivante pour créer une image :

```
gcloud compute images create "Image name" --guest-os-features=
    MULTI_IP_SUBNET --source-uri="gsutil URI of uploaded connector-
    appliance.tar.gz file"
```

7. Dans le menu principal, sélectionnez **Compute Engine** > **Instances de VM**.
8. Sélectionnez **Créer une instance**. Dans le volet qui s'ouvre, spécifiez les informations suivantes :

   a) Dans le champ **Nom**, spécifiez un nom pour l'instance de Connector Appliance.
   b) Choisissez la région dans laquelle se trouve Connector Appliance.
   c) Choisissez la configuration de la machine.
   d) Dans la section **Disque de démarrage**, cliquez sur **Modifier**.
   e) Dans la section qui s'ouvre, accédez à l'onglet **Images personnalisées**.
   f) Dans la liste **Image**, sélectionnez l'image que vous avez créée.
   g) Cliquez sur **Sélectionner**.
   h) Dans la section **Pare-feu**, activez le trafic HTTPS pour autoriser l'accès à la page d'administration de Connector Appliance.
   i) Spécifiez toute configuration supplémentaire requise. Par exemple, il se peut que vous ne souhaitiez pas utiliser la configuration réseau par défaut.

   Cliquez sur **Créer**.
9. Dans la section **Instances de VM**, sélectionnez la machine virtuelle nouvellement créée pour afficher ses détails.

Une fois le Connector Appliance déployé et démarré avec succès, la section **Instances de VM** affiche les adresses IP de Connector Appliance.

Si le Connector Appliance dispose d'une adresse IP externe, vous pouvez utiliser cette adresse IP pour accéder à la page d'administration de Connector Appliance depuis votre navigateur et compléter le processus d'enregistrement.

Si le Connector Appliance n'a qu'une adresse IP interne, utilisez un hôte bastion pour accéder à la page d'administration de Connector Appliance depuis votre navigateur et compléter le processus d'

enregistrement. Pour en savoir plus, consultez https://cloud.google.com/compute/docs/connect/ssh-using-bastion-host.

Étape suivante : Enregistrer votre Connector Appliance avec Citrix Cloud

Déployer Connector Appliance à l'aide d'un script PowerShell Pour utiliser le script PowerShell fourni pour déployer Connector Appliance, le SDK Google Cloud doit être installé sur votre système.

1. Sur votre système local, extrayez le contenu de `connector-appliance-gcp.zip` dans un dossier.
2. Dans PowerShell, remplacez le répertoire par le dossier dans lequel se trouvent les fichiers extraits.
3. Exécutez la commande `.\connector-appliance-upload-GCP.ps1`.
4. Dans la fenêtre du navigateur qui s'ouvre, authentifiez-vous auprès du SDK Google Cloud avec un compte qui a accès au projet sur lequel vous souhaitez déployer Connector Appliance.
5. Dans Google Cloud Tools for PowerShell, lorsque le script PowerShell vous y invite, sélectionnez le projet à utiliser. Appuyez sur Entrée.
6. Suivez les invites du script qui vous guident tout au long du chargement du disque, de la création d'une image et de la création d'une machine virtuelle.
7. 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 Connector Appliance déployée et démarrée avec succès, le script affiche l'adresse IP interne de Connector Appliance. Vous pouvez également accéder à la console Google Cloud Platform pour trouver l'adresse IP interne de Connector Appliance. La section **Compute Engine** > **Instances de VM** affiche l'adresse IP de Connector Appliance.

Utilisez un hôte bastion pour accéder à la page d'administration du Connector Appliance à l'adresse IP interne de votre navigateur et complétez le processus d'enregistrement. Pour en savoir plus, consultez https://cloud.google.com/compute/docs/connect/ssh-using-bastion-host.

Étape suivante : Enregistrer votre Connector Appliance avec Citrix Cloud

Enregistrer votre Connector Appliance avec Citrix Cloud

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

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

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

   > **Remarque :**
   >
   > Vous devez inclure `https://` au début de l'adresse IP.

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

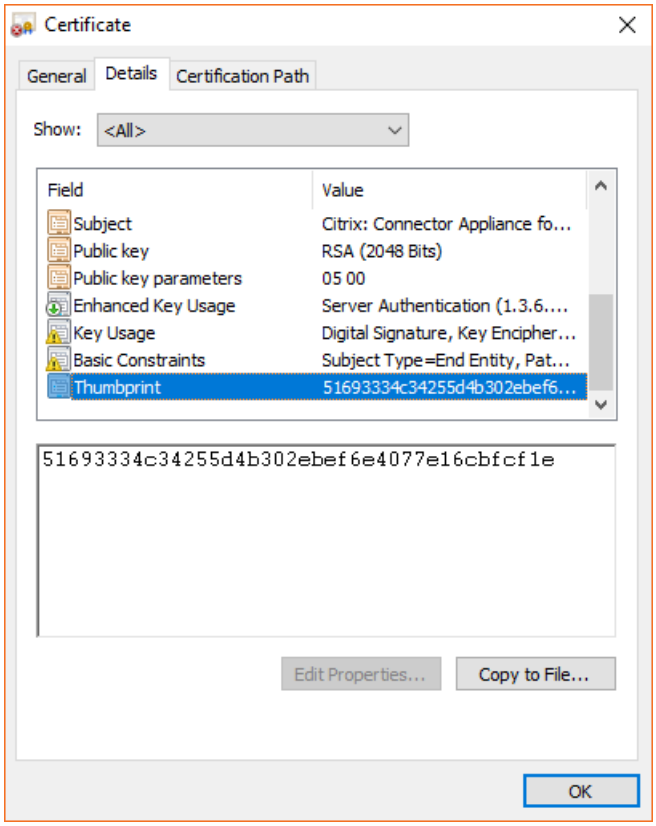
   Par exemple, dans le navigateur Google Chrome, procédez comme suit :

   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 Connector Appliance.

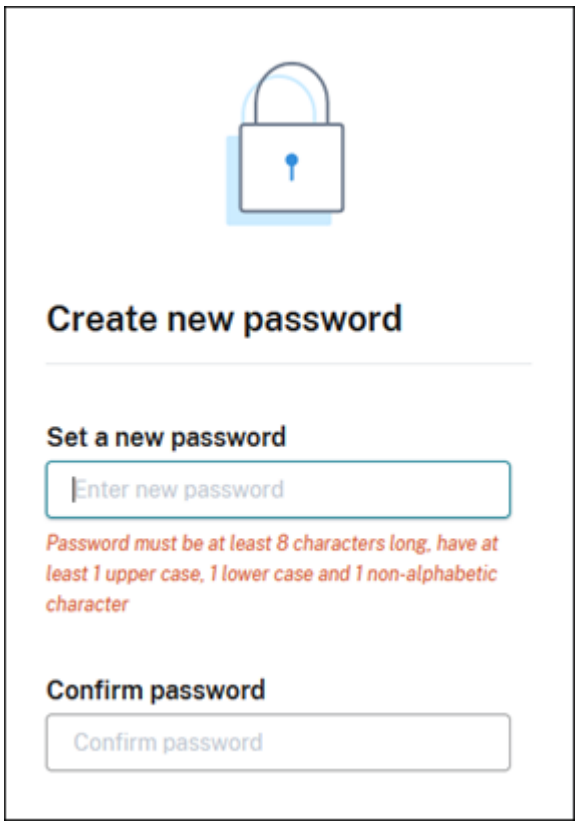


Vous pouvez remplacer ce certificat auto-signé par un des vôtres, signé par votre organisation ou généré à l'aide de la chaîne de confiance de votre organisation. Pour plus d'informations, consultez la section Gestion des certificats.

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 Connector Appliance et cliquez sur **Définir le mot de passe**.

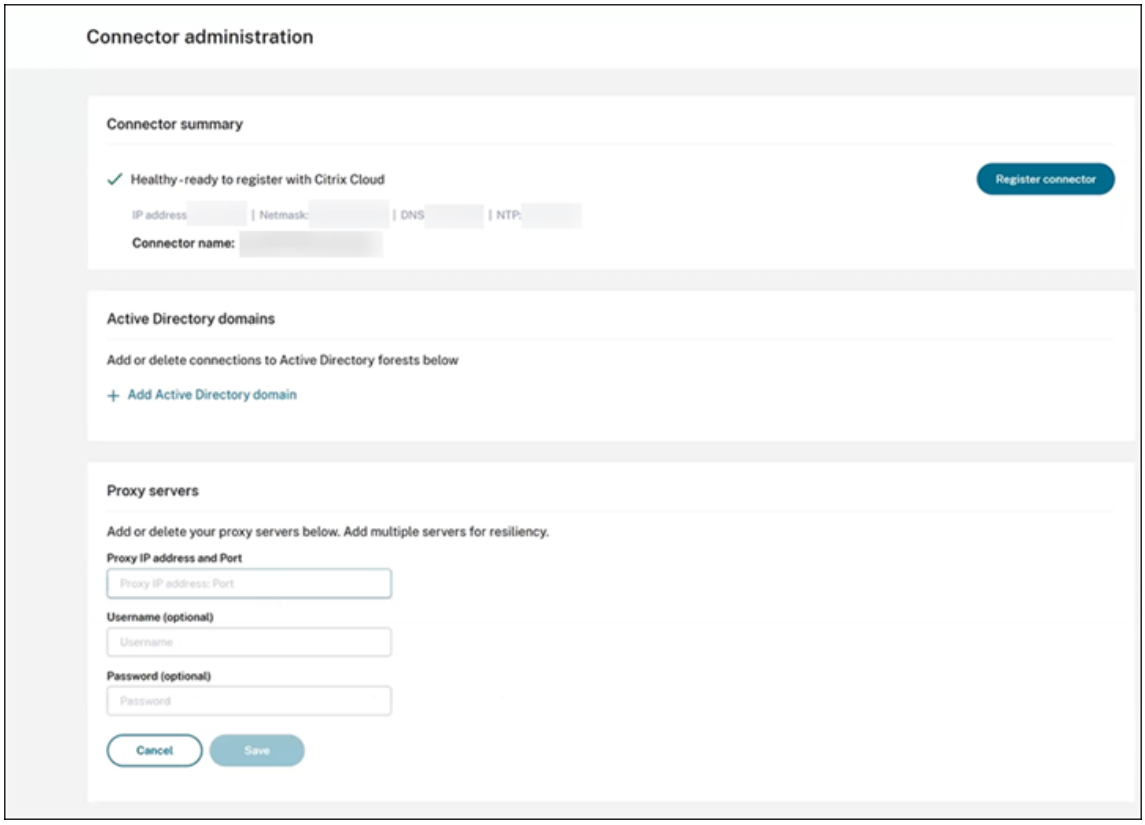


Le mot de passe que vous définissez doit répondre aux conditions suivantes :

- 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 avez défini. La page **Administration du Connector** s'ouvre.



5. (Facultatif) Si vous utilisez un ou plusieurs proxys Web, vous pouvez ajouter les adresses proxy dans la section **Serveurs proxy**. Les proxys non authentifiés et authentifiés sont pris en charge. Pour ajouter un proxy non authentifié, fournissez une **adresse IP et un port de proxy** valides. Pour ajouter un proxy authentifié, fournissez également un **nom d'utilisateur** et un **mot de passe** valides.

   > **Remarque :**
   >
   > Seule l'authentification proxy de base est prise en charge. Les autres formes d'authentification ne sont pas prises en charge.

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

6. (Facultatif) Si votre réseau utilise des proxys Web interceptant le protocole TLS pour accéder à Internet, vous pouvez demander à votre Connector de faire confiance à son autorité de certification racine pour communiquer avec le cloud.

   a) Sous **Autorités de certification racine**, sélectionnez **Ajouter un certificat**.

   b) Copiez le contenu du certificat au format PEM :

   ```
   1 -----BEGIN CERTIFICATE-----
   2 <certificate-base64-bytes>
   ```



```
-----END CERTIFICATE-----
<!--NeedCopy-->
```

c) Dans **Détails complets du certificat**, collez le contenu du certificat.

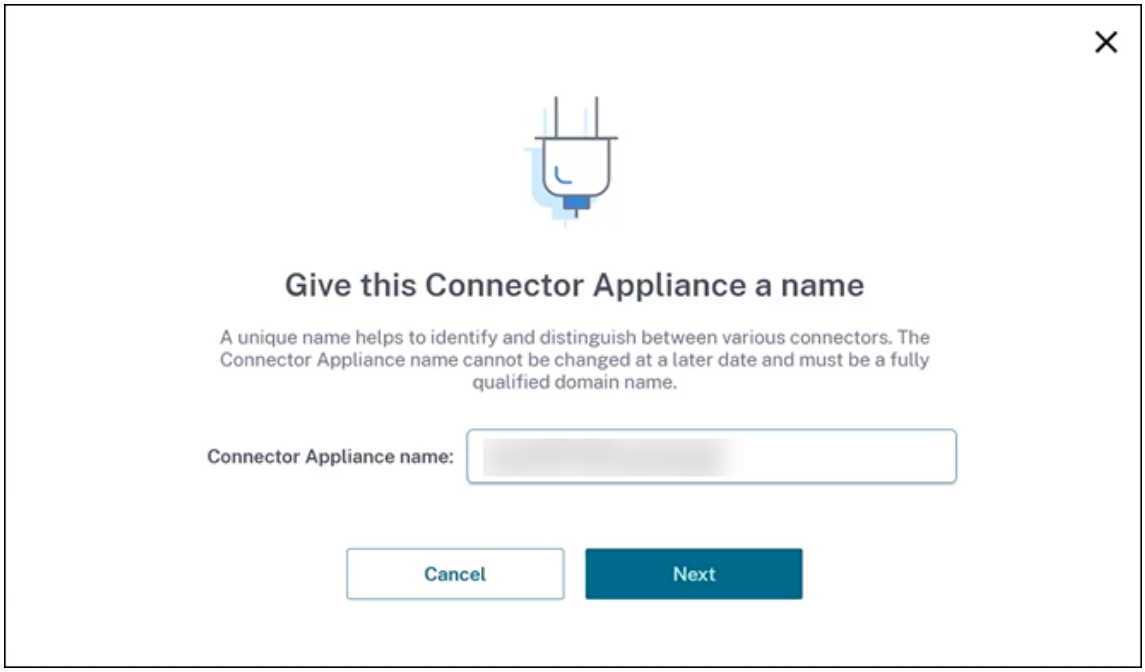
d) Sélectionnez **Ajouter un certificat**.

Pour ajouter un certificat RootCA à l'aide des API Connector Appliance, consultez l'article Managing root certificate authorities dans la documentation de Citrix Developer.

> **Remarque :**
>
> Les certificats qui ont expiré ou expireront dans les 30 prochains jours feront l'objet d'un avertissement.

7. Cliquez sur **Enregistrer Connector** pour ouvrir la tâche d'enregistrement.
8. Donnez un nom à votre Connector Appliance. Ce nom peut vous aider à distinguer les différentes appliances Connector qui existent dans votre emplacement de ressources. Après avoir enregistré votre Connector Appliance, le nom ne peut pas être modifié.

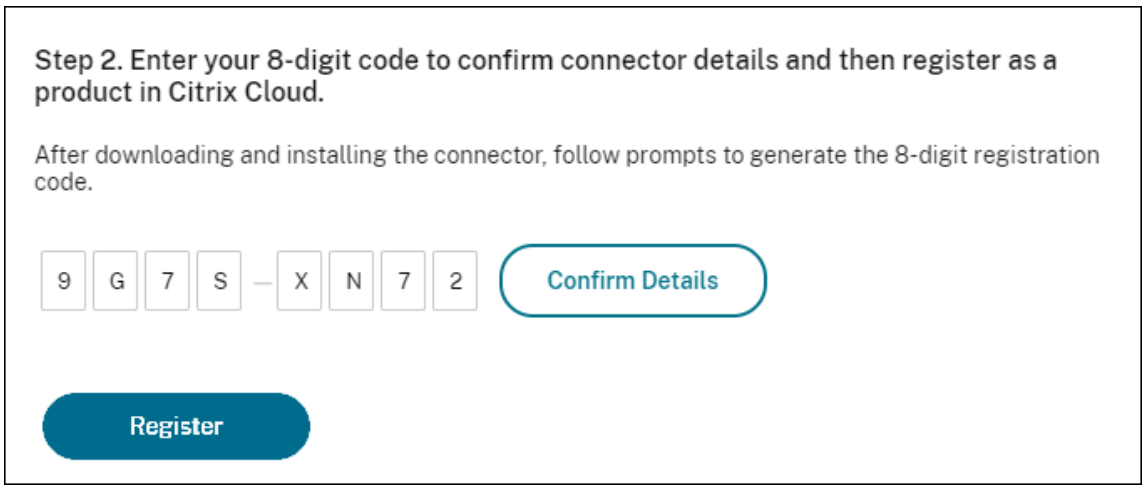
   Entrez le nom dans le champ **Nom de Connector Appliance**, puis cliquez sur **Suivant**.



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

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

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



12. Cliquez sur **Enregistrer**.

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

13. Cliquez sur **Fermer**.

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

Après avoir enregistré votre Connector Appliance

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 Connector Appliance.

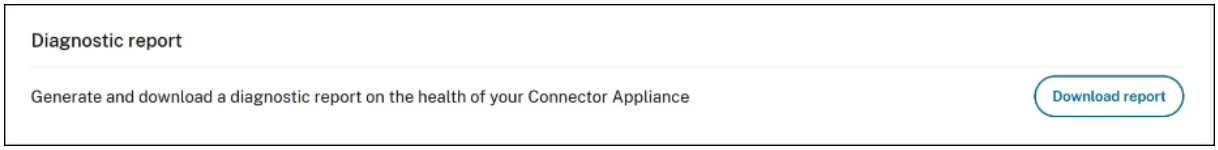
Connector Appliance est mise à jour automatiquement. Vous n'êtes pas obligé de prendre des mesures pour mettre à jour votre connecteur. Vous pouvez spécifier l'heure et le jour où les mises à jour de Connector Appliance doivent être appliquées à votre emplacement de ressources. Pour plus d'informations,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

Vous ne devez pas cloner, suspendre ou prendre un instantané de vos machines virtuelles de Connector Appliance. 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 Connector Appliance. Assurez-vous de stocker ce mot de passe dans un endroit sûr pour une utilisation future. Ce mot de passe ne peut pas être réinitialisé. Si vous oubliez le mot de passe, vous devez réinstaller le Connector Appliance. 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 Connector Appliance.

Génération d'un rapport de diagnostic

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



1. À partir de la console de Connector Appliance 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 Connector Appliance.
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`.

Vérifier votre connexion réseau

Vous pouvez vérifier votre connexion réseau à partir de la **page d'administration de Connector Appliance** en utilisant la vérification de diagnostic **Capture TCP**.

1. Sur la **page d'administration de Connector Appliance**, cliquez sur le nom de votre compte dans la barre d'en-tête et sélectionnez **Diagnostics réseau**.
2. (Facultatif) Dans la section **Capture TCP**, entrez l'adresse IP cible, le nom d'hôte ou le port pour restreindre la capture TCP.
3. Dans le menu **Durée du suivi**, sélectionnez la durée pendant laquelle vous souhaitez que votre suivi soit exécuté.
4. (Facultatif) Activez l'option **Suivi des paquets** pour capturer le contenu des paquets.

   Lorsque le suivi des paquets est désactivé, la fonctionnalité de capture TCP utilise une approche optimale pour capturer les en-têtes à des fins de diagnostic. Cette approche optimisée permet de capturer les 94 premiers octets de chaque paquet. Toutefois, comme les en-têtes n'ont pas une taille fixe, cette approche peut ne pas capturer la totalité de l'en-tête.
5. Cliquez sur **Démarrer le suivi**.
6. Attendez que le suivi soit terminé. Une fois le suivi terminé, vous pouvez télécharger un rapport de suivi ou en démarrer un nouveau.

   - Cliquez sur **Télécharger** pour télécharger le rapport de suivi. Le rapport de suivi est fourni dans un fichier `.pcap`.
   - Cliquez sur **Commencer un nouveau suivi** pour commencer un autre suivi.

Connection de Active Directory à Citrix Cloud

Vous pouvez utiliser des Connector Appliance pour connecter un emplacement de ressources à des forêts qui ne contiennent pas de ressources Citrix Virtual Apps and Desktops. Par exemple, dans le cas des clients Citrix Secure Private Access ou des clients Citrix Virtual Apps and Desktops dont certaines forêts sont uniquement utilisées pour l'authentification des utilisateurs.

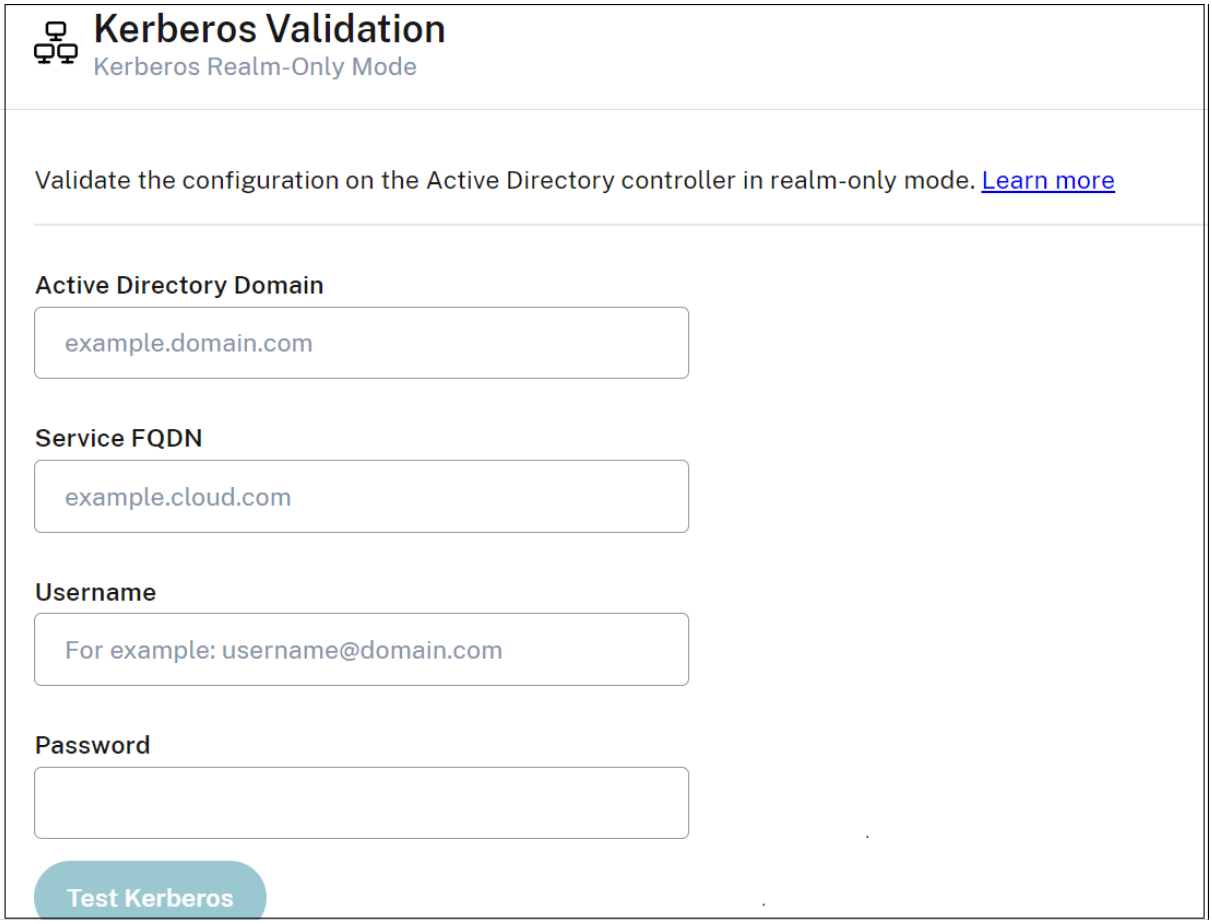
Pour plus d'informations, voir Active Directory avec Connector Appliance

Validation de votre configuration Kerberos

Si vous utilisez Kerberos pour l'authentification unique, vous pouvez vérifier que la configuration sur votre contrôleur Active Directory est correcte à partir de la **page d'administration de Connector Appliance**. La fonctionnalité de **validation Kerberos** vous permet de valider une configuration en mode domaine Kerberos uniquement ou une configuration en mode de délégation Kerberos contrainte (KCD).

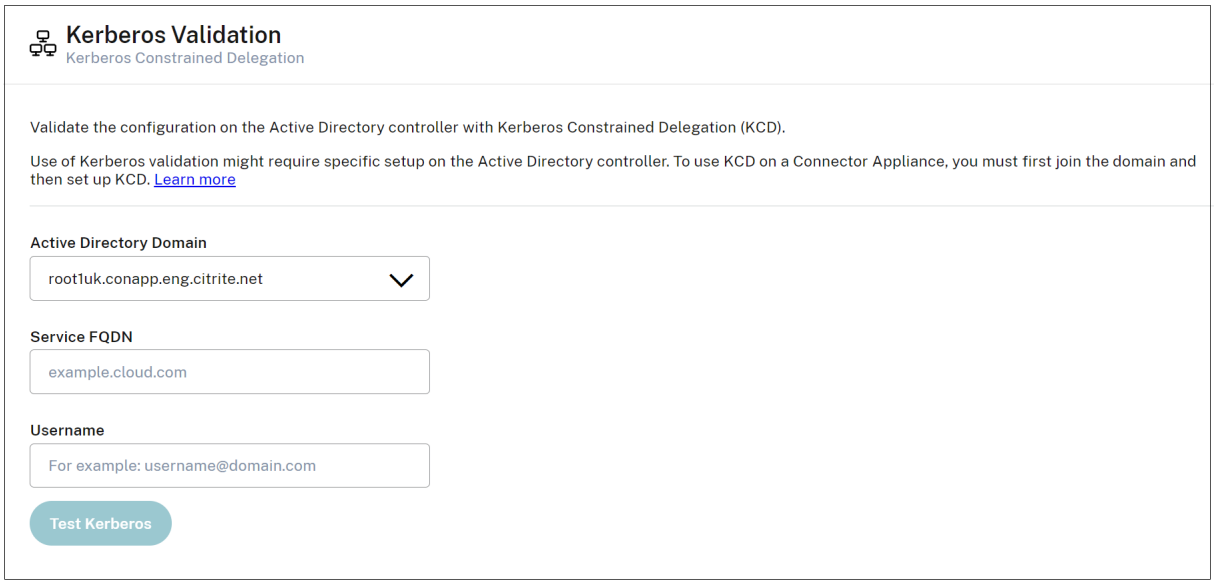
Validez la configuration en mode domaine Kerberos uniquement :

1. Accédez à la **page d'administration de Connector Appliance**.
2. À partir de la console de Connector Appliance de votre hyperviseur, copiez l'adresse IP dans la barre d'adresse de votre navigateur.
3. Entrez le mot de passe que vous avez défini lors de l'enregistrement de votre Connector Appliance.
4. Pour valider votre configuration en mode domaine Kerberos uniquement, sélectionnez **Mode de domaine unique de Kerberos** dans la section **Domaines Active Directory**.
5. Spécifiez le **domaine Active Directory**.
    - Si vous validez une configuration en mode domaine Kerberos uniquement, vous pouvez spécifier n'importe quel domaine Active Directory. Ce mode ne dépend pas de l'appartenance au domaine.
6. Spécifiez le **FQDN du service**. Le nom de service par défaut est supposé être « http ». Si vous spécifiez « ordinateur.exemple.com », celle valeur est considérée comme identique à « https://computer.example.com ».
7. Spécifiez le **nom d'utilisateur**.
8. Spécifiez le **mot de passe**.
9. Cliquez sur **Tester Kerberos**.



Validez la configuration de la délégation Kerberos contrainte (KCD) :

1. Accédez à la **page d'administration de Connector Appliance**.
2. Pour valider le mode **Délégation Kerberos contrainte (KCD)** pour les domaines auxquels Connector Appliance a été joint, sélectionnez **Validation Kerberos** dans le menu de points de suspension (…) du domaine concerné.
3. Spécifiez le **domaine Active Directory**.
    - Si vous validez une configuration de délégation Kerberos contrainte, vous devez sélectionner un domaine dans la liste des domaines joints.
4. Spécifiez le **FQDN du service**. Le nom de service par défaut est supposé être « http ». Par exemple, si vous spécifiez « ordinateur.exemple.com », celle valeur est considérée comme identique à « https://computer.example.com%E2%80%9D ».
5. Spécifiez le **nom d'utilisateur**.
    - Pour le mode de délégation Kerberos contrainte, vous pouvez également valider la configuration de Kerberos à l'aide de comptes de service en sélectionnant l'onglet **Comptes de service**.
6. Cliquez sur **Tester Kerberos**.



Si la configuration Kerberos est correcte, le message « Configuration de Kerberos validée avec succès » s'affiche. Si la configuration Kerberos n'est pas correcte, un message d'erreur s'affiche avec des informations sur la façon dont la validation a échoué.

Pour de plus amples informations sur Kerberos, veuillez consulter la documentation Microsoft.

Paramètres réseau de votre Connector Appliance

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

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

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

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

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

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, Connector Appliance redémarre. Pendant le redémarrage, Connector Appliance est temporairement indisponible. Vous êtes déconnecté de la **page d'administration de Connector Appliance** et l'URL de cette page change. Vous pouvez trouver la nouvelle URL dans la console de Connector Appliance 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, Connector Appliance redémarre. Pendant le redémarrage, Connector Appliance est temporairement indisponible. Vous êtes déconnecté de la **page d'administration de Connector Appliance** et l'URL de cette page change. Vous pouvez trouver la nouvelle URL dans la console de Connector Appliance ou en consultant les informations réseau de votre hyperviseur.

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

Par défaut, l'adresse IP et les paramètres réseau de votre Connector Appliance 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 Connector Appliance**, vous pouvez définir la configuration réseau directement sur la console de Connector Appliance.

Pour définir la configuration réseau, procédez comme suit :

1. Dans votre hyperviseur, redémarrez Connector Appliance.
2. Pendant le démarrage de Connector Appliance, 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>
     <!--NeedCopy-->
     ```

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

6. Appuyez sur **Ctrl+X** pour démarrer Connector Appliance avec la nouvelle configuration.

Modifier le mot de passe utilisateur administrateur pour le Connector Appliance

1. Dans le menu utilisateur en haut à droite de la console, sélectionnez **Modifier le mot de passe**.

   ![Sélectionnez Modifier le mot de passe dans le menu](/en-us/citrix-cloud/media/connector-appliance-change-pw-menu.png)

   La page de modification du mot de passe s'affiche.

   ![Atterrissage sur la page de modification du mot de passe](/en-us/citrix-cloud/media/connector-appliance-change-pw-page.png)

2. Entrez votre mot de passe actuel, puis saisissez et confirmez le nouveau mot de passe. Le nouveau 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
- Ne doit pas être identique au mot de passe actuel

3. Sélectionnez **Modifier le mot de passe** pour enregistrer vos modifications.

Citrix Cloud vous déconnecte automatiquement et vous redirige vers la page de connexion.

Active Directory avec Connector Appliance

April 5, 2024

Vous pouvez utiliser des Connector Appliance pour connecter un emplacement de ressources à des forêts qui ne contiennent pas de ressources Citrix Virtual Apps and Desktops. Par exemple, dans le cas des clients Citrix Secure Private Access ou des clients Citrix Virtual Apps and Desktops dont certaines forêts sont uniquement utilisées pour l'authentification des utilisateurs.

Lors de l'utilisation d'Active Directory multi-domaines avec Connector Appliance, les restrictions suivantes s'appliquent :

- Connector Appliance ne peut pas être utilisé à la place de Cloud Connector dans les forêts contenant des VDA.

Exigences

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 plus d'informations, consultez Scénarios de déploiement d'appliances Connector dans Active Directory dans cet article.
- Chaque forêt Active Directory que vous prévoyez d'utiliser avec Citrix Cloud doit toujours être accessible par deux appliances Connector.
- Connector Appliance 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 l'article Vue d'ensemble du service et exigences relatives aux ports réseau pour Windows

- Utilisez des groupes de sécurité universels au lieu de groupes de sécurité globaux. Cette configuration garantit que l'appartenance au groupe d'utilisateurs peut être obtenue auprès de n'importe quel contrôleur de domaine de la forêt.

Configuration réseau requise

- Être connectée à un réseau qui peut contacter les ressources que vous utilisez dans votre emplacement de ressources.
- Être connectés à Internet. Pour plus d'informations, consultez la section Configuration requise pour le système et la connectivité.

Outre les ports répertoriés dans la section Communication de Connector Appliance, le Connector Appliance nécessite une connexion sortante au domaine Active Directory via les ports suivants :

Service	Port	Protocoles de domaine pris en charge
Kerberos	88	TCP/UDP
Mappeur de points finaux (service de localisation DCE/RPC)	135	TCP
Service de noms NetBIOS	137	UDP
Datagramme NetBIOS	138	UDP
Session NetBIOS	139	TCP
LDAP	389	TCP/UDP
SMB sur TCP	445	TCP
Kerberos kpasswd	464	TCP/UDP
Global Catalog	3268	TCP
Ports RPC dynamiques	49152–65535	TCP

Le Connector Appliance utilise la signature LDAP pour sécuriser les connexions au contrôleur de domaine. Cela signifie que LDAP sur SSL (LDAPS) n'est pas nécessaire. Pour plus d'informations sur la signature LDAP, consultez Comment activer la signature LDAP dans Windows Server et Instructions de Microsoft concernant l'activation de la liaison de canaux LDAP et la signature LDAP.

Niveaux fonctionnels Active Directory pris en charge

Connector Appliance a été testé et est pris en charge avec les niveaux fonctionnels de forêt et de domaine suivants dans Active Directory.

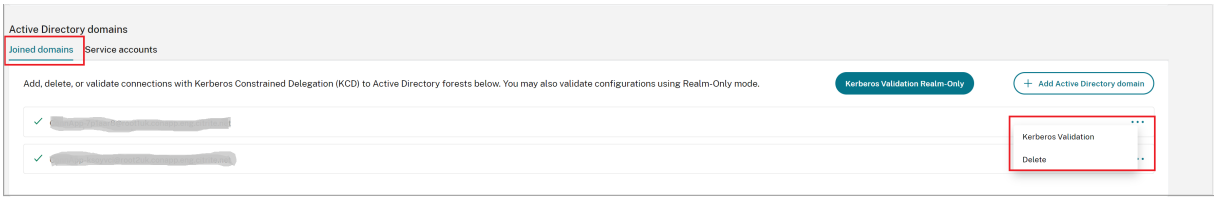
Niveau fonctionnel de la forêt	Niveau fonctionnel du domaine	Contrôleurs de domaine pris en charge
Windows Server 2016	Windows Server 2016	Windows Server 2019

Les autres combinaisons de contrôleur de domaine, de niveau fonctionnel de forêt et de niveau fonctionnel de domaine n'ont pas été testées avec Connector Appliance. Toutefois, ces combinaisons devraient fonctionner et sont également prises en charge.

Connexion d'un domaine Active Directory à Citrix Cloud à l'aide de Connector Appliance (version préliminaire)

Lorsque vous vous connectez à la page Web d'administration de Connector Appliance, la section des domaines Active Directory affiche deux onglets.

- **Domaines joints** : cette configuration est utilisée pour associer Connector Appliance à des domaines AD en créant un compte de machine pour l'appliance dans le domaine. Kerberos peut être validé en cliquant sur le menu de points de suspension sur le côté droit du domaine joint. La présence d'un compte de machine dans le domaine est requise.
- **Comptes de service** : cette configuration est utilisée dans le cadre d'une solution Secure Private Access (SPA) pour obtenir l'authentification unique Kerberos à l'aide d'un compte de service au lieu du compte de machine créé en joignant le domaine. Kerberos peut être validé en cliquant sur le menu de points de suspension sur le côté droit du compte de service. Il n'est pas obligatoire d'associer un domaine spécifique à la machine. Toutefois, même si l'entité Connector Appliance n'est pas connectée au domaine, elle peut toujours se connecter au contrôleur de domaine.



Pour configurer Active Directory pour la connexion à Citrix Cloud via Connector Appliance, procédez comme suit.

1. Installez un Connector Appliance dans votre emplacement de ressources.

   Vous pouvez suivre les informations de la documentation produit de Connector Appliance.

2. Connectez-vous à la page Web d'administration de Connector Appliance dans votre navigateur à l'aide de l'adresse IP fournie dans la console de Connector Appliance.
3. Dans la section **Domaines Active Directory**, accédez à l'onglet **Domaines joints**.
4. Cliquez sur **+ Ajouter un domaine Active Directory** ; une nouvelle fenêtre contextuelle s'affiche pour saisir le nom de domaine.

   Connector Appliance vérifie le domaine. Si la vérification réussit, la boîte de dialogue **Joindre Active Directory** s'ouvre. Cette nouvelle fenêtre vous permet de saisir le nom d'utilisateur et le mot de passe pour joindre le domaine.

5. Cliquez sur **Ajouter**.
6. Fournissez le nom d'utilisateur et le mot de passe d'un utilisateur Active Directory autorisé à joindre le domaine.
7. Connector Appliance suggère un nom de machine. Vous pouvez choisir de remplacer le nom suggéré et de fournir votre propre nom de machine, d'une longueur maximale de 15 caractères.

   Ce nom de machine est créé dans le domaine Active Directory lorsque Connector Appliance le rejoint.

8. Cliquez sur **Joindre**.

   Le domaine est désormais répertorié dans la section **Domaines Active Directory** de l'interface utilisateur Appliance Connector.

9. Pour ajouter d'autres **domaines Active Directory**, sélectionnez **+ Ajouter un domaine Active Directory** et répétez les étapes précédentes.
10. Accédez à la page des domaines dans la **console Citrix Cloud** et sélectionnez **Connector Appliance** pour gérer vos domaines.
11. Si vous n'avez pas encore enregistré votre Connector Appliance, poursuivez avec les étapes décrites dans Enregistrer votre Connector Appliance auprès de Citrix Cloud.

Si vous recevez un message d'erreur lorsque vous rejoignez le domaine, vérifiez que votre environnement répond aux exigences d'Active Directory et aux exigences de réseau.

Prochaine étape

- Vous pouvez ajouter d'autres domaines à cette Connector Appliance.

  > **Remarque :**
  >
  > Connector Appliance est testé avec jusqu'à 10 forêts.

- Pour des raisons de résilience, ajoutez chaque domaine à plusieurs appliances Connector dans chaque emplacement de ressources.

Affichage de votre configuration Active Directory

Vous pouvez afficher la configuration des domaines Active Directory et des appliances Connector dans vos emplacements de ressources aux endroits suivants :

- Dans Citrix Cloud :

  1. Dans le menu, accédez à la page **Gestion des identités et des accès** .
  2. Accédez à l'onglet **Domaines**.

     Vos domaines Active Directory sont répertoriés avec les emplacements de ressources dont ils font partie.

- Sur la page Web de Connector Appliance :

  1. Connectez-vous à la page Web de Connector Appliance à l'aide de l'adresse IP fournie dans la console de Connector Appliance.
  2. Connectez-vous avec le mot de passe que vous avez créé lors de votre inscription initiale.
  3. Dans la section **Domaines Active Directory** de la page, vous pouvez voir la liste des domaines Active Directory auxquels cette Connector Appliance est jointe.

Suppression d'un domaine Active Directory d'un Connector Appliance

Pour quitter un domaine Active Directory, procédez comme suit :

1. Connectez-vous à la page Web de Connector Appliance à l'aide de l'adresse IP fournie dans la console de Connector Appliance.
2. Connectez-vous avec le mot de passe que vous avez créé lors de votre inscription initiale.

3. Dans la section **Domaines Active Directory** de la page, recherchez le domaine que vous souhaitez quitter dans la liste des domaines Active Directory joints.
4. Notez le nom du compte de machine créé par votre Connector Appliance.
5. Cliquez sur l'icône Supprimer (corbeille) en regard du domaine. Un dialogue de confirmation s'affiche.
6. Cliquez sur **Continuer** pour confirmer l'action.
7. Accédez à votre contrôleur Active Directory.
8. Supprimez le compte de machine créé par votre Connector Appliance du contrôleur.

Scénarios de déploiement pour l'utilisation de Connector Appliance avec Active Directory

Vous pouvez utiliser à la fois un Cloud Connector et un Connector Appliance pour vous connecter aux contrôleurs Active Directory. Le type de connecteur à utiliser dépend de votre déploiement.

Pour plus d'informations sur l'utilisation de Cloud Connector avec Active Directory, consultez la section Scénarios de déploiement de Cloud Connector dans Active Directory.

Utilisez Connector Appliance pour connecter votre emplacement de ressources à la forêt Active Directory dans les situations suivantes :

- Vous configurez Secure Private Access. Pour plus d'informations, consultez Secure Private Access avec Connector Appliance.
- Vous avez une ou plusieurs forêts qui ne sont utilisées que pour l'authentification des utilisateurs
- Vous souhaitez réduire le nombre de connecteurs nécessaires pour prendre en charge plusieurs forêts
- Vous avez besoin d'un connecteur pour d'autres cas d'utilisation

Uniquement les utilisateurs d'une ou plusieurs forêts avec un seul ensemble d'appliances de connexion pour toutes les forêts

Ce scénario s'applique aux clients Workspace Standard ou aux clients utilisant des appliances Connector pour Secure Private Access.

Dans ce scénario, plusieurs forêts ne contiennent que des objets utilisateur (`forest1.local`, `forest2.local`). Ces forêts ne contiennent pas de ressources. Un ensemble d'appliances Connector est déployé dans un emplacement de ressources et joint aux domaines de chacune de ces forêts.

- Relation d'approbation : Aucune

- 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

Utilisateurs et ressources dans des forêts distinctes (avec approbation) avec un seul groupe d'appliances de connecteur pour toutes les forêts

Ce scénario s'applique aux clients Citrix Virtual Apps and Desktops possédant plusieurs forêts.

Dans ce scénario, certaines forêts (`resourceforest1.local`, `resourceforest2.local`) contiennent vos ressources (par exemple, des VDA) et certaines forêts (`userforest1.local`, `userforest2.local`) contiennent uniquement vos utilisateurs. Il existe entre ces forêts une approbation qui permet aux utilisateurs de se connecter aux ressources.

Un groupe de Cloud Connector est déployé dans la forêt `resourceforest1.local`. Un groupe distinct de Cloud Connector est déployé dans la forêt `resourceforest2.local`.

Un groupe d'appliances Connector est déployé dans la forêt `userforest1.local` et le même groupe est déployé dans la forêt `userforest2.local`.

- Relation d'approbation : approbation de forêt bidirectionnelle, ou approbation unidirectionnelle entre les forêts de ressources et les forêts d'utilisateurs
- Domaines répertoriés dans **Gestion des identités et des accès** : `resourceforest1.local`, `resourceforest2.local`, `userforest1.local`, `userforest2.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

Mises à jour de Connector

August 3, 2023

Citrix publie périodiquement des mises à jour pour améliorer les performances, la sécurité et la fiabilité du Cloud Connector ou du Connector Appliance. Par défaut, Citrix Cloud installe les mises à jour sur chaque connecteur, une par une, dès qu'elles sont disponibles. Pour garantir que les mises à jour sont installées en temps opportun sans affecter indûment l'expérience Citrix Cloud de vos utilisateurs, vous pouvez contrôler les mises à jour des connecteurs comme suit :

- Planifiez les mises à jour à l'heure et au jour de la semaine que vous préférez.
- Configurez un délai unique afin que les connecteurs que vous spécifiez soient mis à jour deux semaines plus tard que prévu.

- Si une mise à jour échoue en raison d'un problème sur la machine hôte, redémarrez la mise à jour une fois le problème résolu.

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.

> **Remarque :**
>
> Cet article explique comment planifier les mises à jour des connecteurs à l'aide de la console de gestion Citrix Cloud. Pour plus d'informations sur la planification des mises à jour des connecteurs à l'aide des API Citrix Cloud, consultez Citrix Cloud - Maintenance Schedules dans la documentation Citrix Developer.

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 la section Notifications. En outre, chaque connecteur affiche la date et l'heure auxquelles la mise à jour sera installée.

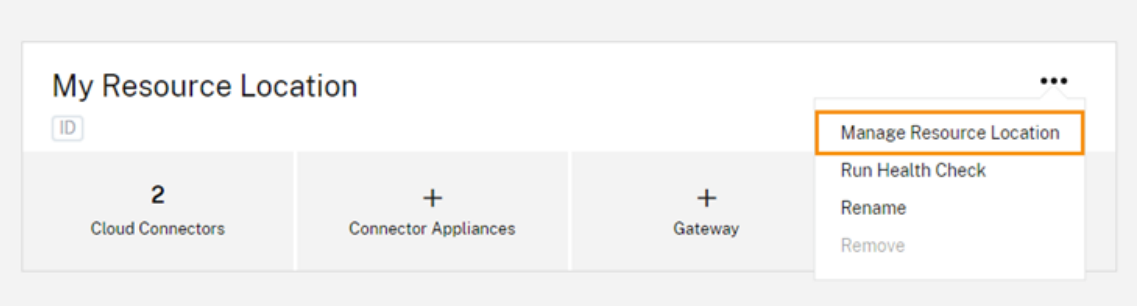
Une fois que Citrix Cloud vous informe d'une mise à jour disponible, chaque connecteur affiche un bouton **Mise à jour** afin que vous puissiez installer la mise à jour plus tôt que votre heure ou jour préféré(e). Après avoir sélectionné **Mettre à jour** pour chaque connecteur, Citrix Cloud met en file 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

Suivez les étapes décrites dans cette section pour planifier les mises à jour des connecteurs via la console de gestion Citrix Cloud. Pour plus d'informations sur la planification des mises à jour à l'aide des API Citrix Cloud, consultez Citrix Cloud - Maintenance Schedules dans la documentation Citrix Developer.

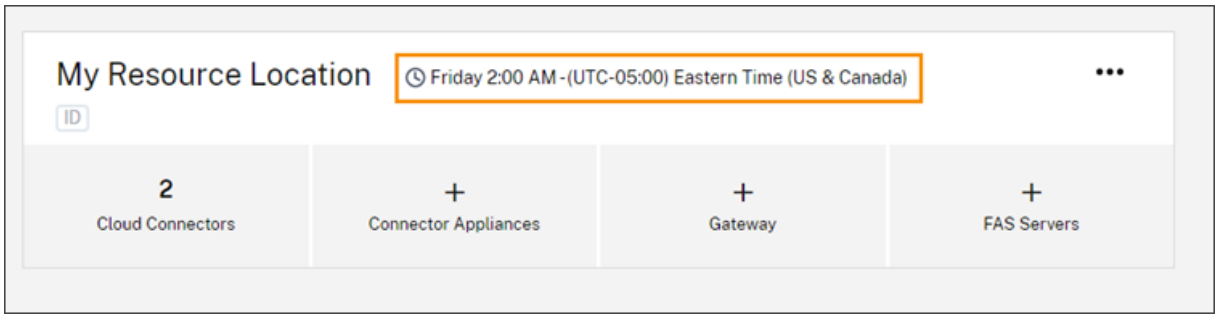
1. Dans le menu Citrix Cloud, sélectionnez **Emplacements des ressources**.
2. Recherchez l'emplacement de ressources à modifier et, dans le menu des points de suspension, sélectionnez **Gérer l'emplacement des ressources**.



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.

Redémarrer les mises à jour

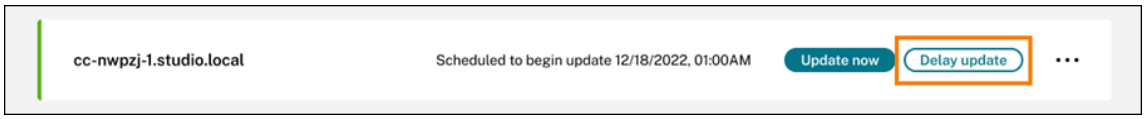
Si le connecteur rencontre un problème lors de l'installation de la mise à jour, l'installation s'interrompt jusqu'à ce que le problème soit résolu. Étant donné que les mises à jour sont installées sur chaque connecteur, une à la fois, une mise à jour interrompue sur un connecteur peut empêcher les mises à jour sur tous les Cloud Connector restants de votre compte Citrix Cloud. Une fois le problème résolu, vous pouvez redémarrer la mise à jour.

1. Dans le menu Citrix Cloud, sélectionnez **Emplacements des ressources**.
2. Localisez l'emplacement de ressources que vous souhaitez gérer et sélectionnez la vignette **Cloud Connector** ou **Connector Appliance**.
3. Localisez le connecteur que vous souhaitez gérer et sélectionnez **Redémarrer les mises à jour**.

Retarder les mises à jour

Vous pouvez retarder une mise à jour planifiée afin qu'elle ait lieu deux semaines plus tard pour les connecteurs que vous spécifiez. Vous ne pouvez retarder une mise à jour planifiée qu'une seule fois. Après avoir retardé la mise à jour une fois, vous ne pouvez pas la retarder à nouveau. Vous ne pouvez pas non plus modifier la période de deux semaines par défaut.

1. Dans le menu Citrix Cloud, sélectionnez **Emplacements des ressources**.
2. Localisez l'emplacement de ressources que vous souhaitez gérer et sélectionnez la vignette **Cloud Connector** ou **Connector Appliance**.
3. Localisez le connecteur que vous souhaitez gérer et sélectionnez **Retarder les mises à jour**.

   La date planifiée est remplacée par une date postérieure de deux semaines à la date initialement prévue.

Mises à jour non planifiées

Même si vous planifiez des mises à jour pour une date et une heure ultérieures, Citrix Cloud peut tout de même installer une mise à jour dès que possible après qu'elle devient disponible. Les mises à jour non planifiées se produisent lorsque :

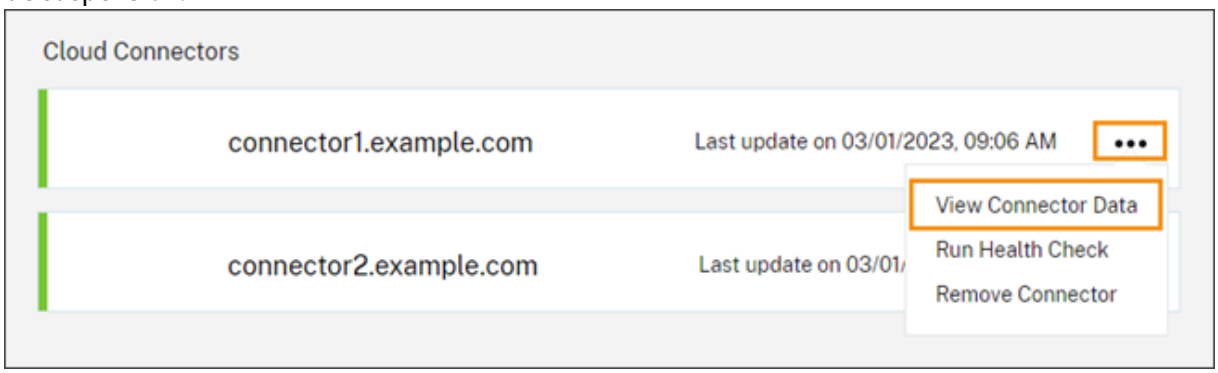
- La mise à jour ne peut pas être installée à l'heure préférée dans les 48 heures suivant sa publication. Par exemple, si votre heure préférée est 2h00 du matin et que le connecteur est hors connexion pendant trois jours suivant la mise à jour, Citrix Cloud installe la mise à jour dès que le connecteur 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

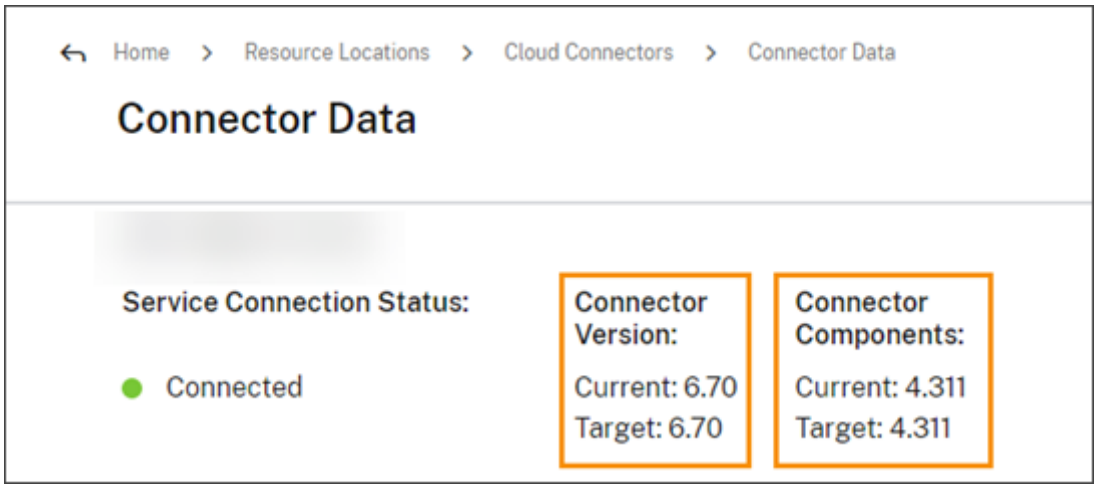
Vous pouvez vérifier la version du Cloud Connector qui s'exécute dans votre emplacement de ressources et s'il s'agit de la dernière version. Ces informations vous aident à vérifier que le Cloud Connector est correctement mis à jour.

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

Dans la page **Emplacements des ressources**, sélectionnez la vignette **Cloud Connector** pour l'emplacement de ressources que vous souhaitez gérer. Localisez le Cloud Connector que vous souhaitez examiner et sélectionnez **Afficher les données du connecteur** dans le menu des points de suspension.



Le numéro de version **En cours** correspond à la version du logiciel Cloud Connector en cours d'exécution sur la machine Cloud Connector. Le numéro de version **Cible** correspond à la dernière version du logiciel Cloud Connector que Citrix a publié. Si la machine a été mise à jour avec succès, les numéros de version En cours et Cible correspondent.



Résolution des échecs de mise à jour

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.

Si la mise à jour du Cloud Connector n'a pas réussi, vous pouvez commencer à résoudre les problèmes en vérifiant les conditions suivantes :

- Utilisez l'utilitaire Cloud Connector Connectivity Check pour vérifier que le Cloud Connector est sous tension et connecté à Citrix Cloud.
- Le proxy et les pare-feu sont configurés correctement.
- Les services Windows requis sont affichés dans l'état Démarré.
- La journalisation avancée est activée sur Cloud Connector.

Pour obtenir des instructions sur la résolution des échecs de mise à jour de Cloud Connector, consultez CTX270718 dans le Centre de connaissances Citrix.

Pour obtenir de l'aide, vous pouvez envoyer les journaux Citrix Cloud Connector à Citrix. Pour plus d'informations, consultez Collecte de journaux pour Citrix Cloud Connector.

Gestion des identités et des accès

July 2, 2024

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

Les fournisseurs d'identité pris en charge pour Citrix Cloud peuvent être utilisés pour authentifier les administrateurs Citrix Cloud, les abonnés à l'espace de travail ou les deux.

Fournisseur d'identité	Authentification des administrateurs	Authentification des abonnés
Fournisseur d'identité Citrix	Oui	Non
Active Directory local	Non	Oui
Active Directory + jeton	Non	Oui

Fournisseur d'identité	Authentification des administrateurs	Authentification des abonnés
Azure Active Directory	Oui	Oui
Citrix Gateway	Non	Oui
Google Cloud Identity	Oui	Oui
Okta	Non	Oui
SAML 2.0	Oui (groupes AD uniquement)	Oui

Par défaut, Citrix Cloud utilise le fournisseur d'identité Citrix pour gérer votre compte Citrix Cloud. Le fournisseur d'identité Citrix authentifie uniquement les administrateurs Citrix Cloud.

Fournisseur d'identité Citrix

Citrix Cloud inclut le fournisseur d'identité Citrix intégré pour authentifier les administrateurs lorsqu'ils se connectent. Dans la console Citrix Cloud, le fournisseur d'identité Citrix est intitulé Citrix Identity.
Si vous utilisez un autre fournisseur d'identité pour l'authentification des administrateurs, Citrix recommande d'avoir au moins un administrateur à accès complet sous le **fournisseur d'identité Citrix**. Cette condition garantit que :

- L'accès à votre compte Citrix Cloud ne sera pas bloqué si votre fournisseur d'identité principal devient indisponible.
- Vous pouvez accéder à votre compte Citrix Cloud pour effectuer certaines opérations qui ne peuvent pas être effectuées lorsque vous êtes connecté sous un autre fournisseur d'identité, tel qu'Azure AD. Par exemple, si Azure AD est le fournisseur d'identité que vous avez sélectionné et que vous devez rétablir la connexion entre votre Azure AD et Citrix Cloud, vous pouvez effectuer cette tâche après vous être connecté à l'aide du fournisseur d'identité Citrix.

Supprimer le fournisseur d'identité Citrix

Le fournisseur d'identité Citrix est connecté par défaut pour tous les nouveaux comptes Citrix Cloud. Si vous choisissez de ne pas utiliser le fournisseur d'identité Citrix, vous pouvez supprimer la connexion, si nécessaire. Par exemple, vous pouvez choisir de supprimer cette connexion pour vous conformer aux stratégies de sécurité et de gestion des administrateurs de votre organisation.

La suppression de cette connexion désactive le fournisseur d'identité Citrix. Il ne peut donc pas être utilisé pour authentifier les administrateurs Citrix Cloud.

Pour pouvoir supprimer la connexion au fournisseur d'identité Citrix, un autre fournisseur d'identité doit être configuré dans Citrix Cloud. Citrix Cloud ne vous permet pas de supprimer cette connexion sans la présence d'un autre fournisseur d'identité configuré.

> **Important**
>
> Si vous perdez l'accès au fournisseur d'identité que vous avez choisi, vous devez contacter le support Citrix pour récupérer votre compte Citrix Cloud. Ce processus peut prendre plusieurs jours.

Pour supprimer la connexion au fournisseur d'identité Citrix, procédez comme suit :

1. Dans le menu Citrix Cloud, sélectionnez **Gestion des identités et des accès**.
2. Dans l'onglet **Authentification**, localisez le fournisseur d'identité Citrix.
3. Cliquez sur le menu des points de suspension et sélectionnez **Supprimer le fournisseur d'identité**.

4. Lorsque vous êtes invité à confirmer la suppression, sélectionnez **Je comprends que la suppression de ce fournisseur d'identité supprime également les données de configuration de ce fournisseur d'identité dans Citrix Cloud**.
5. Cliquez sur **Supprimer le fournisseur d'identité**.

Service d'authentification fédérée de Citrix

Citrix Cloud prend également en charge l'utilisation du Service d'authentification fédérée Citrix pour fournir l'authentification unique aux abonnés à l'espace de travail. Pour plus d'informations, consultez les articles suivants :

- Connecter FAS à Citrix Cloud : Activer l'authentification unique pour les espaces de travail avec Service d'authentification fédérée de Citrix
- Citrix Tech Zone :
  - Architecture de référence : Service d'authentification fédérée
  - Tech Insight : Service d'authentification fédérée

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.

Authentification multifacteur

Citrix Cloud fournit des méthodes d'authentification multifacteur pour les administrateurs et les abonnés à l'espace de travail.

Pour les administrateurs, l'authentification multifacteur est requise lors de la connexion à Citrix Cloud. Les administrateurs peuvent inscrire leur appareil lorsqu'ils intègrent leur compte Citrix Cloud ou après avoir accepté l'invitation d'un autre administrateur. Pour plus d'informations, consultez les articles suivants :

- Configurer l'authentification multifacteur
- Gérer votre méthode de MFA principale
- Gérer vos méthodes de récupération de MFA

Pour les abonnés à l'espace de travail, l'authentification multifacteur est activée lorsque les administrateurs configurent la méthode d'authentification Active Directory + jeton. Active Directory + jeton est le fournisseur d'identité par défaut pour Citrix Workspace. Après la configuration, les abonnés inscrivent leur appareil à l'authentification multifacteur. Pour plus d'informations, consultez les articles suivants :

- Activer l'authentification Active Directory + jeton
- Inscrire un appareil pour l'authentification à deux facteurs
- Réinscrire un appareil

Vous pouvez également utiliser l'authentification multifacteur Azure AD pour les administrateurs Citrix Cloud et les abonnés à l'espace de travail. Pour plus d'informations sur les méthodes de déploiement, consultez la section Microsoft Azure MFA deployment methods.

Ajouter de nouveaux administrateurs

Lors du processus de création d'un compte, un administrateur initial est créé. En tant qu'administrateur initial, vous pouvez ajouter d'autres administrateurs à votre compte 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 ajoutez. La définition de ces autorisations vous permet d'aligner le niveau d'accès avec le rôle de l'administrateur dans votre organisation.

Pour plus d'informations sur l'ajout d'administrateurs et la définition des autorisations d'accès, consultez Gérer l'accès des administrateurs.

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 dans 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 une 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 continuent 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 de Citrix.

Emplacements de ressources principaux

Un emplacement de ressources principal est un emplacement de ressources que vous désignez comme étant « l'emplacement préféré » pour les communications entre votre domaine et Citrix Cloud. Pour définir vos emplacements de ressources principaux, sélectionnez l'emplacement de ressources qui dispose du composant Citrix Cloud Connector offrant les meilleures performances et la meilleure connectivité à votre domaine. La définition de cet emplacement de ressources en tant qu'emplacement de ressources principal permet à vos utilisateurs de se connecter rapidement à Citrix Cloud.

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

Informations supplémentaires

- Apprenez-en plus sur les fournisseurs d'identité pris en charge avec le cours de formation Introduction to Citrix Identity and Authentication. sur le site web Citrix Training.
- Citrix Tech Zone :
  - Fiche technique : Identité Workspace
  - Fiche technique : Authentification unique pour Workspace
  - Tech Insight : Authentification unique mobile

Gérer l'accès des administrateurs à Citrix Cloud

April 5, 2024

Les administrateurs sont gérés à partir de la console Citrix Cloud. En fonction du fournisseur d'identité que vous utilisez pour authentifier les administrateurs, vous pouvez ajouter des administrateurs individuellement ou en utilisant des groupes.

Tous les administrateurs sont tenus d'utiliser des jetons comme deuxième facteur d'authentification lors de la connexion à Citrix Cloud. Après avoir été ajouté un administrateur, celui-ci peut inscrire son 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.

Ajouter de nouveaux administrateurs

Citrix Cloud prend en charge les fournisseurs d'identité suivants pour authentifier les administrateurs :

- Fournisseur d'identité Citrix : fournisseur d'identité par défaut dans Citrix Cloud. Prend uniquement en charge l'ajout d'administrateurs individuels.
- Azure AD : prend en charge l'ajout d'administrateurs individuellement et par le biais de groupes AAD. Les administrateurs des groupes AAD sont limités aux rôles d'accès personnalisés uniquement. Pour plus d'informations, consultez Gérer les groupes d'administrateurs.
- SAML 2.0 : prend en charge l'ajout d'administrateurs uniquement via des groupes AD. Pour plus d'informations, consultez Connecter SAML en tant que fournisseur d'identité à Citrix Cloud.

L'ajout de nouveaux administrateurs utilise le workflow suivant :

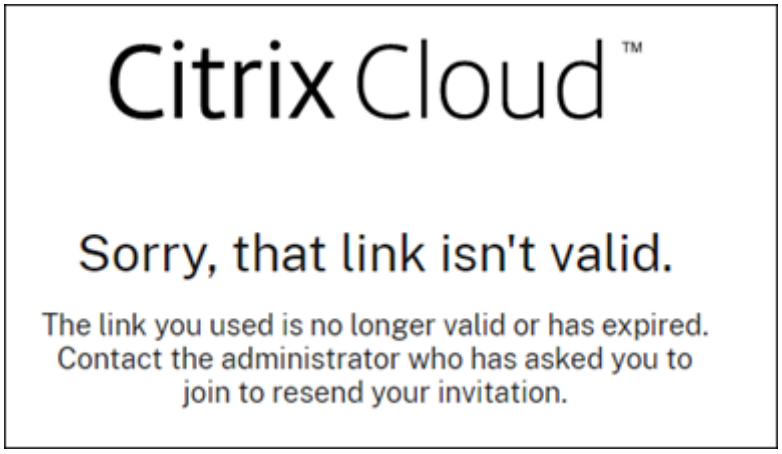
1. Sélectionnez le fournisseur d'identité que vous souhaitez utiliser pour authentifier les administrateurs.

2. Selon le fournisseur d'identité, invitez des administrateurs individuels ou sélectionnez les groupes auxquels les administrateurs appartiennent.
3. Spécifiez les autorisations d'accès qui correspondent aux rôles des administrateurs dans votre organisation. Pour plus d'informations, consultez la section Modifier les autorisations d'administrateur dans cet article.

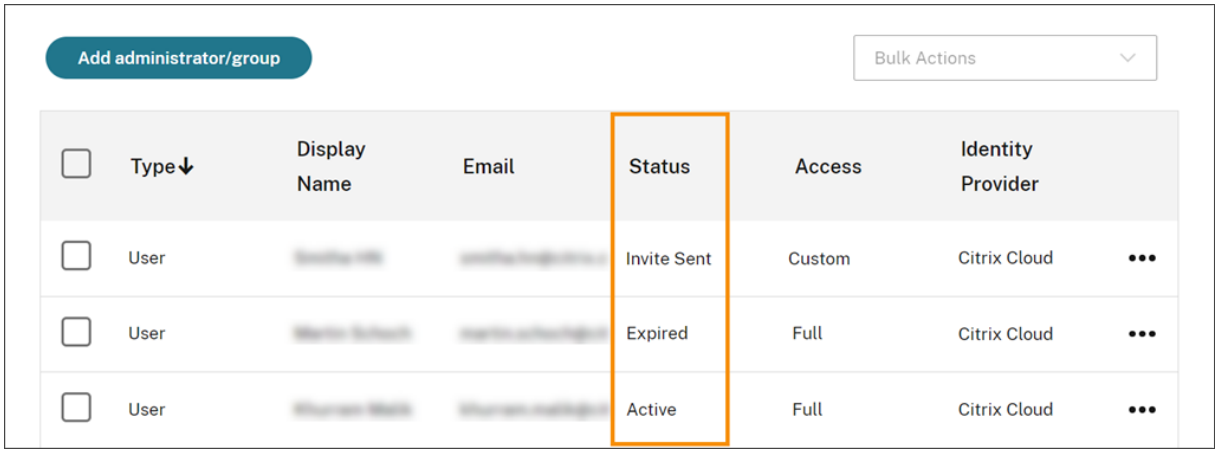
Inviter des administrateurs individuels

L'ajout d'administrateurs individuels implique de les inviter à rejoindre votre compte Citrix Cloud. Lorsque vous ajoutez un administrateur, Citrix lui envoie un e-mail d'invitation. Avant de pouvoir se connecter, l'administrateur doit accepter l'invitation. Les administrateurs que vous ajoutez via des groupes ne reçoivent pas d'invitation et peuvent se connecter immédiatement après avoir été ajoutés.

L'e-mail d'invitation est envoyé depuis `cloud@citrix.com` et explique comment accéder au compte. L'invitation est valable cinq jours consécutifs à compter du jour où vous l'avez envoyée. Au bout de cinq jours, le lien d'invitation expire. Si l'administrateur invité utilise le lien expiré, Citrix Cloud affiche un message indiquant que le lien n'est pas valide.



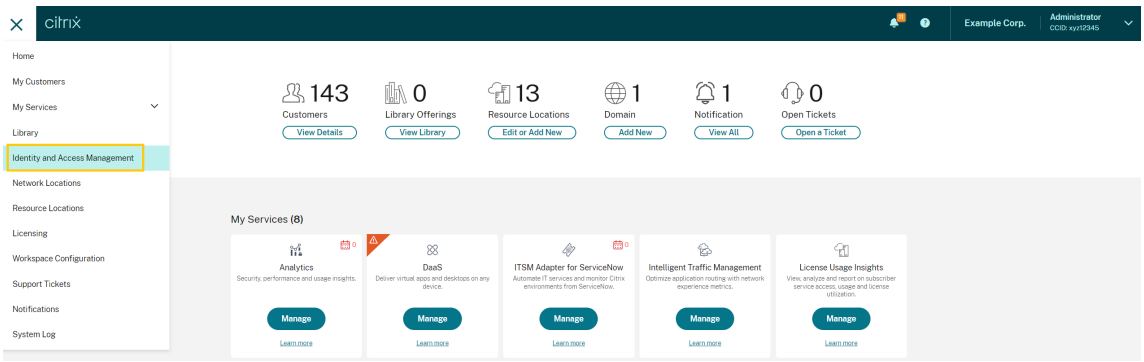
Citrix Cloud affiche également l'état de l'invitation afin que vous puissiez voir si l'administrateur l'a acceptée et s'est connecté à Citrix Cloud.



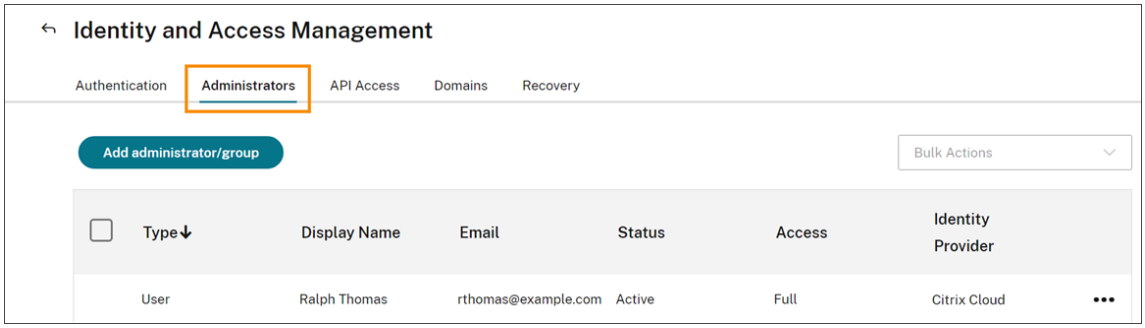
> **Remarque**
>
> Les comptes d'administrateur peuvent être associés à un maximum de 100 comptes clients. Si un administrateur doit gérer plus de 100 comptes clients, il doit créer un compte administrateur distinct avec une adresse e-mail différente pour gérer les clients supplémentaires. Vous pouvez également supprimer l'administrateur des comptes clients qu'il n'a plus besoin de gérer.

Pour inviter un administrateur

1. Connectez-vous à Citrix Cloud, puis sélectionnez **Gestion des identités et des accès** dans le menu.



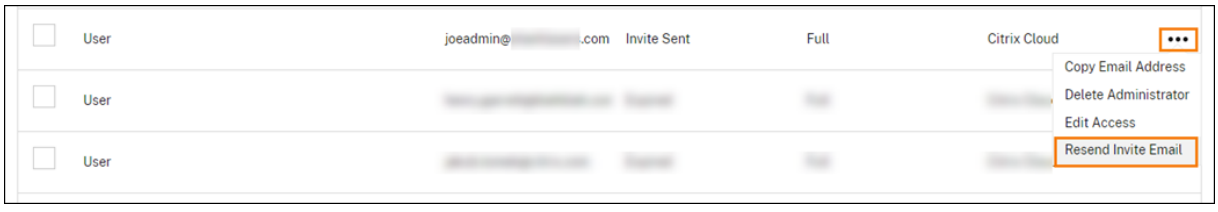
2. Sur la page **Gestion des identités et des accès**, sélectionnez **Administrateurs**. La console affiche tous les administrateurs actuels du compte.



3. Sélectionnez **Ajouter administrateur/groupe**.
4. Dans **Détails de l'administrateur**, sélectionnez le fournisseur d'identité que vous souhaitez utiliser. Si vous utilisez Azure AD, Citrix Cloud peut d'abord vous demander de vous connecter.
5. Si **Identité Citrix** est sélectionné, entrez l'adresse e-mail de l'utilisateur et sélectionnez **Suivant**.
6. Si **Azure Active Directory** est sélectionné, entrez le nom de l'utilisateur que vous souhaitez ajouter et cliquez sur **Suivant**. L'invitation d'utilisateurs invités AAD n'est pas prise en charge.
7. Dans **Définir l'accès**, 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.
8. Vérifiez les détails de l'administrateur. Sélectionnez **Précédent** pour apporter des modifications.
9. Sélectionnez **Envoyer invitation**. Citrix Cloud envoie une invitation à l'utilisateur que vous avez spécifié et ajoute l'administrateur à la liste.

Renvoyer une invitation

Pour renvoyer l'invitation, sélectionnez **Renvoyer e-mail d'invitation** dans le menu des points de suspension à droite de la console. Le renvoi d'une invitation n'affecte pas le délai de cinq jours avant l'expiration de l'invitation.



Renvoyer une invitation avec un nouveau lien de connexion

Si l'e-mail d'invitation d'origine expire, vous pouvez en envoyer un nouveau à l'administrateur. Procédez comme suit :

1. Supprimez l'administrateur de Citrix Cloud : sur la page **Administrateurs**, recherchez l'administrateur dans la liste, puis sélectionnez **Supprimer un administrateur** dans le menu des points de suspension.
2. Attendez quelques minutes pour vous assurer que Citrix Cloud termine la suppression. Dans certains cas, le fait de réinviter l'administrateur immédiatement après la suppression peut entraîner l'envoi d'une invitation avec un lien de connexion défectueux.
3. Réinvitez l'administrateur comme décrit dans la section Pour inviter un administrateur.

Accepter une invitation d'administrateur

Si vous êtes invité à accéder à un compte Citrix Cloud, Citrix vous envoie un e-mail qui inclut l'ID de l'organisation et le nom du client du compte.

Pour accepter l'invitation, cliquez sur **Connexion**. Une fenêtre de navigateur s'affiche. Si vous n'avez pas encore de compte Citrix Cloud, le navigateur affiche une page où vous pouvez créer votre mot de passe. Si vous avez déjà un compte, Citrix Cloud vous invite à utiliser votre mot de passe existant pour vous connecter.

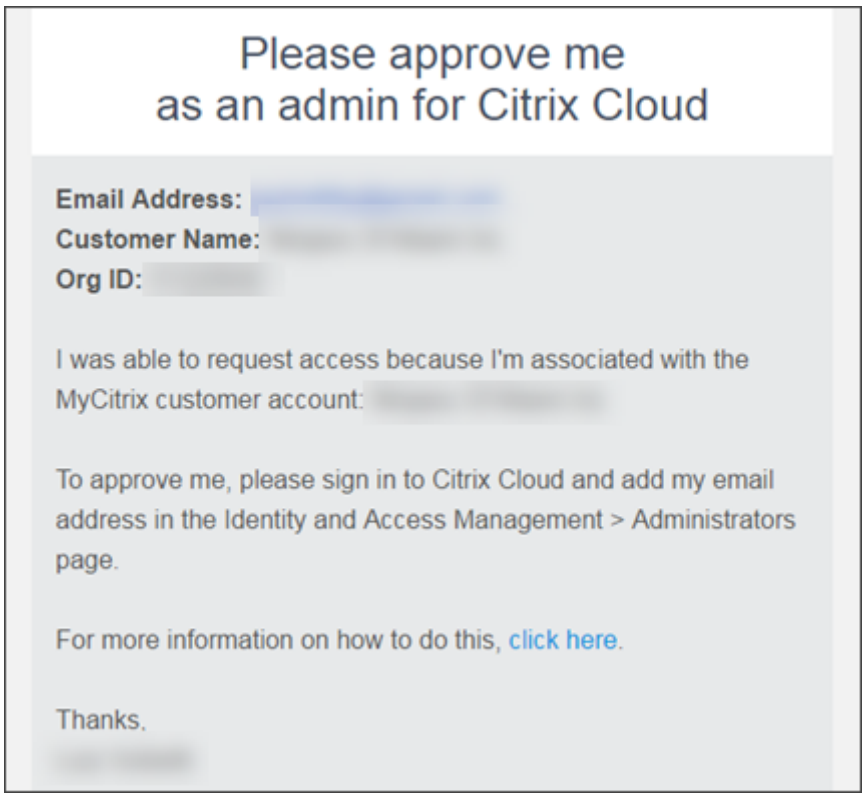
Lors de la connexion, il se peut que vous soyez invité à vous inscrire à l'authentification multifacteur. Pour les instructions d'inscription, consultez Configurer l'authentification multifacteur.

Ajouter des groupes d'administrateurs

Vous pouvez ajouter des administrateurs à l'aide de groupes AD (pour l'authentification SAML) ou de groupes Azure AD (pour l'authentification Azure AD). Pour plus d'informations, consultez Gérer les groupes d'administrateurs.

Approuver les demandes d'adhésion à Citrix Cloud

De temps à autre, vous pouvez recevoir une demande d'approbation de Citrix Cloud de la part d'un membre de votre organisation qui souhaite rejoindre votre compte Citrix Cloud en tant qu'administrateur.



Pour approuver ces demandes, vous devez inviter la personne qui demande l'accès à devenir administrateur, comme décrit dans la section Inviter des administrateurs individuels de cet article. Vous devez utiliser la même adresse e-mail que celle qui apparaît dans l'e-mail de demande d'approbation.

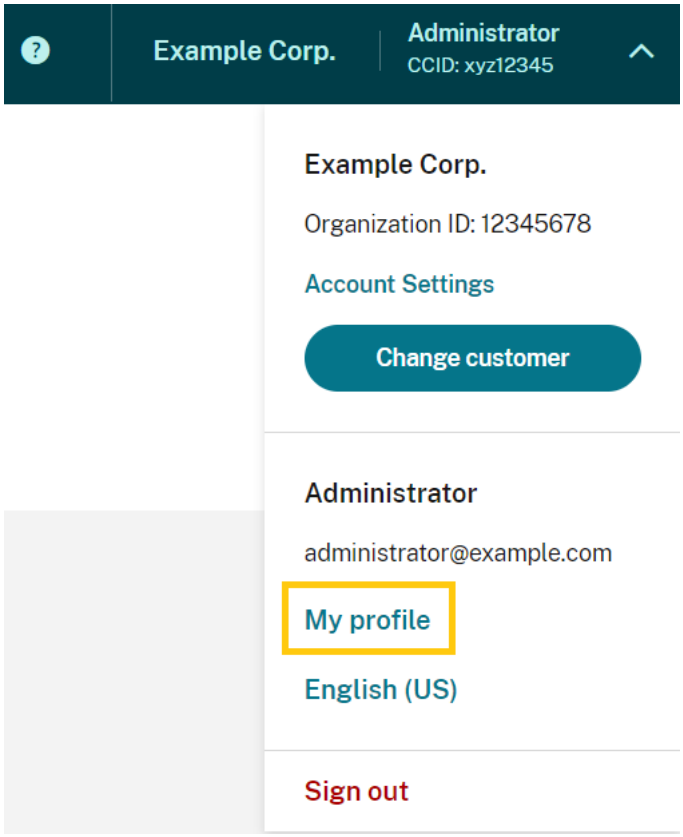
Après avoir reçu l'invitation, la personne demandant l'accès clique sur le lien **Connexion** pour accepter l'invitation. Cette personne peut ensuite créer un mot de passe pour Citrix Cloud et se connecter à votre compte.

Pour plus d'informations sur la façon dont les demandes d'approbation sont générées, consultez Que se passe-t-il si le compte est déjà utilisé.

Modifier votre adresse e-mail

Vous pouvez modifier votre propre adresse e-mail dans Citrix Cloud. Votre nouvelle adresse doit être différente de votre adresse e-mail de récupération pour l'authentification multifacteur (MFA). Lorsque vous modifiez votre adresse e-mail, Citrix Cloud envoie un e-mail de vérification à la nouvelle adresse. Après vérification, Citrix Cloud vous déconnecte afin que la modification puisse être effectuée. Après quelques minutes, vous pouvez vous reconnecter avec votre nouvelle adresse e-mail.

1. Dans le menu en haut à droite, sélectionnez **Mes paramètres**.



2. Dans **Adresse e-mail**, sélectionnez **Changer e-mail**.
3. Entrez la nouvelle adresse e-mail, puis sélectionnez **Envoyer e-mail de vérification**.
4. Entrez le code de vérification à 6 chiffres indiqué dans l'e-mail, puis sélectionnez **Vérifier et compléter**.
5. Sélectionnez **Oui, changer mon adresse e-mail** pour confirmer la modification.

Après avoir confirmé vos modifications, Citrix Cloud vous déconnecte. Après quelques minutes, vous pouvez vous reconnecter avec votre nouvelle adresse e-mail.

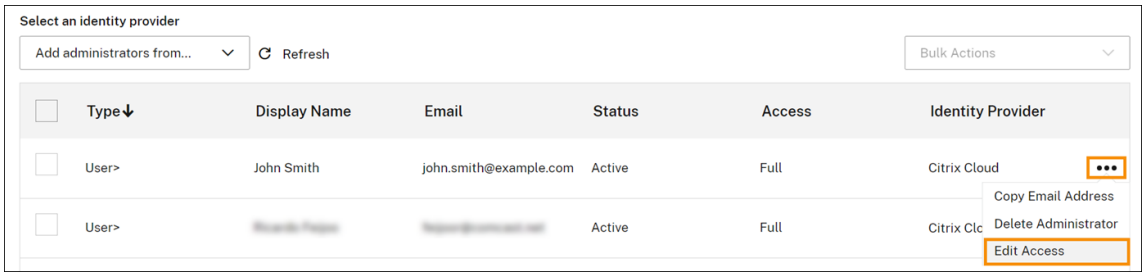
Modifier les autorisations d'administrateur

Lorsque vous ajoutez des administrateurs à votre compte Citrix Cloud, vous définissez les autorisations d'administrateur appropriées selon leur rôle dans votre organisation. Par défaut, les nouveaux administrateurs se voient attribuer des *autorisations d'accès complet* à toutes les fonctions du compte Citrix Cloud et aux services disponibles. Si vous souhaitez limiter l'accès à certaines zones de la console de gestion ou à des services spécifiques, vous pouvez définir des *autorisations d'accès personnalisées*.

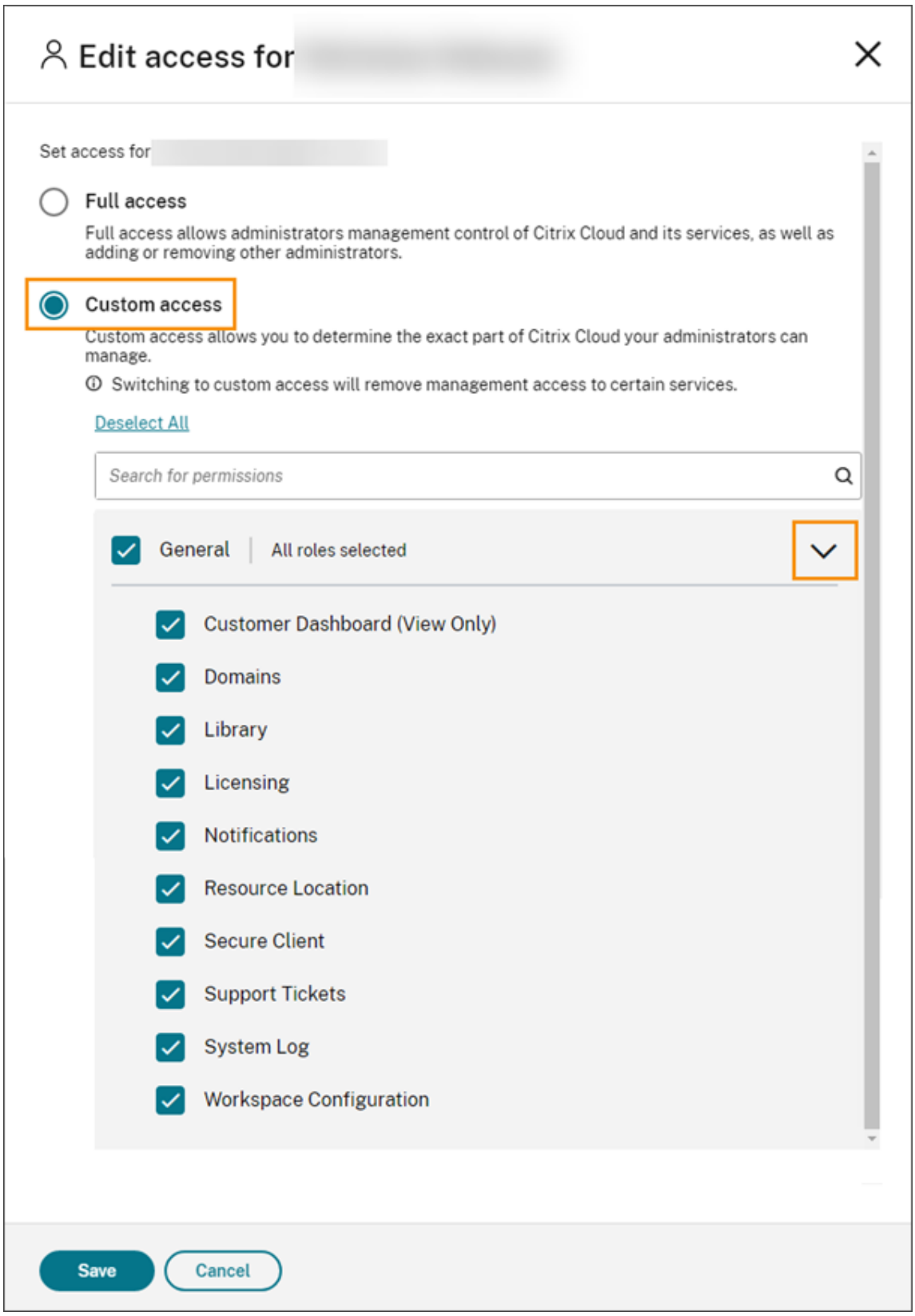
Seuls les administrateurs Citrix Cloud possédant un accès complet peuvent définir des autorisations pour d'autres d'administrateurs.

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. Sélectionnez le fournisseur d'identité que vous souhaitez gérer : Identité Citrix (par défaut), Active Directory (si vous utilisez SAML comme fournisseur d'identité) ou Azure AD (si vous êtes connecté).
4. Recherchez l'administrateur ou le groupe que vous souhaitez gérer, cliquez sur le bouton représentant des points de suspension et sélectionnez **Modifier l'accès**.



5. Pour autoriser ou interdire des autorisations spécifiques, sélectionnez **Accès personnalisé**. Pour autoriser l'accès à toutes les fonctions de Citrix Cloud, sélectionnez **Accès complet**.
6. Pour localiser rapidement les autorisations de service, commencez à taper dans la zone de recherche. Citrix Cloud affiche les autorisations correspondantes lorsque vous tapez. Par exemple, si vous commencez à taper « lecture seule », les autorisations dont le titre contient « lecture seule » s'affichent. La recherche d'autorisations ne respecte pas la casse.
7. Pour définir des autorisations d'accès personnalisées pour la console de gestion Citrix Cloud, développez **Général**.



8. Pour définir des autorisations d'accès personnalisées pour un service spécifique, développez

le service.

9. Pour chaque autorisation, sélectionnez ou désélectionnez la case à cocher selon vos besoins.
10. Sélectionnez **Save**.

Autorisations de la console

Cette section décrit les autorisations d'accès personnalisées disponibles pour la console de gestion Citrix Cloud. Pour plus d'informations sur les autorisations d'accès personnalisées pour un service spécifique, consultez la documentation du service.

- **Tableau de bord client (lecture seule) :** pour les partenaires Citrix Service Provider (CSP) uniquement. Accorde l'accès en lecture seule au tableau de bord client.
- **Domaines :** accorde l'accès à l'onglet **Gestion des identités et des accès > Domaines**. Les administrateurs peuvent ajouter un domaine Active Directory en téléchargeant le logiciel Citrix Cloud Connector à partir de cet onglet et en l'installant sur un serveur du domaine.
- **Bibliothèque :** accorde l'accès à la page **Bibliothèque** de la console. Selon les services auxquels les administrateurs sont autorisés à accéder, les administrateurs peuvent attribuer aux utilisateurs des groupes de mise à disposition pour Citrix DaaS, ajouter des applications gérées par Intune à partir de Endpoint Management ou autoriser les administrateurs en lecture seule à afficher les détails des applications pour Secure Private Access.
- **Licences :** accorde l'accès aux onglets **Cloud Services** et **Déploiements sous licence** de la page **Système de licences** de la console.
- **Notifications :** accorde l'accès à la page **Notifications** de la console. Les administrateurs peuvent afficher et ignorer les notifications Citrix Cloud.
- **Emplacements des ressources :** accorde l'accès à la page **Emplacements des ressources** de la console. Les administrateurs peuvent ajouter de nouveaux emplacements de ressources et ajouter des serveurs FAS pour l'authentification unique Citrix Workspace. Ils peuvent également gérer les mises à jour des connecteurs.
- **Client sécurisé :** accorde l'accès à l'onglet **Gestion des identités et des accès > Accès API > Clients sécurisés**. Les administrateurs peuvent créer et gérer leurs propres clients sécurisés à utiliser avec les API Citrix Cloud. Cette autorisation n'inclut pas l'accès à l'onglet **Gestion des identités et des accès > Accès API > Enregistrements de produits**. Seuls les administrateurs ayant un accès complet peuvent accéder à l'onglet **Enregistrements de produits**.
- **Tickets d'assistance :** donne accès à l'option de menu de la console **Tickets de support** et à l'option de menu d'aide **Ouvrir un ticket**. La sélection de l'une de ces options dirige l'administrateur vers le portail My Support. Pour plus d'informations, consultez la section Support technique.
- **Journal du système :** accorde l'accès à la page **Journal du système** de la console. Les administrateurs peuvent afficher les événements du journal système et exporter les événements dans

un fichier CSV.

- **Configuration de l'espace de travail :** autorise l'accès à la page **Configuration de l'espace de travail** de la console. Les administrateurs peuvent modifier les méthodes d'authentification, personnaliser l'apparence et le comportement de l'espace de travail, activer et désactiver des services et configurer l'agrégation de sites Pour plus d'informations, consultez la documentation produit de Citrix Workspace.
- **Clients OAuth de Workspace (version Technical Preview) :** accorde l'accès à l'onglet **Gestion des identités et des accès > Accès aux API > API de Workspace**. Les administrateurs peuvent créer et gérer leur propre client OAuth pour interagir avec les API de la plateforme Citrix Workspace. Les clients OAuth sont utilisés exclusivement pour les API de Workspace et incluent la possibilité de créer des clients privés qui expirent automatiquement.

> **Remarque :**
>
> Il est recommandé d'attribuer le rôle personnalisé **Clients OAuth de Workspace** avec prudence. Les privilèges d'accès associés à ce rôle peuvent permettre aux administrateurs d'accéder aux ressources de l'utilisateur final (VDA ou applications) sur la plate-forme Workspace. Il est également important de noter que les administrateurs avec un **accès complet** disposeront automatiquement d'autorisations d'accès équivalentes à celles d'un administrateur disposant de l'autorisation **Clients OAuth de Workspace**.

Gérer votre méthode de MFA principale

Pour vous connecter à Citrix Cloud avec l'authentification multifacteur (MFA), vous pouvez utiliser une application d'authentification ou votre adresse e-mail. Cette section explique comment modifier l'inscription de votre appareil pour utiliser la MFA ou passer à une autre méthode de MFA.

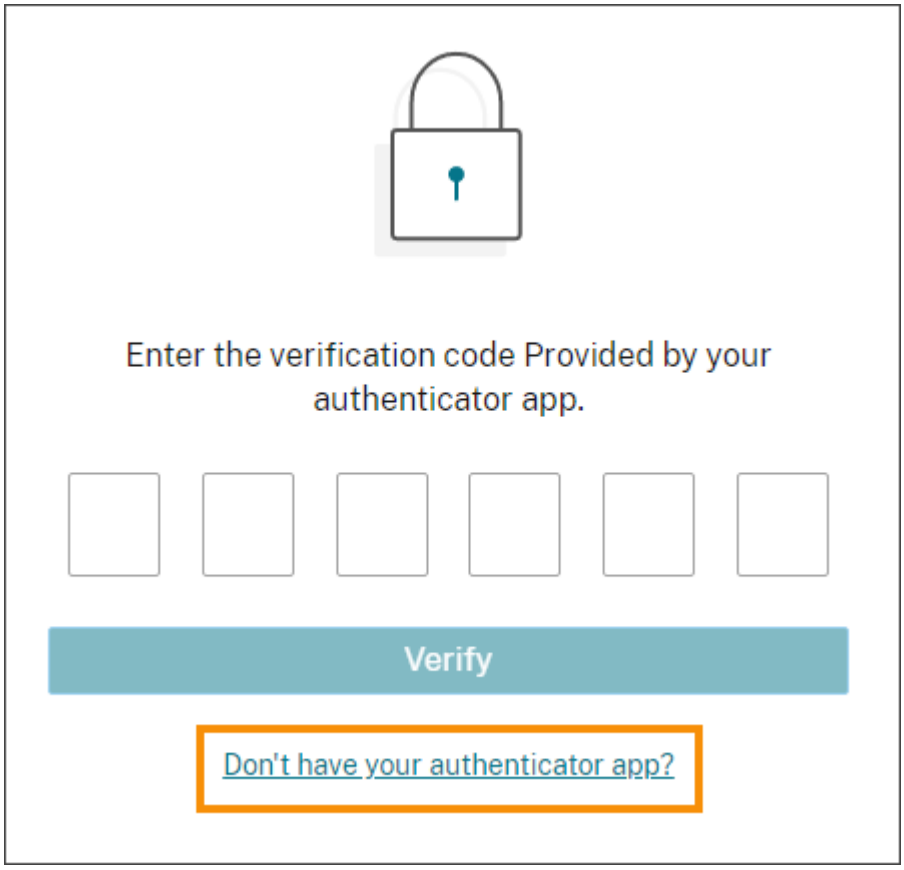
Changer votre appareil pour utiliser la MFA

Si vous perdez votre appareil inscrit, que vous souhaitez utiliser un autre appareil avec Citrix Cloud ou réinitialiser votre application d'authentification, vous pouvez vous réinscrire à la MFA 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 dif-

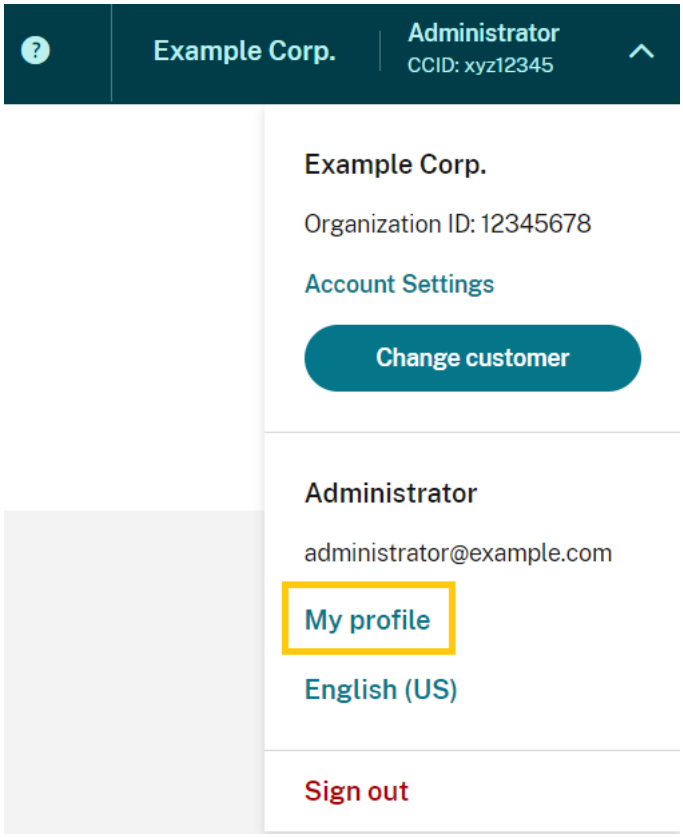
férents, ce qui peut causer de la confusion lors de la connexion à Citrix Cloud.
- Si vous vous réinscrivez avec un nouvel appareil et que vous ne disposez pas d'une application d'authentification, vous pouvez en télécharger une à partir du magasin d'applications de votre appareil. Pour une expérience 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.

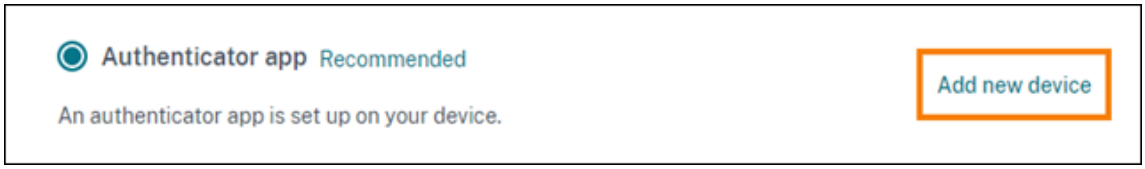


   Si vous n'avez pas votre application d'authentification, cliquez sur **Vous n'avez pas d'application d'authentification ?** et sélectionnez une méthode de récupération pour vous aider à vous connecter. Selon la méthode de récupération sélectionnée, entrez le code de récupération que vous avez reçu ou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



4. Dans l'**application d'authentification**, sélectionnez **Ajouter un nouvel appareil**.



5. Lorsque vous êtes invité à confirmer le changement d'appareil, sélectionnez **Oui, changer d'appareil**.
6. Vérifiez votre identité en saisissant un code de vérification depuis votre application d'authentification. Si vous ne possédez pas d'application d'authentification, sélectionnez **Utiliser une méthode de récupération** pour vérifier votre identité à l'aide de la méthode de récupération de votre choix. 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 et continuer**.
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**.

Après avoir changé d'appareil, Citrix recommande vivement de vérifier que les méthodes de vérification de votre page Mon profil sont à jour.

Changer votre méthode de MFA

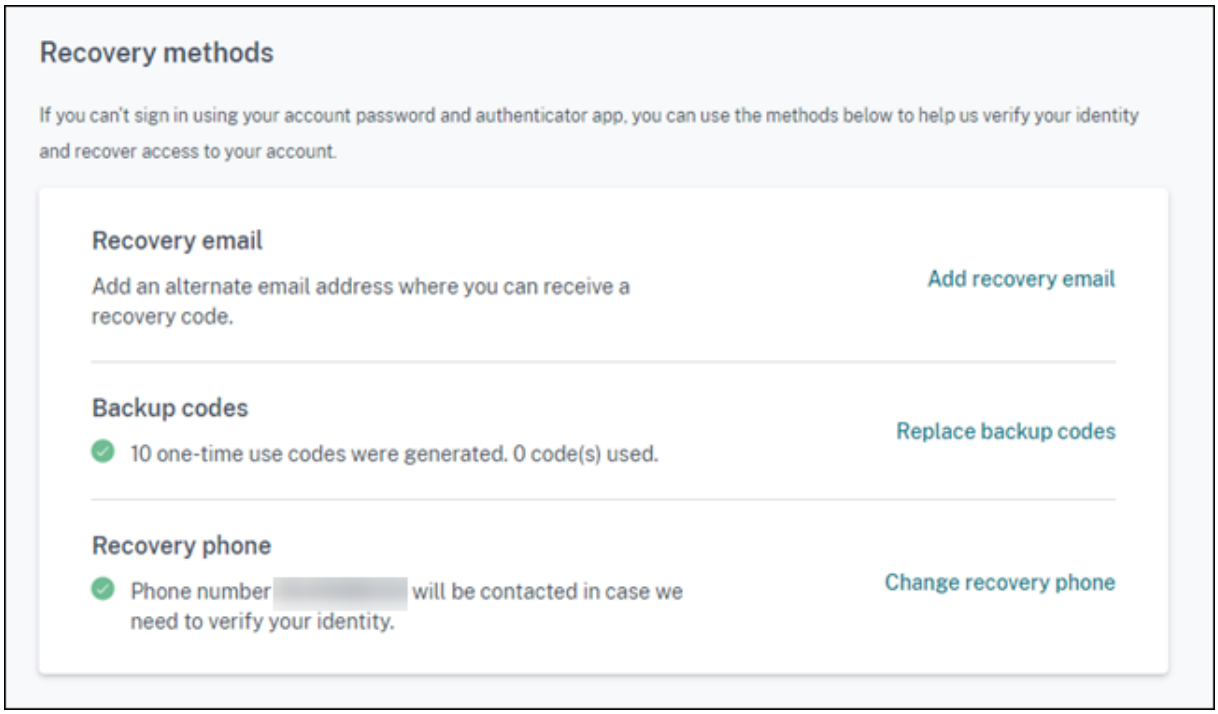
Si vous vous êtes inscrit à la MFA à l'aide d'une application d'authentification et que vous souhaitez passer à l'utilisation de votre adresse e-mail, sachez que la modification de votre méthode d'authentification entraîne la suppression de l'inscription de votre appareil. Si vous souhaitez recommencer à utiliser une application d'authentification pour l'authentification MFA, vous devez réinscrire votre appareil.

1. Dans le menu en haut à droite de la console Citrix Cloud, sélectionnez **Mes paramètres**.
2. Sous **Authentification multifacteur (MFA)**, sélectionnez la méthode d'authentification que vous souhaitez utiliser.
3. Si vous passez à la MFA par e-mail :
    a) Sélectionnez **Oui, utiliser e-mail** pour confirmer que vous souhaitez modifier votre méthode de MFA.
    b) Entrez le code de votre application d'authentification ou utilisez une méthode de récupération pour confirmer votre identité.
    c) Sélectionnez **Vérifier et continuer** pour terminer la modification.
4. Si vous passez à une application d'authentification :
    a) Lorsque vous y êtes invité, entrez le code de vérification que Citrix Cloud envoie à votre adresse e-mail et sélectionnez **Vérifier et continuer**. Vous pouvez également utiliser une méthode de récupération pour confirmer votre identité.
    b) À l'aide de votre application d'authentification, scannez le code QR avec l'appareil photo de votre appareil ou saisissez la clé alphanumérique.
    c) Sous **Vérifiez votre application d'authentification**, entrez le code à 6 chiffres de votre application d'authentification.
    d) Cliquez sur **Vérifier le code** pour terminer l'inscription de l'appareil.

Gérer vos méthodes de récupération de MFA

> **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 ou l'adresse e-mail de la MFA, ces méthodes de vérification sont la seule façon de récupérer l'accès à votre compte.



Ajouter ou modifier votre e-mail de récupération

1. Dans le menu en haut à droite, sélectionnez **Mes paramètres**.
2. Sous **Méthodes de récupération**, dans **E-mail de récupération**, sélectionnez **Ajouter un e-mail de récupération** si vous n'avez pas encore ajouté d'adresse e-mail de récupération. Si vous avez déjà ajouté une adresse e-mail de récupération, sélectionnez **Modifier l'e-mail de récupération**.
3. Lorsque vous y êtes invité, entrez le code de vérification de votre application d'authentification ou le code envoyé à votre adresse e-mail.
4. Entrez la nouvelle adresse e-mail que vous souhaitez utiliser, puis sélectionnez **Envoyer e-mail de vérification**. Cette adresse e-mail doit être différente de celle que vous utilisez pour votre compte Citrix Cloud. Citrix Cloud vous envoie un e-mail de vérification à l'adresse e-mail que vous avez saisie.
5. Entrez le code figurant dans l'e-mail de vérification, puis cliquez sur **Vérifier le code et compléter**.

Générer de nouveaux codes de secours

Vous pouvez générer un nouveau jeu de codes de secours à tout moment. Lorsque vous utilisez des codes de secours, Citrix Cloud enregistre le numéro qui a été utilisé dans votre page Mon profil.

Après avoir généré de nouveaux codes de secours, assurez-vous de les stocker dans un endroit sûr.

1. Dans le menu en haut à droite, sélectionnez **Mes paramètres**.
2. Sous **Méthodes de récupération**, dans **Codes de secours**, sélectionnez **Générer des codes de secours** si vous n'avez jamais généré de codes de secours auparavant. Si vous avez précédemment généré des codes de secours, sélectionnez **Remplacer les codes de secours**.
3. Lorsque vous êtes invité à remplacer vos codes de secours, sélectionnez **Oui, remplacer mes codes**.
4. Vérifiez votre identité en saisissant un code de vérification depuis votre application d'authentification ou le code envoyé à votre adresse e-mail.
5. Sélectionnez **Vérifier et continuer**. Citrix Cloud génère et affiche un nouvel ensemble de codes de secours.
6. Sélectionnez **Télécharger les codes** pour télécharger vos nouveaux codes sous forme de fichier texte. Sélectionnez ensuite **J'ai stocké mes codes de secours**.
7. Sélectionnez **J'ai stocké mes codes de secours** pour terminer le remplacement de vos codes de secours.

Modifier votre numéro de téléphone de récupération

1. Dans le menu en haut à droite, sélectionnez **Mes paramètres**.
2. Sous **Méthodes de récupération**, dans **N° de téléphone de récupération**, sélectionnez **Changer le n° de téléphone de récupération**.
3. Entrez le code de vérification de votre application d'authentification ou le code envoyé à votre adresse e-mail. Sélectionnez **Vérifier et continuer**.
4. Entrez le nouveau numéro de téléphone que vous souhaitez utiliser. Entrez à nouveau le numéro de téléphone pour le confirmer.
5. Sélectionnez **Enregistrer le numéro de téléphone de récupération**.

> **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.

Gérer les groupes d'administrateurs

February 15, 2024

Vous pouvez ajouter des administrateurs à votre compte Citrix Cloud à l'aide de groupes dans votre Active Directory, Azure Active Directory (AD) ou Google Cloud Identity. Vous pouvez ensuite gérer les autorisations d'accès aux services pour tous les administrateurs du groupe.

Prérequis d'AD

Citrix Cloud prend en charge l'authentification des groupes AD via SAML 2.0. Avant d'ajouter des membres de vos groupes d'administrateurs AD à Citrix Cloud, vous devez configurer une connexion entre Citrix Cloud et votre fournisseur SAML. Pour plus d'informations, consultez Connecter SAML en tant que fournisseur d'identité à Citrix Cloud.

Si vous disposez déjà d'une connexion SAML dans Citrix Cloud, vous devez reconnecter votre fournisseur SAML à Citrix Cloud avant d'ajouter des groupes d'administrateurs AD. Si vous ne reconnectez pas SAML, l'ajout de groupes d'administrateurs AD peut échouer. Pour plus d'informations, consultez la section Utilisation d'une connexion SAML existante pour l'authentification des administrateurs.

Prérequis d'Azure AD

L'utilisation de l'authentification de groupes Azure AD nécessite la dernière version de l'application Azure AD pour connecter votre Azure AD à Citrix Cloud. Citrix Cloud a acquis cette application lorsque vous avez connecté votre Azure AD pour la première fois. Si vous avez 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. Citrix Cloud ne peut pas afficher vos groupes Azure AD si votre compte n'utilise pas l'application la plus récente.

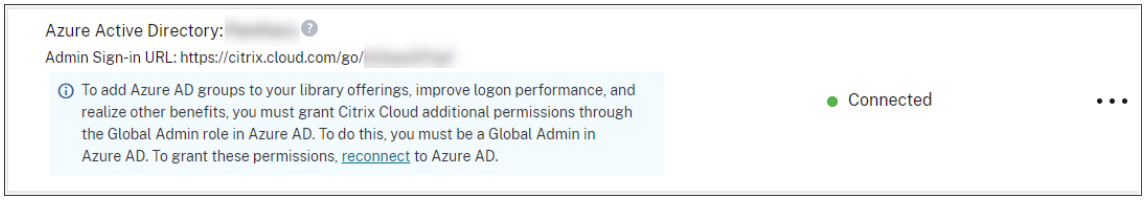
Avant d'utiliser les groupes Azure AD dans Citrix Cloud, effectuez les tâches suivantes :

1. Vérifiez que vous utilisez la dernière application pour votre connexion Azure AD. Citrix Cloud affiche une notification si vous n'utilisez pas l'application la plus récente.
2. Si l'application doit être mise à jour, reconnectez votre Azure AD à Citrix Cloud. En vous reconnectant à votre 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 votre Azure AD en votre nom. Lors de la reconnexion, une liste de ces autorisations s'affiche. Pour plus d'informations sur les autorisations demandées par Citrix Cloud, consultez Autorisations Azure Active Directory pour Citrix Cloud.

> **Important :**
>
> Vous devez être un administrateur global dans Azure AD pour effectuer cette tâche. Vous devez également être connecté à Citrix Cloud à l'aide d'un compte d'administrateur avec accès complet sous le fournisseur d'identité Citrix. Si vous vous connectez avec vos informations d'identification Azure AD, la reconnexion échoue. Si aucun administrateur n'utilise le fournisseur d'identité Citrix, vous pouvez en ajouter un temporairement pour effectuer cette tâche, puis le supprimer par la suite.

Pour vérifier votre connexion à Azure AD

1. Connectez-vous à Citrix Cloud à l'aide d'un compte d'administrateur avec accès complet sous le fournisseur d'identité Citrix.
2. Dans le menu Citrix Cloud, sélectionnez **Gestion des identités et des accès**, puis sélectionnez **Authentification**.
3. Recherchez **Azure Active Directory**. Une notification s'affiche si Citrix Cloud doit mettre à jour l'application pour votre connexion Azure AD.



   Si Citrix Cloud utilise déjà l'application la plus récente, aucune notification ne s'affiche.

Pour se reconnecter à Azure AD

1. Dans la notification Azure AD de la console Citrix Cloud, cliquez sur le lien de **reconnexion**. La liste des autorisations Azure demandées s'affiche.
2. Vérifiez les autorisations, puis sélectionnez **Accepter**.

Google Cloud Identity

Citrix Cloud prend en charge l'authentification de groupes d'administrateurs via Google Cloud Identity. Avant d'ajouter vos groupes d'administrateurs à Citrix Cloud, vous devez configurer une connexion entre Citrix Cloud et Google Cloud Identity. Pour plus d'informations, consultez Connecter Google Cloud Identity en tant que fournisseur d'identité à Citrix Cloud.

Services pris en charge

Les services suivants prennent en charge les autorisations d'accès personnalisées pour les groupes d'administrateurs :

- Citrix Analytics
- Console NetScaler
- Citrix DaaS
- Workspace Environment Management Service
- License Usage Insights

Autorisations prises en charge

Vous pouvez attribuer des autorisations d'accès personnalisées uniquement aux services pris en charge et à certaines fonctionnalités de la plate-forme Citrix Cloud. Les autorisations avec accès complet ne sont pas prises en charge.

Pour les fonctionnalités de la plate-forme Citrix Cloud, les autorisations d'accès personnalisées suivantes sont prises en charge :

- Domaines
- Licences
- Emplacements des ressources
- Tickets de support
- Journal du système
- Configuration de Workspace

Pour plus d'informations sur ces autorisations, consultez la section Autorisations de la console.

Les groupes d'administrateurs n'ont accès à aucun autre service. Ils ne peuvent gérer que les services pris en charge auxquels ils sont autorisés à accéder.

Les modifications apportées aux autorisations d'un membre du groupe d'administrateurs déjà connecté ne prendront effet qu'après déconnexion puis reconnexion.

Autorisations résultantes pour les administrateurs avec identités Citrix, AD, Azure AD et Google Cloud

Lorsqu'un administrateur se connecte à Citrix Cloud, seules certaines autorisations peuvent être disponibles si l'administrateur possède à la fois une identité Citrix (le fournisseur d'identité par défaut dans Citrix Cloud) et une identité mono-utilisateur ou groupe via AD, Azure AD ou Google Cloud Identity. Le tableau de cette section décrit les autorisations disponibles pour chaque combinaison de ces identités.

L'identité mono-utilisateur fait référence aux autorisations AD, Azure AD ou Google Cloud Identity qui sont accordées à l'administrateur via un compte individuel. *L'identité basée sur groupe* fait référence aux autorisations AD, Azure AD ou Google Cloud Identity qui sont accordées en tant que membre d'un groupe.

Identité Citrix	Identité Azure AD ou AD mono-utilisateur	Identité AD ou Azure AD basée sur un groupe	Google Cloud Identity basé sur un seul utilisateur ou un groupe	Autorisations disponibles après l'authentification
X	X			L'administrateur dispose d'autorisations cumulées sur les deux identités après une authentification réussie avec l'identité Citrix, l'identité AD ou l'identité Azure AD.
X		X		Chaque identité est traitée comme une entité indépendante. Les autorisations disponibles varient selon que l'administrateur s'authentifie à l'aide de l'identité Citrix ou de l'identité Azure AD.

Identité Citrix	Identité Azure AD ou AD mono-utilisateur	Identité AD ou Azure AD basée sur un groupe	Google Cloud Identity basé sur un seul utilisateur ou un groupe	Autorisations disponibles après l'authentification
X			X	Chaque identité est traitée comme une entité indépendante. Les autorisations disponibles varient selon que l'administrateur s'authentifie à l'aide de l'identité Citrix ou de Google Cloud Identity.
	X	X		L'administrateur dispose d'autorisations cumulées pour les deux identités lors de l'authentification auprès de Citrix Cloud avec AD ou Azure AD.

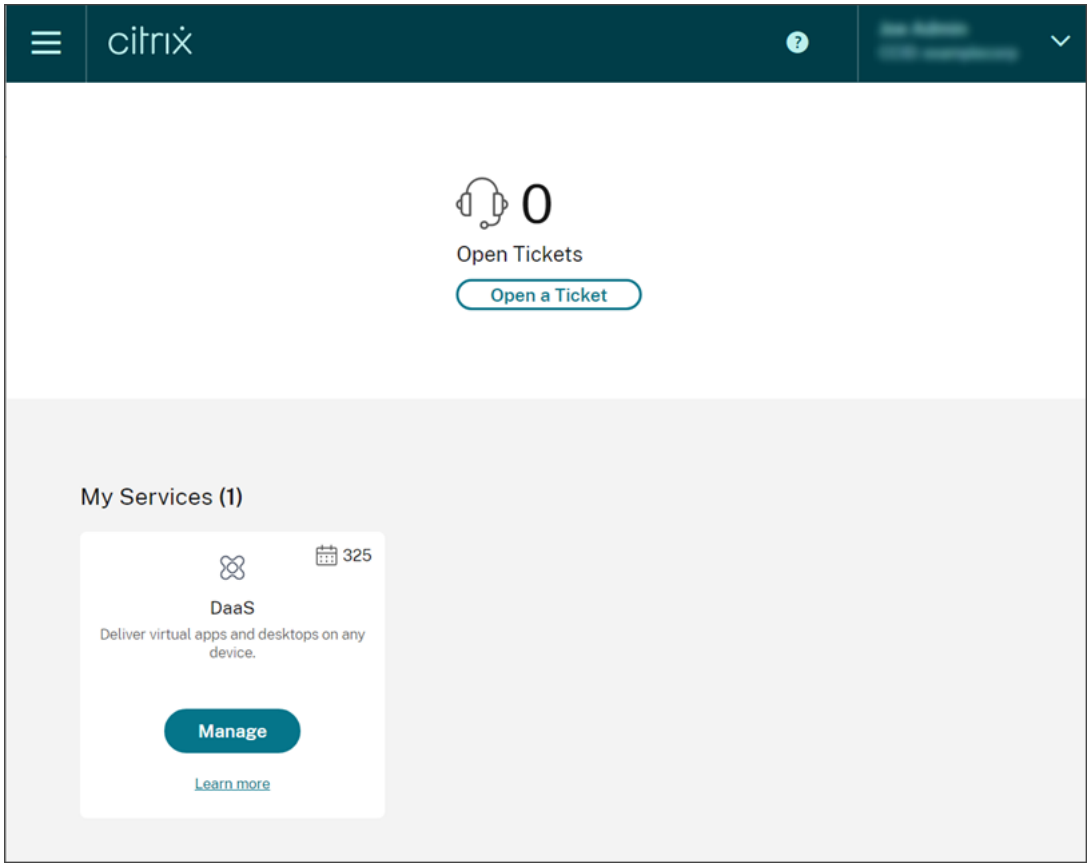
Identité Citrix	Identité Azure AD ou AD mono-utilisateur	Identité AD ou Azure AD basée sur un groupe	Google Cloud Identity basé sur un seul utilisateur ou un groupe	Autorisations disponibles après l'authentification
	X		X	Chaque identité est traitée comme une entité indépendante. Les autorisations disponibles varient selon que l'administrateur s'authentifie à l'aide de l'identité Citrix ou de Google Cloud Identity.
		X	X	Chaque identité est traitée comme une entité indépendante. Les autorisations disponibles varient selon que l'administrateur s'authentifie à l'aide de l'identité Citrix ou de Google Cloud Identity.

Identité Citrix	Identité Azure AD ou AD mono-utilisateur	Identité AD ou Azure AD basée sur un groupe	Google Cloud Identity basé sur un seul utilisateur ou un groupe	Autorisations disponibles après l'authentification
X	X	X		Lors de l'authentification avec son identité Citrix, l'administrateur dispose d'autorisations cumulées à la fois sur l'identité Citrix et sur l'identité Azure AD mono-utilisateur. Lors de l'authentification avec Azure AD, l'administrateur dispose des autorisations cumulées des trois identités.

Expérience de connexion pour les administrateurs

Après avoir ajouté un groupe à Citrix Cloud et défini les autorisations de service, les administrateurs du groupe se connectent simplement en sélectionnant **Se connecter avec les informations d'identification de mon entreprise** sur la page de connexion Citrix Cloud et en saisissant leur URL de connexion pour le compte (par exemple, `https://citrix.cloud.com/go/mycompany`). Contrairement à l'ajout d'administrateurs individuels, les administrateurs du groupe ne sont pas explicitement invités. Ils ne recevront donc aucun e-mail leur demandant d'accepter une invitation à devenir administrateurs Citrix Cloud.

Une fois connectés, les administrateurs sélectionnent **Gérer** dans la vignette du service pour accéder à la console de gestion du service.



Les administrateurs qui disposent d'autorisations uniquement en tant que membres de groupes peuvent accéder au compte Citrix Cloud à l'aide de l'URL de connexion du compte Citrix Cloud.

Les administrateurs qui obtiennent des autorisations via un compte individuel et en tant que membre d'un groupe peuvent choisir le compte Citrix Cloud auquel ils souhaitent accéder. Si l'administrateur est membre de plusieurs comptes Citrix Cloud, il peut sélectionner un compte Citrix Cloud dans le sélecteur de client après s'être authentifié avec succès.

Limitations

Accès aux fonctionnalités de la plateforme et du service

Les autorisations d'accès personnalisées pour les fonctionnalités suivantes de la plate-forme Citrix Cloud ne sont pas disponibles pour les membres des groupes d'administrateurs :

- Bibliothèque
- Notifications
- Clients sécurisés

Pour plus d'informations sur les autorisations disponibles, consultez la section Autorisations prises en charge dans cet article.

Les fonctionnalités Citrix DaaS qui reposent sur les fonctionnalités de la plate-forme Citrix Cloud, telles que l'attribution d'utilisateurs avec Déploiement rapide, ne sont pas disponibles.

Impact de plusieurs groupes sur les performances de l'application

Citrix recommande qu'un seul administrateur n'appartienne pas à plus de 20 groupes qui ont été ajoutés à Citrix Cloud. L'appartenance à un plus grand nombre de groupes peut entraîner une réduction des performances des applications.

Impact de plusieurs groupes sur l'authentification

Si l'administrateur d'un groupe est affecté à plusieurs groupes dans AD ou Azure AD, l'authentification peut échouer car le nombre de groupes est trop important. Ce problème se produit en raison d'une limitation de l'intégration de Citrix Cloud avec AD et Azure AD. Lorsque l'administrateur tente de se connecter, Citrix Cloud tente de compresser le nombre de groupes récupérés. Si Citrix Cloud ne parvient pas à appliquer la compression correctement, les groupes ne peuvent pas tous être récupérés et l'authentification échoue.

Ce problème peut également affecter les utilisateurs qui s'authentifient auprès de Citrix Workspace via AD ou Azure AD. Si un utilisateur appartient à plusieurs groupes, l'authentification peut échouer car le nombre de groupes est trop important.

Pour résoudre ce problème, examinez le compte d'administrateur ou d'utilisateur et vérifiez qu'il appartient uniquement aux groupes requis pour son rôle dans l'organisation.

L'ajout de groupes échoue en raison d'un trop grand nombre d'attributions de paires rôle/étendue

Lors de l'ajout d'un groupe avec plusieurs paires rôle/étendue, une erreur peut se produire indiquant que le groupe ne peut pas être créé. Cette erreur se produit parce que le nombre de paires rôle/étendue attribuées au groupe est trop important. Pour résoudre cette erreur, divisez les paires rôle/étendue entre deux groupes ou plus et affectez les administrateurs à ces groupes.

Ajouter un groupe d'administrateurs à Citrix Cloud

1. Dans le menu Citrix Cloud, sélectionnez **Gestion des identités et des accès**, puis sélectionnez **Administrateurs**.
2. Sélectionnez **Ajouter administrateur/groupe**.

3. Dans **Détails de l'administrateur**, sélectionnez le fournisseur d'identité que vous souhaitez utiliser. Si Azure AD est sélectionné, connectez-vous à votre Azure, si nécessaire. Sélectionnez **Suivant**.
4. Si nécessaire, sélectionnez le domaine que vous souhaitez utiliser.
5. Recherchez le groupe que vous souhaitez ajouter et sélectionnez-le.
6. Dans **Définir l'accès**, sélectionnez les rôles que vous souhaitez attribuer au groupe. Vous devez sélectionner au moins un rôle.
7. Lorsque vous avez terminé, sélectionnez **Enregistrer**.

Modifier les autorisations de service d'un groupe d'administrateurs

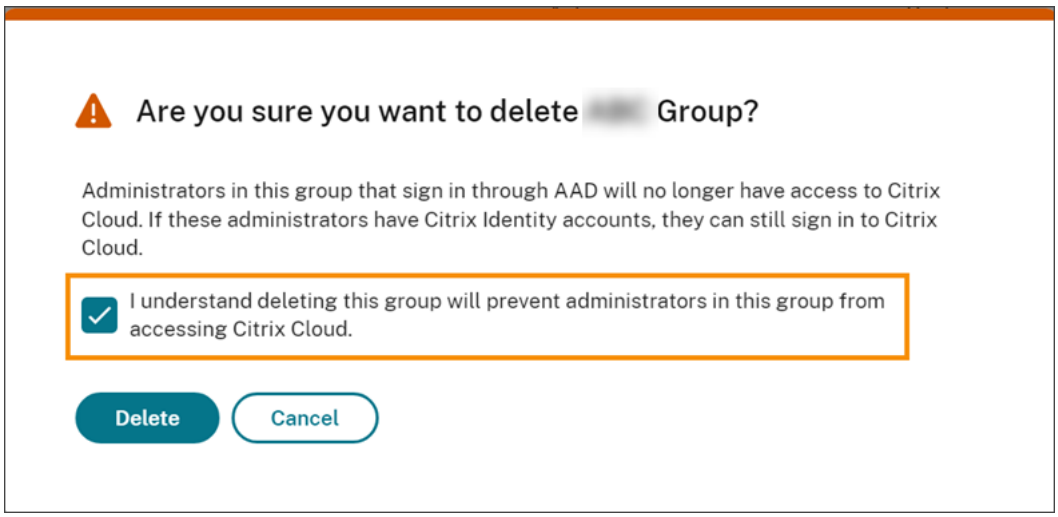
1. Dans le menu Citrix Cloud, sélectionnez **Gestion des identités et des accès**, puis sélectionnez **Administrateurs**.
2. Recherchez le groupe Azure AD que vous souhaitez gérer et, dans le menu des points de suspension, sélectionnez **Modifier l'accès**.

3. Sélectionnez ou décochez les cases en regard d'une ou de plusieurs paires de rôles et d'étendues selon vos besoins.
4. Lorsque vous avez terminé, sélectionnez **Enregistrer**.

Supprimer un groupe d'administrateurs

1. Dans le menu Citrix Cloud, sélectionnez **Gestion des identités et des accès**, puis sélectionnez **Administrateurs**.
2. Recherchez le groupe d'administrateurs que vous souhaitez gérer et, dans le menu des points de suspension, sélectionnez **Supprimer le groupe**.

Un message de confirmation s'affiche.

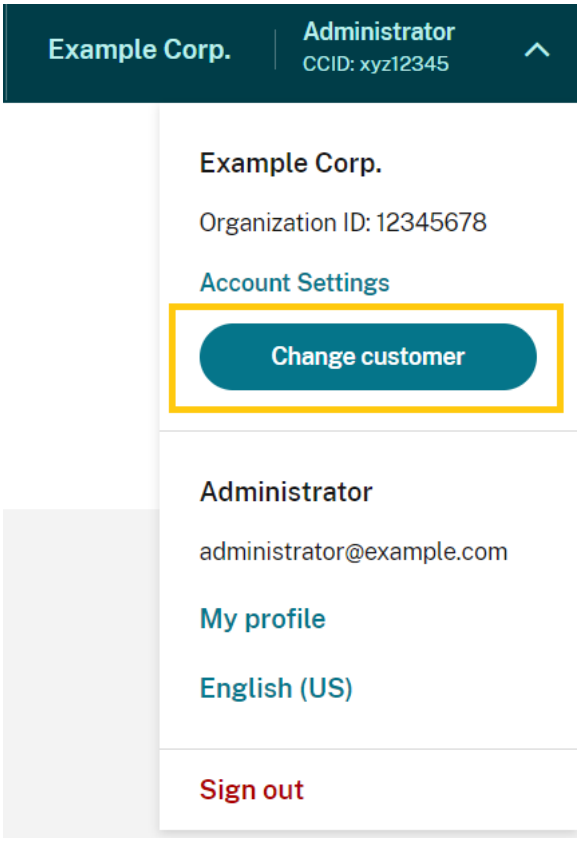


3. Choisissez **Je comprends que la suppression de ce groupe empêchera les administrateurs de ce groupe d'accéder à Citrix Cloud** pour confirmer que vous êtes conscient des effets de la suppression du groupe.
4. Sélectionnez **Supprimer**.

Basculer entre plusieurs comptes Citrix Cloud

> **Remarque :**
>
> Cette section décrit un scénario qui affecte uniquement les membres des groupes d'administrateurs Azure AD.

Par défaut, les membres des groupes d'administrateurs Azure AD ne peuvent pas basculer entre les autres comptes Citrix Cloud auxquels ils ont accès. Pour ces administrateurs, l'option **Changer de client**, illustrée dans l'image ci-dessous, n'apparaît pas dans le menu utilisateur de Citrix Cloud.

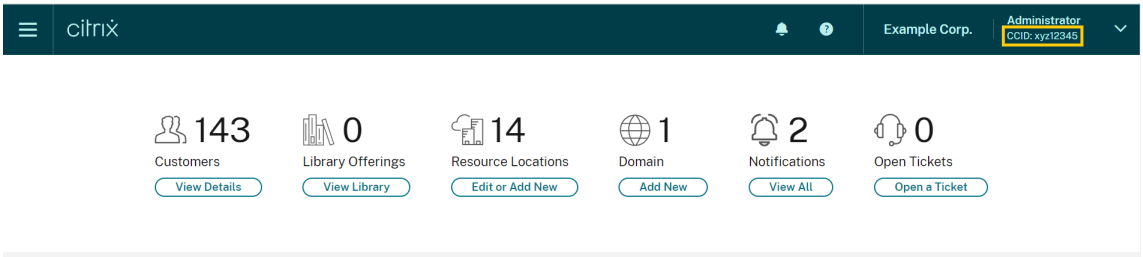


Pour activer cette option de menu et permettre aux membres du groupe Azure AD de basculer entre d'autres comptes Citrix Cloud, vous devez lier les comptes auxquels vous souhaitez accéder.

Lier des comptes Citrix Cloud implique une approche « hub and spoke ». Avant de lier des comptes, décidez quel compte Citrix Cloud agira en tant que compte à partir duquel les autres comptes sont accessibles (le « hub ») et quels comptes vous souhaitez faire figurer dans le sélecteur de client (les « spoke »).

Avant de lier des comptes, assurez-vous que les conditions suivantes sont remplies :

- Vous disposez d'autorisations d'accès complètes dans Citrix Cloud.
- Vous avez accès à Windows PowerShell Integrated Scripting Environment (ISE).
- Vous disposez des ID client des comptes Citrix Cloud que vous souhaitez lier. L'ID client apparaît dans le coin supérieur droit de la console de gestion pour chaque compte.



- Vous disposez du jeton du porteur Citrix CWSAuth pour le compte Citrix Cloud que vous

souhaitez lier en tant que compte hub. Pour récupérer ce jeton, suivez les instructions de l'article CTX330675. Vous devez fournir ces informations lorsque vous liez vos comptes Citrix Cloud.

Pour lier des comptes Citrix Cloud

1. Ouvrez PowerShell ISE et collez le script suivant dans le volet de travail :

```
1  $headers = @{
2    }
3
4  $headers.Add("Accept","application/json")
5  $headers.Add("Content-Type","application/json")
6  $headers.Add("Authorization","CWSAuth bearer=XXXXXXX")
7
8  $uri = "https://trust.citrixworkspacesapi.net/HubCustomerID/links"
9
10 $resp = Invoke-RestMethod -Method Get -Uri $uri -Headers $headers
11 $allLinks = $resp.linkedCustomers + @("SpokeCustomerID")
12
13 $body = @{
14  "customers"=$allLinks }
15
16 $bodyjson = $body | ConvertTo-Json
17
18 $resp = Invoke-WebRequest -Method Post -Uri $uri -Headers $headers
       -Body $bodyjson -ContentType 'application/json'
19 Write-Host "Citrix Cloud Status Code: $($resp.RawContent)"
20 <!--NeedCopy-->
```

2. Sur la ligne 4, remplacez `CWSAuth bearer=XXXXXXX` par votre valeur CWSAuth (par exemple, `CWSAuth bearer=AbCdef123Ghik...`). Cette valeur est un hachage long qui ressemble à une clé de certificat.
3. Sur la ligne 6, remplacez `HubCustomerID` par l'ID client du compte hub.
4. Sur la ligne 9, remplacez `SpokeCustomerID` par l'ID client du compte spoke.
5. Exécutez le script.
6. Répétez les étapes 3 à 5 pour lier d'autres comptes en tant que spokes.

Pour dissocier des comptes Citrix Cloud

1. Ouvrez PowerShell ISE. Si PowerShell ISE est déjà ouvert, désactivez le volet de travail.
2. Collez le script suivant dans le volet de travail :

```
1  $headers = @{
```



```
2    }
3
4  $headers.Add("Accept","application/json")
5  $headers.Add("Content-Type","application/json")
6  $headers.Add("Authorization","CWSAuth bearer=XXXXXXX")
7
8  $uri = "https://trust.citrixworkspacesapi.net/HubCustomerID/links/
       SpokeCustomerID"
9
10 $resp = Invoke-WebRequest -Method Delete -Uri $uri -Headers
       $headers
11 Write-Host "Response: $($resp.RawContent)"
12 <!--NeedCopy-->
```

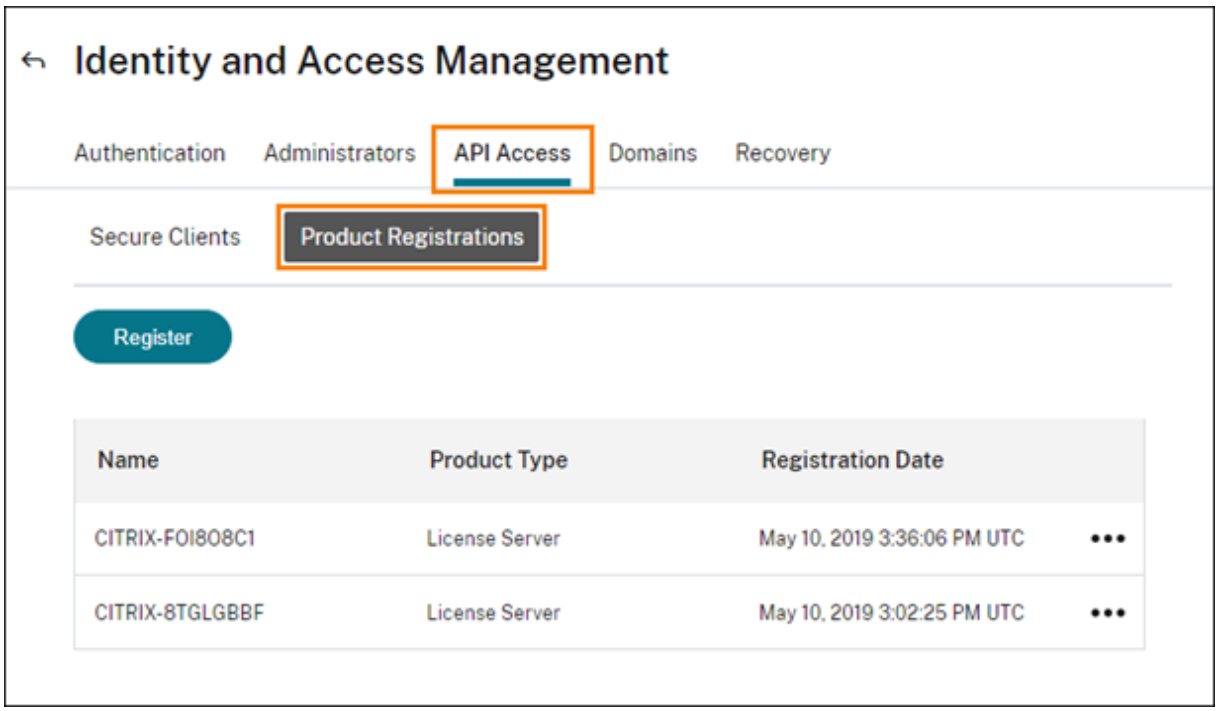
3. Sur la ligne 4, remplacez `CWSAuth bearer=xxxxxxx1` par votre valeur CWSAuth (par exemple, `CWSAuth bearer=AbCdef123Ghik...`). Cette valeur est un hachage long qui ressemble à une clé de certificat.
4. Sur la ligne 6, remplacez `HubCustomerID` par l'ID client du compte hub.
5. Sur la ligne 6, remplacez `SpokeCustomerID` par l'ID client du compte spoke.
6. Exécutez le script.
7. Répétez les étapes 4 à 6 pour dissocier d'autres comptes.

Enregistrer des produits locaux avec Citrix Cloud

October 4, 2023

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.

Après l'enregistrement, la page Enregistrements de produits (**Gestion des identités et des accès > Accès API > Enregistrements de produits**) affiche les serveurs sur lesquels résident vos produits enregistrés.



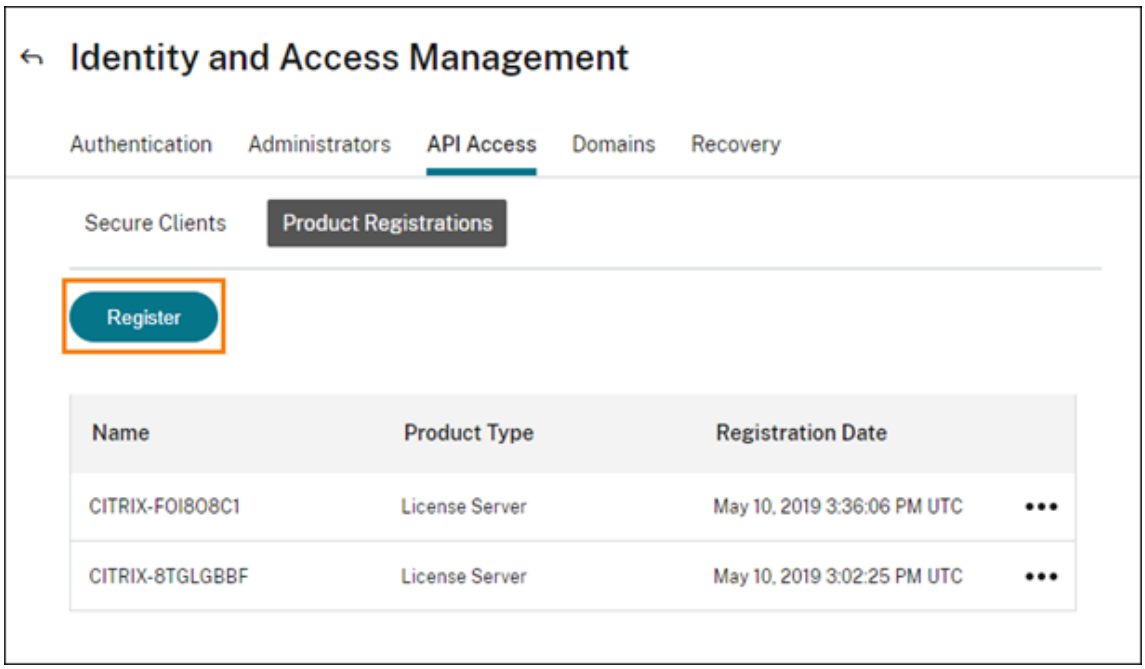
Les produits sur site que vous pouvez enregistrer auprès de Citrix Cloud incluent :

- Citrix Connector Appliance pour les services cloud
- Service d'authentification fédérée de Citrix
- Serveur de licences Citrix
- Citrix Virtual Apps and Desktops, lors de l'enregistrement d'un site auprès de Citrix Analytics for Performance

> **Remarque :**
>
> Cet article décrit les étapes à suivre pour enregistrer un produit sur site auprès de Citrix Cloud. Pour connaître les exigences spécifiques au produit, consultez la documentation de ce produit.

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**.

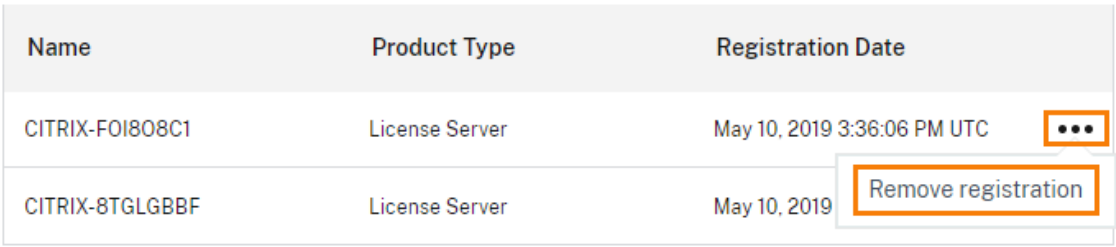


3. Entrez le code alphanumérique à 8 caractères correspondant à votre produit Citrix et cliquez sur **Continuer**.
4. Vérifiez les détails de l'enregistrement, puis cliquez sur **Enregistrer**.

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**.

Connecter Active Directory à Citrix Cloud

July 2, 2024

Citrix Cloud prend en charge l'utilisation de votre instance Active Directory (AD) locale pour authentifier les abonnés à l'espace de travail. En outre, certaines méthodes d'authentification d'espace de travail nécessitent une connexion entre votre AD et Citrix Cloud. Pour plus d'informations, consultez Choisir ou modifier les méthodes d'authentification.

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.

Connexion à Active Directory

La connexion de votre Active Directory à Citrix Cloud implique l'installation de connecteurs dans votre domaine. Vous pouvez choisir d'utiliser des Cloud Connector ou Connector Appliance comme connecteurs pour Active Directory. Pour choisir le type de connecteur à utiliser pour votre environnement, consultez les articles suivants :

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

Connexion à Active Directory via des Connector Appliance

Vous pouvez utiliser des Connector Appliance pour connecter un emplacement de ressources à des forêts qui ne contiennent pas de ressources Citrix Virtual Apps and Desktops. Par exemple, dans le cas des clients Citrix Secure Private Access ou des clients Citrix Virtual Apps and Desktops dont certaines forêts sont uniquement utilisées pour l'authentification des utilisateurs.

Pour plus d'informations, voir Active Directory avec Connector Appliance

Connexion à Active Directory via des Cloud Connector

Au moins deux Cloud Connector sont nécessaires pour garantir une connexion haute disponibilité à Citrix Cloud. Pour plus d'informations, consultez les articles suivants :

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

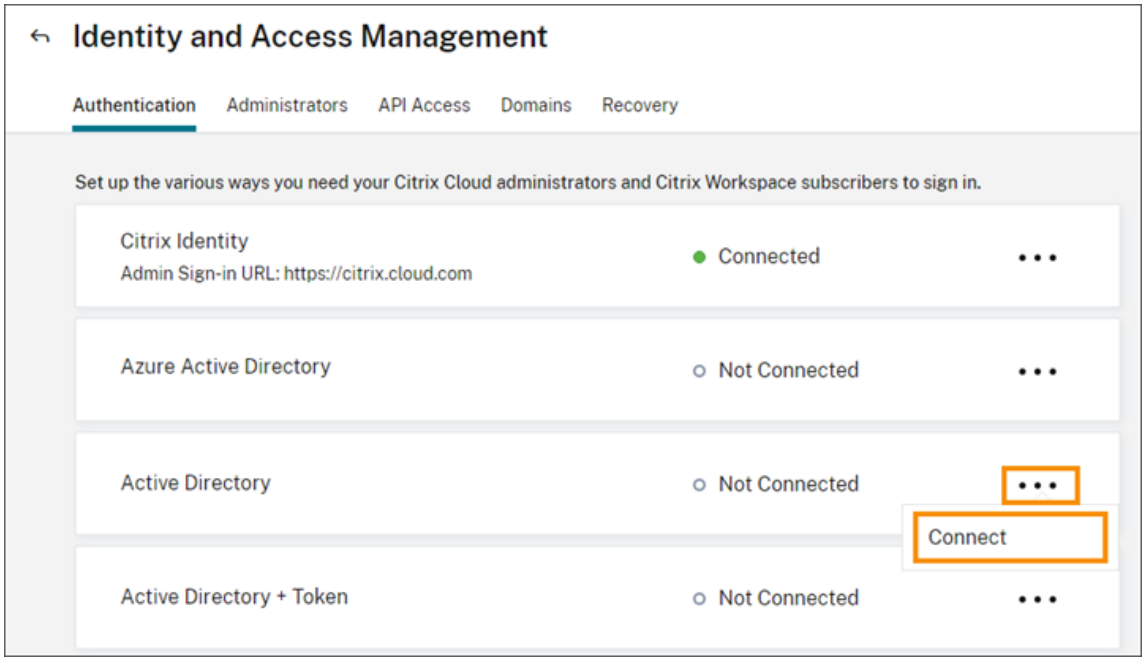
La connexion d'Active Directory à Citrix Cloud implique les tâches suivantes :

1. Installez 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.

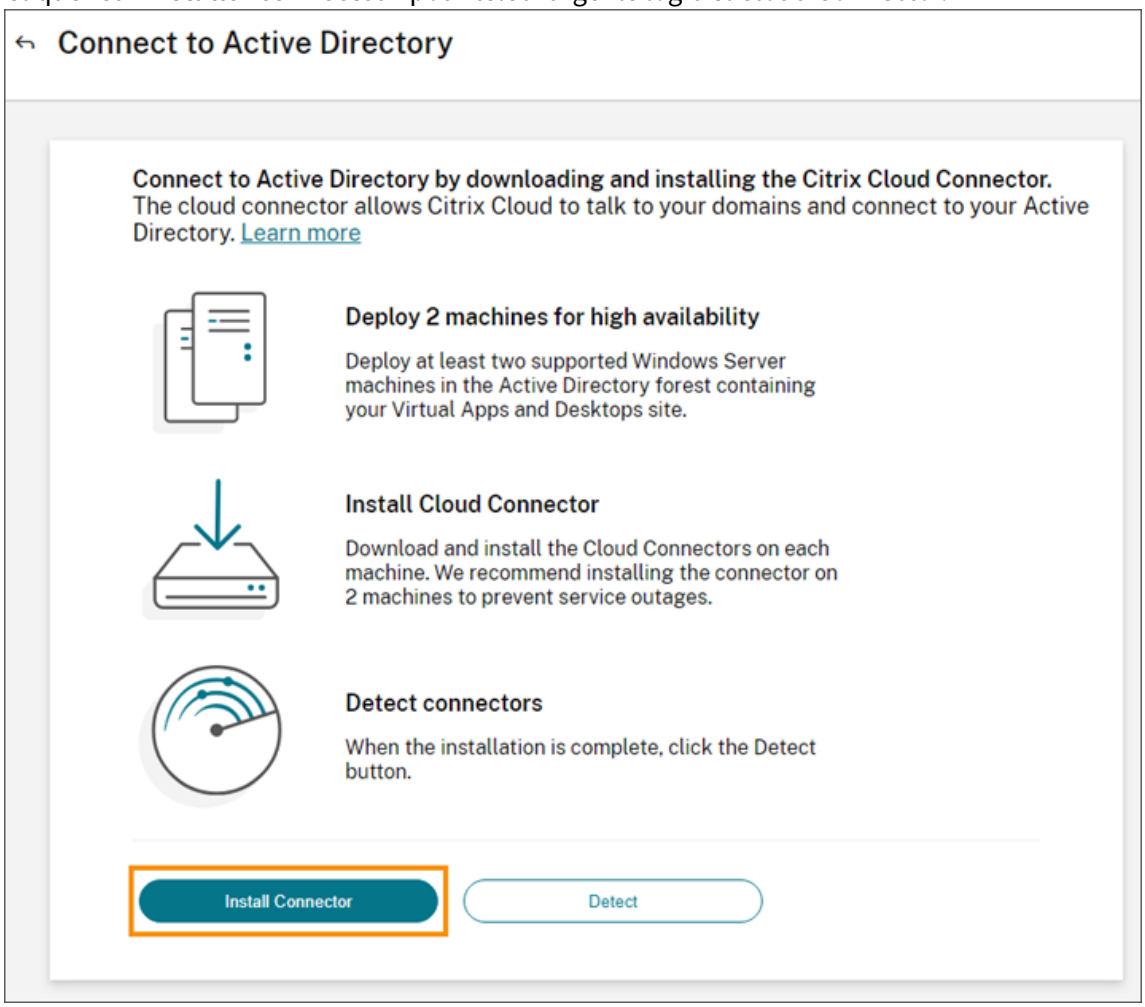
> **Important :**
>
> Si vous déployez des Cloud Connector pour les utiliser avec Citrix DaaS, des étapes supplémentaires peuvent être nécessaires pour garantir que vos domaines AD sont enregistrés et actifs après le déploiement des Cloud Connector. En vérifiant que vos domaines AD sont actifs dans Citrix Cloud, vous garantissez une configuration fluide du catalogue de machines. Pour plus d'informations sur les étapes à suivre après le déploiement de Citrix DaaS, consultez Ajouter un type de ressource ou activer un domaine inutilisé dans Citrix Cloud dans la documentation du produit Citrix DaaS.

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.

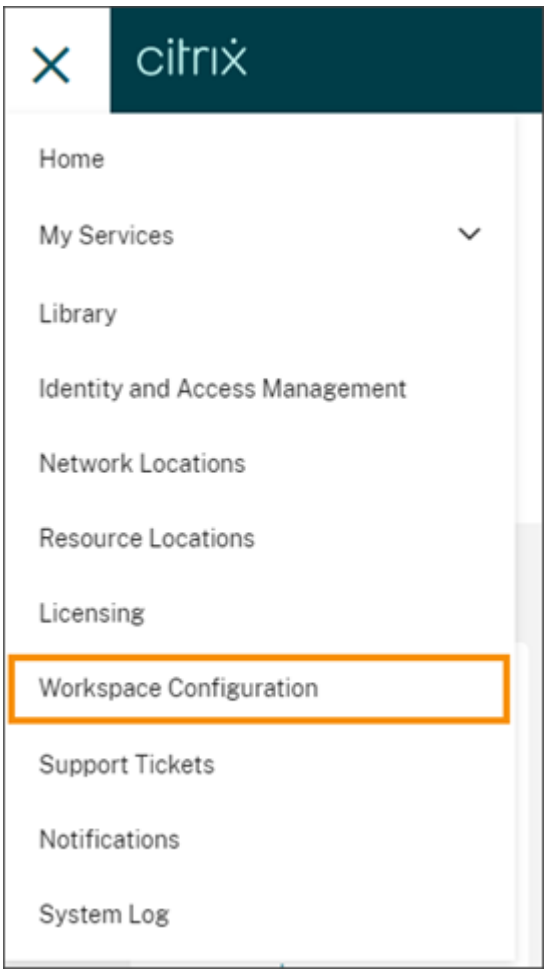


4. Lancez le programme d'installation de Cloud Connector et suivez les instructions de l'assistant d'installation.
5. Dans la page **Se connecter à Active Directory**, cliquez sur **Détecter**. Après vérification, Citrix Cloud affiche un message indiquant que votre Active Directory est connecté.
6. Cliquez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

Activer l'authentification Active Directory + jeton

1. Connectez Active Directory à Citrix Cloud à l'aide de Connector Appliance ou de Cloud Connector.
2. Dans la section **Gestion des identités et des accès** de Citrix Cloud, sous l'onglet **Authentification**, vérifiez que l'entrée **Active Directory** est marquée comme **Activé**.
3. Cliquez sur **Suivant**. La page **Configurer un jeton** s'affiche et l'option **Appareil unique** est sélectionnée par défaut.
4. Cliquez sur **Enregistrer et terminer** pour terminer la configuration. Sous l'onglet **Authentification**, l'entrée **Active Directory + jeton** est marquée comme **Activé**.
5. 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 à l'espace de travail peuvent 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 la section Authentification à deux facteurs (facultatif).

Pour connaître les options de réinscription des appareils des abonnés, consultez la section Réinscrire un appareil.

Informations supplémentaires

Citrix Tech Zone :

- Tech Insight : Authentification - TOTP
- Tech Insight : Authentification - Push

Connecter Azure Active Directory à Citrix Cloud

May 31, 2024

Citrix Cloud prend en charge l'utilisation d'Azure Active Directory (AD) pour authentifier les administrateurs Citrix Cloud et les abonnés à l'espace de travail.

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.

Application Azure AD et autorisations

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 l'introduction de cette application, Citrix a publié des mises à jour qui améliorent les performances et prennent en charge de nouvelles fonctionnalités et autorisations.

Si vous disposez d'une connexion Azure AD existante à Citrix Cloud et que vous souhaitez utiliser la dernière application mise à jour, vous devez mettre à jour votre connexion Azure AD dans Citrix Cloud. Pour plus d'informations, consultez Se reconnecter à Azure AD pour l'application mise à niveau dans cet article. Si vous choisissez de ne pas mettre à jour l'application, votre connexion existante continue de fonctionner normalement.

Pour plus d'informations sur les applications Azure AD et les autorisations que Citrix Cloud utilise pour se connecter à votre instance Azure AD, consultez Autorisations Azure Active Directory pour 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.

Authentification avec plusieurs comptes Citrix Cloud

Cet article explique comment connecter Azure AD en tant que fournisseur d'identité à un seul compte Citrix Cloud. Si vous possédez plusieurs comptes Citrix Cloud, vous pouvez les connecter au même locataire Azure AD. Effectuez les tâches suivantes :

1. Connectez-vous à votre compte Citrix Cloud et sélectionnez l'ID client approprié dans le sélecteur de clients.
2. Si le client sélectionné est le premier que vous connectez à votre Azure AD, suivez toutes les étapes décrites dans cet article pour synchroniser votre AD et Azure AD, connecter le client à Citrix Cloud et ajouter des administrateurs.
3. Pour connecter un autre client, cliquez sur le menu utilisateur dans le coin supérieur droit de la console Citrix Cloud, sélectionnez **Changer de client**, puis sélectionnez l'ID client suivant que vous souhaitez connecter.
4. Connectez le client à votre Azure AD comme décrit dans Connecter Citrix Cloud à Azure AD dans cet article.
5. Répétez les étapes 3 et 4 pour chaque ID client.

Préparer votre Active Directory et Azure AD

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

- Vous devez disposer d'un compte Microsoft Azure. Azure AD est fourni gratuitement avec chaque compte Azure. Si vous ne disposez pas d'un compte Azure, inscrivez-vous sur https://azure.microsoft.com/en-us/free/?v=17.36.
- Vous disposez du rôle d'administrateur général 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 l'article Prise en main d'Azure AD Connect à l'aide de paramètres express sur le site Web 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 (ou le profil de l'utilisateur connecté) ainsi qu'aux profils de base des utilisateurs dans votre instance 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. Pour plus d'informations sur les autorisations d'application demandées par Citrix Cloud, consultez Autorisations Azure Active Directory pour Citrix Cloud.

> **Important :**
>
> Vous devez disposer du rôle d'administrateur général dans Azure AD pour effectuer cette tâche ou demander à un administrateur général de d'appliquer les conditions préalables avant de vous connecter à Citrix Cloud.

1. Cliquez sur **Menu** dans le coin supérieur gauche de la page et sélectionnez **Gestion des identités et des accès**.
2. Recherchez Azure Active Directory et sélectionnez **Se connecter** dans le menu des points de suspension.
3. 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.
4. 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. La plupart de ces autorisations sont en lecture seule et 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 plus d'informations, consultez Autorisations Azure Active Directory pour Citrix Cloud.
5. Cliquez sur **Accepter** pour accepter la demande d'autorisations.

Méthode de connexion alternative

Vous pouvez séparer le flux de connexion selon les deux phases suivantes :

1. Création de l'application Azure AD (Entra ID) dans Azure.
2. Connexion Citrix Cloud à l'application Azure AD (Entra ID) dans Citrix Cloud.

Tout d'abord, vous devez créer une URL que l'administrateur général peut utiliser pour ajouter les applications d'entreprise au locataire. Pour plus d'informations, voir Construire l'URL pour accorder le consentement de l'administrateur au niveau du locataire.

Voici l'explication de l'URL construite.
`https://login.microsoftonline.com/<tenant url>/adminconsent?client_id=f9c0e999-22e7-409f-bb5e-956986abdf02&redirect_uri=https://portal.azure.com`

où :
`tenant url` est l'URL ou l'ID de votre locataire.
`f9c0e999-22e7-409f-bb5e-956986abdf02` est l'ID de client de Citrix Cloud.

Ajouter des administrateurs à Citrix Cloud depuis Azure AD

Citrix Cloud prend en charge l'ajout d'administrateurs individuellement ou en tant que groupes Azure AD.

Pour ajouter des administrateurs individuels à partir d'Azure AD, voir Gérer l'accès des administrateurs.

Pour ajouter des groupes d'administrateurs Azure AD à Citrix Cloud, consultez Gérer les groupes d'administrateurs.

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

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

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

Activer l'authentification Azure AD pour les espaces de travail

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

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

1. Dans Citrix Cloud, cliquez sur le bouton de menu situé dans le coin supérieur gauche et sélectionnez **Configuration de l'espace de travail**.
2. Dans l'onglet **Authentification**, sélectionnez **Azure Active Directory**.
3. Cliquez sur **Confirmer** pour accepter les modifications apportées à l'expérience d'espace de travail lorsque l'authentification Azure AD est activée.

Activer les fonctionnalités avancées d'Azure AD

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

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

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

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 l'introduction de cette application, Citrix a effectué les mises à jour suivantes :

- En août 2018, l'application a été mise à niveau pour améliorer les performances et vous permettre d'être prêt pour les versions futures.
- En mai 2019, l'application a été mise à jour pour prendre en charge l'ajout de groupes d'administrateurs Azure AD à Citrix Cloud.
- En avril 2022, l'application a été mise à jour pour utiliser l'autorisation GroupMember.Read.All qui remplace l'autorisation Group.Read.All.

Si vous avez connecté votre instance Azure AD à Citrix Cloud avant la publication de ces mises à jour et que vous souhaitez utiliser la dernière application mise à jour, vous devez déconnecter votre instance

Azure AD de Citrix Cloud, puis la reconnecter. L'utilisation de la dernière application est facultative. Si vous choisissez de ne pas mettre à jour l'application, votre connexion existante continue de fonctionner normalement.

Exigences

Avant de reconnecter votre instance Azure AD, vérifiez que vous répondez aux exigences suivantes :

- Vous devez être un administrateur disposant d'autorisations d'accès complet sous le fournisseur d'identité Citrix par défaut. Si vous êtes connecté à Citrix Cloud avec vos informations d'identification Azure AD, la reconnexion échoue. Si aucun administrateur n'utilise le fournisseur d'identité Citrix dans votre compte, vous pouvez en ajouter un temporairement et le supprimer après avoir reconnecté votre instance Azure AD. Pour obtenir des instructions, voir Inviter des administrateurs individuels.
- Si vous utilisez Azure AD pour authentifier les abonnés de l'espace de travail, sélectionnez temporairement un autre fournisseur d'identité. Citrix Cloud ne vous permet pas de déconnecter votre instance Azure AD si elle est également utilisée comme méthode d'authentification pour Citrix Workspace. Pour plus d'informations, consultez la section Choisir ou modifier les méthodes d'authentification dans la documentation de Citrix Workspace.

Pour se reconnecter à Azure AD

1. Connectez-vous à Citrix Cloud en tant qu'administrateur disposant d'autorisations d'accès complet sous le fournisseur d'identité Citrix.
2. Dans le menu Citrix Cloud, sélectionnez **Gestion des identités et des accès**, puis sélectionnez **Authentification**.
3. Recherchez **Azure Active Directory** et sélectionnez **Déconnecter** dans le menu des points de suspension à droite de la page.
4. Dans le menu des points de suspension, sélectionnez **Connecter**.

> **Remarque :**
>
> Si vous déconnectez Azure Active Directory comme indiqué à l'étape 3, Citrix Cloud demande à l'administrateur de supprimer tous les profils d'administrateur sous ce fournisseur d'identité. Pour contourner cet effort, l'administrateur peut suivre les étapes ci-dessous pour reconnecter le fournisseur d'identité Azure AD.
>
> 1. En tant qu'administrateur général, accédez à Azure et supprimez l'application.
> 2. Connectez-vous à Citrix Cloud, accédez à **Gestion des identités et des accès**, puis cliquez sur **Authentification**. Dans l'onglet **Authentification**, vous pouvez remarquer qu'Azure AD est toujours connecté.

3. Ajoutez un nouvel administrateur dans Citrix Cloud pour Azure AD.

Cela déclenchera la recréation de l'application et la reconnexion sans supprimer les administrateurs.

Autorisations Azure Active Directory pour Citrix Cloud

December 13, 2023

Cet article décrit les autorisations demandées par Citrix Cloud lors de la connexion et de l'utilisation d'Azure Active Directory (AD). Selon la façon dont Azure AD est utilisé avec le compte Citrix Cloud, une ou plusieurs applications d'entreprise peuvent être créées dans le locataire Azure AD cible. Vous pouvez connecter plusieurs comptes Citrix Cloud à un locataire Azure AD et utiliser les mêmes applications d'entreprise, sans créer d'ensemble d'applications pour chaque compte.

Remarque :

En avril 2022, l'application Azure AD utilisée par Citrix Cloud pour connecter votre instance Azure AD a été mise à jour pour utiliser l'autorisation GroupMember.Read.All au lieu de l'autorisation Group.Read.All. Si vous disposez d'une connexion Azure AD existante (avant avril 2022) et que vous souhaitez que l'application utilise la nouvelle autorisation, vous devez déconnecter, puis reconnecter votre instance Azure AD à Citrix Cloud. Cette action garantit que votre compte utilise la dernière application Azure AD dans Citrix Cloud. Pour plus d'informations, consultez Se reconnecter à Azure AD pour l'application mise à niveau.

Si vous choisissez de ne pas mettre à jour l'application, votre connexion existante continue de fonctionner normalement.

Applications d'entreprise

Le tableau suivant répertorie les applications d'entreprise Azure AD que Citrix Cloud utilise lors de la connexion et de l'utilisation d'Azure AD et la fonction de chaque application.

Nom	ID de l'application	Utilisation
Citrix Cloud	e95c4605-aeab-48d9-9c36-1a262ef8048e	Connexion de l'abonné Workspace
Citrix Cloud	f9c0e999-22e7-409f-bb5e-956986abdf02	Connexion par défaut entre Azure AD et Citrix Cloud

Nom	ID de l'application	Utilisation
Citrix Cloud	1b32f261-b20c-4399-8368-c8f0092b4470	Invitations et connexions d'administrateur
Citrix Cloud	5c913119-2257-4316-9994-5e8f3832265b	Connexion par défaut entre Azure AD et Citrix Cloud avec Citrix Endpoint Management
Citrix Cloud	e067934c-b52d-4e92-b1ca-70700bd1124e	Ancienne connexion entre Azure AD et Citrix Cloud avec Citrix Endpoint Management

Autorisations

Les autorisations dans les applications d'entreprise de Citrix Cloud permettent à Citrix Cloud d'accéder à certaines données de votre locataire Azure AD. Citrix Cloud utilise ces données pour effectuer des fonctions spécifiques, telles que la connexion à votre locataire Azure AD, la possibilité pour les administrateurs de se connecter à Citrix Cloud à l'aide d'une URL de connexion dédiée et la connexion de votre locataire Azure AD à Endpoint Management. Citrix Cloud ne peut accéder à ces données qu'avec votre consentement. Ces autorisations représentent le minimum de privilèges requis par Citrix Cloud pour fonctionner avec votre Azure AD. Pour plus d'informations sur les autorisations et le consentement pour Azure AD, consultez Autorisations et consentement dans la plateforme d'identités Microsoft sur le site Web de la documentation Microsoft Azure.

Dans cet article, chaque ensemble d'autorisations d'application Azure AD inclut les informations suivantes :

- **Nom de l'API :** applications de ressources auprès desquelles Citrix Cloud demande des autorisations. Ces applications sont Microsoft Graph et Windows Azure Active Directory. Citrix Cloud demande les mêmes autorisations à ces deux applications de ressources.
- **Type :** niveaux d'accès requis par Citrix Cloud pour une autorisation donnée. Les autorisations d'une application d'entreprise donnée peuvent avoir l'un des niveaux d'accès suivants :
  - Les **autorisations déléguées** sont utilisées pour agir au nom d'un utilisateur connecté, par exemple lors de l'interrogation du profil de l'utilisateur.
  - Les **autorisations d'application** sont utilisées lorsque l'application exécute une action sans la présence de l'utilisateur, par exemple lors de l'interrogation d'utilisateurs au sein d'un groupe particulier. Ce type d'autorisation nécessite le consentement d'un administrateur général dans Azure AD.
- **Valeur de revendication :** chaîne d'informations qu'Azure AD attribue à une autorisation donnée. Les autorisations d'une application d'entreprise donnée peuvent avoir l'une des valeurs

de revendication suivantes :

- **User.Read :** permet aux administrateurs Citrix Cloud d'ajouter des utilisateurs de l'instance Azure AD connectée en tant qu'administrateurs sur le compte Citrix Cloud.
- **User.ReadBasic.All :** collecte des informations de base à partir du profil de l'utilisateur. Il s'agit d'un sous-ensemble de User.Read.All, mais l'autorisation elle-même est conservée pour la rétrocompatibilité.
- **User.Read.All :** Citrix Cloud appelle List users dans Microsoft Graph pour permettre la recherche et la sélection d'utilisateurs de l'instance Azure AD connectée du client. Par exemple, les utilisateurs d'Azure AD peuvent avoir accès à une ressource Citrix DaaS avec l'espace de travail. Citrix Cloud ne peut pas utiliser `User.ReadBasic.All` car Citrix Cloud doit accéder à des propriétés en dehors du profil de base telles que `onPremisesSecurityIdentifier`.
- **GroupMember.Read.All :** Citrix Cloud appelle List groups dans Microsoft Graph pour permettre la recherche et la sélection de groupes de l'instance Azure AD connectée du client. Par exemple, les groupes d'Azure AD peuvent également avoir accès aux applications Citrix DaaS.
- **Directory.Read.All :** Citrix Cloud appelle List memberOf dans Microsoft Graph pour obtenir l'appartenance à un groupe de l'utilisateur, car `Groups.Read.All` ne suffit pas.
- **DeviceManagementApps.ReadWrite.All :** permet à Citrix Cloud de lire et d'écrire les propriétés, les attributions de groupe, l'état des applications, les configurations d'applications et les stratégies de protection des applications gérées par Microsoft Intune.
- **Directory.AccessAsUser.All :** permet à Citrix Cloud d'avoir le même accès aux informations de répertoire que l'utilisateur connecté.

> **Remarque :**
>
> **Directory.Read.All** s'applique uniquement à la **connexion par défaut entre Azure AD et Citrix Cloud avec Endpoint Management**.

Connexion de l'abonné Workspace

Cette application Citrix Cloud (ID : e95c4605-aeab-48d9-9c36-1a262ef8048e) utilise les autorisations suivantes :

API Name	Valeur de revendication	Nom de l'autorisation	Type
Microsoft Graph	User.Read	Connecter et lire le profil utilisateur	Délégué

Connexion par défaut entre Azure AD et Citrix Cloud

Cette application Citrix Cloud (ID : f9c0e999-22e7-409f-bb5e-956986abdf02) utilise les autorisations suivantes :

API Name	Valeur de revendication	Autorisation	Type
Microsoft Graph	GroupMember.Read.All	Lire tous les groupes	Délégué
Microsoft Graph	User.ReadBasic.All	Lire les profils de base de tous les utilisateurs	Délégué
Microsoft Graph	User.Read.All	Lire les profils complets de tous les utilisateurs	Délégué
Microsoft Graph	User.Read	Connecter et lire le profil utilisateur	Délégué
Microsoft Graph	GroupMember.Read.All	Lire tous les groupes	Application
Microsoft Graph	User.Read.All	Lire les profils complets de tous les utilisateurs	Application
Microsoft Graph	User.Read	Connecter et lire le profil utilisateur	Application

Invitations et connexions d'administrateur

Cette application Citrix Cloud (ID : 1b32f261-b20c-4399-8368-c8f0092b4470) utilise les autorisations suivantes :

API Name	Valeur de revendication	Nom de l'autorisation	Type
Microsoft Graph	User.Read	Connecter et lire le profil utilisateur	Délégué
Microsoft Graph	User.ReadBasic.All	Lire les profils de base de tous les utilisateurs	Délégué

Connexion par défaut entre Azure AD et Citrix Cloud avec Endpoint Management

Cette application Citrix Cloud (ID : 5c913119-2257-4316-9994-5e8f3832265b) utilise les autorisations suivantes :

API Name	Valeur de revendication	Nom de l'autorisation	Type
Microsoft Graph	GroupMember.Read.All	Lire tous les groupes	Délégué
Microsoft Graph	User.ReadBasic.All	Lire les profils de base de tous les utilisateurs	Délégué
Microsoft Graph	User.Read	Connecter et lire le profil utilisateur	Délégué
Microsoft Graph	Directory.Read.All	Lire les données de répertoire	Application
Microsoft Graph	Directory.Read.All	Lire les données de répertoire	Délégué
Microsoft Graph	DeviceManagementApps.ReadWrite.All	Lire et écrire des applications Microsoft Intune	Délégué
Microsoft Graph	Directory.AccessAsUser.All	Accéder au répertoire en tant qu'utilisateur connecté	Délégué

Connexion d'ancienne génération entre Azure AD et Citrix Cloud avec Endpoint Management

Cette application Citrix Cloud (ID : e067934c-b52d-4e92-b1ca-70700bd1124e) utilise les autorisations suivantes :

API Name	Valeur de revendication	Nom de l'autorisation	Type
Microsoft Graph	GroupMember.Read.All	Lire tous les groupes	Délégué
Microsoft Graph	User.ReadBasic.All	Lire les profils de base de tous les utilisateurs	Délégué
Microsoft Graph	User.Read	Connecter et lire le profil utilisateur	Délégué
Microsoft Graph	DeviceManagementApps.ReadWrite.All	Lire et écrire des applications Microsoft Intune	Délégué
Microsoft Graph	Directory.AccessAsUser.All	Accéder au répertoire en tant qu'utilisateur connecté	Délégué

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

July 2, 2024

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 :

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

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

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

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, consultez 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 (MFA) 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.

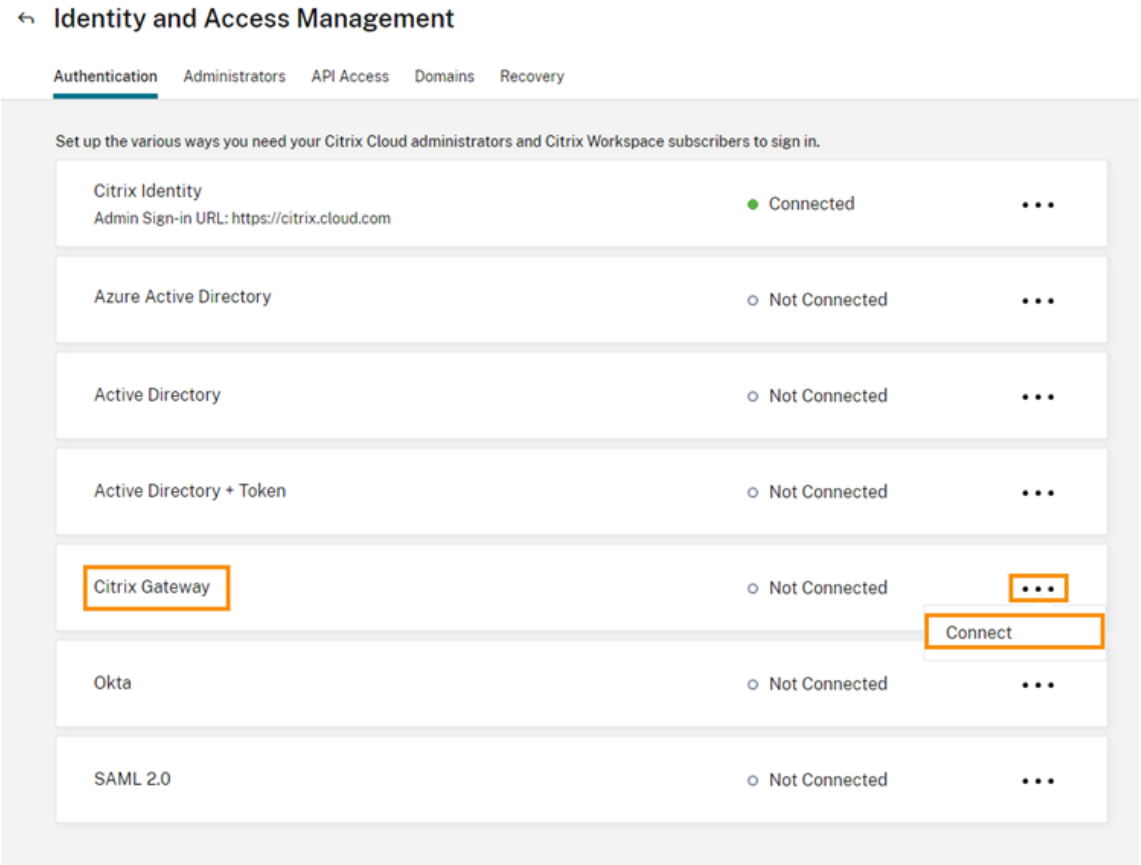
Vue d'ensemble des tâches

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

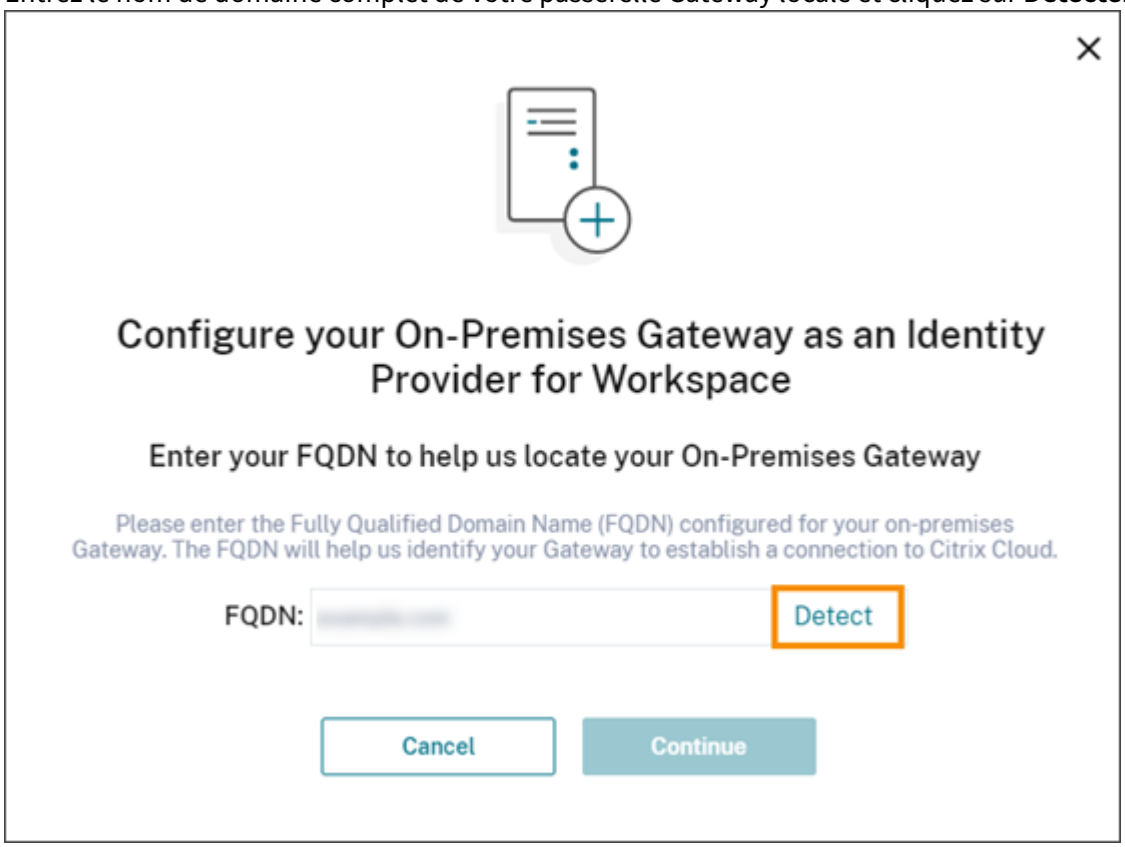
1. Dans **Gestion des identités et des accès**, commencez à configurer la connexion à votre passerelle. Au cours de cette étape, vous générez l'ID client, le secret et l'URL de redirection pour Gateway.
2. Sur Gateway, créez une stratégie avancée de fournisseur d'identité OAuth à l'aide des informations 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 à 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**.



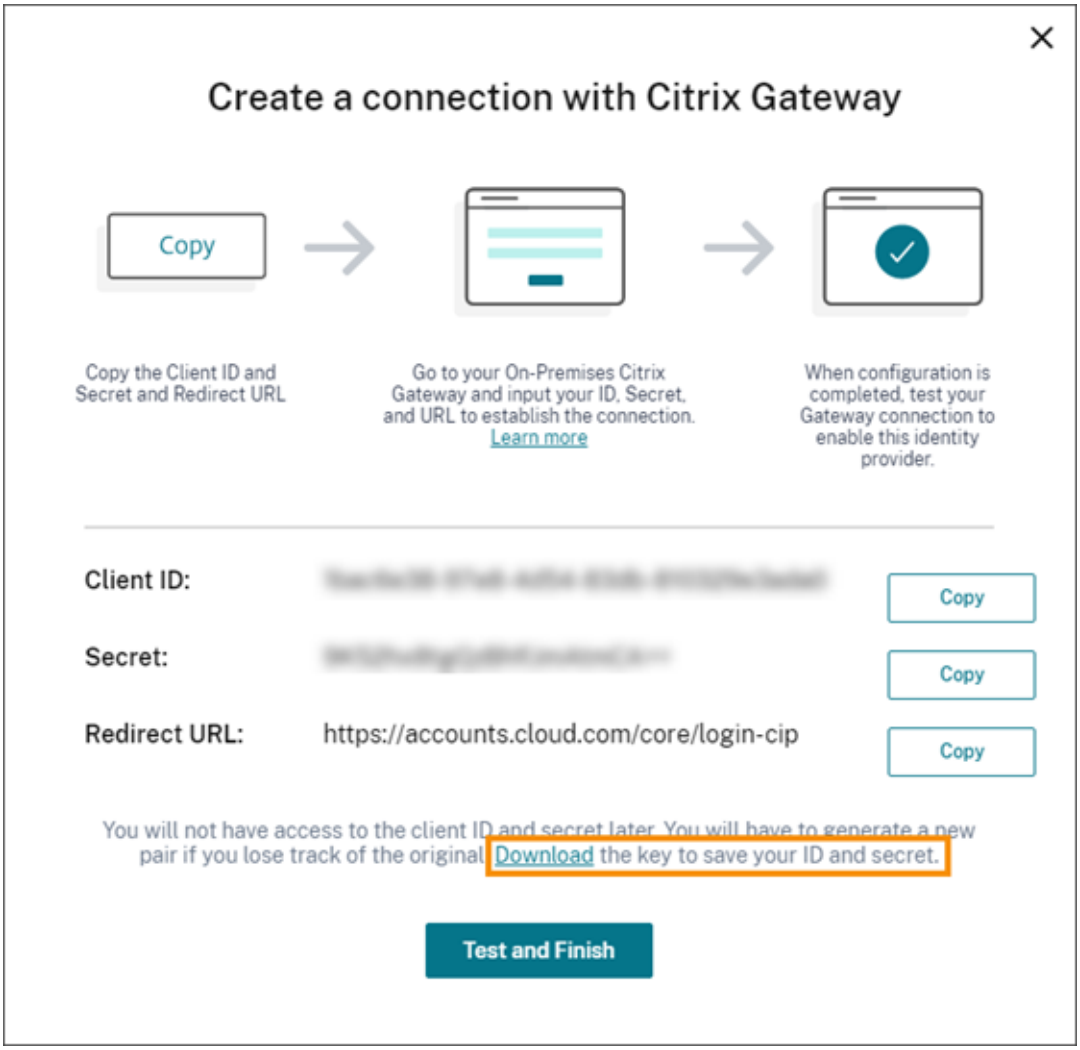
3. Entrez le nom de domaine complet de votre passerelle Gateway locale et cliquez sur **Détecter**.



   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 également 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 :

- 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

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**.

Dépannage

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 Gateway dans Citrix Cloud.
- Vous avez entré correctement l'URL de Gateway dans le paramètre `-issuer` de la stratégie de fournisseur d'identité OAuth. Exemple : `-issuer https://GatewayFQDN.com`. Le paramètre `issuer` est sensible à la casse.
- Les valeurs d'ID client, de clé secrète client 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 (MFA) 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.

Informations supplémentaires

Citrix Tech Zone : Tech Insight : Authentification - Passerelle

Connecter Google Cloud Identity en tant que fournisseur d'identité à Citrix Cloud

October 4, 2023

Citrix Cloud prend en charge l'utilisation de Google Cloud Identity en tant que fournisseur d'identité pour authentifier les abonnés qui se connectent à leurs espaces de travail. En connectant le compte Google de votre organisation à Citrix Cloud, vous pouvez fournir une expérience de connexion unifiée pour accéder aux ressources de Citrix Workspace et de Google.

Exigences relatives à une configuration appartenant ou non à un domaine

Vous pouvez configurer Google Cloud Identity en tant que fournisseur d'identité dans Citrix Cloud à l'aide d'une machine appartenant ou non à un domaine.

- L'appartenance à un domaine signifie que les machines sont jointes à un domaine de votre Active Directory (AD) local et que l'authentification utilise les profils utilisateur qui y sont stockés.
- L'absence d'appartenance à un domaine signifie que les machines ne sont pas jointes à un domaine AD et que l'authentification utilise les profils utilisateur stockés dans votre annuaire Google Workspace (également appelés utilisateurs natifs de Google).

Le tableau suivant répertorie les exigences pour chaque type de configuration.

Exigences	Joint à un domaine	Non joint au domaine	Informations supplémentaires
AD local	Oui	Non	Consultez la section Préparer Active Directory et les Citrix Cloud Connector dans cet article.
Citrix Cloud Connector déployés dans votre emplacement de ressources	Oui	Non ; les Cloud Connector ne sont pas nécessaires pour accéder aux machines n'appartenant pas à un domaine.	Préparer Active Directory et les Citrix Cloud Connector dans cet article.
Synchronisation d'AD avec Google Cloud	Facultatif uniquement si vous utilisez Gateway Service et aucun autre service. Dans le cas contraire, cette tâche est obligatoire.	Non	Consultez Synchroniser Active Directory avec Google Cloud Identity dans cet article.
Un compte développeur avec accès à la console Google Cloud Platform. Utilisé pour créer un compte de service et une clé, et activer Admin SDK API.	Oui	Oui	Consultez les sections Créer un compte de service, Créer une clé de compte de serviceet Configurer la délégation au niveau du domaine dans cet article.
Un compte administrateur avec accès à la console d'administration de Google Workspace. Utilisé pour configurer la délégation au niveau du domaine et un compte utilisateur d'API en lecture seule.	Oui	Oui	Consultez les sections Configurer la délégation au niveau du domaine et Ajouter un compte utilisateur d'API en lecture seule dans cet article.

Authentification avec plusieurs comptes Citrix Cloud

Cet article explique comment connecter Google Cloud Identity en tant que fournisseur d'identité à un seul compte Citrix Cloud. Si vous disposez de plusieurs comptes Citrix Cloud, vous pouvez connecter chacun d'eux au même compte Google Cloud à l'aide du même compte de service et du même compte utilisateur d'API en lecture seule. Il vous suffit de vous connecter à Citrix Cloud et de sélectionner l'ID client approprié dans le sélecteur de clients.

Préparer Active Directory et les Citrix Cloud Connector

Si vous utilisez une machine **jointe à un domaine** avec Google Cloud Identity, utilisez cette section pour préparer votre AD local. Si vous utilisez une machine non jointe à un domaine, ignorez cette tâche et passez à la section Créer un compte de service dans cet article.

Vous devez disposer d'au moins deux (2) serveurs dans votre domaine Active Directory sur lesquels installer le logiciel Citrix Cloud Connector. Les composants Cloud Connector sont requis pour établir la communication entre Citrix Cloud et vos emplacements des ressources. Au moins deux Cloud Connector sont nécessaires pour garantir une connexion haute disponibilité avec Citrix Cloud. Ces serveurs doivent satisfaire aux exigences suivantes :

- Répondre aux exigences décrites dans Détails techniques sur Cloud Connector.
- Aucun autre composant Citrix ne doit être installé sur ces serveurs, ils ne doivent pas être un contrôleur de domaine Active Directory ou une machine critique à votre infrastructure d'emplacement de ressources.
- 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 la section 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.

Synchroniser Active Directory avec Google Cloud Identity

Si vous utilisez une machine **jointe à un domaine** avec Google Cloud Identity, utilisez cette section pour préparer votre AD local. Si vous utilisez une machine non jointe à un domaine, ignorez cette tâche et passez à la section Créer un compte de service dans cet article.

La synchronisation de votre AD avec Google Cloud Identity est facultative si vous utilisez uniquement Citrix Gateway Service, et qu'aucun autre service n'est activé. Pour ces services uniquement, vous pouvez utiliser des utilisateurs natifs de Google sans avoir à vous synchroniser avec votre AD.

Si vous utilisez d'autres services Citrix Cloud, la synchronisation de votre AD avec Google Cloud Identity est requise. Google Cloud doit transmettre les attributs d'utilisateur AD suivants à Citrix Cloud :

- SecurityIDentifier (SID)
- objectGUID
- userPrincipalName (UPN)

Pour synchroniser votre AD avec Google Cloud

1. Téléchargez et installez l'utilitaire Google Cloud Directory Sync à partir du site Web de Google. Pour plus d'informations sur cet utilitaire, consultez la documentation Google Cloud Directory Sync sur le site Web de Google.
2. Après avoir installé l'utilitaire, lancez Configuration Manager (**Démarrer > Configuration Manager**).
3. Spécifiez les paramètres de domaine Google et les paramètres LDAP comme décrit dans la section Configurer la synchronisation avec le gestionnaire de configuration de la documentation de l'utilitaire.
4. Dans **General Settings**, sélectionnez **Custom Schemas**. Laissez les sélections par défaut inchangées.
5. Configurez un schéma personnalisé à appliquer à tous les comptes d'utilisateurs. Saisissez les informations requises en utilisant la casse et l'orthographe exactes spécifiées dans cette section.

    a) Sélectionnez l'onglet **Custom Schemas**, puis **Add Schema**.
    b) Sélectionnez **Use rules defined dans "User Accounts"**.
    c) Dans **Schema Name**, saisissez **citrix-schema**.
    d) Sélectionnez **Add Field**, puis entrez les informations suivantes :
        - Sous **Schema field template**, dans **Schema Field**, sélectionnez **userPrincipalName**.
        - Sous **Google field details**, dans **Field Name**, saisissez **UPN**.
    e) Répétez l'étape 4 pour créer les champs suivants :
        - objectGUID : sous **Schema field template**, sélectionnez **objectGUID**. Sous **Google field details**, saisissez **objectGUID**.
        - SID : sous **Schema field template**, sélectionnez **Custom**. Sous **Google field details**, saisissez **SID**.
        - objectSID : sous **Schema field template**, sélectionnez **Custom**. Sous **Google field details**, saisissez **objectSID**.

f) Cliquez sur **OK** pour enregistrer vos entrées.

6. Terminez la configuration des paramètres restants pour votre organisation et vérifiez les paramètres de synchronisation comme décrit dans la section Configurer la synchronisation avec le gestionnaire de configuration de la documentation de l'utilitaire.
7. Sélectionnez **Sync & apply changes** pour synchroniser votre Active Directory avec votre compte Google.

Une fois la synchronisation terminée, la section User Information de Google Cloud affiche les informations Active Directory des utilisateurs.

Créer un compte de service

Pour effectuer cette tâche, vous devez disposer d'un compte développeur Google Cloud Platform.

1. Connectez-vous à https://console.cloud.google.com.
2. Dans la barre latérale du Tableau de bord, sélectionnez **IAM et Administration**, puis **Comptes de service**.
3. Sélectionnez **Créer un compte de service**.
4. Sous **Détails du compte de service**, saisissez le nom du compte de service et l'ID du compte de service.
5. Sélectionnez **Terminé**.

Créer une clé de compte de service

1. Sur la page **Comptes de service**, sélectionnez le compte de service que vous avez créé.
2. Sélectionnez l'onglet **Clés**, puis sélectionnez **Ajouter une clé > Créer une clé**.
3. Laissez l'option de type de clé JSON par défaut sélectionnée.
4. Sélectionnez **Créer**. Conservez la clé dans un emplacement sécurisé auquel vous pourrez accéder ultérieurement. Vous entrez la clé privée dans la console Citrix Cloud lorsque vous connectez Google Cloud Identity en tant que fournisseur d'identité.

Configurer la délégation au niveau du domaine

1. Activez Admin SDK API :

   a) Dans le menu Google Cloud Platform, sélectionnez **API et services > API et services activés**.
   b) Sélectionnez **Activer les API et les services** en haut de la console. La page d'accueil de la bibliothèque d'API apparaît.
   c) Recherchez **Admin SDK API** et sélectionnez-la dans la liste des résultats.

d) Sélectionnez **Activer**.

2. Créez un client API pour le compte de service :

a) Dans le menu Google Cloud Platform, sélectionnez **IAM et Administration > Comptes de service**, puis sélectionnez le compte de service que vous avez créé précédemment.

b) Dans l'onglet **Détails** du compte de service, développez **Paramètres avancés**.

c) Sous **Délégation au niveau du domaine**, copiez l'ID client, puis sélectionnez **Afficher la console d'administration Google Workspace**.

d) Le cas échéant, sélectionnez le compte d'administrateur Google Workspace que vous souhaitez utiliser. La console d'administration Google s'affiche.

e) Dans la barre latérale Google Admin, sélectionnez **Sécurité > Contrôle de l'accès et des données > Commandes des API**.

f) Sous **Délégation au niveau du domaine**, cliquez sur **Gérer la délégation au niveau du domaine**.

g) Sélectionnez **Ajouter**.

h) Dans **ID client**, collez l'ID client du compte de service que vous avez copié à l'étape C.

i) Dans les **Habilitations OAuth**, entrez les habilitations suivantes sur une seule ligne délimitée par des virgules :

```
1 https://www.googleapis.com/auth/admin.directory.user.readonly,
     https://www.googleapis.com/auth/admin.directory.group.
     readonly,https://www.googleapis.com/auth/admin.directory.
     domain.readonly
2 <!--NeedCopy-->
```

j) Sélectionnez **Autoriser**.

Ajouter un compte utilisateur d'API en lecture seule

Dans cette tâche, vous allez créer un compte d'utilisateur Google Workspace disposant d'un accès API en lecture seule pour Citrix Cloud. Ce compte n'est utilisé à aucune autre fin et ne dispose d'aucun autre privilège.

1. Dans le menu Administration de Google, sélectionnez **Annuaire > Utilisateurs**.
2. Sélectionnez **Ajouter un utilisateur** et saisissez les informations utilisateur appropriées.
3. Sélectionnez **Ajouter un utilisateur** pour enregistrer les informations du compte.
4. Créez un rôle personnalisé pour le compte d'utilisateur en lecture seule :

a) Dans le menu Administration de Google, sélectionnez **Compte > Rôles d'administrateur**.

b) Sélectionnez **Créer un rôle**.

c) Entrez un nom pour le nouveau rôle. Exemple : API-Readonly

d) Sélectionnez **Continue**.
e) Sous **Droits de l'API Admin**, sélectionnez les droits suivants :
   - Utilisateurs > Lire
   - Groupes > Lire
   - Gestion des domaines
f) Sélectionnez **Continuer**, puis **Créer un rôle**.

5. Attribuez le rôle personnalisé au compte d'utilisateur en lecture seule que vous avez créé précédemment :
   a) Sur la page des détails du rôle personnalisé, dans le volet **Admins**, sélectionnez **Attribuer des utilisateurs**.
   b) Commencez à taper le nom du compte d'utilisateur en lecture seule et sélectionnez-le dans la liste des utilisateurs.
   c) Sélectionnez **Attribuer un rôle**.
   d) Pour vérifier l'attribution des rôles, revenez à la page Utilisateurs (**Annuaire > Utilisateurs**) et sélectionnez le compte d'utilisateur en lecture seule. L'attribution de rôle personnalisé s'affiche sous **Rôles et droits d'administrateur**.

Connecter Google Cloud Identity à Citrix Cloud

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 **Google Cloud Identity** et sélectionnez **Connecter** dans le menu des points de suspension.
4. Lorsque vous y êtes invité, saisissez un identifiant court et descriptif pour votre entreprise et sélectionnez **Enregistrer et continuer**. L'identifiant que vous choisissez doit être globalement unique au sein de Citrix Cloud.
5. Sélectionnez **Importer un fichier**, puis sélectionnez le fichier JSON que vous avez enregistré lorsque vous avez créé la clé pour le compte de service. Cette action importe votre clé privée et l'adresse e-mail du compte de service Google Cloud que vous avez créé.
6. Dans **Utilisateur représenté**, entrez le nom du compte utilisateur de l'API en lecture seule.
7. Sélectionnez **Suivant**. Citrix Cloud vérifie les détails de votre compte Google et teste la connexion.
8. Passez en revue les domaines associés répertoriés. S'ils sont corrects, sélectionnez **Confirmer** pour enregistrer votre configuration.

Ajouter des administrateurs à Citrix Cloud

Vous pouvez ajouter des administrateurs Citrix Cloud individuels et des groupes d'administrateurs via Google Cloud. Pour plus d'informations, consultez les articles suivants :

- Pour les administrateurs individuels : Gérer l'accès des administrateurs à Citrix Cloud
- Pour les groupes d'administrateurs : Gérer les groupes d'administrateurs

Une fois que vous avez ajouté des administrateurs à Citrix Cloud, ils peuvent se connecter à l'aide de l'une des méthodes suivantes :

- Accéder à l'URL de connexion administrateur que vous avez configurée lors de la configuration initiale de Google Cloud en tant que fournisseur d'identité. Exemple : `https://citrix.cloud.com/go/mycompany`
- À partir de la page de connexion de Citrix Cloud, sélectionner **Se connecter avec mes identifiants d'entreprise**, entrer l'identifiant unique pour leur entreprise (par exemple « monentreprise ») et cliquer sur **Continuer**.

Activer Google Cloud Identity pour l'authentification de l'espace de travail

1. Dans le menu Citrix Cloud, sélectionnez **Configuration de l'espace de travail > Authentification**.
2. Sélectionnez **Google Cloud Identity**. Lorsque vous y êtes invité, sélectionnez **Je comprends l'impact sur l'expérience des abonnés** et cliquez sur **Enregistrer**.

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

July 2, 2024

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 DaaS (anciennement 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 la section Connecter le Service d'authentification fédérée Citrix à Citrix Cloud.

Conditions préalables

Cloud Connector ou appliances Connector

Les Cloud Connector ou les appliances Connector sont requis pour établir la communication entre Citrix Cloud et vos emplacements des ressources. Au moins deux Cloud Connector ou deux appliances Connector sont nécessaires pour garantir une connexion haute disponibilité avec Citrix Cloud. Vous devez associer au moins deux connecteurs à votre domaine Active Directory. Il peut s'agir de Cloud Connector ou d'appliances Connector.

Les connecteurs doivent répondre aux exigences suivantes :

- Répondre aux exigences décrites dans leurs documentations respectives
- Appartenir à votre domaine Active Directory (AD). Si les utilisateurs de votre espace de travail résident dans plusieurs domaines, la fonctionnalité multi-domaines de l'appliance Connector peut être utilisée pour joindre plusieurs domaines.
- 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 la section 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.
Pour plus d'informations sur l'installation des appliances Connector, consultez la section Installation des appliances 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 Customize the Okta URL domain sur le site Web Okta.

Pour savoir comment trouver le domaine personnalisé de votre organisation, consultez la page Finding Your Okta Domain 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 intégration d'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 d'API, consultez Créer un jeton API Okta dans cet article. Pour plus d'informations sur les jetons API, consultez la page Create an API token 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, consultez la page Get started with Active Directory integration sur le site Web Okta.

Vous importez ensuite vos utilisateurs et groupes AD dans Okta. Lors de l'importation, incluez les valeurs suivantes associées à vos comptes AD :

- E-mail
- SID
- UPN
- OID

> 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 et les instructions d'importation Okta, consultez la page Manage Active Directory users and groups sur le site Web d'Okta.

Créer une intégration d'application Web Okta OIDC

1. Dans la console de gestion Okta, sous **Applications**, sélectionnez **Applications**.
2. Sélectionnez **Create App Integration**.
3. Dans **Sign in method**, sélectionnez **OIDC - OpenID Connect**.
4. Dans **Application type**, sélectionnez **Web Application**. Sélectionnez **Suivant**.
5. Dans **App Integration Name**, entrez un nom convivial pour l'intégration de l'application.
6. Dans **Grant type**, sélectionnez un code d'autorisation sous **Authorization Code** (sélectionné par défaut).

7. Dans **Sign-in redirect URIs**, entrez `https://accounts.cloud.com/core/login-okta`.
8. Dans **Sign-out redirect URIs**, entrez l'URL de votre espace de travail à partir de Citrix Cloud.
9. Sous **Assignments**, dans **Controlled access**, indiquez si vous souhaitez attribuer l'intégration de l'application à tous les membres de votre organisation, uniquement aux groupes que vous spécifiez, ou si vous souhaitez attribuer un accès ultérieurement.
10. Sélectionnez **Save**. Après avoir enregistré l'intégration de l'application, la console affiche la page de configuration de l'application.
11. Dans la section **Client Credentials**, copiez les valeurs de **Client ID** et **Client Secret**. Vous utilisez ces valeurs lorsque vous connectez Citrix Cloud à votre organisation Okta.

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. (Facultatif) Mettez à jour les autorisations du client pour le type d'autorisation implicite. Vous pouvez choisir d'effectuer cette étape si vous préférez accorder le moins de privilèges pour ce type d'autorisation.

    a) Sur la page de configuration de l'application Okta, dans l'onglet **General**, accédez à la section **General Settings** et sélectionnez **Edit**.
    b) Dans la section **Application**, dans **Grant type**, sous **Client acting on behalf of a user**, désactivez le paramètre **Allow Access Token with implicit grant type**.
    c) Sélectionnez **Save**.

2. 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) Sélectionnez le profil **User (default)**. Okta affiche la page de profil **utilisateur**.
    c) Sous **Attributes**, sélectionnez **Add attribute**.
    d) Entrez les informations suivantes :

        - Nom d'affichage : cip_email
        - Nom de la variable : cip_email
        - Description : adresse e-mail de l'utilisateur AD
        - Longueur de l'attribut : sélectionnez **Supérieur à**, puis entrez **1**.
        - Attribut requis : Oui

    e) Sélectionnez **Save and Add Another**.
    f) 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 : sélectionnez **Supérieur à**, puis entrez **1**.
- Attribut requis : Oui

g) Sélectionnez **Save and Add Another**.

h) 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 : sélectionnez **Supérieur à**, puis entrez **1**.
- Attribut requis : Oui

i) Sélectionnez **Save and Add Another**.

j) Entrez les informations suivantes :

- Nom complet : cip_oid
- Nom de la variable : cip_oid
- Description : GUID utilisateur AD
- Longueur de l'attribut : sélectionnez **Supérieur à**, puis entrez **1**.
- Attribut requis : Oui

k) Sélectionnez **Save**.

3. Modifiez les mappages d'attributs pour l'application :

a) Dans la console Okta, sélectionnez **Directory > Profile Editor**.

b) Localisez le profil **active_directory** de votre AD. Ce profil peut être étiqueté à l'aide du format `myDomain User`, où `myDomain` est le nom de votre domaine AD intégré.

c) Sélectionnez **Mappings**. La page User Profile Mappings de votre domaine AD s'affiche et l'onglet permettant de mapper votre AD à Okta User est sélectionné.

d) Dans la colonne **Okta User User Profile**, localisez les attributs que vous avez créés à l'étape 2 et mappez comme suit :

- Pour `cip_email`, sélectionnez `email` dans la colonne Profil utilisateur de votre domaine. Lorsque cette option est sélectionnée, le mappage apparaît comme `appuser.email`.
- Pour `cip_sid`, sélectionnez `objectSid` dans la colonne Profil utilisateur de votre domaine. Lorsque cette option est sélectionnée, le mappage apparaît comme `appuser.objectSid`.
- Pour `cip_upn`, sélectionnez `userName` dans la colonne Profil utilisateur de votre domaine. Lorsque cette option est sélectionnée, le mappage apparaît comme `appuser.userName`.
- Pour `cip_oid`, sélectionnez `externalId` dans la colonne Profil utilisateur de votre domaine. Lorsque cette option est sélectionnée, le mappage apparaît comme

`appuser.externalId`.

e) Sélectionnez **Save Mappings**.
f) Sélectionnez **Apply updates now**. Okta lance une tâche pour appliquer les mappages.
g) Synchronisez Okta avec votre AD.
   i. Dans la console Okta, sélectionnez **Directory > Directory Integrations**.
   ii. Sélectionnez votre AD intégré.
   iii. Sélectionnez l'onglet **Provisioning**.
   iv. Dans **Settings**, sélectionnez **To Okta**.
   v. Accédez à la section **Okta Attribute Mappings**, puis sélectionnez **Force Sync**.

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. Sélectionnez **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 de 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 client** et **Clé secrète client**, entrez l'ID client et la clé secrète de l'intégration de l'application Web OIDC que vous avez créée précédemment. 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.

Une fois la connexion vérifiée, vous pouvez activer l'authentification Okta pour les abonnés à l'espace de travail.

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**.
3. Lorsque vous y êtes invité, sélectionnez **Je comprends l'impact sur l'expérience des abonnés**.
4. Sélectionnez **Save**.

Après le passage à l'authentification Okta, Citrix Cloud désactive temporairement les espaces de travail pendant quelques minutes. Lorsque les espaces de travail sont réactivés, vos abonnés peuvent se connecter via Okta.

Informations supplémentaires

- Citrix Tech Zone :
  - Tech Insight : Authentification - Okta
  - Fiche technique : Identité Workspace
  - Fiche technique : Workspace SSO

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

July 2, 2024

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

À propos de cet article

Cet article décrit les étapes requises pour configurer une connexion entre Citrix Cloud et votre fournisseur SAML. Certaines de ces étapes 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 l'article, en fonction du fournisseur SAML choisi. Ces commandes du fournisseur SAML ne sont fournies qu'à titre d'exemple. Reportez-vous à la documentation de votre fournisseur SAML pour plus d'informations sur les commandes correspondantes de votre fournisseur SAML.

Configurations des fournisseurs SAML

Citrix propose les guides de configuration suivants pour garantir une interaction fluide entre votre fournisseur SAML et Citrix Cloud :

- SAML avec Active Directory Federated Services (ADFS) : consultez Configurer l'authentification SAML dans Citrix Cloud à l'aide d'ADFS.
- SAML avec identités Azure Active Directory : consultez Se connecter à des espaces de travail avec SAML à l'aide des identités Azure Active Directory.
- Application Citrix Cloud SAML SSO pour Azure AD : consultez Tutoriel : Intégration de l'authentification unique (SSO) Azure Active Directory à l'authentification unique SAML Citrix Cloud sur le site Web de documentation de l'application Microsoft Azure AD.
- SAML avec domaines personnalisés Citrix Workspace : consultez Se connecter à des espaces de travail avec SAML à l'aide de domaines personnalisés.
- SAML avec Okta : consultez Configurer Okta en tant que fournisseur SAML pour l'authentification de l'espace de travail.

Fournisseurs SAML pris en charge

Les fournisseurs SAML qui prennent en charge la spécification officielle SAML 2.0 sont compatibles avec Citrix Cloud.

Citrix a testé les fournisseurs SAML suivants pour l'authentification des administrateurs Citrix Cloud et pour l'authentification des abonnés Citrix Workspace à l'aide de l'authentification unique (SSO) et de la déconnexion unique (SLO). Les fournisseurs SAML qui ne figurent pas dans cette liste sont également pris en charge.

- Microsoft ADFS
- Microsoft Azure AD
- Duo
- Okta
- OneLogin
- PingOne SSO
- PingFederate

Lors du test de ces fournisseurs, Citrix a utilisé les paramètres suivants pour configurer la connexion SAML dans la console Citrix Cloud :

- Mécanisme de liaison : HTTP Post
- Réponse SAML : Signer la réponse ou l'assertion
- Contexte d'authentification : Non spécifié, Exact

Les valeurs de ces paramètres sont configurées par défaut lorsque vous configurez votre connexion SAML dans Citrix Cloud. Citrix recommande d'utiliser ces paramètres lors de la configuration de la connexion avec le fournisseur SAML que vous avez choisi.

Pour plus d'informations sur ces paramètres, consultez la section Ajouter des métadonnées du fournisseur SAML à Citrix Cloud dans cet article.

Prise en charge des ID d'entité étendue

Cet article explique comment configurer l'authentification SAML à l'aide d'une seule application SAML et de l'ID d'entité générique par défaut de Citrix Cloud.

Si vos exigences en matière d'authentification SAML incluent la nécessité de disposer de plusieurs applications SAML au sein d'un même fournisseur SAML, reportez-vous à la section Configurer une application SAML avec un ID d'entité étendue dans Citrix Cloud.

Logiciels requis

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

- Fournisseur SAML prenant en charge SAML 2.0
- Domaine AD 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 au moins deux serveurs pour garantir la haute disponibilité de Cloud Connector. Ces serveurs doivent satisfaire aux exigences suivantes :

- Répondre aux exigences système décrites dans Détails techniques sur Cloud Connector.
- Aucun autre composant Citrix ne doit être installé sur ces serveurs, ils ne doivent pas être un contrôleur de domaine AD 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 plus d'informations, consultez la section Configuration requise pour le système et la connectivité.

Pour de plus amples 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 les abonnés à votre espace de travail possèdent des comptes utilisateur dans votre AD. Les abonnés sans compte AD ne peuvent pas se connecter à leurs espaces de travail lorsque l'authentification SAML est configurée.
- Connectez votre AD à votre compte Citrix Cloud en déployant des Cloud Connector dans votre 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.

Attributs utilisateur AD Les attributs suivants sont obligatoires pour tous les objets utilisateur Active Directory et doivent être renseignés :

- Nom commun
- Nom du compte SAM
- User Principal Name (UPN)
- GUID d'objet
- SID

Citrix Cloud utilise les attributs GUID d'objet et SID de votre AD pour établir le contexte utilisateur lorsque les abonnés se connectent à Citrix Workspace. Si l'une ou l'autre de ces propriétés n'est pas renseignée, les abonnés ne peuvent pas se connecter.

Les attributs suivants ne sont pas obligatoires pour utiliser l'authentification SAML avec Citrix Cloud, mais Citrix recommande de les renseigner pour garantir une expérience utilisateur optimale :

- Adresse e-mail
- Nom d'affichage

Citrix Cloud utilise l'attribut Nom d'affichage pour afficher correctement les noms des abonnés dans Citrix Workspace. Si cet attribut n'est pas renseigné, les abonnés peuvent toujours se connecter, mais leur nom risque de ne pas s'afficher comme prévu.

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 :

- objectSID (SID)
- objectGUID (OID)
- userPrincipalName (UPN)
- Mail (adresse e-mail)
- Display Name (displayName)

Vous pouvez configurer un sous-ensemble de ces attributs, à condition que les attributs SID ou UPN soient inclus dans l'assertion SAML. Citrix Cloud récupère les autres attributs de votre AD selon les besoins.

> **Remarque :**
>
> Pour garantir des performances optimales, Citrix recommande de configurer tous les attributs mentionnés dans cette section.

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. Si vous utilisez ADFS comme fournisseur SAML, cette étape n'est pas obligatoire.
2. Créez des attributs personnalisés et associez-les aux attributs utilisateur AD requis mentionnés plus haut dans cette section. Pour référence, les étapes générales de cette tâche sont décrites dans la section Créer et mapper des attributs SAML personnalisés de cet article.
3. Synchronisez vos utilisateurs AD avec votre fournisseur SAML.

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

Authentification de l'administrateur avec SAML 2.0

Citrix Cloud prend en charge l'utilisation de SAML 2.0 pour authentifier les membres des groupes d'administrateurs dans AD. Pour plus d'informations sur l'ajout de groupes d'administrateurs à Citrix Cloud, consultez Gérer les groupes d'administrateurs.

Utilisation d'une connexion SAML existante pour l'authentification des administrateurs

Si vous disposez déjà d'une connexion SAML 2.0 dans Citrix Cloud et que vous souhaitez l'utiliser pour authentifier les administrateurs, vous devez d'abord déconnecter SAML 2.0 dans **Gestion des identités et des accès**, puis reconfigurer la connexion. Si vous utilisez votre connexion SAML pour authentifier les abonnés à Citrix Workspace, vous devez également désactiver la méthode d'authentification SAML dans **Configuration de l'espace de travail**. Après avoir reconfiguré la connexion SAML, vous pouvez ajouter des groupes d'administrateurs à Citrix Cloud.

Si vous essayez d'ajouter des groupes d'administrateurs sans avoir préalablement déconnecté et reconnecté SAML 2.0, l'option d'identité **Active Directory** décrite dans Ajouter un groupe d'administrateurs à Citrix Cloud n'apparaît pas.

Vue d'ensemble des tâches relatives à la configuration d'une nouvelle connexion SAML

Pour configurer une nouvelle connexion SAML 2.0 dans Citrix Cloud, vous devez effectuer 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. Configurez l'URL de connexion que les administrateurs peuvent utiliser pour se connecter à Citrix Cloud.
4. 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.

Vue d'ensemble des tâches relatives à l'utilisation d'une connexion SAML existante pour les administrateurs Citrix Cloud

Si vous disposez déjà d'une connexion SAML 2.0 dans Citrix Cloud et que vous souhaitez l'utiliser pour l'authentification des administrateurs, effectuez les tâches suivantes :

1. Le cas échéant, désactivez l'authentification SAML 2.0 Workspace : Dans **Configuration de l'espace de travail > Authentification**, sélectionnez une autre méthode d'authentification, puis sélectionnez **Confirmer** lorsque vous y êtes invité.
2. Déconnectez votre connexion SAML 2.0 existante : dans **Gestion des identités et des accès > Authentification**, localisez la connexion SAML. Dans le menu de points de suspension tout à droite, sélectionnez **Déconnecter**. Sélectionnez **Oui, déconnecter** pour confirmer l'action.

3. Reconnectez SAML 2.0 et configurez la connexion : dans le menu de points de suspension pour **SAML 2.0**, sélectionnez **Connecter**.
4. Lorsque vous y êtes invité, entrez un identifiant unique pour l'URL de connexion que les administrateurs utiliseront pour se connecter.
5. Configurez la connexion SAML comme décrit dans la section Configurer les métadonnées du fournisseur SAML de cet article.

Après avoir configuré votre connexion SAML, vous pouvez ajouter vos groupes d'administrateurs AD à Citrix Cloud comme décrit dans Gérer les groupes d'administrateurs. Vous pouvez également réactiver SAML pour les abonnés à Workspace comme décrit dans cet article.

Créer et mapper des attributs SAML personnalisés

Si vous disposez déjà d'attributs personnalisés pour les attributs SID, UPN, OID, email et displayName 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 5.

> **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 des attributs pour les propriétés AD suivantes. Nommez les attributs en utilisant les valeurs par défaut affichées.

Propriété AD	Requis ou facultatif	Valeur par défaut
userPrincipalName	Obligatoire si vous n'ajoutez pas d'attribut pour SID (recommandé).	`cip_upn`
objectSID	Obligatoire si vous n'ajoutez pas d'attribut pour UPN.	`cip_sid`

Propriété AD	Requis ou facultatif	Valeur par défaut
objectGUID	Facultatif pour l'authentification	`cip_oid`
mail	Facultatif pour l'authentification	`cip_email`
displayName	Requis par l'interface utilisateur de Workspace	`displayName`
givenName	Requis par l'interface utilisateur de Workspace	`firstName`
sn	Requis par l'interface utilisateur de Workspace	`lastName`
AD Forest	Facultatif pour l'authentification	`cip_forest`
AD Domain	Facultatif pour l'authentification	`cip_domain`

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 :
   - Si vous avez ajouté l'attribut pour SID à l'étape 2 (par exemple `cip_sid`), sélectionnez **objectSid** et associez-le à l'attribut que vous avez créé.
   - Si vous avez ajouté l'attribut pour UPN à l'étape 2 (par exemple `cip_upn`), sélectionnez **UserPrincipalName** et associez-le à l'attribut que vous avez créé.
   - Si vous avez ajouté l'attribut ObjectGUID à l'étape 2 (par exemple `cip_oid`), sélectionnez **ObjectGUID** et associez-le à l'attribut que vous avez créé.
   - Si vous avez ajouté l'attribut Mail à l'étape 2 (par exemple `cip_email`), sélectionnez **mail** et associez-le à l'attribut que vous avez créé.
   - Si vous avez ajouté l'attribut Display Name à l'étape 2 (par exemple, `displayName`), sélectionnez **displayName** et associez-le à l'attribut que vous avez créé.

Configurer l'URL de connexion de l'administrateur

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 de points de suspension.
4. Lorsque vous y êtes invité, saisissez un identifiant court et descriptif pour votre entreprise et sélectionnez **Enregistrer et continuer**. La page **Configurer SAML** s'affiche.
5. Passez à la section suivante pour configurer la connexion SAML à Citrix Cloud.

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. 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)**.
2. Le cas échéant, entrez un nom complet et enregistrez l'application.
3. 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.

   > **Remarque :**
   >
   > Si nécessaire, vous pouvez également télécharger ce fichier depuis `https://saml.cloud.com/saml/metadata.xml`. Ce point de terminaison peut être plus facile d'accès pour certains fournisseurs d'identité lors de l'importation et du monitoring des métadonnées du fournisseur SAML.

4. 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`.

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

Créer ce champ	Attribuer cet attribut personnalisé
cip_sid	L'attribut personnalisé que vous avez créé pour SID. Exemple : cip_sid
cip_upn	L'attribut personnalisé que vous avez créé pour UPN. Exemple : cip_upn
cip_oid	L'attribut personnalisé que vous avez créé pour ObjectGUID. Exemple : cip_oid
cip_email	L'attribut personnalisé que vous avez créé pour Mail. Exemple : cip_email
displayName	L'attribut personnalisé que vous avez créé pour Display Name. Exemple : displayName

6. 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 d'entité du fournisseur d'identité**, entrez la valeur **entityID** de l'élément **EntityDescriptor** dans les métadonnées.

     ```
     <EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="
     https://app. .com/saml/metadata/8c733cbd-c579-41d4-b4e1-4ff034893d19"
     ```

   - 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. Par défaut, **HTTP Post** est sélectionné.
- Dans **Réponse SAML**, sélectionnez la méthode de signature utilisée par votre fournisseur SAML pour la réponse SAML et l'assertion SAML. Par défaut, l'option **Signer la réponse ou l'assertion** est sélectionnée. 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, CRT ou CER encodé au format Base 64.

4. Sur la page **Configurer SAML** dans Citrix Cloud, sous **Certificat X.509**, sélectionnez **Charger le fichier** et sélectionnez le fichier de certificat 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 demander l'authentification dans le contexte sélectionné sans appliquer l'authentification dans ce contexte. Sélectionnez **Exact** pour demander l'authentification dans le contexte sélectionné et appliquer l'authentification uniquement dans ce contexte. 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**. Par défaut, **Non spécifié** et **Exact** sont sélectionnés.
7. Pour **URL de déconnexion** (facultatif), décidez si vous souhaitez que les utilisateurs qui se déconnectent de Citrix Workspace ou de Citrix Cloud se déconnectent également de toutes les applications Web auxquelles ils se sont précédemment connectés via le fournisseur SAML.

   - Si vous souhaitez que les utilisateurs restent connectés à leurs applications Web après s'être déconnectés de Citrix Workspace ou de Citrix Cloud, laissez le champ **URL de déconnexion** vide.
   - Si vous souhaitez que les utilisateurs se déconnectent de toutes les applications Web après s'être déconnectés de Citrix Workspace ou Citrix Cloud, entrez le point de terminaison SingleLogout (SLO) auprès de votre fournisseur SAML. Si vous utilisez Microsoft ADFS ou Azure

Active Directory comme fournisseur SAML, le point de terminaison SLO est identique au point de terminaison d'authentification unique (SSO).

8. Vérifiez que les valeurs d'attribut par défaut suivantes dans Citrix Cloud correspondent aux valeurs d'attribut correspondantes configurées dans votre fournisseur SAML. Pour que Citrix Cloud puisse trouver ces attributs dans l'assertion SAML, les valeurs saisies ici doivent correspondre à celles de votre fournisseur SAML. Si vous n'avez configuré aucun attribut spécifique dans votre fournisseur SAML, vous pouvez utiliser la valeur par défaut dans Citrix Cloud ou laisser le champ vide, sauf indication contraire.

   - **Nom d'attribut du nom d'affichage de l'utilisateur** : la valeur par défaut est `displayName`.
   - **Nom d'attribut du prénom de l'utilisateur** : la valeur par défaut est `firstName`.
   - **Nom d'attribut du nom de famille de l'utilisateur** : la valeur par défaut est `lastName`.
   - **Nom d'attribut de l'identificateur de sécurité (SID)** : vous devez saisir ce nom d'attribut depuis votre fournisseur SAML si vous n'avez pas créé d'attribut pour UPN. La valeur par défaut est `cip_sid`.
   - **Nom d'attribut du nom d'utilisateur principal (UPN)** : vous devez saisir ce nom d'attribut depuis votre fournisseur SAML si vous n'avez pas créé d'attribut pour le SID. La valeur par défaut est `cip_upn`.
   - **Nom d'attribut de l'e-mail** : la valeur par défaut est `cip_email`.
   - **Nom d'attribut de l'identificateur d'objet AD (OID)** : la valeur par défaut est `cip_oid`.
   - **Nom de l'attribut de la forêt AD** : la valeur par défaut est `cip_forest`.
   - **Nom d'attribut du domaine AD** : la valeur par défaut est `cip_domain`.

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

Ajouter des administrateurs à Citrix Cloud depuis AD

Pour obtenir des instructions sur l'ajout et la gestion de groupes AD dans Citrix Cloud, consultez Gérer les groupes d'administrateurs.

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**.

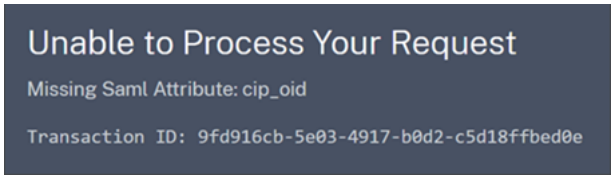
Dépannage

Erreurs d'attribut

Des erreurs d'attribut peuvent survenir dans l'une des conditions suivantes :

- Les attributs requis dans votre configuration SAML ne sont pas correctement codés.
- Les attributs `cip_sid` et `cip_upn` sont absents de l'assertion SAML.
- Les attributs `cip_sid` ou `cip_oid` sont absents de l'assertion SAML et Citrix Cloud ne peut pas les récupérer depuis Active Directory en raison d'un problème de connectivité.

Lorsqu'une erreur d'attribut se produit, Citrix Cloud affiche un message d'erreur qui inclut les attributs défectueux.



Pour résoudre ce type d'erreur, procédez comme suit :

1. Assurez-vous que votre fournisseur SAML envoie les attributs requis avec le codage correct, comme indiqué dans le tableau suivant. Au minimum, l'attribut SID ou UPN doit être inclus.

Attribut	Codage	Obligatoire
cip_email	Doit être au format de chaîne (`user@domain`)	
cip_oid	Doit être au format Base64 ou au format de chaîne	
cip_sid	Doit être au format Base64 ou au format de chaîne	Oui, si vous n'utilisez pas `cip_upn`
cip_upn	Doit être au format de chaîne (`user@domain`)	Oui, si vous n'utilisez pas `cip_sid`

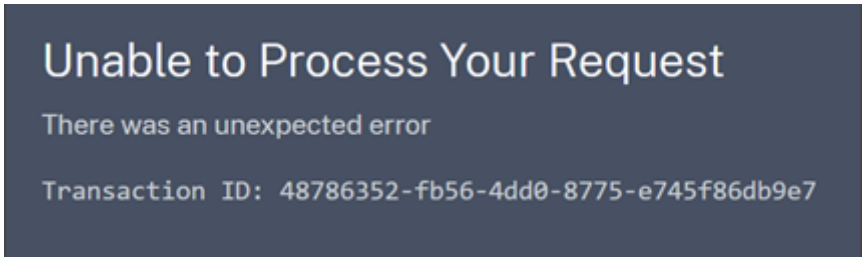
2. Vérifiez que les Cloud Connector sont en ligne et fonctionnent correctement afin que Citrix Cloud puisse récupérer les attributs manquants dont il a besoin. Pour plus d'informations, consultez la section Contrôles d'intégrité avancés de Cloud Connector.

Erreurs inattendues

Citrix Cloud peut rencontrer une erreur inattendue dans les cas suivants :

- Un utilisateur lance une demande SAML à l'aide d'un flux initié par le fournisseur d'identité. Par exemple, la demande est effectuée en sélectionnant une vignette via le portail d'applications du fournisseur d'identité au lieu d'accéder directement à l'URL de l'espace de travail (`customer.cloud.com`).
- Le certificat SAML n'est pas valide ou a expiré.
- Le contexte d'authentification n'est pas valide.
- L'assertion SAML et la signature de réponse ne correspondent pas.

Lorsque cette erreur se produit, Citrix Cloud affiche un message d'erreur générique.

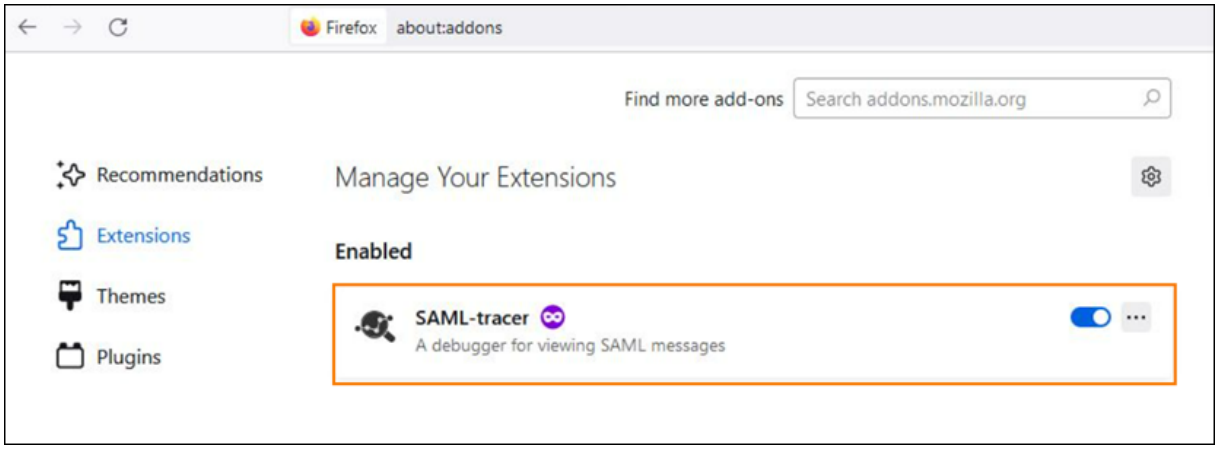


Si cette erreur résulte de la navigation vers Citrix Cloud via le portail d'applications d'un fournisseur d'identité, vous pouvez utiliser la solution suivante :

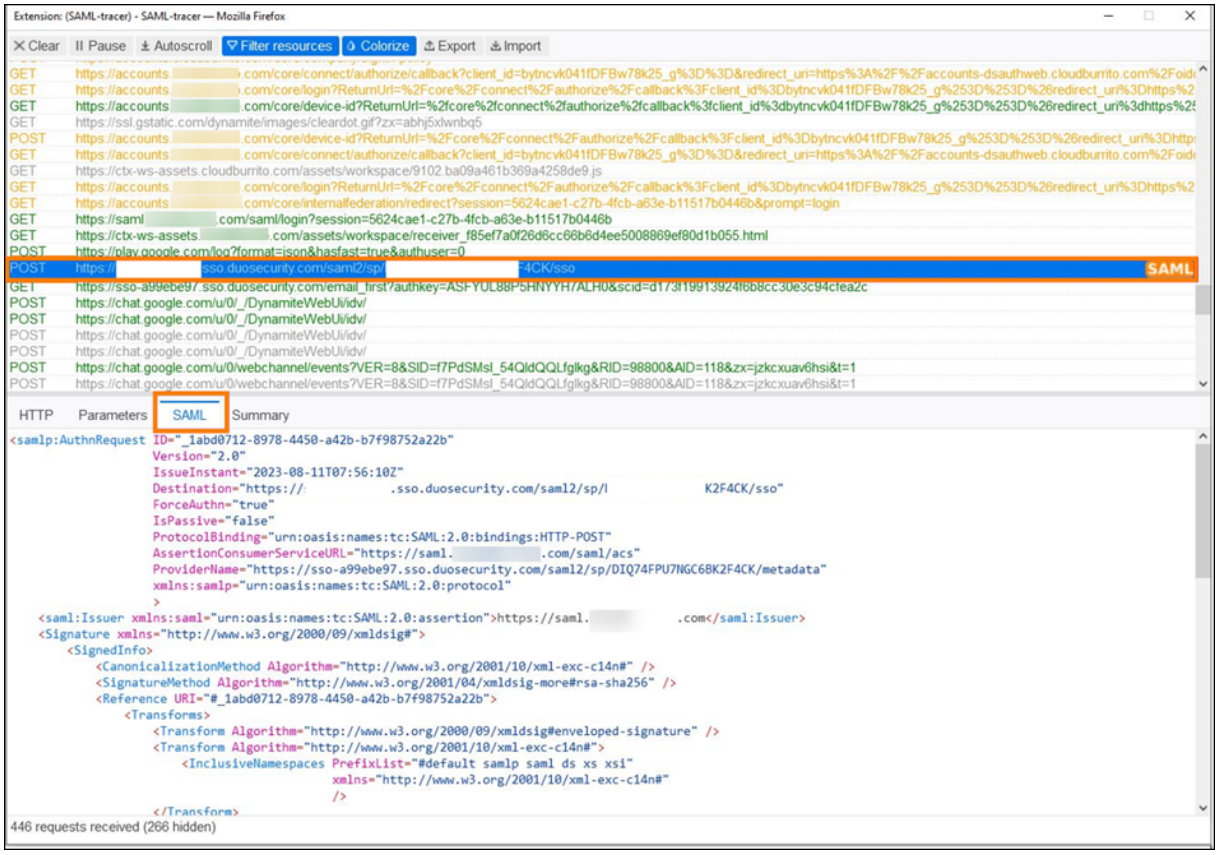
1. Créez une application de signet dans le portail d'applications du fournisseur d'identité qui fait référence à l'URL de votre espace de travail (par exemple, `https://customer.cloud.com`).
2. Attribuez les utilisateurs à la fois à l'application SAML et à l'application de signet.
3. Modifiez les paramètres de visibilité de l'application SAML et de l'application de signet afin que l'application de signet soit visible et que l'application SAML soit masquée dans le portail d'applications.
4. Désactivez le paramètre **Sessions de fournisseur d'identité fédéré** dans la configuration de l'espace de travail pour supprimer les demandes de mot de passe supplémentaires. Pour obtenir des instructions, consultez la section Sessions de fournisseur d'identité fédéré dans la documentation du produit Citrix Workspace.

Recommandations de débogage

Citrix recommande d'utiliser l'extension de navigateur SAML-tracer pour tous les débogages SAML. Cette extension est disponible pour la plupart des navigateurs Web courants. L'extension décode les requêtes et les réponses codées en Base64 en langage XML SAML, et les fournit donc en dans un format intelligible.



Cet outil vous permet, en tant qu'administrateur, de vérifier la valeur des attributs SAML envoyés à l'utilisateur et de rechercher la présence de signatures dans les requêtes et réponses SAML. Si vous avez besoin d'aide pour résoudre un problème lié à SAML, le support Citrix vous demandera de fournir le fichier de suivi SAML afin de comprendre le problème et de vous aider à le résoudre.



Informations supplémentaires

- Microsoft Docs : Tutoriel : Intégration de l'authentification unique (SSO) Azure Active Directory à l'authentification unique SAML Citrix Cloud
- SAML avec Active Directory Federated Services (ADFS) : Configurer l'authentification SAML dans Citrix Cloud à l'aide d'ADFS.
- Citrix Tech Zone : Tech Insight : Authentification - SAML

Configurer une application SAML avec un ID d'entité étendue dans Citrix Cloud

December 13, 2023

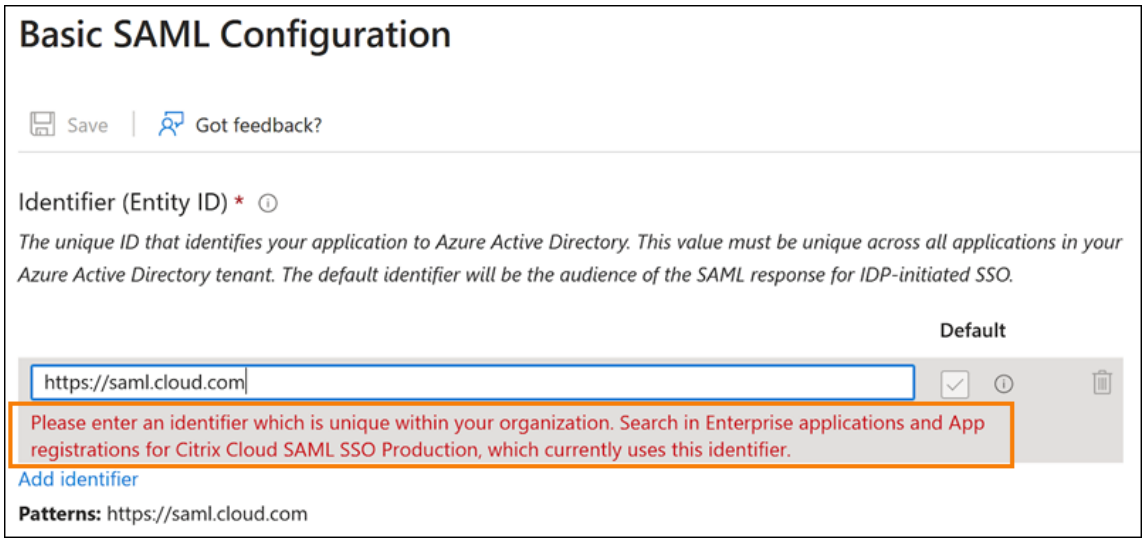
Author:
Mark Dear

Cet article explique comment provisionner plusieurs applications SAML au sein du même fournisseur SAML.

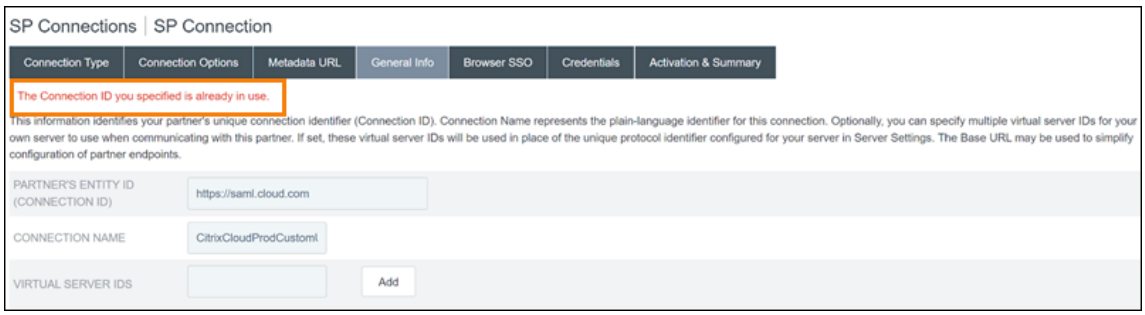
Certains fournisseurs SAML, tels qu'Azure Active Directory (AD), Active Directory Federation Services (ADFS), PingFederate et PingSSO, interdisent de réutiliser le même ID d'entité de fournisseur de services (SP) dans plusieurs applications SAML. Par conséquent, les administrateurs qui créent deux ou plusieurs applications SAML différentes au sein du même fournisseur SAML ne peuvent pas les lier à des locataires Citrix Cloud identiques ou différents. Toute tentative de création d'une deuxième application SAML à l'aide du même ID d'entité SP, par exemple `https:\\saml.cloud.com`, lorsqu'une application SAML existante l'utilise déjà déclenche une erreur au niveau du fournisseur SAML, indiquant que l'ID d'entité est déjà utilisé.

Les images suivantes illustrent cette erreur :

- Dans Azure Active Directory :



- Dans PingFederate :



La fonctionnalité ID d'entité étendue de Citrix Cloud répond à cette limitation afin que vous puissiez créer plusieurs applications SAML au sein du fournisseur SAML (par exemple, un locataire Azure AD) et les lier à un seul locataire Citrix Cloud.

Qu'est-ce qu'un ID d'entité ?

Un ID d'entité SAML est un identifiant unique utilisé pour identifier une entité spécifique dans le protocole d'authentification et d'autorisation SAML. Généralement, l'ID d'entité est une URL ou un URI attribué à l'entité et utilisé dans les messages SAML et les métadonnées. Chaque application SAML que vous créez au sein de votre fournisseur SAML est considérée comme une entité unique.

Dans le cadre d'une connexion SAML entre Citrix Cloud et Azure AD, par exemple, Citrix Cloud est le fournisseur de services (SP) et Azure AD est le fournisseur SAML. Les deux services possèdent un ID d'entité qui doit être configuré de chaque côté de la connexion SAML. Cela signifie que l'ID d'entité de Citrix Cloud doit être configuré dans Azure AD et que l'ID d'entité d'Azure AD doit être configuré dans Citrix Cloud.

Les ID d'entité suivants sont des exemples d'ID d'entité générique et d'ID d'entité étendue dans Citrix Cloud :

- ID d'entité générique : `https://saml.cloud.com`
- ID d'entité étendue : `https://saml.cloud.com/67338f11-4996-4980-8339-535f76d0c8fb`

ID d'entité SP générique et étendue par région

Les connexions SAML existantes dans Citrix Cloud (créées avant novembre 2023) utilisent le même ID d'entité générique pour chaque connexion SAML et chaque locataire Citrix Cloud. Seules les nouvelles connexions SAML Citrix Cloud offrent la possibilité d'utiliser un ID d'entité étendue.

Si vous choisissez d'utiliser des ID d'entité étendue pour les nouvelles connexions, toutes les connexions SAML existantes continuent de fonctionner avec leurs ID d'entité génériques d'origine.

Le tableau suivant répertorie les ID d'entité SP générique et étendue pour chaque région Citrix Cloud :

Région Citrix Cloud	ID d'entité SP générique	ID d'entité étendue
États-Unis, Union européenne, Asie-Pacifique du Sud	`https://saml.cloud.com`	`https://saml.cloud.com/67338f11-4996-4980-8339-535f76d0c8fb`
Japon	`https://saml.citrixcloud.jp`	`https://saml.citrixcloud.jp/db642d4c-ad2c-4304-adcf-f96b6aa16c29`

Région Citrix Cloud	ID d'entité SP générique	ID d'entité étendue
Gouvernement	`https://saml.cloud.us`	`https://saml.cloud.us/20f1cf66-cfe9-4dd3-865c-9c59a6710820`

Générer des ID d'entité SP uniques pour les connexions SAML nouvelles et existantes

Lorsque vous créez une nouvelle connexion SAML, Citrix Cloud génère un ID unique (GUID). Pour générer un ID d'entité étendue, activez le paramètre **Configurer l'ID d'entité SAML étendue** lorsque vous créez la nouvelle connexion.

Si vous souhaitez mettre à jour une connexion SAML existante afin d'utiliser des ID d'entité étendue, vous devez déconnecter, puis reconnecter votre fournisseur SAML depuis la page **Gestion des identités et des accès > Authentification** dans Citrix Cloud. Citrix Cloud ne vous permet pas de modifier directement les connexions SAML existantes. Vous pouvez toutefois cloner la configuration et modifier le clone.

> **Important :**
>
> La fermeture du processus de connexion SAML avant de l'avoir terminé supprime l'ID d'entité généré automatiquement par Citrix Cloud. Lorsque vous redémarrez le processus de connexion SAML, Citrix Cloud génère un nouveau GUID d'entité étendue. Utilisez ce nouvel ID d'entité étendue lorsque vous configurez le fournisseur SAML. Si vous mettez à jour une connexion SAML existante pour utiliser des ID d'entité étendue, vous devez mettre à jour l'application SAML pour cette connexion avec l'ID d'entité étendue généré par Citrix Cloud.

Questions fréquemment posées sur les ID d'entité étendue

Puis-je créer plusieurs applications SAML Azure AD au sein du même locataire Azure AD et les lier à un ou plusieurs locataires Citrix Cloud ?

La fonctionnalité ID d'entité étendue de Citrix Cloud répond aux limites imposées par certains fournisseurs SAML en matière de prévention de la duplication des ID d'entité. Cette fonctionnalité vous permet de provisionner plusieurs applications SAML au sein de votre client Azure AD et de configurer chacune d'entre elles avec un ID d'entité défini à partir d'un seul client Citrix Cloud.

Puis-je toujours lier la même application Azure AD SAML à plusieurs locataires Citrix Cloud ?

Ce scénario est courant chez les clients de Citrix Cloud et Citrix continue de le prendre en charge. Pour mettre en œuvre ce scénario, vous devez répondre aux exigences suivantes :

- Utilisez un ID d'entité générique, tel que `https://saml.cloud.com`.
- N'activez pas les ID d'entité étendue pour votre connexion SAML.

Comment puis-je décider d'utiliser ou non un ID d'entité étendue au sein de mon fournisseur SAML ?

Les ID d'entité étendue dans Citrix Cloud offrent la possibilité d'utiliser un ID d'entité générique ou étendue, en fonction de vos besoins. Prenez en compte le nombre d'applications SAML dont vous avez besoin et le nombre de clients Citrix Cloud dont vous disposez. Déterminez également si chaque locataire peut partager une application SAML existante ou avoir besoin de sa propre application SAML étendue.

> **Important :**
>
> Si votre fournisseur SAML vous autorise déjà à créer plusieurs applications SAML avec le même ID d'entité (tel que `https://saml.cloud.com`), vous n'avez pas besoin d'activer les ID d'entité étendue ou d'apporter des modifications à votre configuration SAML existante. Il n'est pas nécessaire de mettre à jour les paramètres dans Citrix Cloud ou dans votre application SAML.

Fournisseurs SAML concernés

Le tableau suivant répertorie les fournisseurs SAML qui autorisent ou limitent l'utilisation d'ID d'entité en double.

Fournisseur SAML	Prend en charge les ID d'entité en double
Azure AD (cloud)	Non
ADFS (sur site)	Non
PingFederate (sur site)	Non
PingOneSSO (cloud)	Non
Okta (cloud)	Oui
Duo (cloud)	Oui
OneLogin (cloud)	Oui

Cas d'utilisation concernés

Le tableau suivant indique si un ID d'entité générique ou étendue est pris en charge en fonction des applications SAML requises par votre cas d'utilisation et si votre fournisseur SAML prend en charge les ID d'entité en double.

Exigence relative au cas d'utilisation	Prise en charge des ID d'entité en double par le fournisseur SAML ?	Configuration prise en charge
Une seule application SAML	Oui	ID d'entité générique ou étendue
Une seule application SAML	Non	ID d'entité générique ou étendue
Deux applications SAML ou plus	Oui	ID d'entité générique ou étendue
Deux applications SAML ou plus	Non	ID d'entité étendue
Paires d'URL personnalisées et d'applications SAML de l'espace de travail	Oui	ID d'entité générique ou étendue
Paires d'URL personnalisées et d'applications SAML de l'espace de travail	Non	ID d'entité étendue
Lier la même application SAML à plusieurs locataires Citrix Cloud	Oui	ID d'entité générique
Lier la même application SAML à plusieurs locataires Citrix Cloud	Non	ID d'entité générique

Configurer la connexion SAML principale avec un ID d'entité étendue

Dans cette tâche, vous créez une connexion SAML dans Citrix Cloud à l'aide d'un ID d'entité défini pour l'application SAML principale (SAML App 1).

1. Dans le menu Citrix Cloud, sélectionnez **Gestion des identités et des accès**.
2. Dans l'onglet **Authentification**, localisez **SAML 2.0** et sélectionnez **Connecter** dans le menu de points de suspension.
3. Lorsque vous êtes invité à créer votre URL de connexion unique, entrez un identifiant court et descriptif pour votre entreprise (par exemple, `https://citrix.cloud.com/go/mycompany`) et sélectionnez **Enregistrer et continuer**. Cet identifiant doit être unique sur l'ensemble de Citrix Cloud.
4. Sous **Configurer le fournisseur d'identité SAML**, sélectionnez **Configurer l'ID d'entité SAML étendue**. Citrix Cloud génère automatiquement des ID d'entité étendue et renseigne les champs relatifs à l'ID d'entité, au service consommateur d'assertions (ACS) et à l'URL de déconnexion.

5. Sous **Configurer la connexion SAML à Citrix Cloud**, entrez les informations de connexion fournies par votre fournisseur SAML.
6. Acceptez les mappages d'attributs SAML par défaut.
7. Sélectionnez **Tester et terminer**.

Configurer la connexion SAML principale avec un ID d'entité générique

Dans cette tâche, vous créez une connexion SAML dans Citrix Cloud à l'aide de l'ID d'entité générique par défaut pour l'application SAML principale (SAML App 1).

1. Dans le menu Citrix Cloud, sélectionnez **Gestion des identités et des accès**.
2. Dans l'onglet **Authentification**, localisez **SAML 2.0** et sélectionnez **Connecter** dans le menu de points de suspension.
3. Lorsque vous êtes invité à créer votre URL de connexion unique, entrez un identifiant court et descriptif pour votre entreprise (par exemple, `https://citrix.cloud.com/go/mycompany`) et sélectionnez **Enregistrer et continuer**. Cet identifiant doit être unique sur l'ensemble de Citrix Cloud.
4. Sous **Configurer le fournisseur d'identité SAML**, vérifiez que l'option **Configurer l'ID d'entité SAML étendue** est désactivée.
5. Sous **Configurer la connexion SAML à Citrix Cloud**, entrez les informations de connexion fournies par votre fournisseur SAML.
6. Sous **Métadonnées SAML du fournisseur de services**, cliquez sur **Télécharger** pour obtenir une copie des métadonnées SAML génériques, si nécessaire.
7. Acceptez les mappages d'attributs SAML par défaut.
8. Sélectionnez **Tester et terminer**.

Configurer une connexion SAML à l'aide de domaines personnalisés Citrix Workspace

Cette section explique comment configurer une connexion SAML à l'aide d'une URL d'espace de travail personnalisée avec un ID d'entité étendue ou générique.

Les tâches de cette section ne s'appliquent que si vous disposez déjà d'une URL d'espace de travail personnalisée que vous utilisez avec SAML. Si vous n'utilisez pas d'URL d'espace de travail personnalisée avec l'authentification SAML, vous pouvez ignorer les tâches de cette section.

Pour plus d'informations, consultez les articles suivants :

- Configurer un domaine personnalisé
- Se connecter à des espaces de travail avec SAML à l'aide de domaines personnalisés

Configurer une connexion SAML avec une URL d'espace de travail personnalisée et un ID d'entité générique

Dans cette tâche, le paramètre **Configurer l'ID d'entité étendue** est désactivé.

1. Dans le menu Citrix Cloud, sélectionnez **Authentification de Workspace**.
2. Dans **URL d'espace de travail personnalisée**, sélectionnez **Modifier** dans le menu de points de suspension.
3. Sélectionnez **Utiliser à la fois l'URL [NomClient].cloud.com et l'URL du domaine personnalisé**.
4. Entrez l'ID d'entité générique, l'URL SSO et l'URL de déconnexion facultative pour l'application SAML 2, puis téléchargez le certificat de signature que vous avez téléchargé précédemment auprès de votre fournisseur SAML.
5. Si nécessaire, sous **Métadonnées SAML du fournisseur de services pour le domaine personnalisé**, cliquez sur **Télécharger** pour obtenir une copie des métadonnées SAML génériques pour l'application SAML de l'URL d'espace de travail personnalisée
6. Cliquez sur **Enregistrer**.

Configurer une connexion SAML avec une URL d'espace de travail personnalisée et un ID d'entité étendue

Dans cette tâche, le paramètre **Configurer l'ID d'entité étendue** est activé.

1. Dans le menu Citrix Cloud, sélectionnez **Authentification de Workspace**.
2. Dans **URL d'espace de travail personnalisée**, sélectionnez **Modifier** dans le menu de points de suspension.
3. Sélectionnez **Utiliser à la fois l'URL [NomClient].cloud.com et l'URL du domaine personnalisé**.
4. Entrez l'ID d'entité étendue, l'URL SSO et l'URL de déconnexion facultative pour l'application SAML 2, puis téléchargez le certificat de signature SAML que vous avez téléchargé précédemment auprès de votre fournisseur SAML.
5. Cliquez sur **Enregistrer**.

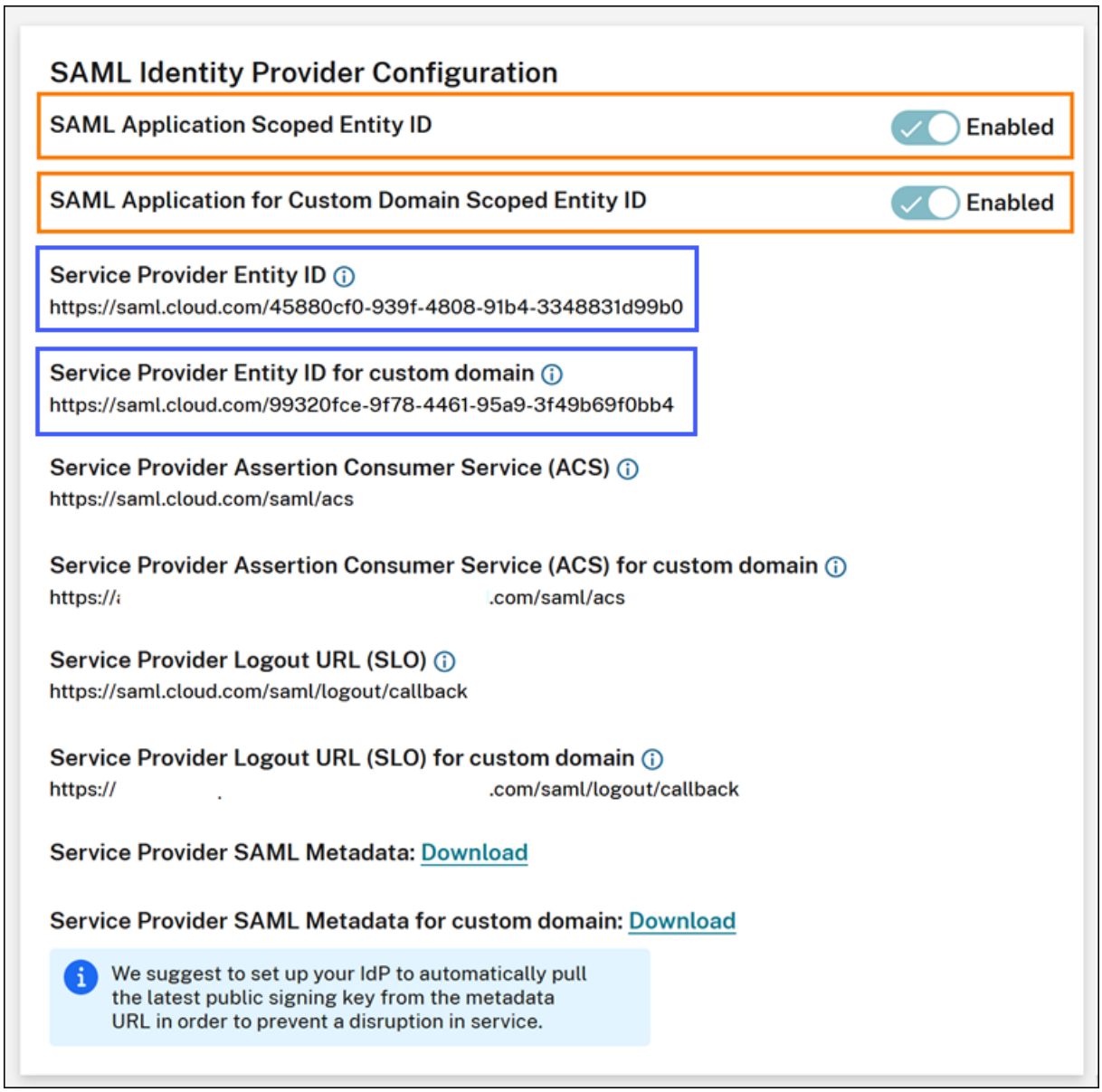
Une fois la configuration enregistrée, Citrix Cloud génère les métadonnées SAML étendues contenant le GUID correct. Si nécessaire, vous pouvez obtenir une copie des métadonnées étendues pour l'application SAML de l'URL d'espace de travail personnalisée

1. Sur la page **Gestion des identités et des accès**, localisez la connexion SAML et sélectionnez **Afficher** dans le menu de points de suspension.
2. Sous **Métadonnées SAML du fournisseur de services pour le domaine personnalisé**, cliquez sur **Télécharger**.

Afficher la configuration SAML des applications SAML de l'URL d'espace de travail principale et personnalisée

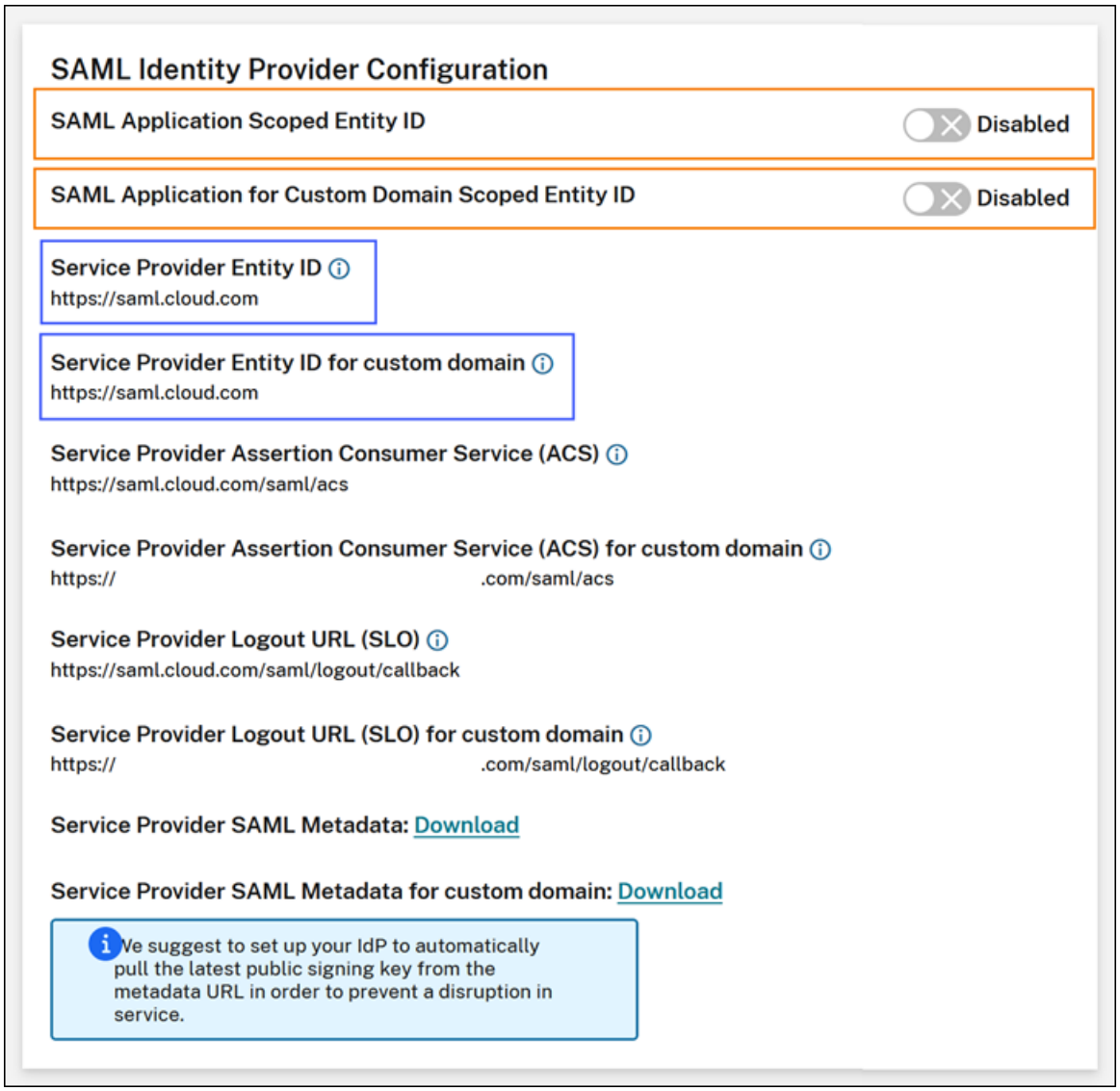
Lorsque vous affichez les détails de configuration de votre connexion SAML étendue, Citrix Cloud affiche les paramètres d'ID d'entité étendue à la fois pour l'application SAML principale et pour l'application SAML avec domaines personnalisés Workspace

Par exemple, lorsque les ID d'entité étendue sont activés, les champs **ID d'entité du fournisseur de services** et **ID d'entité du fournisseur de services pour le domaine personnalisé** contiennent les ID d'entité étendue générés par Citrix Cloud.



Lorsque les ID d'entité étendue sont désactivés, les champs **ID d'entité du fournisseur de services** et **ID d'entité du fournisseur de services pour le domaine personnalisé** contiennent les ID d'entité

générique.



Vous pouvez mettre à jour les applications SAML existantes au sein de votre fournisseur SAML en ajoutant l'ID d'entité étendue à la valeur d'ID d'entité existante.

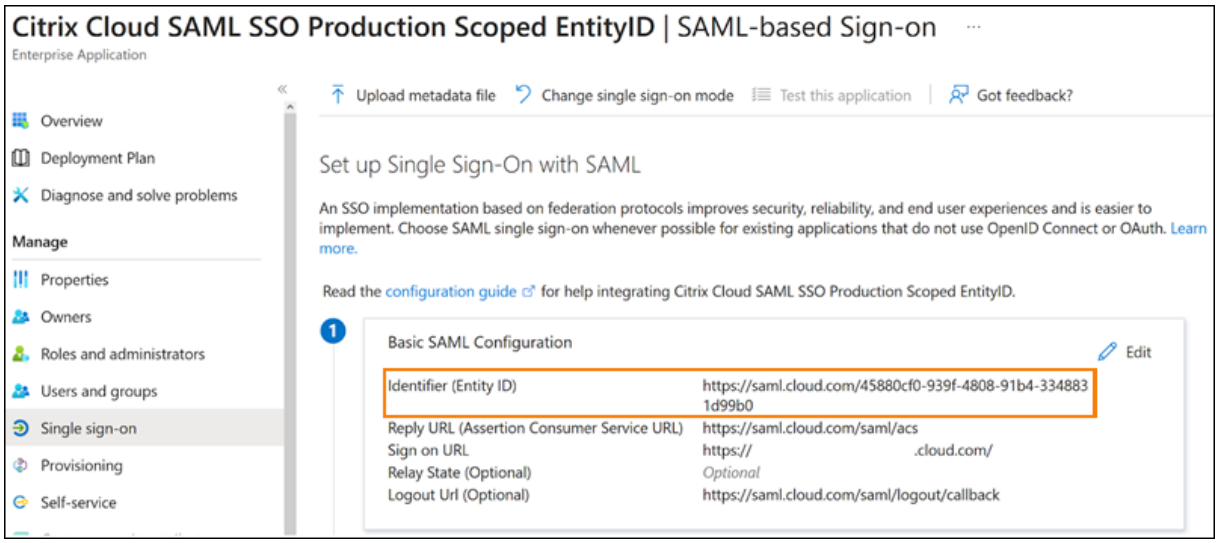
Configuration du fournisseur SAML avec ID d'entité étendue

Après avoir configuré la connexion SAML dans Citrix Cloud avec des ID d'entité étendue, vous pouvez ajouter l'ID d'entité étendue à votre fournisseur SAML.

Cette section inclut des exemples de configuration provenant d'Azure AD et de PingFederate.

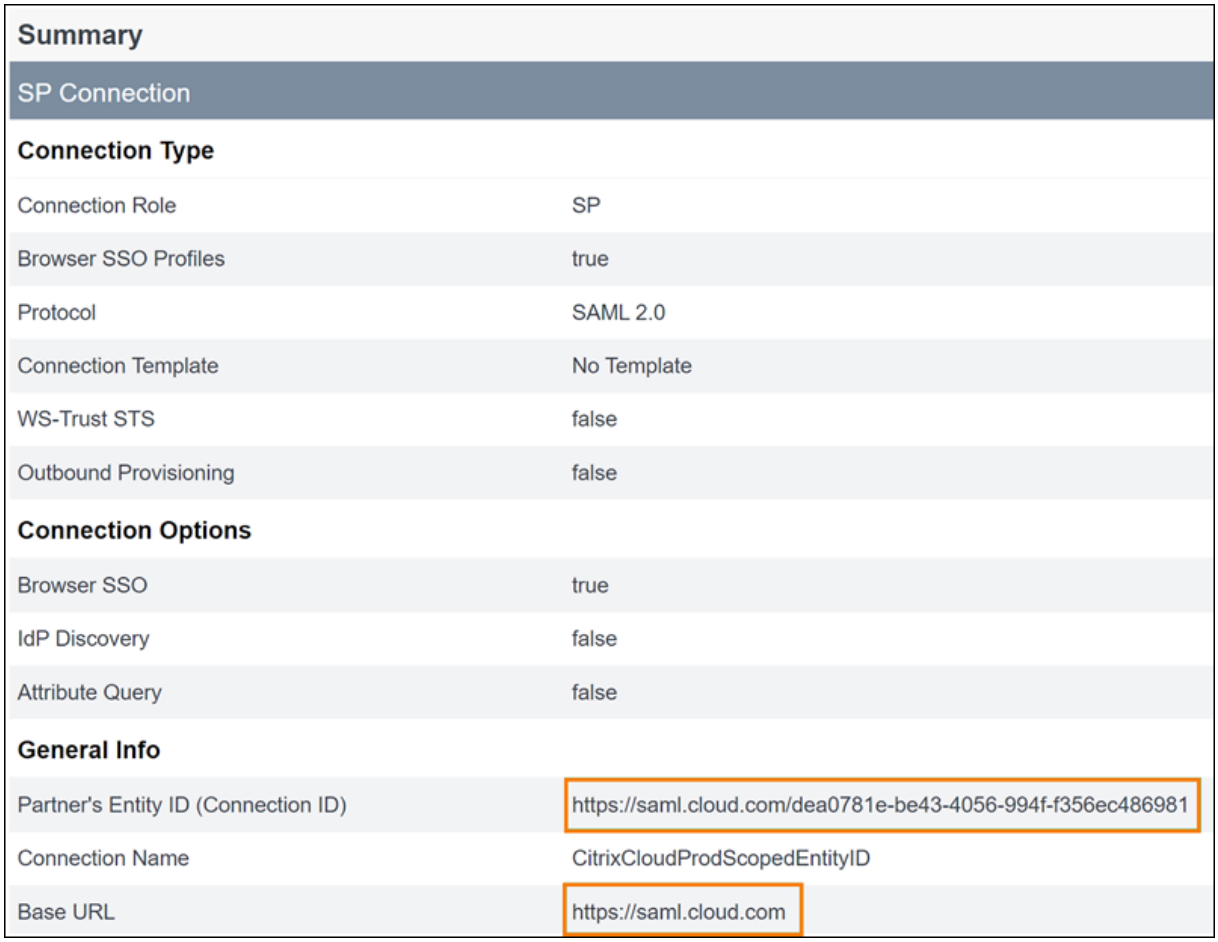
Configuration SAML d'Azure AD avec ID d'entité étendue

Dans cet exemple, l'ID d'entité étendue provenant de Citrix Cloud est saisi dans le champ **Identifiant** d'Azure AD.



Configuration SAML de PingFederate avec ID d'entité étendue

Dans cet exemple, l'ID d'entité étendue et l'ID d'entité générique de Citrix Cloud sont renseignés respectivement dans les champs **Partner's Entity ID** et **Base URL**.



Summary	
SP Connection	
Connection Type	
Connection Role	SP
Browser SSO Profiles	true
Protocol	SAML 2.0
Connection Template	No Template
WS-Trust STS	false
Outbound Provisioning	false
Connection Options	
Browser SSO	true
IdP Discovery	false
Attribute Query	false
General Info	
Partner's Entity ID (Connection ID)	https://saml.cloud.com/dea0781e-be43-4056-994f-f356ec486981
Connection Name	CitrixCloudProdScopedEntityID
Base URL	https://saml.cloud.com

Dépannage

Citrix recommande d'utiliser l'extension de navigateur SAML-Tracer pour résoudre tout problème lié à votre configuration SAML. Cette extension décode les requêtes et réponses codées en Base64 en langage XML SAML, et les fournit donc en dans un format intelligible. Vous pouvez utiliser l'extension SAML-Tracer pour examiner les requêtes SAML SSO et SLO que Citrix Cloud (le fournisseur de services) génère et envoie à votre fournisseur SAML (le fournisseur d'identité). L'extension peut indiquer si l'étendue de l'ID d'entité (GUID) est incluse dans les deux requêtes.

1. Dans le panneau Extensions de votre navigateur Web, installez et activez l'extension SAML-Tracer.
2. Effectuez une opération de connexion et de déconnexion SAML et capturez l'intégralité du flux avec l'extension SAML-Tracer.
3. Repérez la ligne suivante dans la requête SSO SAML ou la requête SLO.

```
1  <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
       https://saml.cloud.com/cfee4a86-97a8-49cf-9bb6-fd15ab075b92</
       saml:Issuer>
```

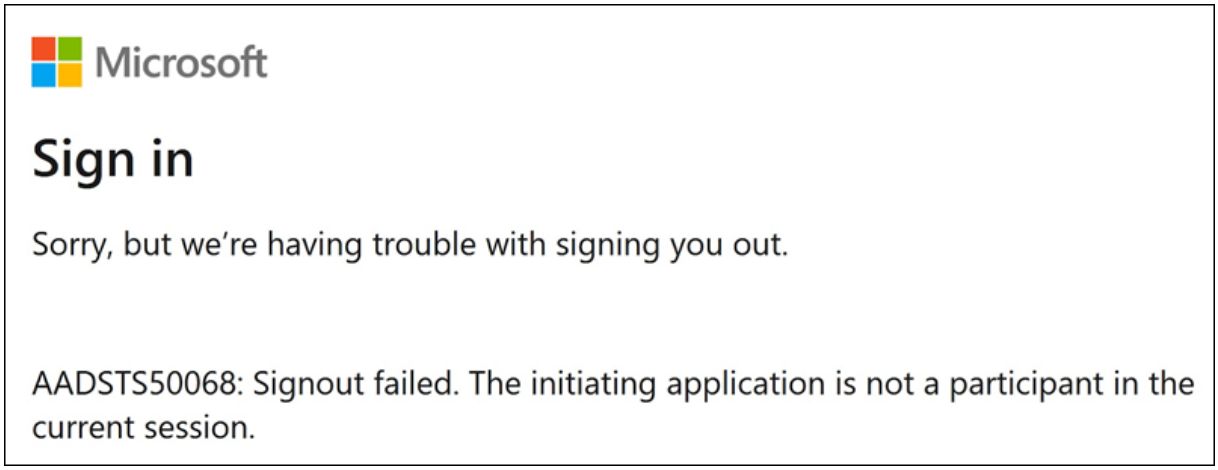


```
<!--NeedCopy-->
```

4. Vérifiez que l'ID d'entité correspond à l'ID d'entité configuré dans l'application de votre fournisseur SAML.
5. Vérifiez que l'ID d'entité étendue est présent dans le champ **Issuer** et assurez-vous qu'il est configuré correctement dans votre fournisseur SAML.
6. Exportez et enregistrez la sortie JSON de l'extension SAML-tracer. Si vous êtes en relation avec le support Citrix pour résoudre un problème, chargez le résultat dans votre dossier de support Citrix.

Résolution des problèmes liés à Azure AD

Problème : la déconnexion d'Azure AD échoue lorsque SLO est configuré. Azure AD affiche l'erreur suivante à l'utilisateur :



Si les ID d'entité étendue sont activés pour la connexion SAML dans Citrix Cloud, ils doivent être envoyés à la fois dans les requêtes SSO et SLO.

Cause : l'entité étendue est configurée mais l'ID d'entité est absent de la requête SLO. Vérifiez que l'ID d'entité étendue est présent dans la requête SLO dans la sortie de l'extension SAML-tracer.

Résolution des problèmes sur site liés à PingFederate

Problème : la connexion ou la déconnexion à PingFederate échoue si le paramètre d'ID d'entité étendue a été activé.

Cause : l'administrateur PingFederate a ajouté l'ID d'entité étendue à l'URL de base de connexion du SP.

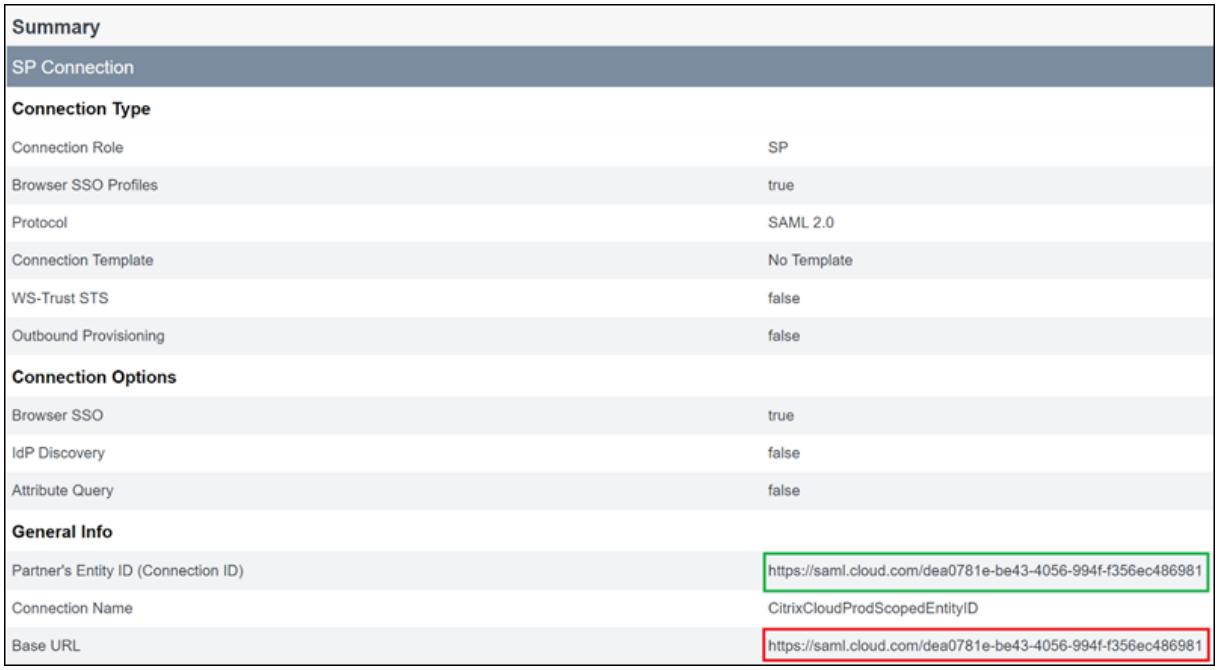
Pour résoudre ce problème, ajoutez l'ID d'entité étendue au champ **Partner's EntityID** uniquement. L'ajout de l'ID d'entité étendue à l'URL de base entraîne un point de terminaison SAML incorrect. Si

l'URL de base de Citrix Cloud n'est pas correctement mise à jour, toutes les autres URL relatives au point de terminaison SAML dérivées de l'URL de base entraînent des échecs de connexion.

Les points de terminaison suivants sont des exemples de points de terminaison SAML Citrix Cloud incorrects qui peuvent apparaître dans la sortie SAML-Tracer :

- `https://saml.cloud.com/<GUID>/saml/acs`
- `https://saml.cloud.com/<GUID>/saml/logout/callback`

L'image suivante montre une application SAML PingFederate qui n'a pas été configurée correctement. Le champ qui a été correctement configuré est affiché en vert. Le champ qui n'a pas été configuré correctement est affiché en rouge.



Summary	
SP Connection	
Connection Type	
Connection Role	SP
Browser SSO Profiles	true
Protocol	SAML 2.0
Connection Template	No Template
WS-Trust STS	false
Outbound Provisioning	false
Connection Options	
Browser SSO	true
IdP Discovery	false
Attribute Query	false
General Info	
Partner's Entity ID (Connection ID)	https://saml.cloud.com/dea0781e-be43-4056-994f-f356ec486981
Connection Name	CitrixCloudProdScopedEntityID
Base URL	https://saml.cloud.com/dea0781e-be43-4056-994f-f356ec486981

SAML à l'aide des identités Azure AD et AAD pour l'authentification de Workspace

March 11, 2024

Author:
Mark Dear

Cet article décrit comment configurer SAML pour l'authentification de Workspace à l'aide des identités Azure Active Directory (AD) au lieu des identités AD. Utilisez cette configuration si vos utilisateurs Azure AD ne peuvent pas énumérer les PC Windows 365 Cloud ou les VDA joints à un domaine Azure AD

après s'être connectés à Citrix Workspace avec le comportement SAML par défaut. Une fois la configuration terminée, vos utilisateurs peuvent se connecter à Citrix Workspace à l'aide de l'authentification SAML pour accéder aux applications et aux bureaux HDX via Citrix DaaS et aux PC Windows 365 Cloud via Azure.

Le comportement par défaut pour Citrix Cloud et l'authentification SAML auprès de Citrix Workspace consiste à confirmer l'identité d'un utilisateur AD. Pour la configuration décrite dans cet article, il est nécessaire d'utiliser Azure AD Connect pour importer vos identités AD dans votre instance Azure AD. Les identités AD contiennent le SID utilisateur que Citrix Workspace peut envoyer à Citrix DaaS et permet d'énumérer et de lancer les ressources HDX. Étant donné que la version Azure AD des identités des utilisateurs est utilisée, les utilisateurs peuvent également énumérer et lancer des ressources Azure telles que les PC Windows 365 Cloud depuis Citrix Workspace.

> **Important :**
>
> L'énumération fait référence à la liste des ressources que les utilisateurs voient une fois qu'ils se connectent à Citrix Workspace. Les ressources auxquelles un utilisateur donné est autorisé à accéder dépendent de son identité utilisateur et des ressources associées à cette identité dans Citrix DaaS. Un article connexe fournit des instructions sur l'utilisation des identités Azure AD et AD en tant que fournisseur SAML pour l'authentification dans Workspace. Vous trouverez des instructions détaillées dans SAML à l'aide des identités Azure AD et AD pour l'authentification de Workspace

Étendue des fonctionnalités

Cet article s'adresse aux utilisateurs qui utilisent la combinaison suivante de fonctionnalités Citrix Cloud et Azure :

- SAML pour l'authentification de Workspace
- Énumération des ressources Citrix DaaS et HDX publiées à l'aide de VDA joints à un domaine AD
- Énumération des ressources de VDA joints à un domaine Azure AD
- Énumération des ressources de VDA joints à un domaine Azure hybride
- Énumération et lancement de W365 PC Cloud

> **Important :**
>
> N'utilisez pas ce flux SAML AAD pour la connexion SAML à Citrix Cloud car cela nécessite que l'administrateur Citrix Cloud soit membre d'un groupe AD et une identité d'utilisateur AD doit donc être utilisée. Vous trouverez des instructions détaillées dans SAML à l'aide des identités Azure AD et AD pour l'authentification de Workspace

Qu'est-ce qui est le mieux : les identités AD ou les identités Azure AD ?

Pour déterminer si les utilisateurs de votre espace de travail doivent s'authentifier à l'aide des identités SAML AD ou SAML Azure AD :

1. Décidez de la combinaison de ressources que vous souhaitez mettre à la disposition de vos utilisateurs dans Citrix Workspace.
2. Utilisez le tableau suivant pour déterminer le type d'identité utilisateur approprié pour chaque type de ressource.

Type de ressource (VDA)	Identité de l'utilisateur lors de la connexion à Citrix Workspace	Une identité SAML avec Azure AD est-elle requise ?	Le FAS fournit-il une authentification unique (SSO) au VDA ?
Joint à AD	AD, Azure AD importé depuis AD (contient le SID)	Non. Utilisez le protocole SAML par défaut.	Oui
Joint à Azure Hybride	AD, Azure AD importé depuis AD (contient le SID)	Non. Utilisez le protocole SAML par défaut.	Oui, pour AD en tant que fournisseur d'identité. FAS n'est pas requis si Azure AD est sélectionné pour le VDA.
Joint à Azure AD	Utilisateur natif Azure AD, Azure AD importé depuis AD (contient le SID)	Oui, utilisez SAML via Azure AD.	Le SSO fonctionne avec l'authentification moderne Azure AD. Le FA n'est pas requis.
PC Windows 365 Cloud	Utilisateur natif Azure AD, Azure AD importé depuis AD (contient le SID)	Oui, utilisez SAML via Azure AD.	Le SSO fonctionne avec l'authentification moderne Azure AD. Le FA n'est pas requis.
Joint à AD, joint à Azure AD, PC Windows 365 Cloud	Azure AD importé depuis AD (contient le SID)	Oui, utilisez SAML via Azure AD.	Oui, pour les VDA joints à AD. Non, pour les VDA joints à Azure AD et les PC Windows 365 Cloud.

Informations supplémentaires

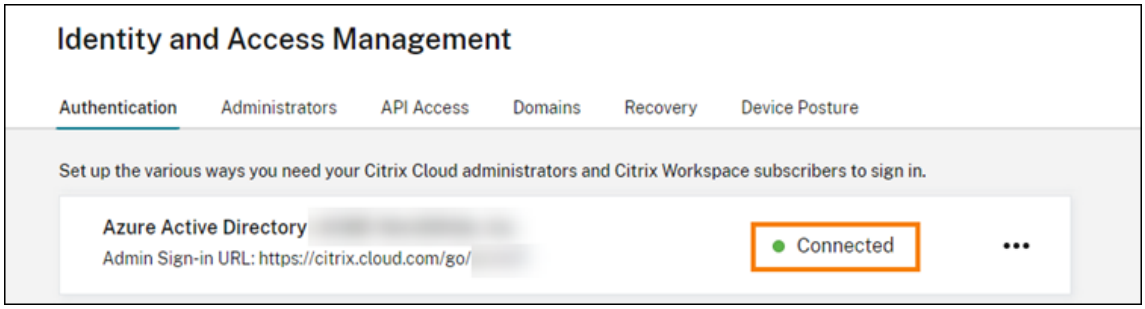
- Documentation Citrix DaaS :

  - Identités des machines
  - Citrix HDX Plus pour Windows 365

- Documentation Citrix FAS : Installer et configurer
- Documentation Microsoft Azure : Qu'est-ce qu'Azure AD Connect ?

Exigences

- Votre locataire Azure AD doit être connecté à votre locataire Citrix Cloud. Dans la console Citrix Cloud, vous pouvez trouver votre connexion Azure AD en sélectionnant **Gestion des identités et des accès > Authentification**.



- La méthode d'authentification de l'espace de travail doit être définie sur **SAML 2.0**. N'utilisez pas Azure AD comme méthode d'authentification. Pour modifier la méthode d'authentification de l'espace de travail, accédez à **Configuration de l'espace de travail > Authentification** dans la console Citrix Cloud.
- Le suffixe UPN `@yourdomain.com` doit être importé et vérifié dans Azure AD en tant que nom de domaine personnalisé. Dans le portail Azure, il se trouve sous **Azure Active Directory > Noms de domaine personnalisés**.
- Les identités des utilisateurs Azure AD doivent être importées depuis AD à l'aide de Microsoft Azure AD Connect. Cela garantit que les identités des utilisateurs sont importées correctement et contiennent le suffixe UPN approprié. Les utilisateurs d'Azure AD avec les suffixes UPN `@yourtenant.onmicrosoft.com` ne sont pas pris en charge.
- Citrix FAS doit être déployé et connecté au locataire et à l'emplacement des ressources Citrix Cloud. FAS fournit une authentification unique aux bureaux et applications HDX lancés depuis Citrix Workspace. Vous n'avez pas besoin de configurer des comptes fictifs AD car l'UPN `user@customerdomain` des identités utilisateur AD et Azure AD doit correspondre. FAS génère les certificats utilisateur nécessaires avec l'UPN correct et effectue une connexion par carte à puce lorsque les ressources HDX sont lancées.

Configurer l'application Azure AD Enterprise SAML personnalisée

Par défaut, le comportement de la connexion SAML aux espaces de travail consiste à confirmer l'identité d'un utilisateur AD. L'attribut SAML **cip_directory** est une valeur de chaîne codée en dur qui est la même pour tous les abonnés et qui agit comme un commutateur. Citrix Cloud et Citrix Workspace détectent cet attribut lors de la connexion, permettant ainsi à SAML de confirmer la version Azure AD de l'identité de l'utilisateur. L'utilisation du paramètre **azuread** avec cet attribut remplace le comportement SAML par défaut, déclenchant plutôt l'utilisation de SAML dans Azure AD.

Bien que les étapes décrites dans cette section concernent Azure AD, vous pouvez créer une application SAML similaire à l'aide d'un autre fournisseur SAML 2.0 (par exemple, ADFS, Duo, Okta, OneLogin, PingOneSSO, etc.), à condition d'effectuer les mêmes tâches. Votre fournisseur SAML doit vous autoriser à configurer un attribut SAML codé en dur (cip_directory = azuread) dans l'application SAML. Créez simplement les mêmes mappages d'attributs SAML que ceux décrits dans cette section.

1. Connectez-vous au portail Azure.
2. Dans le menu du portail, sélectionnez **Azure Active Directory**.
3. Dans le volet de gauche, sous **Gérer**, sélectionnez **Applications d'entreprise**.
4. Dans la barre de commandes du volet de travail, sélectionnez **Nouvelle application**.
5. Dans la barre de commandes, sélectionnez **Créer votre propre application**. N'utilisez pas le modèle d'application d'entreprise Citrix Cloud SAML SSO. Ce modèle ne vous permet pas de modifier la liste des revendications et des attributs SAML.
6. Donnez un nom à l'application, puis sélectionnez **Intégrer une autre application que vous ne trouvez pas dans la galerie (non-galerie)**. Cliquez sur **Créer**. La page de présentation de l'application s'affiche.
7. Dans le volet de gauche, sélectionnez **Authentification unique**. Dans le volet de travail, sélectionnez **SAML**.
8. Dans la section **Configuration SAML de base**, sélectionnez **Modifier** et configurez les paramètres suivants :

    a) Dans la section **Identifiant (ID d'entité)**, sélectionnez **Ajouter un identifiant**, puis entrez la valeur associée à la région dans laquelle se trouve votre client Citrix Cloud :
        - Pour les régions de l'Union européenne, des États-Unis et du sud de l'Asie-Pacifique, entrez `https://saml.cloud.com`.
        - Pour la région du Japon, entrez `https://saml.citrixcloud.jp`.
        - Pour la région Citrix Cloud Government, entrez `https://saml.cloud.us`.

    b) Dans la section **URL de réponse (URL du service consommateur d'assertion)**, sélectionnez **Ajouter une URL de réponse**, puis entrez la valeur associée à la région dans laquelle se trouve votre client Citrix Cloud :

- Pour les régions de l'Union européenne, des États-Unis et du sud de l'Asie-Pacifique, entrez `https://saml.cloud.com/saml/acs`.
- Pour la région du Japon, entrez `https://saml.citrixcloud.jp/saml/acs`.
- Pour la région Citrix Cloud Government, entrez `https://saml.cloud.us/saml/acs`.

c) Dans la section **URL de déconnexion (facultatif)**, entrez la valeur associée à la région dans laquelle se trouve votre client Citrix Cloud :

- Pour les régions de l'Union européenne, des États-Unis et du sud de l'Asie-Pacifique, entrez `https://saml.cloud.com/saml/logout/callback`.
- Pour la région du Japon, entrez `https://saml.citrixcloud.jp/saml/logout/callback`.
- Pour la région Citrix Cloud Government, entrez `https://saml.cloud.us/saml/logout/callback`.

d) Dans la barre de commandes, sélectionnez **Enregistrer**.

9. Dans la section **Attributs et revendications**, sélectionnez **Modifier** pour configurer les revendications suivantes. Ces revendications apparaissent dans l'assertion SAML contenue dans la réponse SAML.

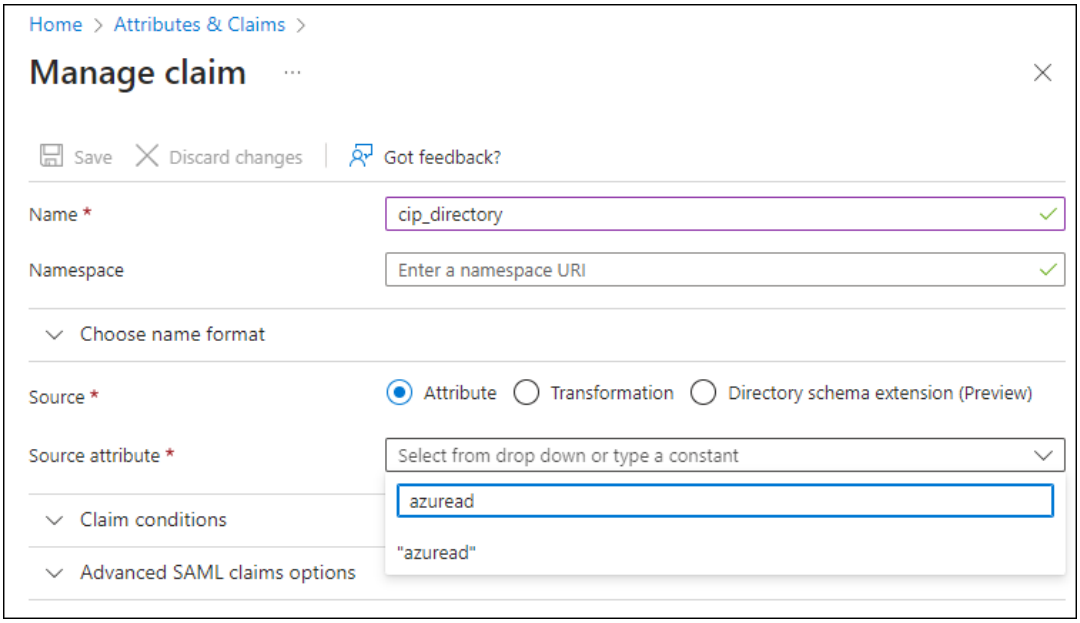
a) Sous la revendication **Identifiant d'utilisateur unique (ID de nom)**, laissez la valeur par défaut `user.userprincipalname`.

b) Dans la barre de commandes, sélectionnez **Ajouter une revendication**.

c) Sous **Nom**, entrez **cip_directory**.

d) Sous **Source**, laissez le champ **Attribut** sélectionné.

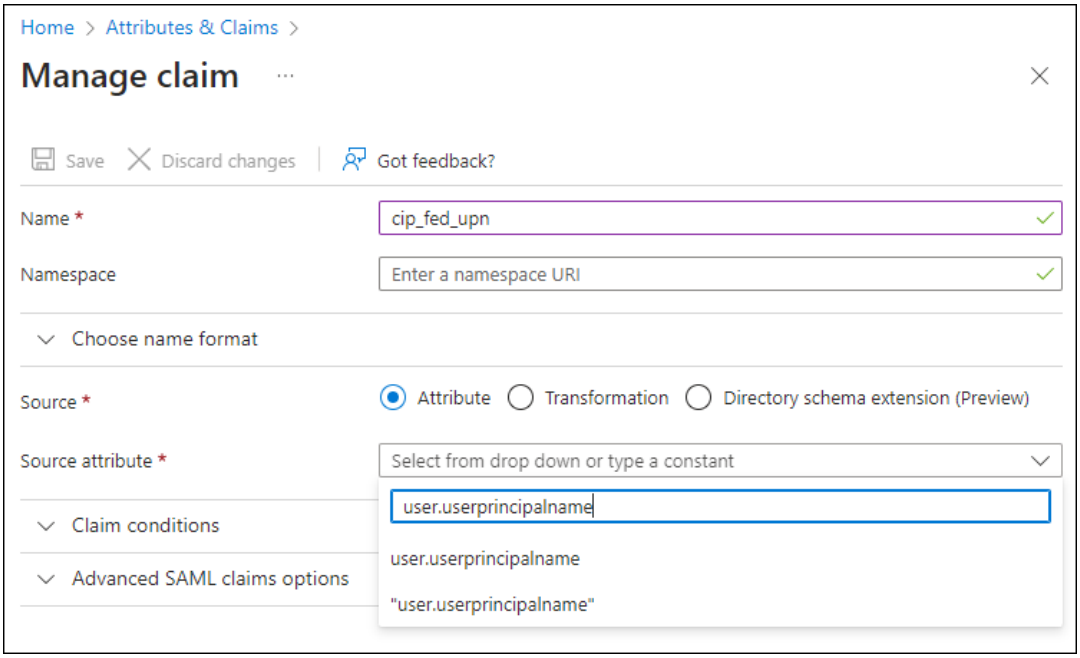
e) Sous **Attribut source**, entrez **azuread**. Cette valeur apparaît entre guillemets une fois que vous l'avez saisie.



f) Dans la barre de commandes, sélectionnez **Enregistrer**.

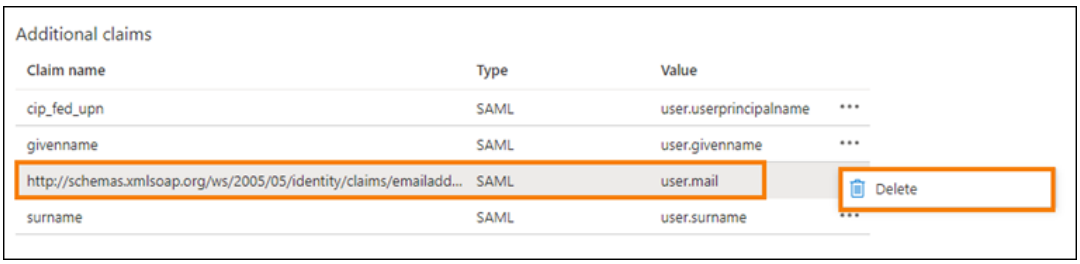
g) Créez des revendications supplémentaires avec les valeurs suivantes dans les champs **Nom** et **Attribut source** :

Nom	Attribut source
cip_fed_upn	user.userprincipalname
displayName	user.displayname
firstName	user.givenname
lastName	user.surname



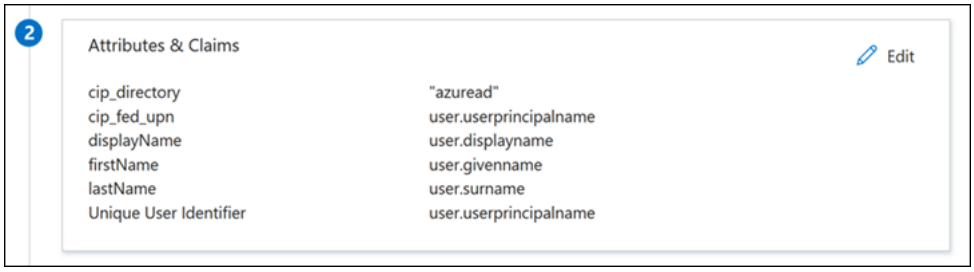
> **Important :**
>
> Vous pouvez créer ces revendications supplémentaires soit en répétant les étapes b à f pour chaque revendication, soit en modifiant les revendications par défaut dans la section **Autres revendications** qui possèdent déjà les attributs source répertoriés dans le tableau ci-dessus. Les revendications par défaut incluent l'espace de noms `http://schemas.xmlsoap.org/ws/2005/05/identity/claims`.
>
> Si vous modifiez les revendications par défaut, vous devez supprimer l'espace de noms de chaque revendication. Si vous créez de nouvelles revendications, vous devez supprimer celles qui incluent l'espace de noms. Si des revendications avec cet espace de noms sont incluses dans l'assertion SAML résultante, l'assertion ne sera pas valide et inclura des noms d'attributs SAML incorrects.

h) Dans la section **Autres revendications**, pour toutes les revendications restantes avec l'espace de noms `http://schemas.xmlsoap.org/ws/2005/05/identity/claims`, cliquez sur le bouton représentant des points de suspension (…), puis sur **Supprimer**.

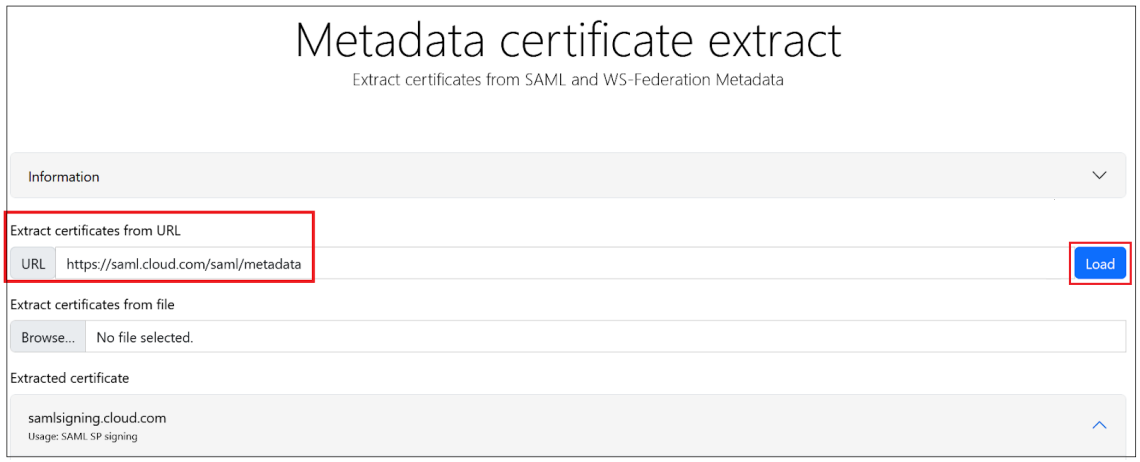


Lorsque vous avez terminé, la section **Attributs et revendications** apparaît comme illustré ci-

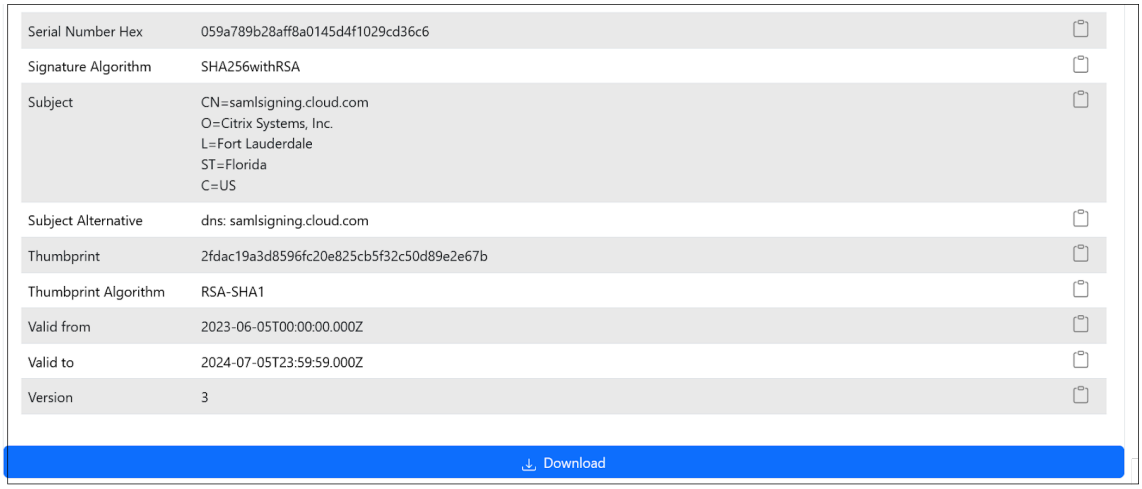
dessous :

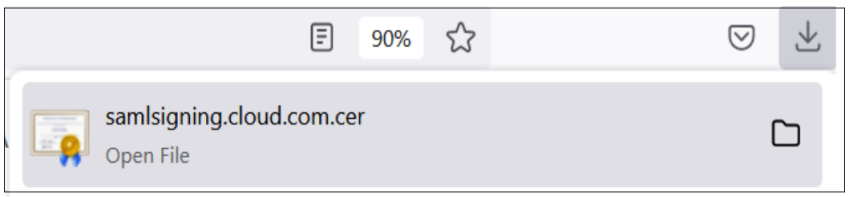


10. Obtenez une copie du certificat de signature SAML Citrix Cloud à l'aide de cet outil en ligne tiers.
11. Entrez https://saml.cloud.com/saml/metadata dans le champ URL et cliquez sur **Charger**.



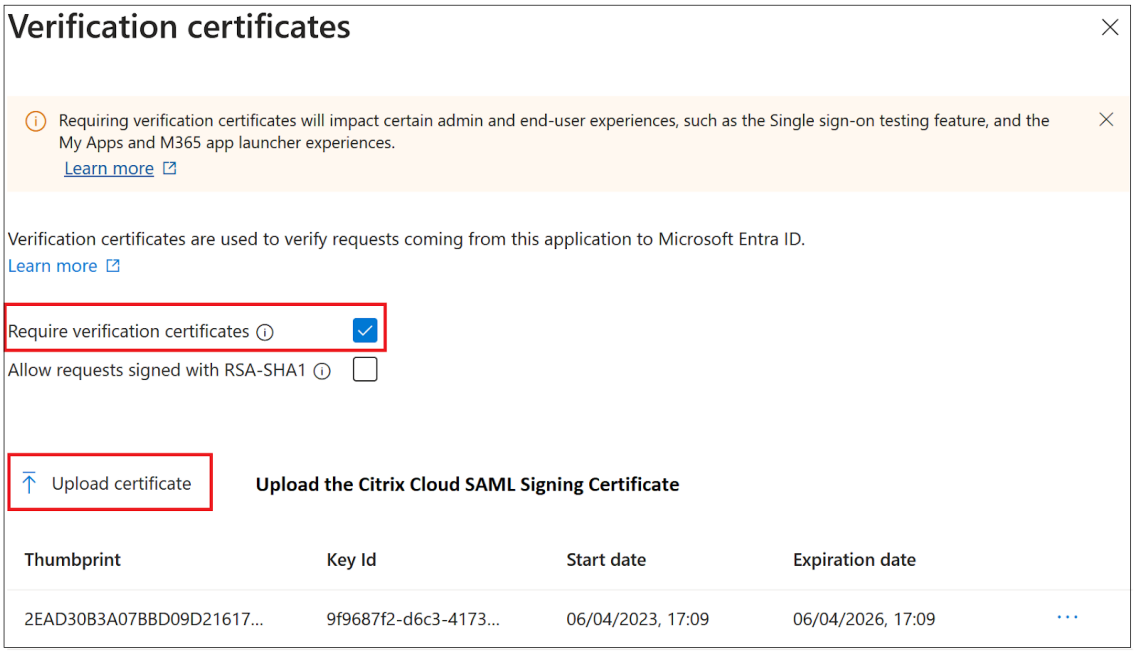
12. Faites défiler la page vers le bas et cliquez sur **Télécharger**.

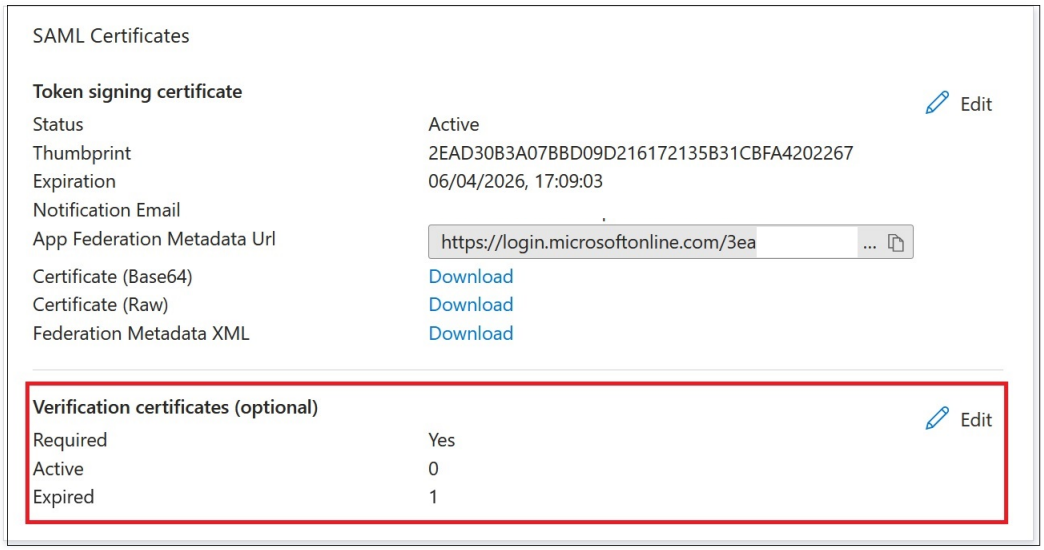




13. Configurez les paramètres de signature de l'application SAML Azure Active Directory.
14. Téléchargez le certificat de signature SAML de production obtenu à l'étape 10 dans l'application SAML Azure Active Directory.

    - Activez **Exiger des certificats de vérification**.





Dépannage

1. Vérifiez que vos assertions SAML contiennent les attributs utilisateur corrects à l'aide d'un outil réseau SAML, tel que l'extension de navigateur SAML-tracer.

2. Localisez la réponse SAML affichée en jaune et comparez-la à cet exemple :

3. Cliquez sur l'onglet **SAML** dans le volet inférieur pour décoder la réponse SAML et l'afficher au format XML.

4. Faites défiler la réponse vers le bas et vérifiez que l'assertion SAML contient les attributs SAML et les valeurs utilisateur corrects.

Si vos abonnés ne parviennent toujours pas à se connecter à leur espace de travail, contactez le support Citrix et fournissez les informations suivantes :

- Capture d'écran de l'extension SAML-tracer
- Date et heure d'échec de la connexion à Citrix Workspace
- Nom d'utilisateur concerné
- Adresse IP de l'appelant de l'ordinateur client que vous avez utilisé pour vous connecter à Citrix Workspace. Vous pouvez utiliser un outil tel que https://whatismyip.com pour obtenir cette adresse IP.

SAML à l'aide des identités Azure AD et AD pour l'authentification de Workspace

May 31, 2024

Author:
Mark Dear

Cet article décrit comment configurer SAML pour l'authentification de Workspace à l'aide des identités Active Directory (AD). Le comportement par défaut pour l'authentification Citrix Cloud et SAML auprès de Citrix Workspace ou de Citrix Cloud, quel que soit le fournisseur SAML utilisé, consiste à affirmer l'identité d'un utilisateur AD. Pour la configuration décrite dans cet article, il est nécessaire d'utiliser Azure AD Connect pour importer vos identités AD dans votre instance Azure AD.

> **Important :**
>
> Il est essentiel de déterminer le flux SAML approprié pour les utilisateurs finaux de votre espace de travail, car cela a un impact direct sur leur processus de connexion et la visibilité des ressources. L'identité choisie influence les types de ressources accessibles à un utilisateur de Workspace.
> Un article connexe fournit des instructions sur l'utilisation d'Azure AD en tant que fournisseur SAML pour l'authentification dans Workspace à l'aide d'identités AAD. Vous trouverez des instructions détaillées dans SAML à l'aide des identités Azure AD et AAD pour l'authentification de Workspace.
> En général, les utilisateurs de Workspace doivent généralement ouvrir des applications et des bureaux fournis par des VDA joints au domaine AD. Il est essentiel d'examiner attentivement les cas d'utilisation décrits dans les deux articles avant de choisir le flux SAML le plus adapté à votre organisation. En cas de doute, Citrix recommande d'utiliser le **flux AD SAML** et de suivre les instructions de cet article, car il correspond au scénario DaaS le plus courant.

Étendue des fonctionnalités

Cet article s'adresse aux utilisateurs qui utilisent la combinaison suivante de fonctionnalités Citrix Cloud et Azure :

- SAML pour l'authentification de Workspace à l'aide des identités AD
- SAML pour la connexion administrateur Citrix Cloud à l'aide d'identités AD
- Énumération des ressources Citrix DaaS et HDX publiées à l'aide de VDA joints à un domaine AD
- Énumération des ressources de VDA joints à un domaine AD

Qu'est-ce qui est le mieux : les identités AD ou les identités Azure AD ?

Pour déterminer si les utilisateurs de votre espace de travail doivent s'authentifier à l'aide des identités SAML AD ou SAML Azure AD :

1. Décidez de la combinaison de ressources que vous souhaitez mettre à la disposition de vos utilisateurs dans Citrix Workspace.

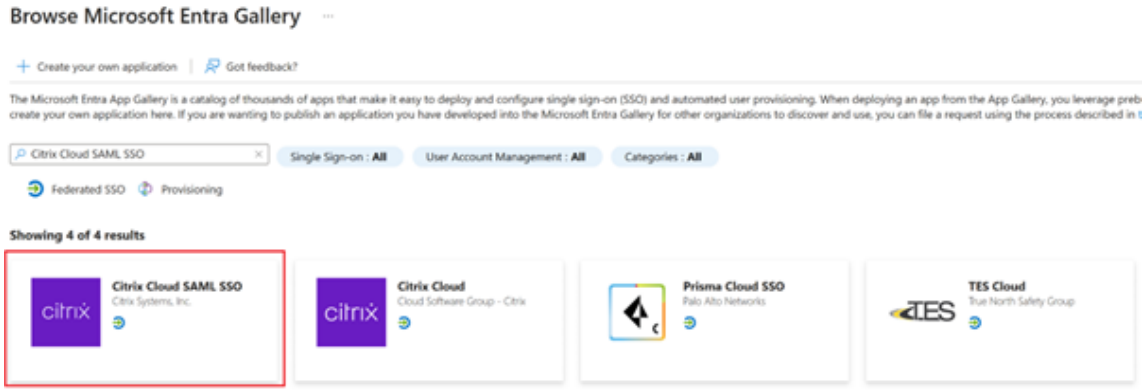
2. Utilisez le tableau suivant pour déterminer le type d'identité utilisateur approprié pour chaque type de ressource.

Type de ressource (VDA)	Identité de l'utilisateur lors de la connexion à Citrix Workspace	Une identité SAML avec Azure AD est-elle requise ?	Le FAS fournit-il une authentification unique (SSO) au VDA ?
Joint à AD	AD, Azure AD importé depuis AD (contient le SID)	Non. Utilisez le protocole SAML par défaut.	Oui

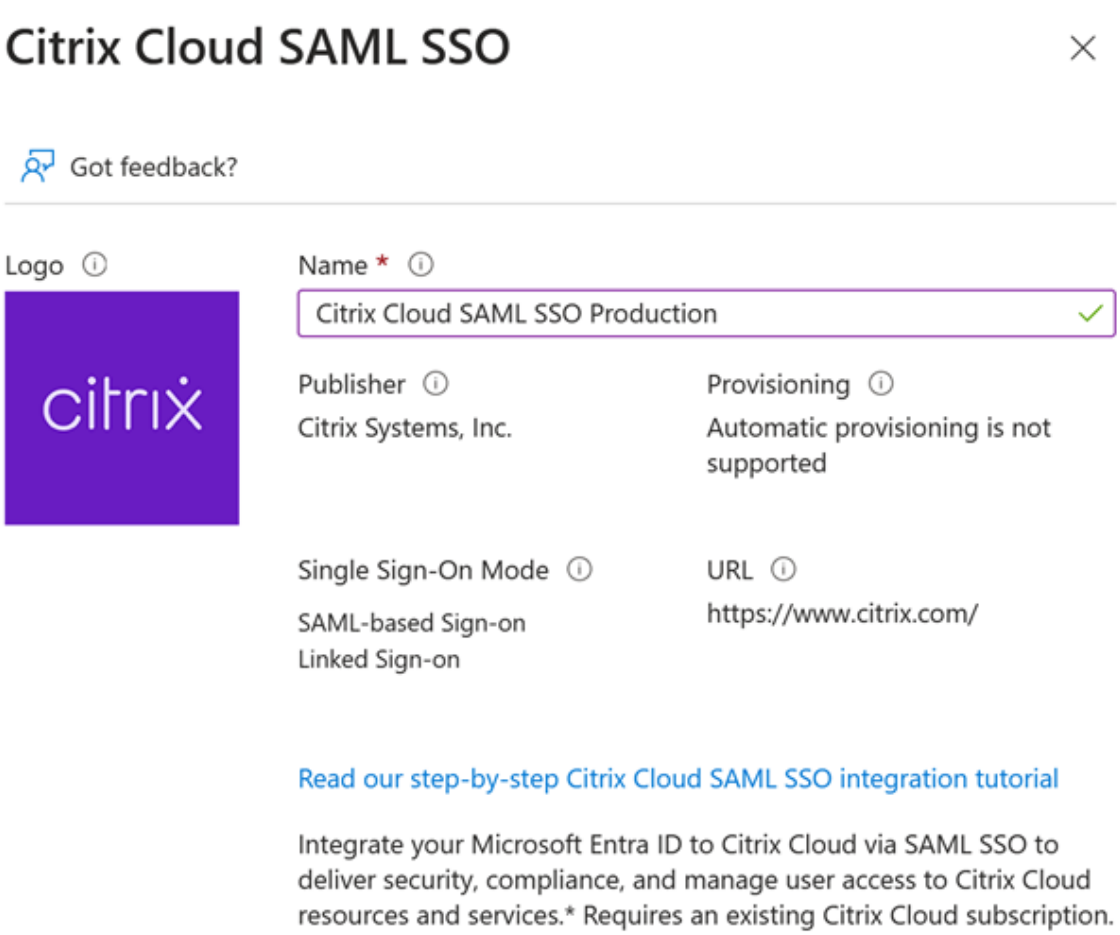
Configurer l'application Azure AD Enterprise SAML personnalisée

Par défaut, le comportement de la connexion SAML aux espaces de travail consiste à confirmer l'identité d'un utilisateur AD.

1. Connectez-vous au portail Azure.
2. Dans le menu du portail, sélectionnez **Azure Active Directory**.
3. Dans le volet de gauche, sous **Gérer**, sélectionnez **Applications d'entreprise**.
4. Dans la zone de recherche, entrez `Citrix Cloud SAML SSO` pour localiser le modèle d'application Citrix SAML.



5. Entrez un nom approprié pour l'application SAML, comme `Citrix Cloud SAML SSO Production`



6. Dans le volet de navigation de gauche, sélectionnez **Authentification unique**, puis, dans le volet de travail, cliquez sur **SAML**.
7. Dans la section **Configuration SAML de base**, sélectionnez **Modifier** et configurez les paramètres suivants :

   a) Dans la section **Identifiant (ID d'entité)**, sélectionnez **Ajouter un identifiant**, puis entrez la valeur associée à la région dans laquelle se trouve votre client Citrix Cloud :
      - Pour les régions de l'Europe, des États-Unis et du sud de l'Asie-Pacifique, entrez `https://saml.cloud.com`.
      - Pour la région du Japon, entrez `https://saml.citrixcloud.jp`.
      - Pour la région Citrix Cloud Government, entrez `https://saml.cloud.us`.

   b) Dans la section **URL de réponse (URL du service consommateur d'assertion)**, sélectionnez **Ajouter une URL de réponse**, puis entrez la valeur associée à la région dans laquelle se trouve votre client Citrix Cloud :
      - Pour les régions de l'Europe, des États-Unis et du sud de l'Asie-Pacifique, entrez `https://saml.cloud.com/saml/acs`.
      - Pour la région du Japon, entrez `https://saml.citrixcloud.jp/saml/acs`.

- Pour la région Citrix Cloud Government, entrez `https://saml.cloud.us/saml/acs`.

c) Dans la section **URL de connexion**, entrez votre URL Workspace.

d) Dans la section **URL de déconnexion (facultatif)**, entrez la valeur associée à la région dans laquelle se trouve votre client Citrix Cloud :

- Pour les régions de l'Europe, des États-Unis et du sud de l'Asie-Pacifique, entrez `https://saml.cloud.com/saml/logout/callback`.
- Pour la région du Japon, entrez `https://saml.citrixcloud.jp/saml/logout/callback`.
- Pour la région Citrix Cloud Government, entrez `https://saml.cloud.us/saml/logout/callback`.

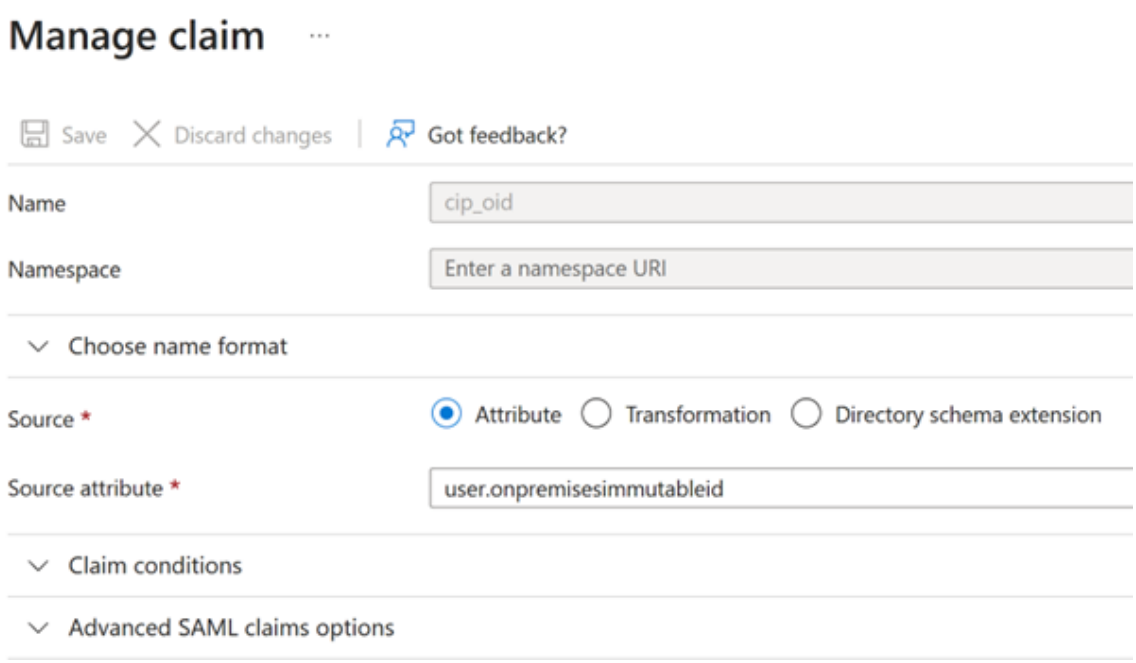
e) Dans la barre de commandes, cliquez sur **Enregistrer**. La section **Configuration SAML de base** apparaît comme suit :

8. Dans la section **Attributs et revendications**, cliquez sur **Modifier** pour configurer les revendications suivantes. Ces revendications apparaissent dans l'assertion SAML contenue dans la réponse SAML. Après avoir créé l'application SAML, configurez les attributs suivants.

a) Sous la revendication **Identifiant d'utilisateur unique (ID de nom)**, laissez la valeur par défaut `user.userprincipalname`.

b) Pour la réclamation **cip_upn**, laissez la valeur par défaut de `user.userprincipalname` .

c) Pour la réclamation **cip_email**, laissez la valeur par défaut de `user.mail`.
d) Pour la réclamation **cip_sid**, laissez la valeur par défaut de `user.onpremisesecurityidentitie`
.
e) Pour la revendication **cip_oid**, modifiez la réclamation existante et sélectionnez **Attribut source**. Recherchez la chaîne `object` et sélectionnez `user.onpremisesimmutableid`
.



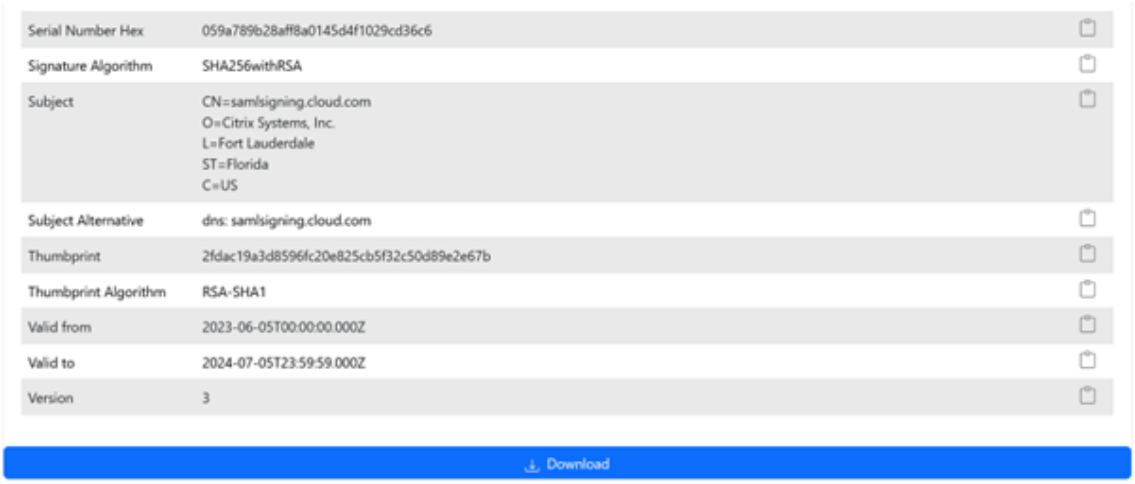
a) Pour **displayName**, laissez la valeur par défaut de `user.displayname`.
b) Dans la section **Autres revendications**, pour toutes les revendications restantes avec l'espace de noms `http://schemas.xmlsoap.org/ws/2005/05/identity/claims`, cliquez sur le bouton représentant des points de suspension (...), puis sur **Supprimer**. Il n'est pas nécessaire d'inclure ces revendications car elles sont des doublons des attributs utilisateur ci-dessus.

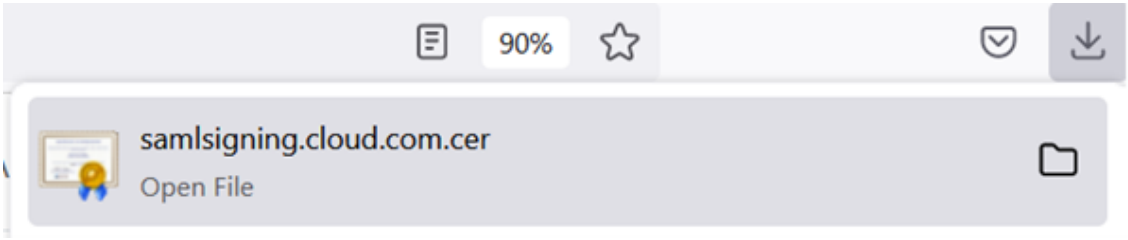
Lorsque vous avez terminé, la section **Attributs et revendications** apparaît comme illustré ci-dessous :

a) Obtenez une copie du certificat de signature SAML Citrix Cloud à l'aide de cet outil en ligne tiers.

b) Entrez `https://saml.cloud.com/saml/metadata` dans le champ URL et cliquez sur **Charger**.

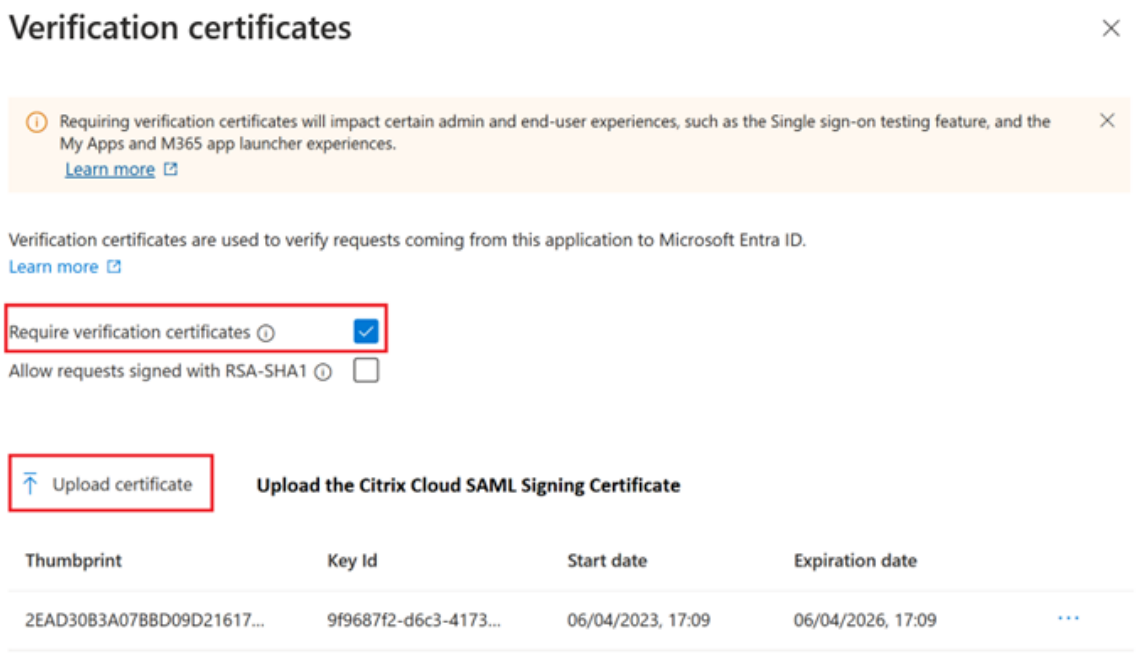
9. Faites défiler la page vers le bas et cliquez sur **Télécharger**.

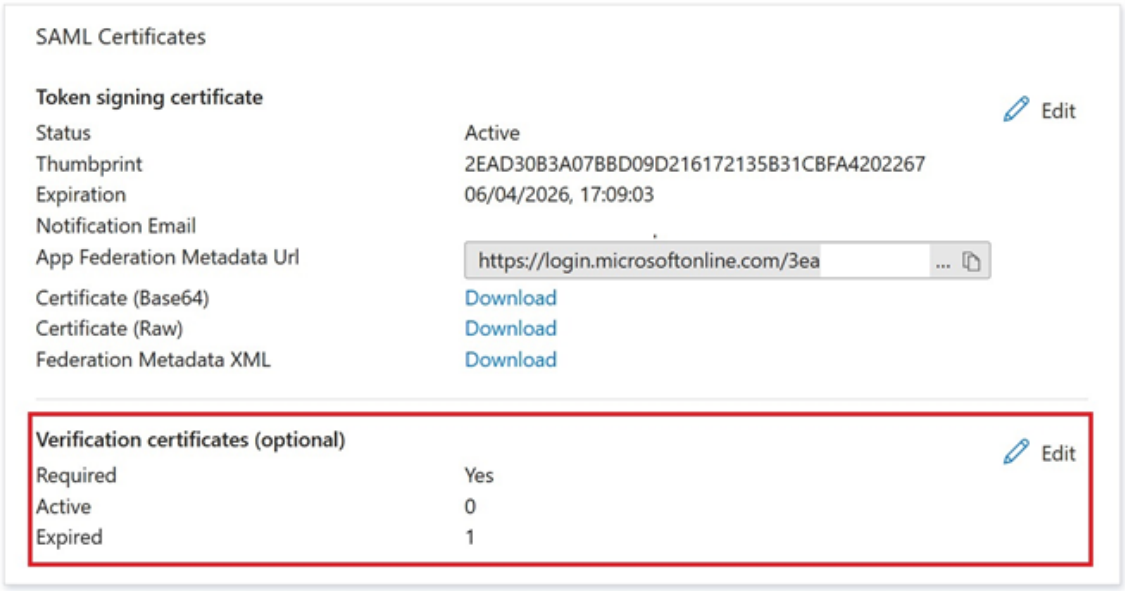




10. Configurez les paramètres de signature de l'application SAML Azure Active Directory.
11. Charger le certificat de signature SAML de production obtenu à l'étape 10 dans l'application SAML Azure Active Directory

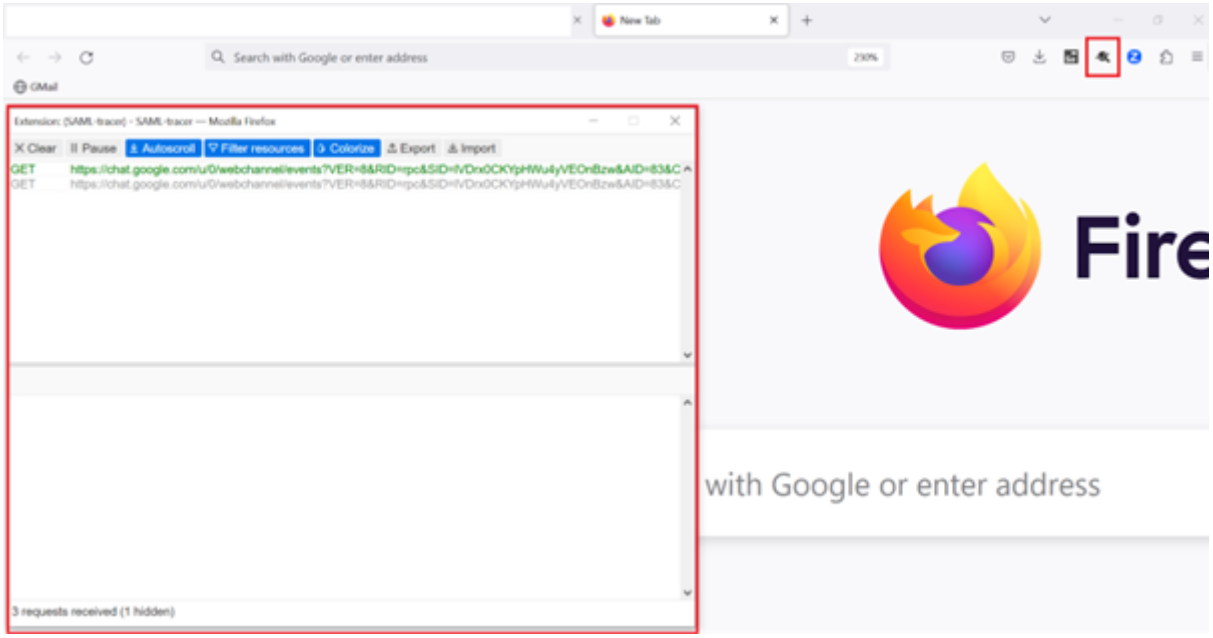
    a) Activez **Exiger des certificats de vérification**.





Dépannage

1. Vérifiez que vos assertions SAML contiennent les attributs utilisateur corrects à l'aide d'un outil réseau SAML, tel que l'extension de navigateur SAML-tracer.



1. Localisez la réponse SAML affichée en jaune et comparez-la à cet exemple :

2. Cliquez sur l'onglet **SAML** dans le volet inférieur pour décoder la réponse SAML et l'afficher au format XML.
3. Faites défiler la réponse vers le bas et vérifiez que l'assertion SAML contient les attributs SAML et les valeurs utilisateur corrects.

Si vos abonnés ne peuvent toujours pas se connecter à leur espace de travail ou s'ils ne peuvent pas voir leurs bureaux Citrix HDX Plus pour Windows 365, contactez le support Citrix et fournissez les informations suivantes :

- Capture d'écran de l'extension SAML-tracer
- Date et heure d'échec de la connexion à Citrix Workspace
- Nom d'utilisateur concerné
- Adresse IP de l'appelant de l'ordinateur client que vous avez utilisé pour vous connecter à Citrix Workspace. Vous pouvez utiliser un outil tel que https://whatismyip.com pour obtenir cette adresse IP.

Configurer l'authentification SAML simplifiée pour les utilisateurs SAML natifs et invités

July 2, 2024

Author:
Mark Dear, Javier Lopez Santacruz

Avant d'appliquer les recommandations de cet article, il est essentiel de savoir si « l'authentification SAML simplifiée » convient à votre cas d'utilisation. Lisez attentivement les descriptions des cas d'utilisation et les questions fréquentes avant de décider de mettre en œuvre cette solution SAML adaptée à des cas particuliers. Avant de poursuivre, assurez-vous de bien comprendre les scénarios dans lesquels l'authentification SAML simplifiée est appropriée et quels types d'identités vous devez utiliser. Dans la plupart des cas d'utilisation de SAML, vous pouvez configurer l'authentification SAML en suivant d'autres articles dédiés et en transmettant les quatre attributs cip_* d'authentification.

> **Remarque :**
>
> L'« authentification SAML simplifiée » augmente la charge des connecteurs Citrix Cloud, car ils doivent rechercher l'adresse e-mail, le SID et l'OID des utilisateurs pour chaque ouverture de session Workspace au lieu de transmettre ces valeurs dans l'assertion SAML. Si l'authentification SAML simplifiée ne s'avère pas particulièrement nécessaire, il est préférable de transmettre les quatre attributs cip_* dans l'assertion SAML afin de garantir les performances du connecteur Citrix Cloud.

Logiciels requis

- Une application SAML spécifiquement configurée pour l'authentification SAML simplifiée, qui envoie uniquement l'attribut **cip_upn** à des fins d'authentification dans l'assertion SAML.
- Des utilisateurs frontend au sein de votre fournisseur SAML.
- Un emplacement de ressources contenant une paire de connecteurs Citrix Cloud connectés à la forêt AD et au domaine dans lequel les comptes fantôme AD sont créés.
- Des suffixes d'UPN alternatifs ajoutés à la forêt AD principale où les comptes fantôme AD sont créés.
- Des comptes fantôme AD principaux avec leurs UPN correspondants.
- Des ressources DaaS ou CVAD mappées aux utilisateurs du compte fantôme AD.
- Un ou plusieurs serveurs FAS liés au même emplacement de ressources.

Questions fréquentes

Pourquoi utiliser l'authentification SAML simplifiée ?

Il est très fréquent pour les grandes entreprises d'inviter des contractants et des employés temporaires sur leur plateforme d'identité. L'objectif est d'accorder aux contractants un accès temporaire à Citrix Workspace en utilisant une identité utilisateur existante, telle que l'adresse e-mail d'un contractant ou une adresse e-mail extérieure à votre entreprise. L'authentification SAML simplifiée per-

met d'utiliser des identités frontend natives ou invitées qui n'existent pas dans le domaine AD où les ressources DaaS sont publiées.

Qu'est-ce que l'authentification SAML simplifiée ?

En règle générale, lors de la connexion à Citrix Workspace, quatre attributs SAML cip_* et leurs attributs d'utilisateur AD correspondants sont utilisés pour authentifier les utilisateurs. Ces quatre attributs SAML doivent normalement figurer dans l'assertion SAML et être renseignés via les attributs d'utilisateur AD. L'authentification SAML simplifiée signifie que seul l'attribut SAML cip_upn est requis pour que l'authentification réussisse.

Attribut AD	Nom d'attribut par défaut dans l'assertion SAML
userPrincipalName	cip_upn
Messagerie	cip_email
objectSID	cip_sid
objectGUID	cip_oid

Les trois autres attributs d'utilisateur AD, objectSID, objectGUID et l'adresse e-mail, requis pour l'authentification sont obtenus via des connecteurs Citrix Cloud associés au domaine AD où existe le compte fantôme AD. Il n'est donc plus nécessaire de les inclure dans l'assertion SAML lors d'un flux de connexion SAML à Workspace ou Citrix Cloud.

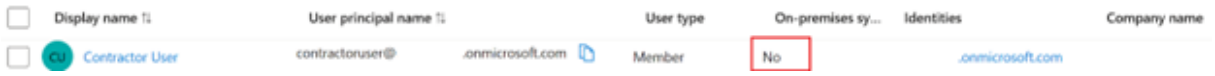
Attribut AD	Nom d'attribut par défaut dans l'assertion SAML
userPrincipalName	cip_upn

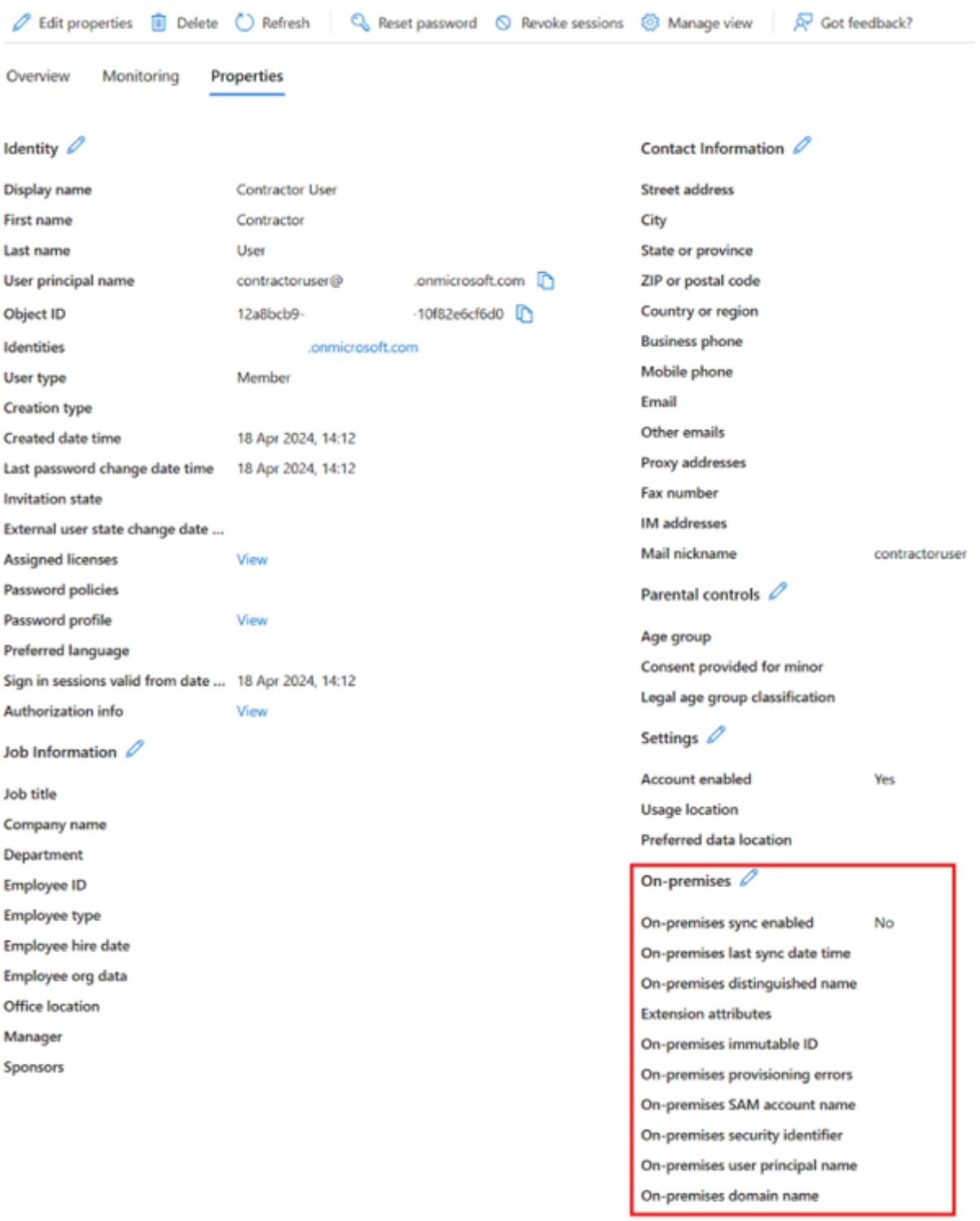
> **Important :**
>
> Il demeure toujours nécessaire de transmettre l'attribut **displayName** pour tous les flux SAML, y compris l'authentification SAML simplifiée. L'interface utilisateur de Workspace a besoin de l'attribut **displayName** pour afficher correctement le nom complet de l'utilisateur de Workspace.

Qu'est-ce qu'une identité utilisateur SAML native ?

Un utilisateur SAML natif est une identité utilisateur qui n'existe que dans le répertoire de votre fournisseur SAML, par exemple Entra ID ou Okta. Ces identités ne contiennent pas d'attributs utilisateur locaux, car elles ne sont pas créées via des outils de synchronisation AD tels qu'Entra ID connect.

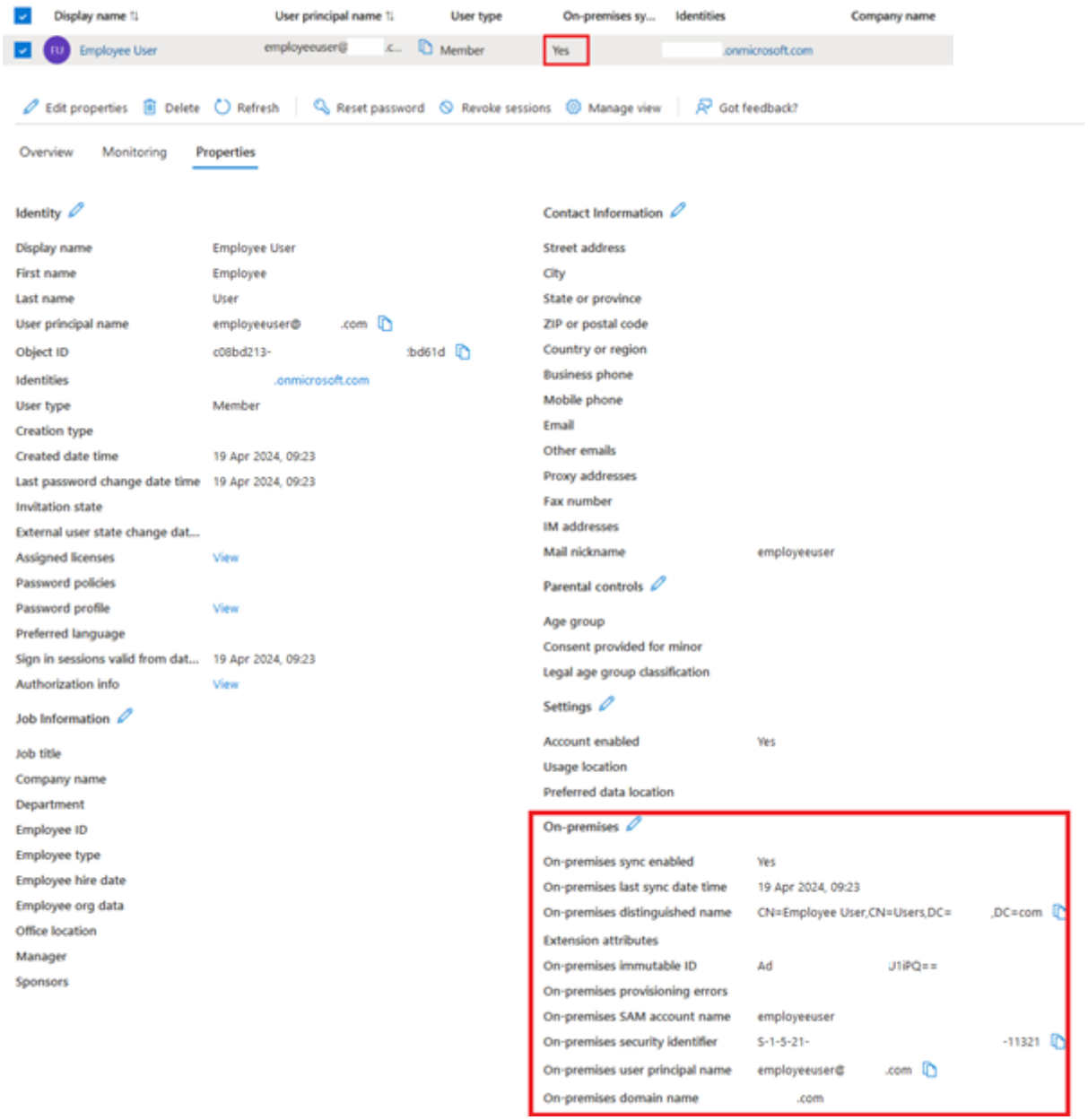
Elles nécessitent des comptes fantôme correspondant au compte principal pour pouvoir énumérer et lancer des ressources DaaS. L'utilisateur SAML natif doit être mappé à un compte correspondant dans Active Directory.





Qu'est-ce qu'une identité utilisateur SAML basée sur AD ?

Un utilisateur SAML basé sur AD est une identité utilisateur qui existe à la fois dans le répertoire de votre fournisseur SAML, comme Entra ID ou Okta, et dans votre forêt AD locale. Ces identités contiennent des attributs utilisateur locaux, car elles sont créées via des outils de synchronisation AD tels qu'Entra ID connect. Les comptes fantôme du compte AD principal ne sont pas nécessaires pour ces utilisateurs, car ils contiennent des SID et des OID locaux et peuvent donc énumérer et lancer des ressources DaaS.

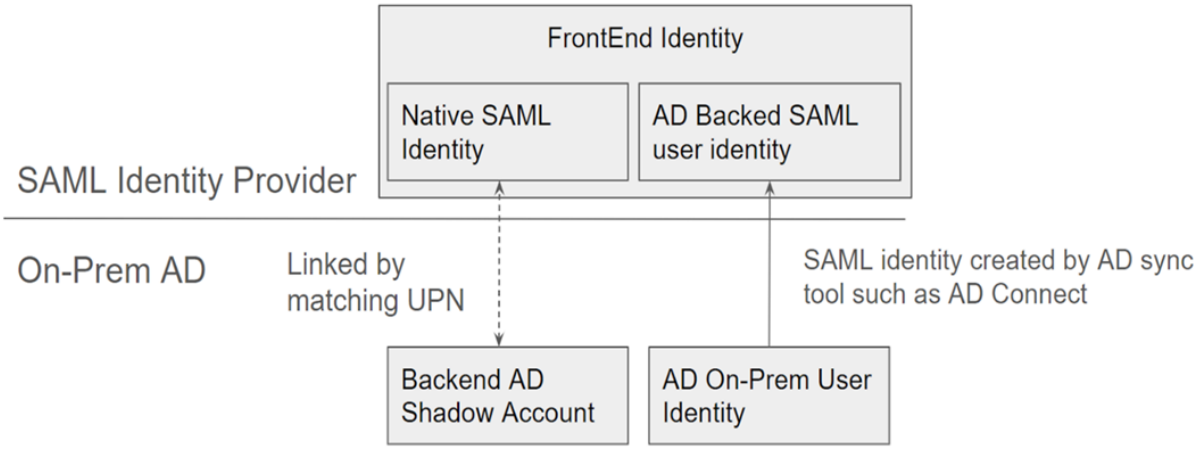


Qu'est-ce qu'une identité frontend ?

Une identité frontend est l'identité utilisée pour se connecter à la fois au fournisseur SAML et à Workspace. Les identités frontend ont des attributs utilisateur différents selon la manière dont elles ont été créées au sein du fournisseur SAML.

1. Identité utilisateur SAML native
2. Identité utilisateur SAML basée sur AD

Votre fournisseur SAML peut avoir une combinaison de ces deux types d'identités. Par exemple, si vous avez à la fois des contractants et des employés permanents au sein de votre plateforme d'identité, l'authentification SAML simplifiée fonctionnera pour les deux types d'identités frontend, mais n'est obligatoire que si certains comptes utilisent un type identité utilisateur SAML native.



Qu'est-ce qu'un compte fantôme AD principal ?

Un compte fantôme AD principal est un compte AD utilisé par le DaaS et mappé à une identité frontend correspondante au sein de votre fournisseur SAML.

Pourquoi est-il nécessaire de créer des comptes fantôme AD principaux ?

L'énumération de ressources DaaS ou CVAD publiées à l'aide de VDA joints à un domaine AD nécessite de créer des comptes AD au sein de la forêt Active Directory à laquelle les VDA sont joints. Mappez les ressources de votre groupe de mise à disposition DaaS aux utilisateurs des comptes fantôme ainsi qu'aux groupes AD contenant des comptes fantôme au sein du domaine AD auquel vous avez connecté vos VDA.

> **Important :**
>
> Seuls les utilisateurs SAML natifs sans attributs de domaine AD ont besoin de comptes fantôme

> AD correspondants. Si vos identités frontend sont importées depuis Active Directory, vous n'avez pas besoin de recourir à l'authentificatione SAML simplifiée ni de créer des comptes AD fantômes principaux.

Comment associer une identité frontend au compte fantôme AD principal correspondant ?

La méthode permettant de lier l'identité frontend à l'identité principale consiste à utiliser les UPN correspondants. Les deux identités liées doivent avoir des UPN identiques afin que Workspace puisse déterminer qu'elles représentent bien le même utilisateur qui se connecte à Workspace pour énumérer et lancer des ressources DaaS.

Le service d'authentification fédérée de Citrix est-il nécessaire pour utiliser l'authentification SAML simplifiée ?

Oui. Le service d'authentification fédérée (FAS) est requis pour l'authentification unique auprès du VDA lors du lancement lorsque vous vous connectez à Workspace à l'aide d'une méthode d'authentification fédérée.

Qu'est-ce que le « problème de non-concordance des SID » et quand peut-il survenir ?

Le « problème de non-concordance des SID » se produit lorsque l'assertion SAML contient un SID d'utilisateur frontend qui ne correspond pas au SID de l'utilisateur du compte fantôme AD. Cela peut se produire lorsque le compte qui se connecte à votre fournisseur SAML possède un SID local différent du SID de l'utilisateur du compte fantôme. Ce problème ne se produit que lorsque l'identité frontend est fournie par des outils de synchronisation AD tels qu'Entra ID Connect à partir d'une forêt AD différente de celle où le compte fantôme a été créé.

L'authentification SAML simplifiée empêche le « problème de non-concordance des SID » de se produire. Le SID correct de l'utilisateur du compte fantôme est toujours récupéré via les connecteurs Citrix Cloud joints au domaine AD principal. La recherche de l'utilisateur du compte fantôme s'effectue à l'aide de l'UPN de l'utilisateur frontend, qui est ensuite mis en correspondance avec l'utilisateur du compte fantôme principal associé.

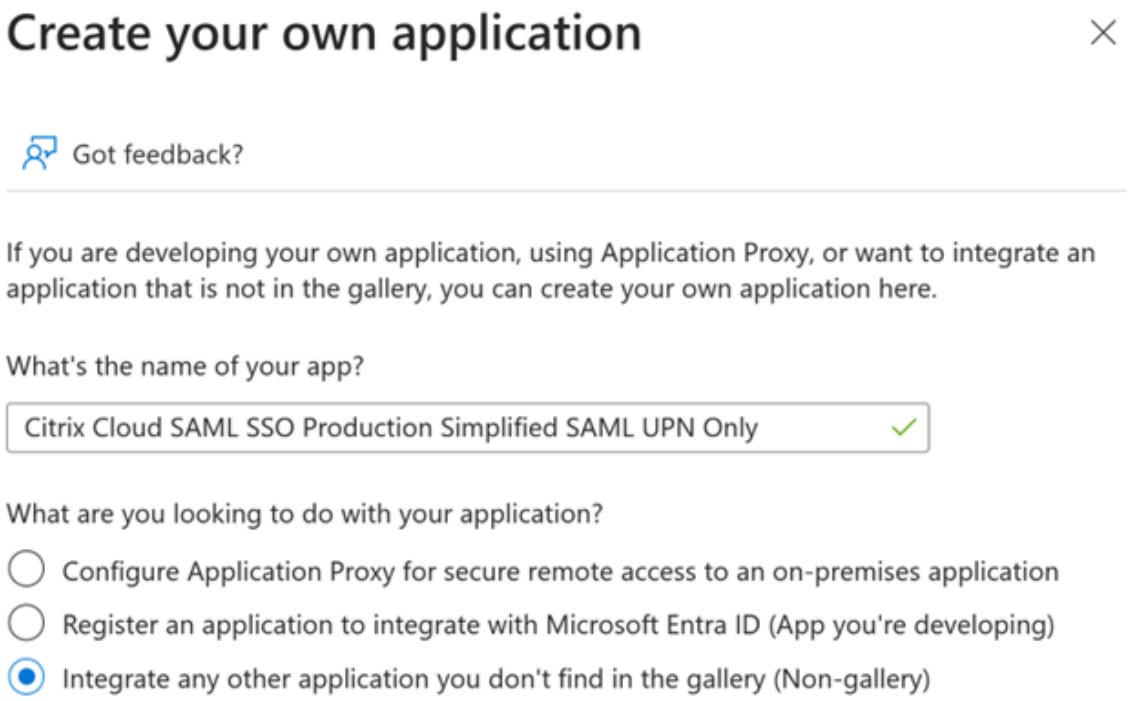
Exemple de problème de non-concordance des SID :
l'utilisateur frontend a été créé par Entra ID Connect et est synchronisé depuis la **forêt AD 1**.
`S-1-5-21-000000000-0000000000-0000000001-0001`

Utilisateur du compte fantôme principal créé dans la **forêt AD 2** et mappé aux ressources DaaS
`S-1-5-21-000000000-0000000000-0000000002-0002`

L'assertion SAML contient les quatre attributs cip_* et **cip_sid** contient la valeur `S-1-5-21-000000000-00000`, qui ne correspond pas au SID du compte fantôme, ce qui déclenche une erreur.

Configurer l'authentification SAML simplifiée avec Entra ID pour les comptes d'invités externes

1. Connectez-vous au portail Azure.
2. Dans le menu du portail, sélectionnez **Entra ID**.
3. Dans le volet de gauche, sous **Gérer**, sélectionnez **Applications d'entreprise**.
4. Sélectionnez **Créer votre propre application**.
5. Entrez un nom approprié pour l'application SAML, tel que `Citrix Cloud SAML SSO Production Simplified SAML`.



6. Dans le volet de navigation de gauche, sélectionnez **Authentification unique** puis, dans le volet de travail, cliquez sur **SAML**.
7. Dans la section **Configuration SAML de base**, sélectionnez **Modifier** et configurez les paramètres suivants :

    a) Dans la section **Identifiant (ID d'entité)**, sélectionnez **Ajouter un identifiant**, puis entrez la valeur associée à la région dans laquelle se trouve votre locataire Citrix Cloud :

    - Pour les régions de l'Europe, des États-Unis et du sud de l'Asie-Pacifique, entrez `https://saml.cloud.com`.
    - Pour la région du Japon, entrez `https://saml.citrixcloud.jp`.
    - Pour la région Citrix Cloud Government, entrez `https://saml.cloud.us`.

b) Dans la section **URL de réponse (URL du service consommateur d'assertion)**, sélectionnez **Ajouter une URL de réponse**, puis entrez la valeur associée à la région dans laquelle se trouve votre client Citrix Cloud :

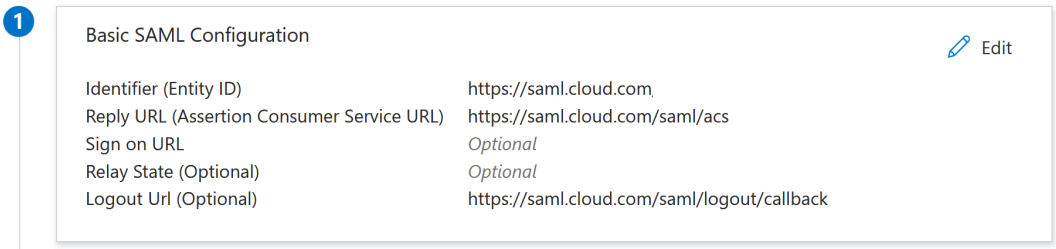
- Pour les régions de l'Europe, des États-Unis et du sud de l'Asie-Pacifique, entrez `https://saml.cloud.com/saml/acs`.
- Pour la région du Japon, entrez `https://saml.citrixcloud.jp/saml/acs`.
- Pour la région Citrix Cloud Government, entrez `https://saml.cloud.us/saml/acs`.

c) Dans la section **URL de connexion**, entrez votre URL Workspace.

d) Dans la section **URL de déconnexion (facultatif)**, entrez la valeur associée à la région dans laquelle se trouve votre client Citrix Cloud :

- Pour les régions de l'Europe, des États-Unis et du sud de l'Asie-Pacifique, entrez `https://saml.cloud.com/saml/logout/callback`.
- Pour la région du Japon, entrez `https://saml.citrixcloud.jp/saml/logout/callback`.
- Pour la région Citrix Cloud Government, entrez `https://saml.cloud.us/saml/logout/callback`.

e) Dans la barre de commandes, cliquez sur **Enregistrer**. La section **Configuration SAML de base** apparaît comme suit :



8. Dans la section **Attributs et revendications**, cliquez sur **Modifier** pour configurer les revendications suivantes. Ces revendications apparaissent dans l'assertion SAML contenue dans la réponse SAML. Après avoir créé l'application SAML, configurez les attributs suivants.

a) Sous la revendication **Identifiant d'utilisateur unique (ID de nom)**, laissez la valeur par

défaut `user.userprincipalname`.

b) Pour la revendication **cip_upn**, laissez la valeur par défaut de `user.userprincipalname` .

c) Pour **displayName**, laissez la valeur par défaut de `user.displayname`.

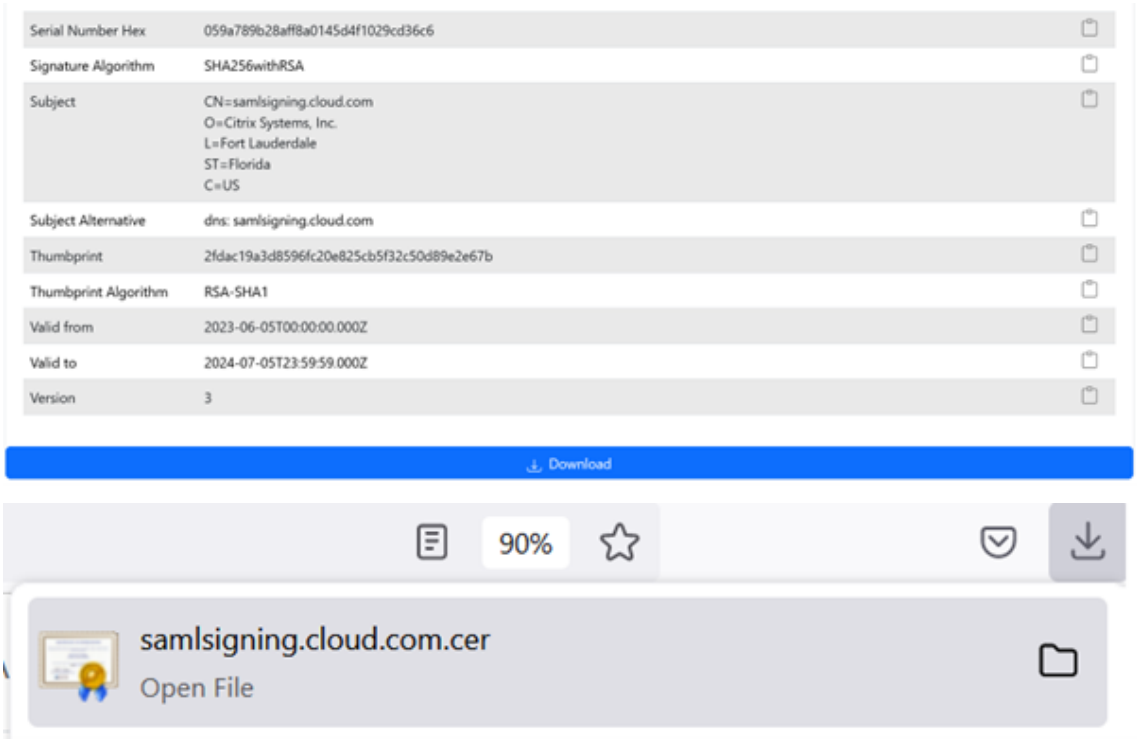
d) Dans la section **Autres revendications**, pour toutes les revendications restantes avec l'espace de noms `http://schemas.xmlsoap.org/ws/2005/05/identity/claims`, cliquez sur le bouton représentant des points de suspension (...), puis sur **Supprimer**. Il n'est pas nécessaire d'inclure ces revendications car elles sont des doublons des attributs utilisateur ci-dessus.

Lorsque vous avez terminé, la section **Attributs et revendications** apparaît comme illustré ci-dessous :

e) Obtenez une copie du certificat de signature SAML Citrix Cloud à l'aide de cet outil en ligne tiers.

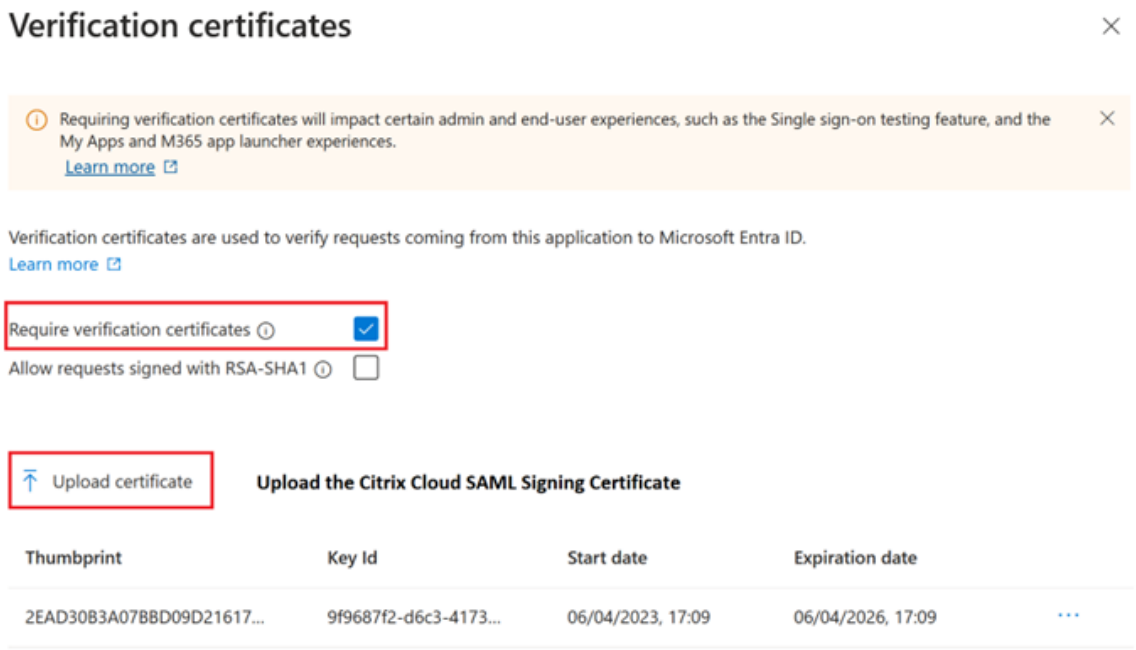
f) Entrez `https://saml.cloud.com/saml/metadata` dans le champ URL et cliquez sur **Charger**.

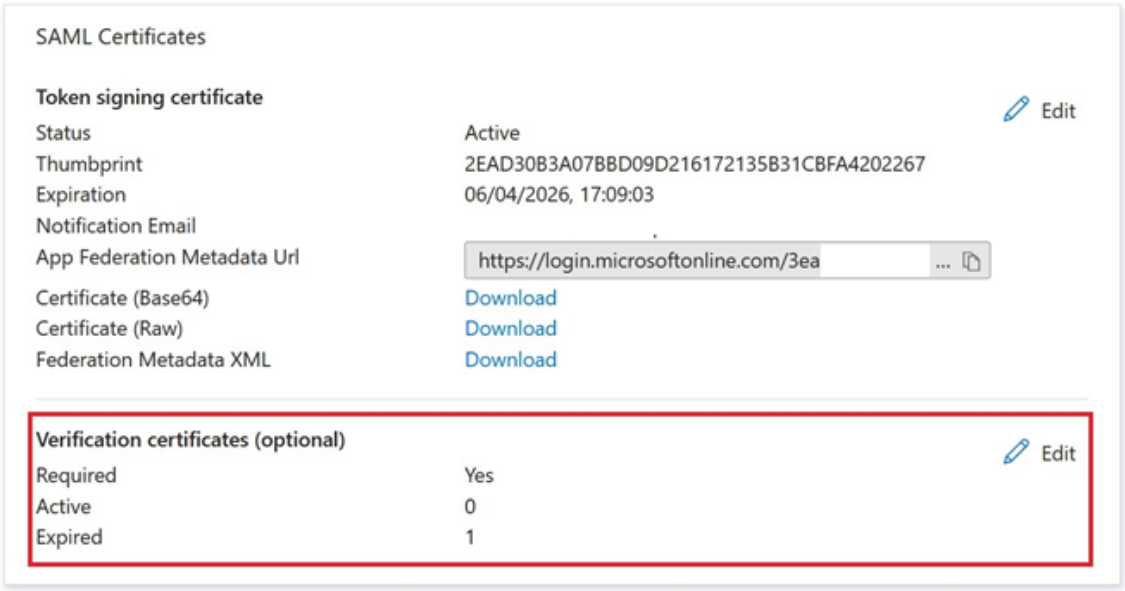
9. Faites défiler la page vers le bas et cliquez sur **Télécharger**.



10. Configurez les paramètres de signature de l'application SAML Azure Active Directory.
11. Charger le certificat de signature SAML de production obtenu à l'étape 10 dans l'application SAML Azure Active Directory

    a) Activez **Exiger des certificats de vérification**.

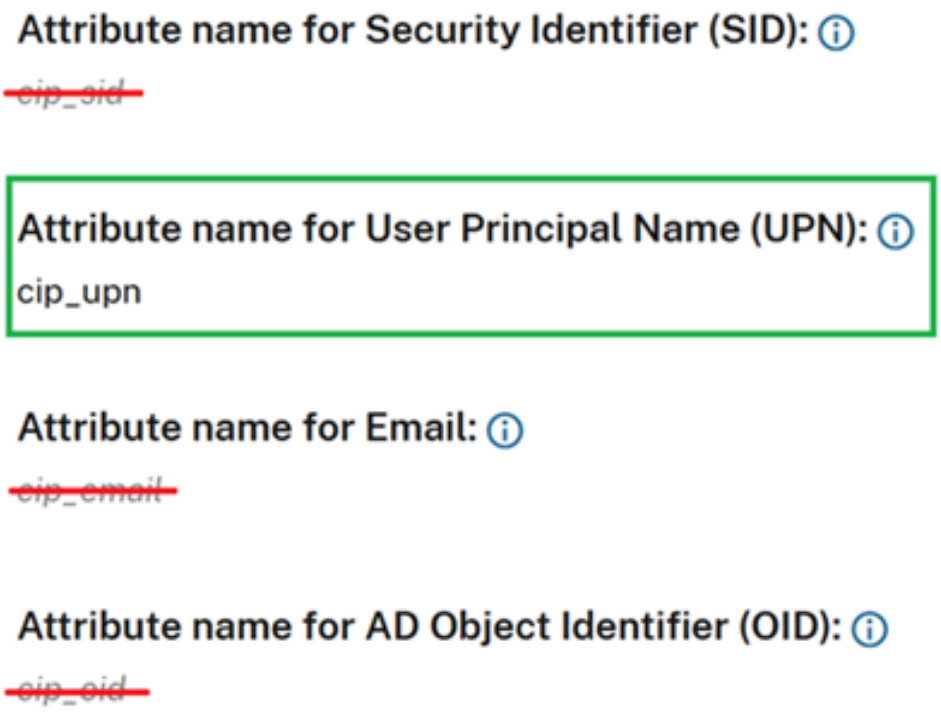




Configurer la connexion à Citrix Cloud via l'authentification SAML simplifiée

Par défaut, Citrix Cloud s'attend à ce que les attributs cip_upn, cip_email, cip_sid et cip_oid soient présents dans l'assertion SAML et empêchera la connexion SAML s'il ne sont pas transmis. Pour éviter ce problème, supprimez les vérifications de ces attributs lorsque vous créez votre nouvelle connexion SAML.

1. Créez une connexion SAML en utilisant les paramètres par défaut.
2. Accédez à la section **Configuration des mappages d'attributs SAML** en bas et modifiez les paramètres avant d'enregistrer la nouvelle configuration SAML.
3. Supprimez le nom d'attribut SAML de chacun des champs **cip_email**, **cip_sid**et **cip_oid**.
4. Ne supprimez pas **cip_upn** de son champ.
5. Ne supprimez aucun autre attribut de leurs champs respectifs. L'attribut **displayName** est toujours nécessaire pour l'interface utilisateur de Workspace et ne doit pas être modifié.



Configurer l'emplacement de ressources et les connecteurs du compte fantôme AD

Il est nécessaire de configurer un emplacement de ressources et une paire de connecteurs au sein de la forêt AD du compte fantôme principal. Citrix Cloud fait appel à ces connecteurs au sein de la forêt AD pour rechercher les identités et les attributs cip_email, cip_sid et cip_oid des utilisateurs des comptes fantôme, lorsque seul l'attribut cip_upn est transmis directement dans l'assertion SAML.

1. Créez un **emplacement de ressources** qui contiendra les connecteurs Citrix Cloud joints à la forêt AD du compte fantôme principal.

2. Nommez l'emplacement de ressources en fonction de la forêt AD où résident les comptes fantômes AD principaux que vous souhaitez utiliser.
3. Configurez une paire de connecteurs Citrix Cloud dans l'emplacement de ressources nouvellement créé.

Par exemple
`ccconnector1.shadowaccountforest.com`
`ccconnector2.shadowaccountforest.com`

Configurer le service d'authentification fédérée dans la forêt AD principale

Les contractants utilisateurs du compte principal auront bel et bien besoin du FAS. En effet, pour lancer les services DaaS, ces utilisateurs ne pourront pas saisir manuellement les informations d'identification Windows , car ils ne connaîtront probablement pas le mot de passe du compte fantôme AD.

1. Configurez un ou plusieurs serveurs FAS dans la forêt AD principale dans laquelle vos comptes fantôme ont été créés.
2. Ensuite, liez les serveurs FAS au même emplacement de ressources qui contient une paire de connecteurs Citrix Cloud joints à la forêt AD principale dans laquelle vos comptes fantôme ont été créés.

Configurer des suffixes d'UPN alternatifs dans le domaine AD

> **Important :**
>
> Un UPN n'est pas identique à l'adresse e-mail de l'utilisateur. Dans de nombreux cas, bien que leur valeur soit la même pour des raisons de facilité d'utilisation, l'UPN et l'adresse e-mail électronique sont utilisés à des fins internes différentes et définis dans des attributs Active Directory différents.

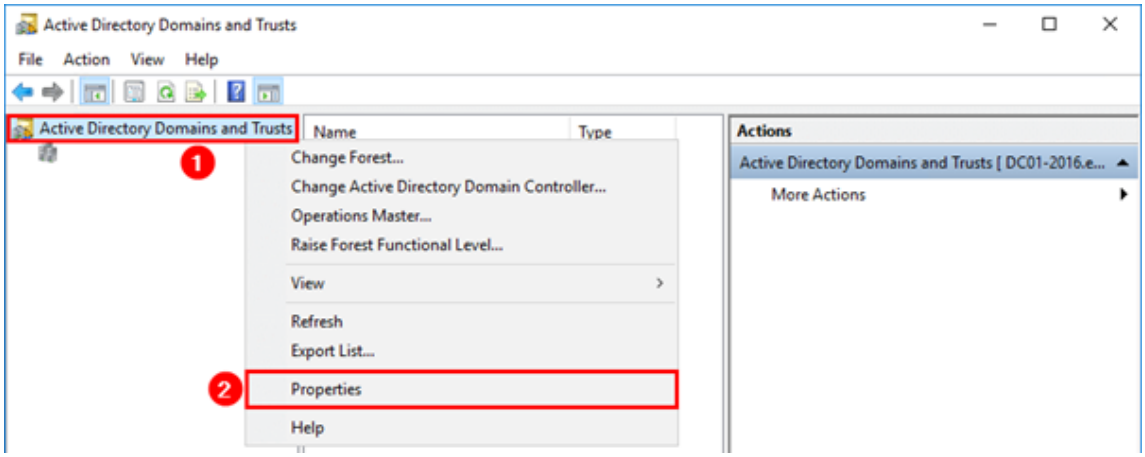
Le suffixe du nom d'utilisateur principal (UPN) fait partie du nom de connexion dans AD. Lorsque vous créez un compte, celui-ci utilise le suffixe d'UPN implicite de votre forêt AD par défaut, tel que « yourforest.com ». Vous devrez ajouter un suffixe d'UPN alternatif correspondant pour chaque utilisateur externe du compte frontend que vous souhaitez inviter dans vos locataires Okta ou Azure AD.

Par exemple, si vous invitez un utilisateur externe `contractoruser@hotmail.co.uk` et que vous souhaitez l'associer à un compte fantôme AD principal `contractoruser@yourforest.com`, ajoutez `yourforest.com` comme suffixe alternatif d'UPN dans votre forêt AD.

Ajouter des suffixes d'UPN alternatifs dans Active Directory à l'aide de l'interface utilisateur Active Directory Domains and Trusts

1. Connectez-vous à un contrôleur de domaine au sein de votre forêt AD principale.
2. Ouvrez la **boîte de dialogue Exécuter**, tapez `domain.msc`, puis cliquez sur **OK**.

3. Dans la fenêtre Active Directory Domains and Trusts, cliquez avec le bouton droit sur **Active Directory Domains and Trusts**, puis sélectionnez **Propriétés**.
4. Sous l'onglet **Suffixes d'UPN**, dans la zone « Suffixes d'UPN alternatifs », ajoutez un autre suffixe d'UPN, puis sélectionnez **Ajouter**.



5. Cliquez sur **OK**.

Gérer les suffixes d'UPN de votre forêt AD principale à l'aide de PowerShell

Pour créer les UPN de compte fantôme nécessaires, vous devrez peut-être ajouter un grand nombre de nouveaux suffixes d'UPN à votre forêt AD principale. Le nombre de suffixes d'UPN alternatifs à ajouter à la forêt AD principale dépend du nombre d'utilisateurs externes que vous souhaitez inviter dans votre locataire de fournisseur SAML.

Voici quelques commandes PowerShell à utiliser si vous devez créer un grand nombre de suffixes d'UPN alternatifs.

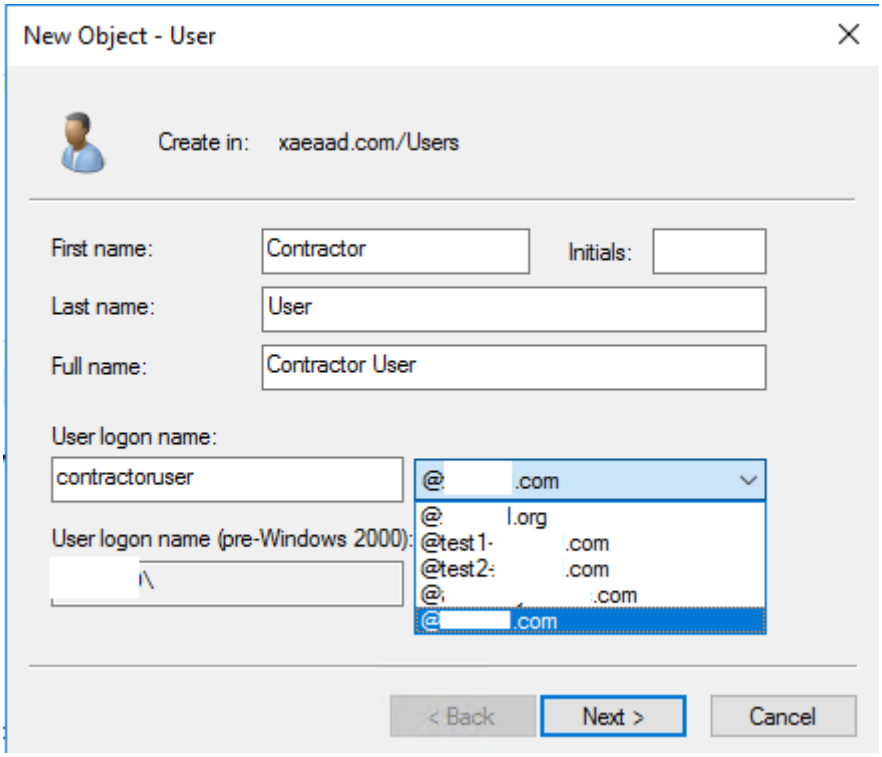
```
# Get the list of existing ALT UPN suffixes within your AD Forest
(Get-ADForest).UPNSuffixes

# Add or remove ALT UPN Suffixes
$NewUPNSuffixes = @("yourforest.com","externalusers.com")

# Set action to "add" or "remove" depending on the operation you wish
    to perform.
$Action = "add"
foreach($NewUPNSuffix in $NewUPNSuffixes)
{

    Get-ADForest | Set-ADForest -UPNSuffixes @{
 $Action=$NewUPNSuffix }

 }

```



```
<!--NeedCopy-->
```

Configurer un compte fantôme AD dans la forêt AD principale

1. Créez un utilisateur de compte fantôme AD.
2. L'UPN implicite de la forêt AD, tel que `yourforest.local` est sélectionné par défaut pour les nouveaux utilisateurs AD. Sélectionnez le suffixe d'UPN alternatif approprié créé précédemment. Par exemple, sélectionnez `yourforest.com` comme suffixe d'UPN pour l'utilisateur du compte fantôme.



Vous pouvez également mettre à jour l'UPN de l'utilisateur du compte fantôme via PowerShell.

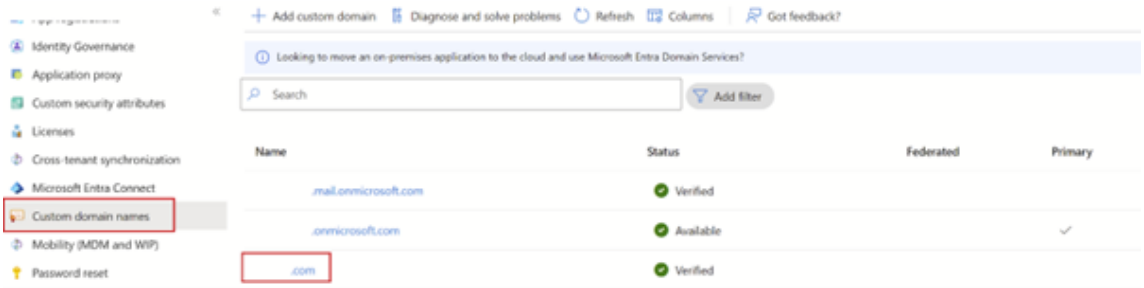
```
Set-ADUser "contractoruser" -UserPrincipalName "
   contractoruser@yourforest.com"
<!--NeedCopy-->
```

3. L'UPN de l'utilisateur du compte fantôme doit correspondre exactement à l'UPN de l'identité frontend de l'utilisateur externe.
4. Testez la connexion de l'utilisateur frontend à Workspace.
5. Une fois la connexion réussie, vérifiez que toutes les ressources attendues sont énumérées dans Workspace. Les ressources mappées au compte fantôme AD devraient alors s'afficher.

Configurer l'UPN utilisateur Guest Entra ID de sorte qu'il corresponde à l'UPN du compte AD fantôme

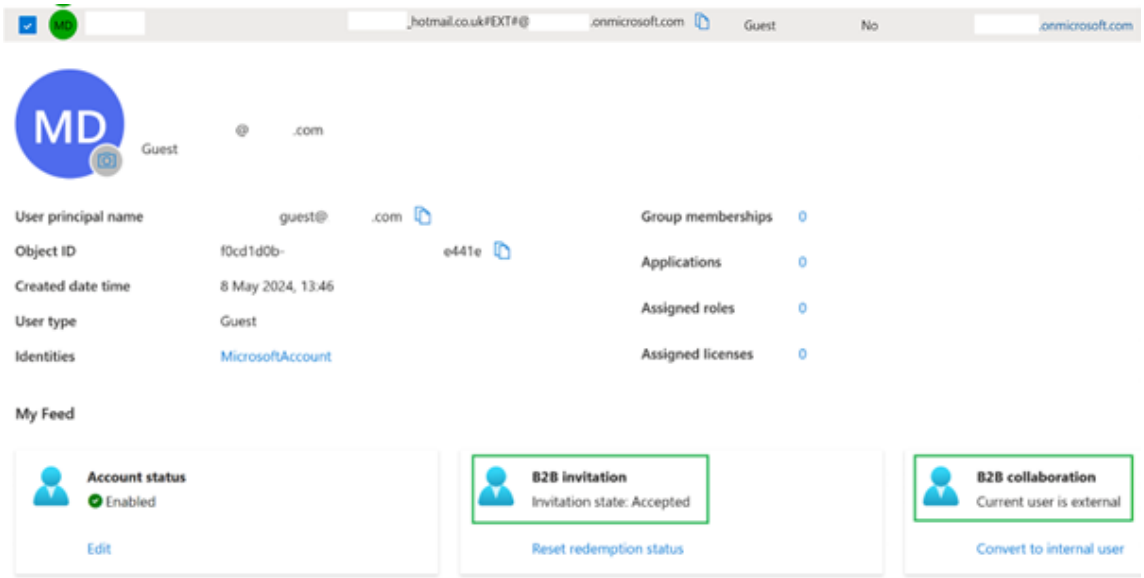
Lorsque des utilisateurs externes sont invités à rejoindre un locataire Entra ID, un UPN est automatiquement généré pour indiquer qu'il s'agit d'utilisateurs externes. L'utilisateur externe Entra ID se verra automatiquement attribuer le suffixe d'UPN @Entra IDtenant.onmicrosoft.com, qui ne convient pas à l'utilisation de l'authentification SAML simplifiée et ne correspond pas au compte AD fantôme. L'UPN devra être mis à jour de sorte qu'il corresponde à un domaine DNS importé dans Entra ID et au suffixe d'UPN alternatif que vous avez créé dans votre forêt AD.

1. Importez un domaine personnalisé dans Entra ID qui correspond au suffixe d'UPN alternatif que vous avez ajouté à votre forêt AD.



2. Invitez un utilisateur, tel que `contractoruser@hotmail.co.uk`, et assurez-vous qu'il accepte l'invitation Microsoft adressée au locataire Entra ID.

   Exemple de format d'UPN pour un utilisateur invité externe généré par Microsoft. `contractoruser_hotmail.co.uk#EXT#@yourEntra IDtenant.onmicrosoft.com`



> **Important :**
>
> Citrix Cloud et Workspace ne peuvent pas utiliser d'UPN contenant le caractère # pour l'authentification SAML.

3. Pour pouvoir gérer les utilisateurs Entra ID, installez les modules Azure PowerShell Graph requis.

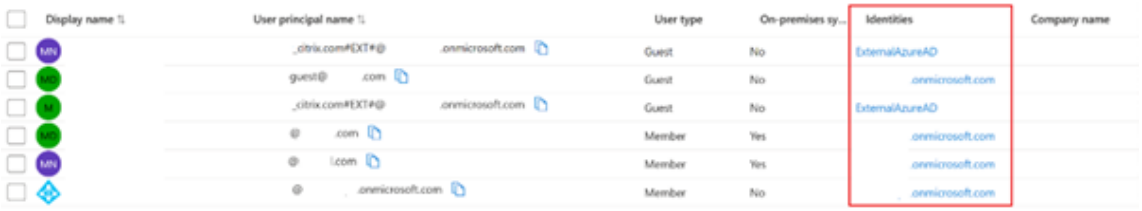
```
Install-Module -Name "Microsoft.Graph" -Force
Get-InstalledModule -Name  "Microsoft.Graph"
<!--NeedCopy-->
```

4. Connectez-vous à votre locataire Entra ID à l'aide d'un compte administrateur global avec l'étendue `Directory.AccessAsUser.All`.

> **Important :**
>
> Si vous utilisez un compte avec des privilèges moindres ou si vous ne spécifiez pas l'étendue `Directory.AccessAsUser.All`, vous ne pourrez pas terminer l'étape 4 et mettre à jour l'UPN de l'utilisateur invité.

```
$EntraTenantID = "<yourEntraTenantID>"
Connect-MgGraph -Tenant $EntraTenantID -Scopes "Directory.
    AccessAsUser.All"
<!--NeedCopy-->
```

5. Obtenez la liste complète des utilisateurs invités externes au sein de votre locataire Entra ID (facultatif).




```
Get-MgUser -filter "userType eq 'Guest'" | Select Id,DisplayName,
    UserPrincipalName,Mail
<!--NeedCopy-->
```

6. Obtenez l'identité de l'utilisateur invité dont l'UPN doit être mis à jour, puis mettez à jour son suffixe.

```
$GuestUserId = (Get-MgUser -UserId "contractoruser_hotmail.co.uk#
    EXT#@yourEntra IDtenant.onmicrosoft.com").Id

Update-MgUser -UserId $GuestUserId -UserPrincipalName "
    contractoruser@yourforest.com"
<!--NeedCopy-->
```

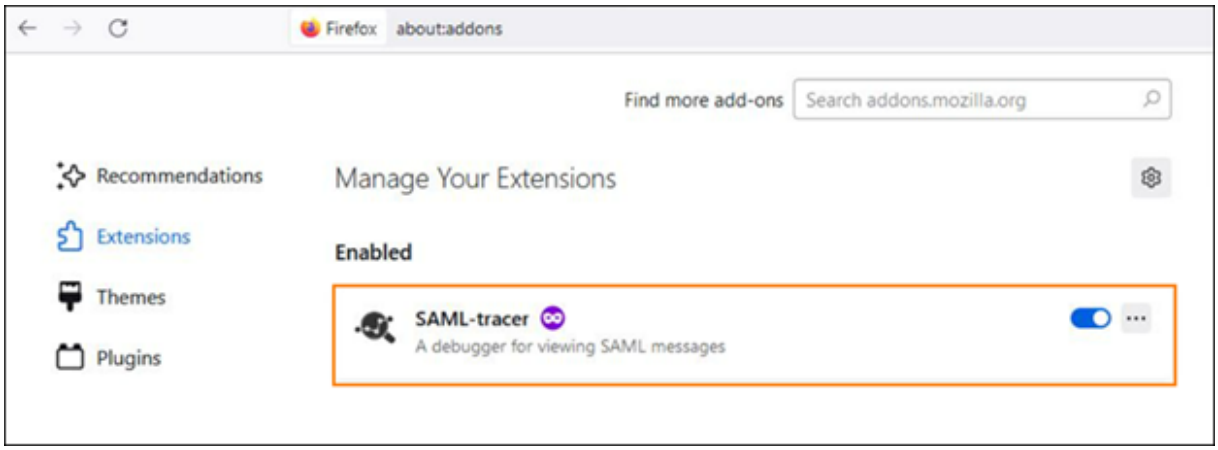

7. Vérifiez que l'identité de l'utilisateur invité peut se retrouver à l'aide de l'UPN récemment mis à jour.

```
Get-MgUser -UserId "contractoruser@yourforest.com"
<!--NeedCopy-->
```

Test de la solution d'authentification SAML simplifiée

Une fois que toutes les étapes de ce document ont été effectuées dans AD, Citrix Cloud et votre fournisseur SAML, vous devez tester la connexion et vérifier que la liste de ressources correcte est affichée pour l'utilisateur invité dans Workspace.

Citrix recommande d'utiliser l'extension de navigateur SAML-tracer pour tous les débogages SAML. Cette extension est disponible pour la plupart des navigateurs Web courants. L'extension décode les requêtes et les réponses codées en Base64 en langage XML SAML, et les fournit donc en dans un format intelligible.



Exemple d'assertion SAML simplifiée utilisant uniquement l'attribut cip_upn pour l'authentification capturée à l'aide d'un traceur SAML.


```
<AttributeStatement>
    <Attribute Name="http://schemas.microsoft.com/identity/claims/tenantid">
        <AttributeValue>                                    </AttributeValue>
    </Attribute>
    <Attribute Name="http://schemas.microsoft.com/identity/claims/objectidentifier">
        <AttributeValue>                                    </AttributeValue>
    </Attribute>
    <Attribute Name="http://schemas.microsoft.com/identity/claims/identityprovider">
        <AttributeValue>https://sts.windows.net/                                    /</AttributeValue>
    </Attribute>
    <Attribute Name="http://schemas.microsoft.com/claims/authnmethodsreferences">
        <AttributeValue>http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/        </AttributeValue>
    </Attribute>
    <Attribute Name="cip_upn">
        <AttributeValue>                    </AttributeValue>
    </Attribute>
    <Attribute Name="lastName">
        <AttributeValue>    </AttributeValue>
    </Attribute>
    <Attribute Name="firstName">
        <AttributeValue>    </AttributeValue>
    </Attribute>
    <Attribute Name="displayName">
        <AttributeValue>          </AttributeValue>
    </Attribute>
</AttributeStatement>
```

FrontEnd Identity Type	Synched from AD	Has Connectors in AD	Needs AD Shadow Account	Login using Attribute
Internal AD Backed User in Shadow Account Forest	Yes	Yes	No	UPN
Internal AD Backed User in Different Forest	Yes	No	Yes	UPN
Internal Native User	No	Not applicable	Yes	UPN
External Guest User	No	Not applicable	Yes	Email

1. Mappez les ressources DaaS appropriées aux utilisateurs ou groupes des comptes basés sur AD ou aux groupes qui les contiennent.
2. Démarrez l'extension de l'outil de navigateur SAML-Tracer et capturez l'intégralité du flux d'ouverture et de fermeture de session.
3. Connectez-vous à Workspace à l'aide de l'attribut spécifié dans le tableau pour l'utilisateur de type frontend que vous souhaitez tester.

   Ouverture de session utilisateur invité Entra ID : l'utilisateur contractant que vous avez invité à rejoindre votre locataire Entra ID possède l'adresse e-mail `contractoruser@hotmail.co.uk`.

   Entrez l'**adresse e-mail** de l'utilisateur invité lorsque vous y êtes invité par Entra ID.

   OU

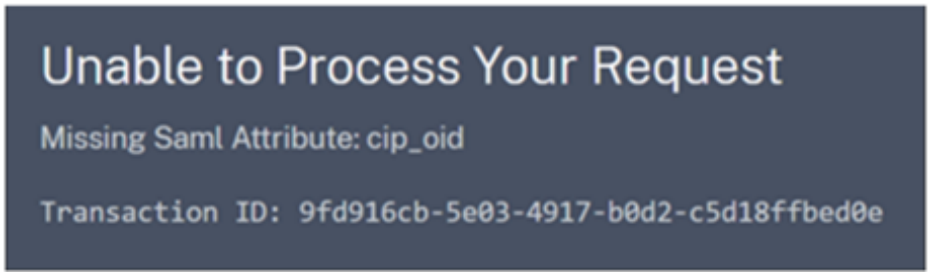
   Utilisateur EntraID basé sur AD ou connexion utilisateur EntraID natif : ces utilisateurs Entra ID auront des UPN au format `adbackeduser@yourforest.com` ou `nativeuser@yourforest.com`.

   Entrez l'**UPN** de l'utilisateur lorsque vous y êtes invité par Entra ID.
4. Vérifiez que l'assertion ne contient que l'attribut **cip_upn** pour l'authentification, ainsi que l'attribut **displayName** requis par l'interface utilisateur de Workspace.

5. Vérifiez que les ressources DaaS nécessaires s'affichent bien dans l'interface utilisateur.

Dépannage des problèmes liés à la solution SAML simplifiée

Erreurs d'attribut cip_* manquant



Cause 1 : L'attribut SAML n'est pas présent dans l'assertion SAML mais Citrix Cloud est configuré pour s'attendre à le recevoir. Vous n'avez pas réussi à supprimer les attributs cip_* inutiles de la connexion SAML Citrix Cloud dans la section Attributs SAML. Déconnectez et reconnectez SAML pour supprimer les références aux attributs cip_* inutiles.

Cause 2 : Cette erreur peut également se produire s'il n'existe aucun compte fantôme AD associé que les connecteurs Citrix Cloud peuvent rechercher dans la forêt AD principale. Vous avez peut-être correctement configuré l'identité frontend, mais l'identité du compte fantôme AD principal associée à un UPN n'existe pas ou est introuvable.

La connexion réussit, mais aucune ressource DaaS ne s'affiche une fois l'utilisateur connecté à Workspace

Cause : Cela est probablement dû à des mappages d'UPN incorrects entre les identités frontend et principale.

Assurez-vous que l'UPN des deux identités frontend et principale sont exactement identiques et représentent le même utilisateur qui se connecte à Workspace. Vérifiez que le groupe de mise à disposition DaaS contient des mappages vers les bons utilisateurs du compte fantôme AD ou les groupes AD qui les contiennent.

Lors du lancement des ressources DaaS, l'authentification unique via le FAS auprès des VDA joints au domaine AD échoue

Lorsque les utilisateurs de Workspace tentent de lancer des ressources DaaS, ils sont invités à saisir leurs informations d'identification Windows dans GINA. L'ID d'événement 103 s'affiche également dans les journaux d'événements Windows de vos serveurs FAS.

[S103] Le serveur [CC:FASServer] a demandé l'UPN [frontenduser@yourforest.com] `SID S-1-5-21-000000000-0000000000-0000000001-0001`, mais la recherche a renvoyé `SID S-1-5-21-000000000-0000000000-0000000001-0002`. [corrélation : cc #967472c8-4342-489b-9589-044a24ca57d1]

Cause : votre déploiement SAML simplifié présente un « problème de non-concordance des SID ». Des identités frontend contiennent des SID provenant d'une forêt AD différente de la forêt AD du compte fantôme principal.
Ne transmettez pas l'attribut **cip_sid** dans l'assertion SAML.

L'ouverture de session échoue pour les utilisateurs connectés à AD lorsque le même suffixe d'UPN existe dans plusieurs forêts AD connectées

Citrix Cloud possède plusieurs emplacements de ressources et connecteurs associés à différentes forêts AD. L'ouverture de session échoue lorsque des utilisateurs basés sur AD et importés dans Entra ID depuis une forêt AD différente de celle du compte fantôme AD sont utilisés.

La forêt AD 1 est synchronisée avec Entra ID pour créer des utilisateurs frontend dotés d'UPN tels que `frontenduser@yourforest.com`.

La forêt AD 2 contient les comptes fantômes principaux dotés d'UPN tels que `frontenduser@yourforest.com`.

Cause : votre déploiement SAML simplifié présente un « problème d'ambiguïté d'UPN ». Citrix Cloud ne parvient pas à déterminer les connecteurs à utiliser pour rechercher l'identité principale de l'utilisateur.

Ne transmettez pas l'attribut **cip_sid** dans l'assertion SAML.
L'UPN de votre utilisateur existe dans plusieurs forêts AD connectées à Citrix Cloud.

Configurer un serveur PingFederate local en tant que fournisseur SAML pour Workspace et Citrix Cloud

April 26, 2024

Author:
Mark Dear

Cet article a été rédigé dans le cadre d'une collaboration entre les ingénieurs de Citrix et de Ping et a été révisé par les deux parties pour en garantir l'exactitude technique au moment de la rédaction. Reportez-vous à la documentation Ping pour savoir comment provisionner, configurer et octroyer une

licence à un serveur PingFederate local à utiliser en tant que fournisseur SAML, car cela dépasse le cadre de cet article.

Ce document a été écrit à l'aide des versions 11.3 et 12 de PingFederate.

Pré-requis

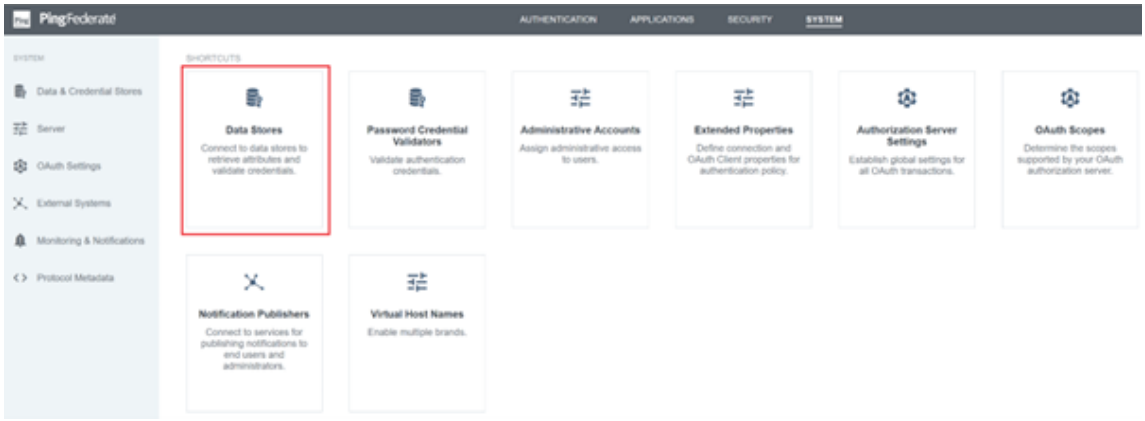
Cet article traite spécifiquement de la configuration SAML et garantit que les conditions suivantes sont remplies.

- Vous avez déjà provisionné un serveur PingFederate local au sein de votre organisation et obtenu la licence nécessaire. Pour plus d'informations, consultez la section Installation de PingFederate.
- Vous devez avoir installé une version compatible de Java sur le serveur PingFederate. Consultez la documentation de Ping Identity pour connaître les versions Java prises en charge. Pour plus d'informations, consultez la section Configuration requise pour Java PingFederate.
- Vous avez configuré les règles de réseau et de pare-feu requises pour permettre à Citrix Cloud et Workspace de rediriger vers le serveur PingFederate local pendant le processus d'ouverture de session SAML de la console d'administration Workspace/Citrix Cloud. Pour plus d'informations, consultez la section Configuration réseau requise pour PingFederate.
- Vous avez importé un certificat x509 signé publiquement sur votre serveur PingFederate qui peut faire office de certificat de serveur pour le serveur PingFederate.
- Vous avez importé un certificat x509 signé publiquement sur votre serveur PingFederate qui peut faire office de certificat de signature SAML pour le fournisseur d'identité. Ce certificat doit être chargé vers Citrix Cloud pendant le processus de connexion SAML.
- Vous avez connecté votre Active Directory local à PingFederate. Pour plus d'informations, consultez Magasin de données LDAP PingFederate.

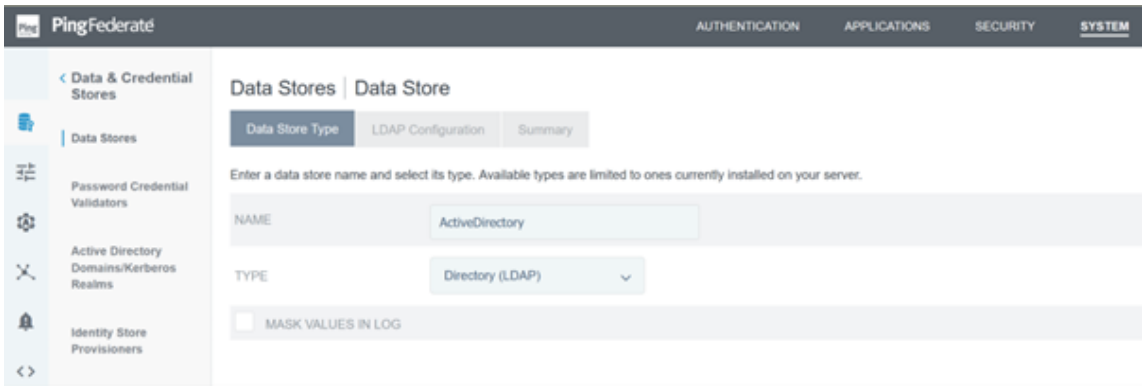
> **Remarque :**
>
> Lors de la configuration de PingFederate pour une utilisation avec Citrix Cloud et Workspace, consultez la documentation de PingFederate pour comprendre le fonctionnement de chaque paramètre SAML et pour compléter les instructions fournies ici.

Configurer une connexion Active Directory à votre domaine AD à l'aide d'un magasin de donnée dans PingFederate

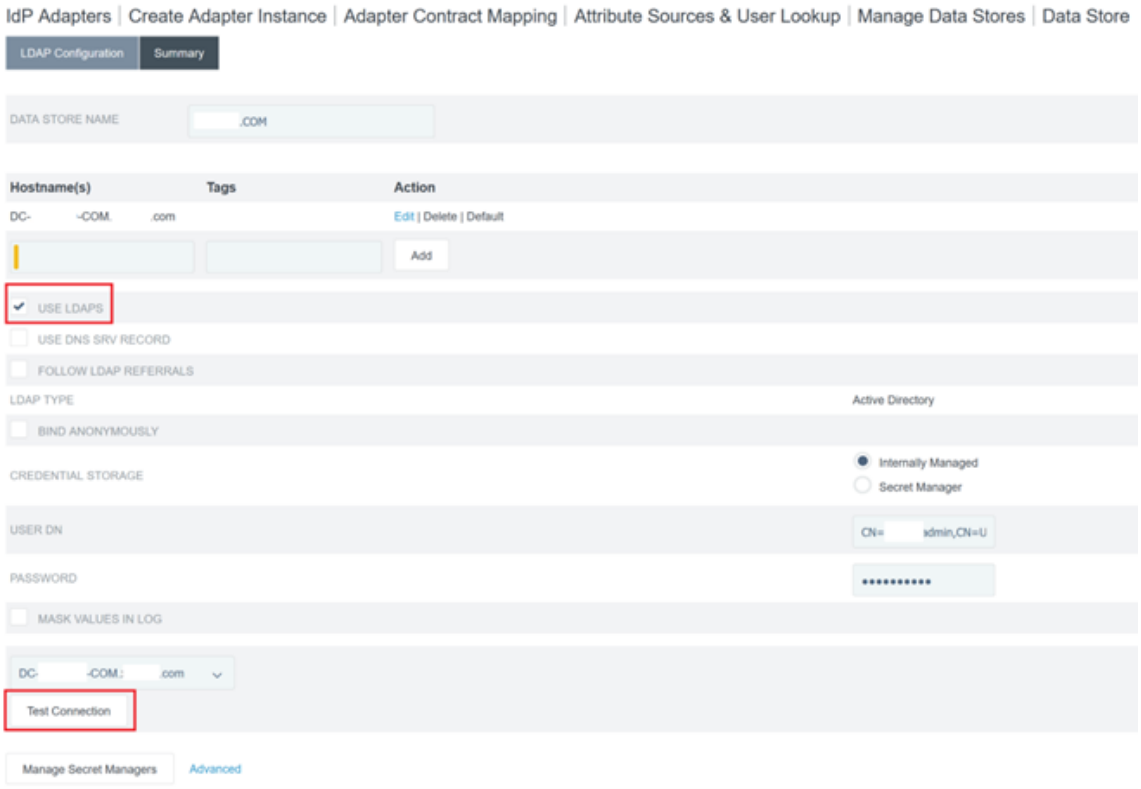
1. Configurez une connexion Active Directory dans des magasins de données.



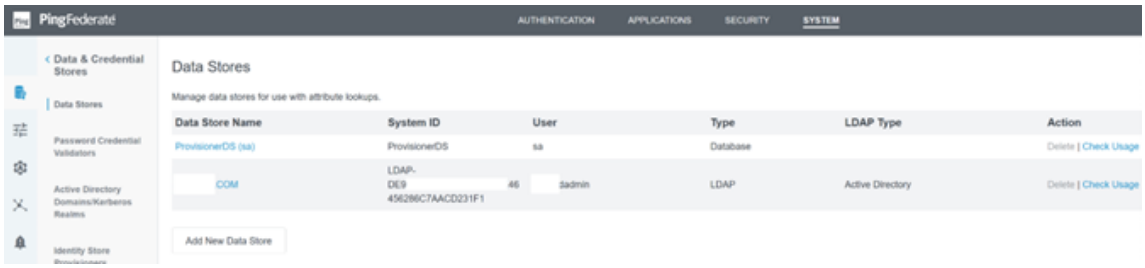
2. Sélectionnez le type **Annuaire (LDAP)**.



3. Configurez vos contrôleurs de domaine pour les connexions LDAPS et ajoutez la liste des noms de domaine complets des contrôleurs de domaine dans le champ des noms d'hôte. Cliquez ensuite sur **Tester la connexion**.

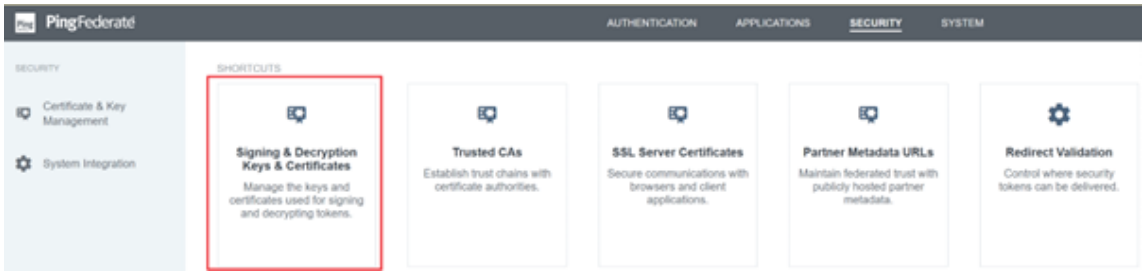


4. Une fois configurée, la connexion Active Directory devrait ressembler à l'exemple suivant :



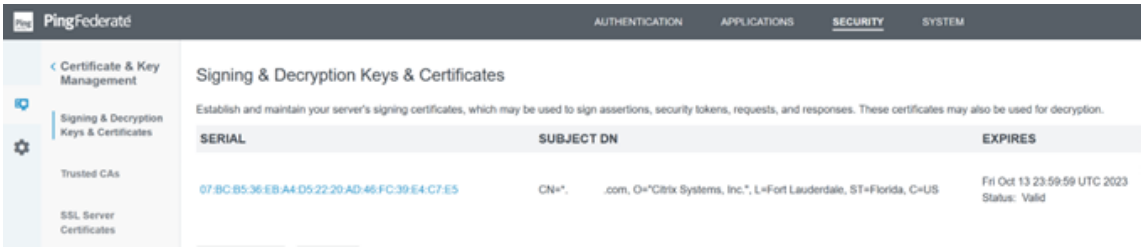
Charger le certificat de signature SAML Citrix Cloud

1. Cliquez sur l'onglet **Sécurité**
2. Chargez le certificat de signature SAML que vous souhaitez que PingFederate utilise dans les **clés et certificats de signature et de décryptage**.

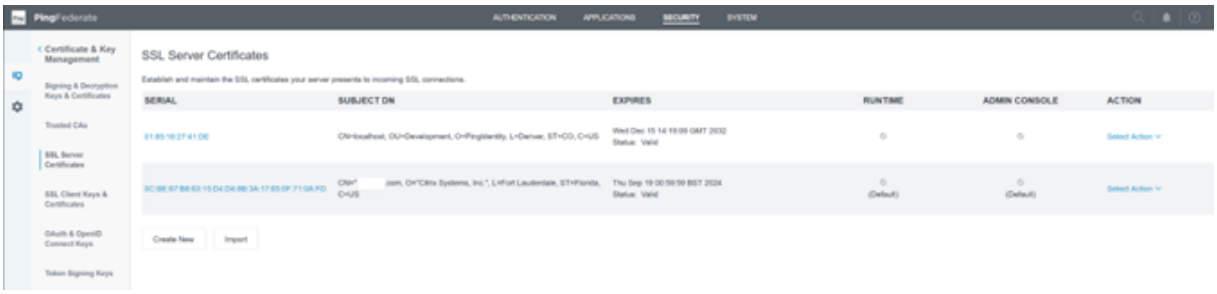


> **Remarque :**
>
> Le certificat utilisé est un certificat Digicert `pingfederateserver.domain.com` signé publiquement dans cet exemple.

3. Chargez tous les certificats CA utilisés pour signer le certificat de signature SAML de votre serveur PingFederate.



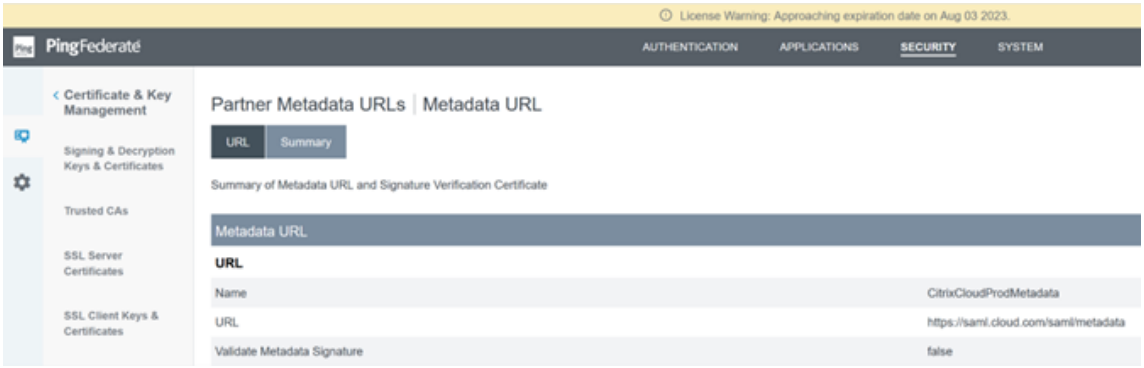
> **Remarque :**
>
> Le certificat de serveur PingFederate et le certificat de signature SAML peuvent être identiques ou vous pouvez utiliser des certificats SSL différents. Vous devez fournir une copie du certificat de signature SAML à Citrix Cloud lorsque vous configurez la connexion SAML.



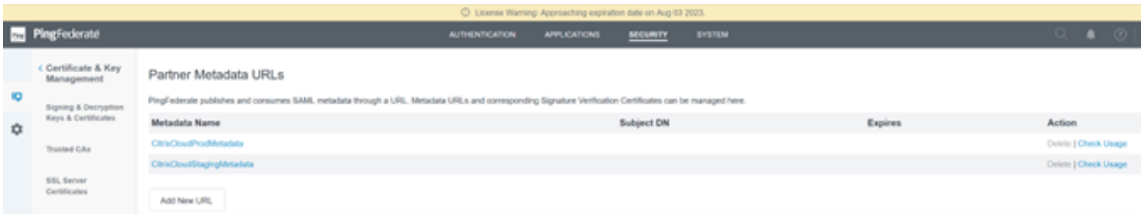
Charger les métadonnées Citrix Cloud

1. Donnez un nom aux métadonnées Citrix Cloud et entrez l'URL des métadonnées correspondant à la région Citrix Cloud dans laquelle se trouve votre locataire Citrix Cloud.

   - https://saml.cloud.com/saml/metadata - Régions commerciales d'Europe, des États-Unis et de l'Asie-Pacifique Sud
   - https://saml.citrixcloud.jp/saml/metadata - Japon
   - https://saml.cloud.us/saml/metadata - Gouvernement



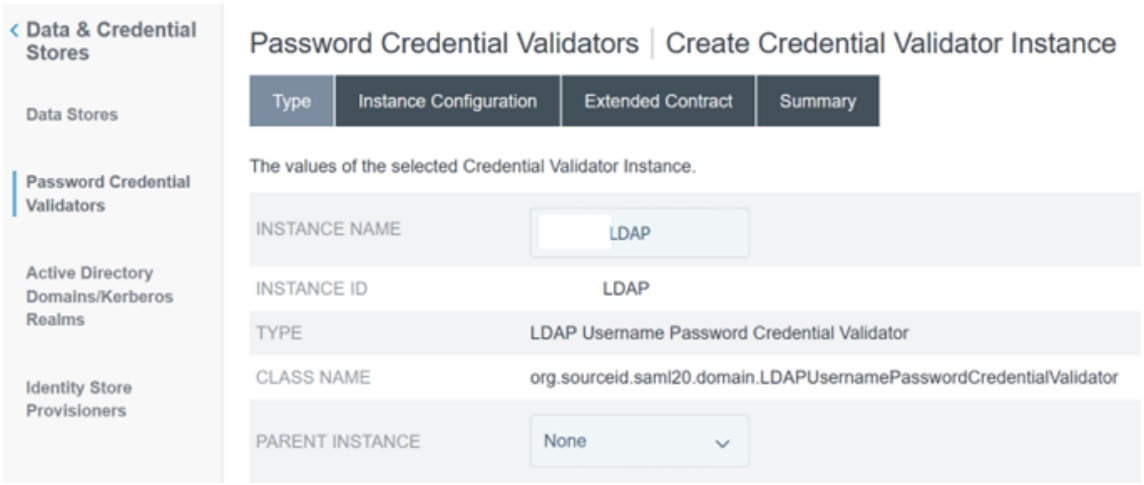
2. Une fois configurée, la configuration des métadonnées de Citrix Cloud doit ressembler à l'exemple suivant.



Configurer un validateur de mot de passe dans PingFederate

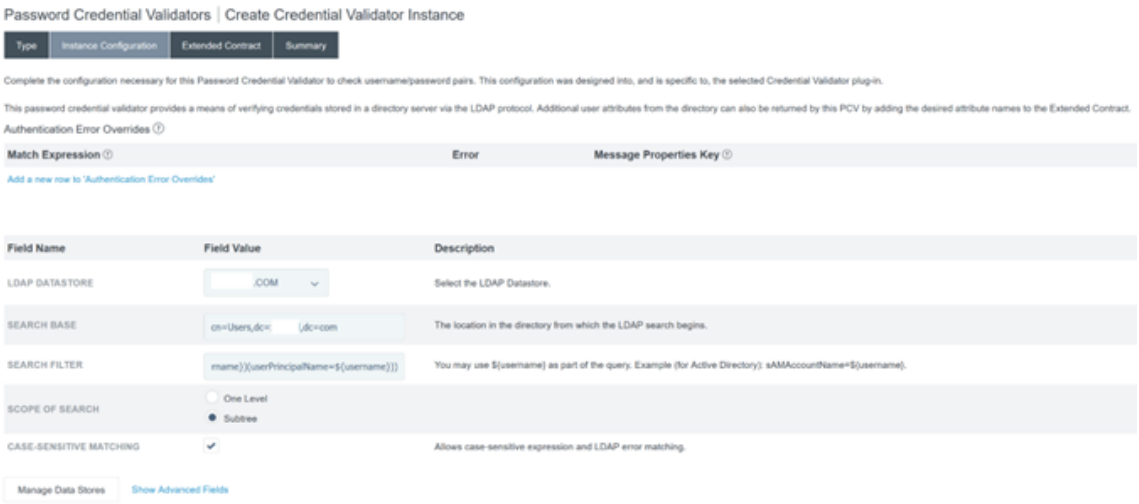
Pour plus d'informations, consultez la section Validateur de mot de passe PingFederate

1. Configurez le type de validateur de mot de passe comme nom d'utilisateur et mot de passe LDAP.



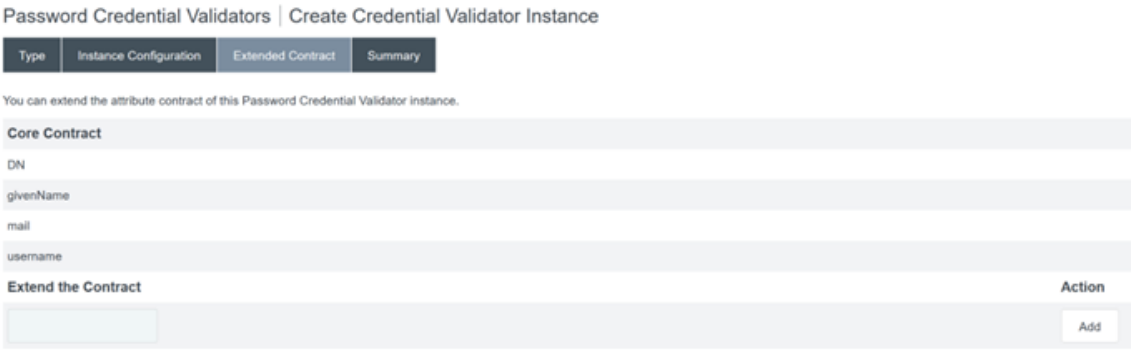
2. Configurez la **configuration d'instance**. Sélectionnez la connexion au domaine AD et le magasin de données que vous avez configurés précédemment. Configurez une connexion Active Directory à votre domaine AD à l'aide d'un magasin de données dans PingFederate Entrez un filtre LDAP approprié comme indiqué dans l'exemple.


```
(((sAMAccountName=${ username } )(userPrincipalName=${ username }
 ))
```

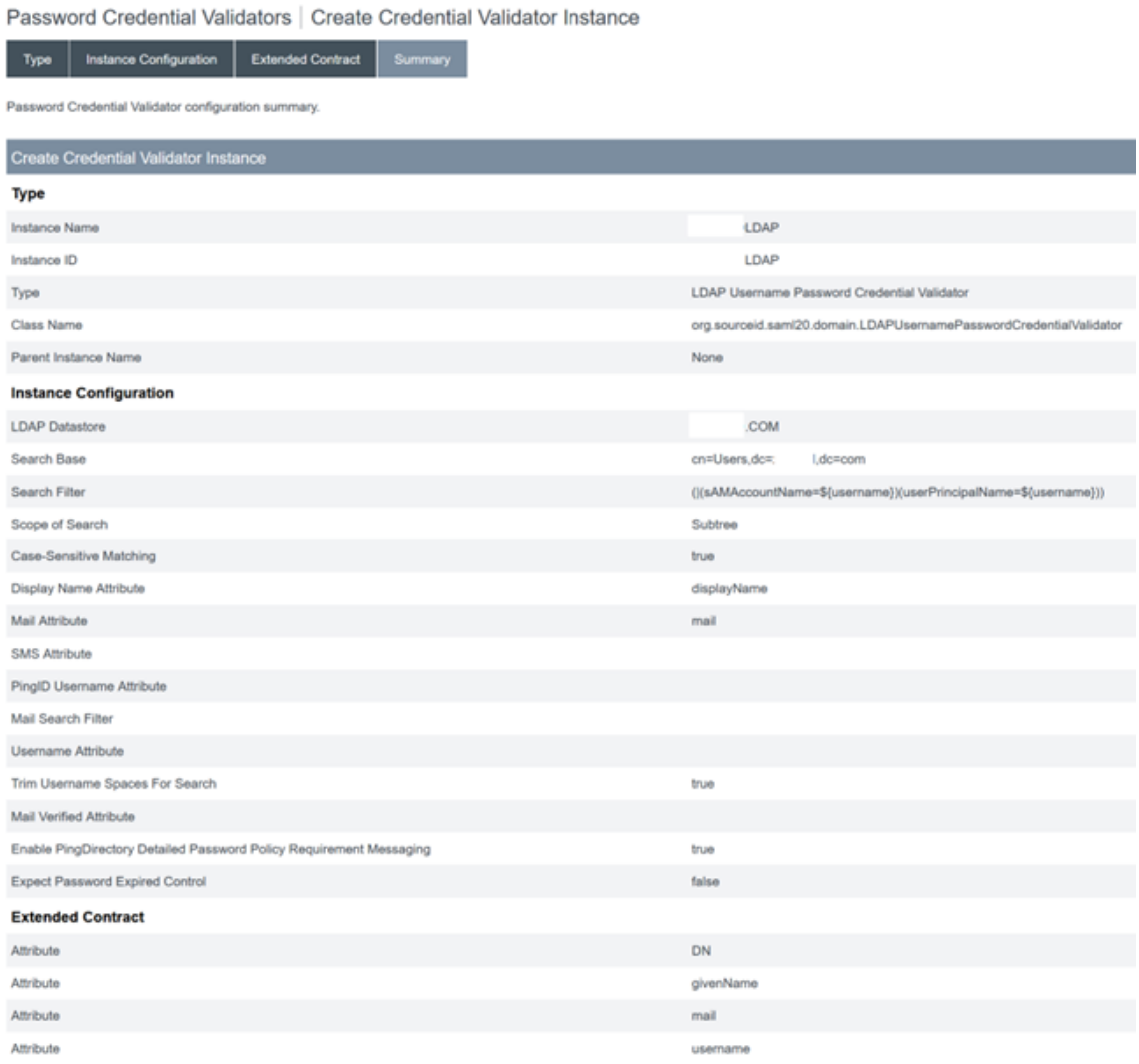


> **Remarque :** l'exemple de filtre correspond aux formats de nom d'utilisateur AD sAMAccountName et userPrincipalName, ce qui permet aux utilisateurs finaux de se connecter à Workspace ou Citrix Cloud avec l'un ou l'autre de ces formats. L'exemple de filtre prend en charge les formats de nom d'utilisateur AD sAMAccountName et userPrincipalName, qui permettent aux utilisateurs finaux de se connecter à Workspace ou Citrix Cloud à l'aide de l'un de ces formats.

3. Configurez le **contrat prolongé**.



4. Le résumé du **validateur de mot de passe** doit ressembler à cet exemple.



Password Credential Validators | Create Credential Validator Instance

Type | Instance Configuration | Extended Contract | Summary

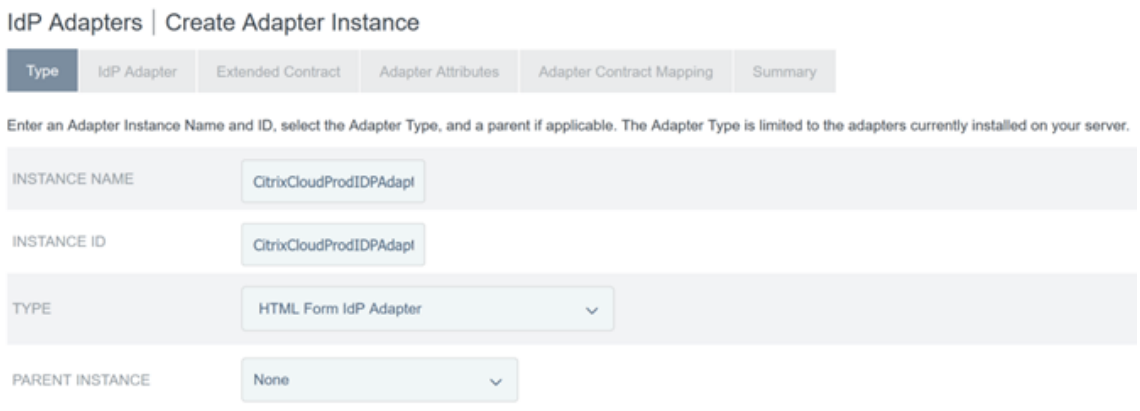
Password Credential Validator configuration summary.

Create Credential Validator Instance	
Type	
Instance Name	LDAP
Instance ID	LDAP
Type	LDAP Username Password Credential Validator
Class Name	org.sourceid.saml20.domain.LDAPUsernamePasswordCredentialValidator
Parent Instance Name	None
Instance Configuration	
LDAP Datastore	.COM
Search Base	cn=Users,dc= l,dc=com
Search Filter	(|(sAMAccountName=${username})(userPrincipalName=${username}))
Scope of Search	Subtree
Case-Sensitive Matching	true
Display Name Attribute	displayName
Mail Attribute	mail
SMS Attribute	
PingID Username Attribute	
Mail Search Filter	
Username Attribute	
Trim Username Spaces For Search	true
Mail Verified Attribute	
Enable PingDirectory Detailed Password Policy Requirement Messaging	true
Expect Password Expired Control	false
Extended Contract	
Attribute	DN
Attribute	givenName
Attribute	mail
Attribute	username

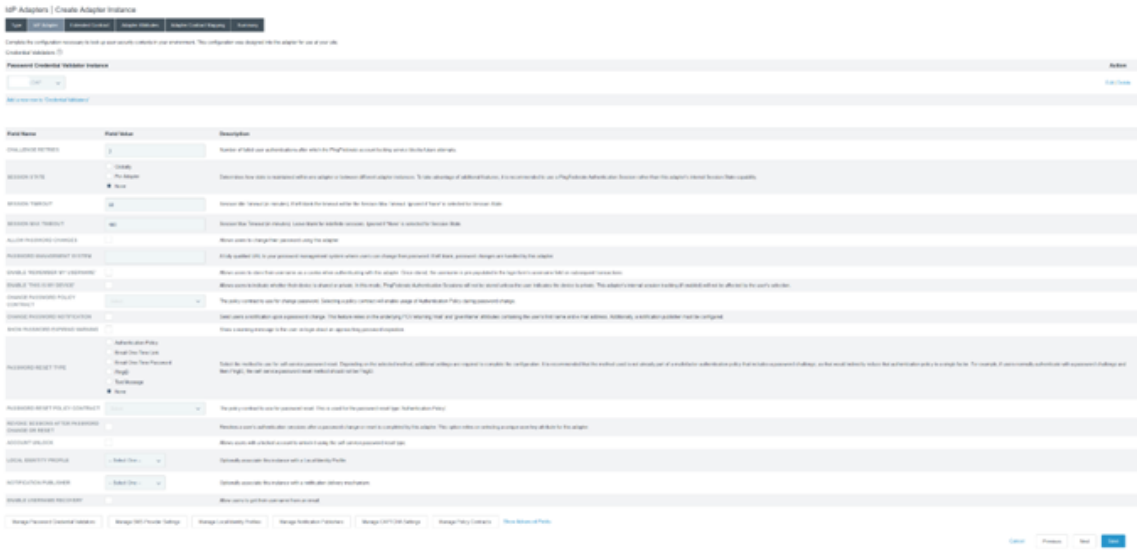
Configurer l'adaptateur IDP dans PingFederate

Pour plus d'informations, consultez la section Adaptateur de formulaire HTML PingFederate

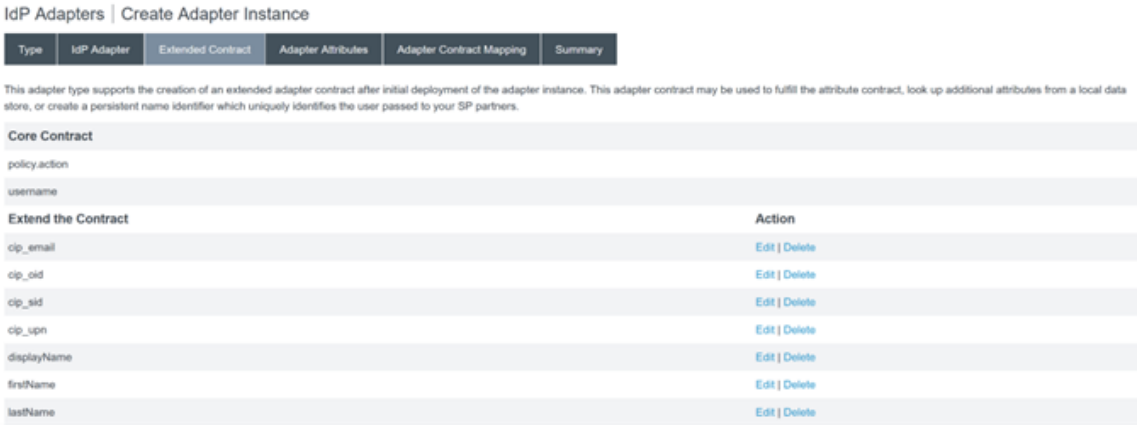
1. Créez un adaptateur IDP de type Adapteur IDP de formulaire HTML.



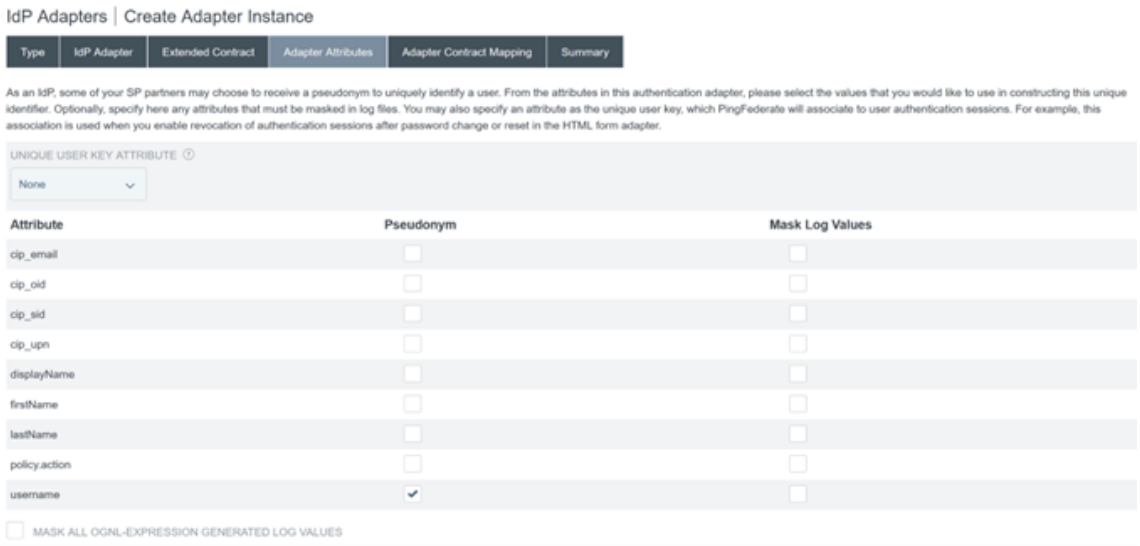
2. Sélectionnez le **validateur de mot de passe** que vous avez configuré précédemment et configurez l'adaptateur IDP. Pour plus d'informations, consultez Configurer un validateur de mot de passe dans PingFederate.



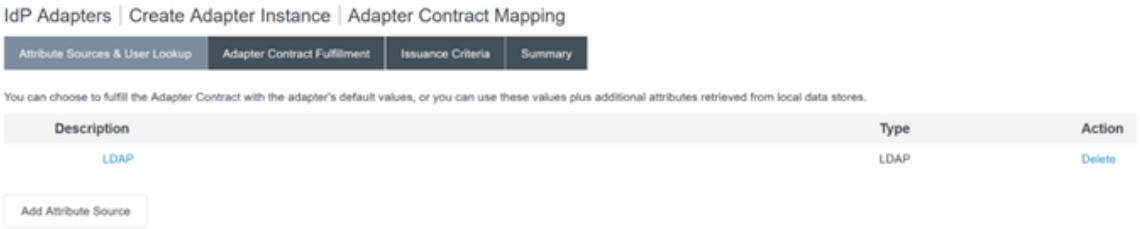
3. Configurez le **contrat prolongé** avec des attributs SAML transmis à Citrix Cloud ou Workspace lors de l'ouverture de session SAML.



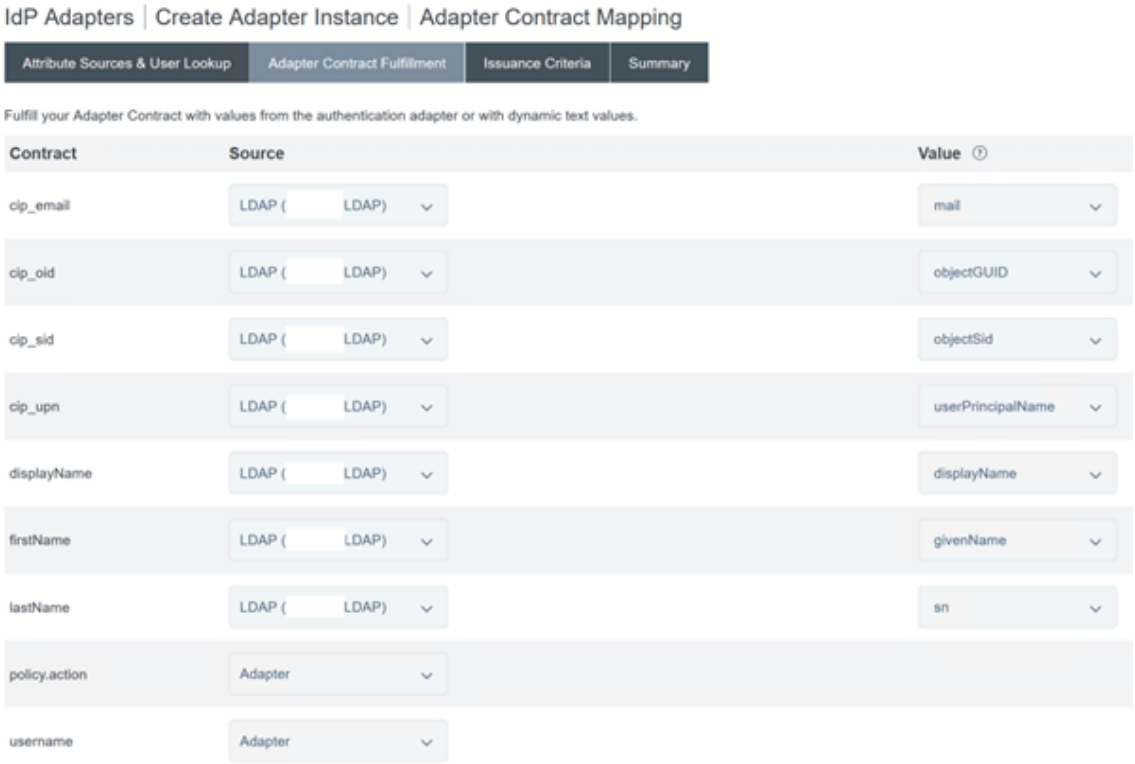
4. Configurez les **attributs d'un adaptateur**.



5. Configurez le **mappage des contrats d'adaptateur** où les attributs SAML sont mappés aux attributs utilisateur LDAP à partir d'identités AD. Cliquez sur **Configurer le contrat d'adaptateur**.
6. Configurez les **sources d'attributs et la recherche d'utilisateurs**.



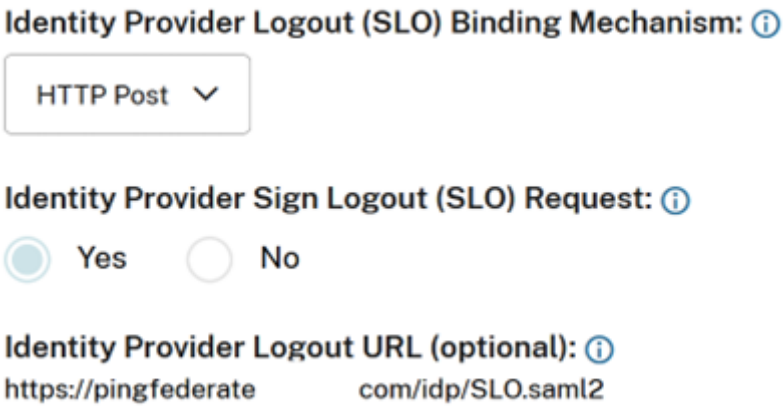
7. Configurez l'**exécution des contrats d'adaptateur**. Sélectionnez **LDAP** et le nom de votre magasin de données Active Directory comme source des données d'attributs utilisateur. La valeur est l'attribut Active Directory de l'utilisateur, par exemple, `objectGUID` ou `objectSid`.



Configuration de la connexion au fournisseur de services (application SAML) pour Citrix Cloud ou Workspace

L'exemple de configuration de PingFederate fourni ci-dessous suppose les exigences d'authentification SAML suivantes au sein de votre organisation.

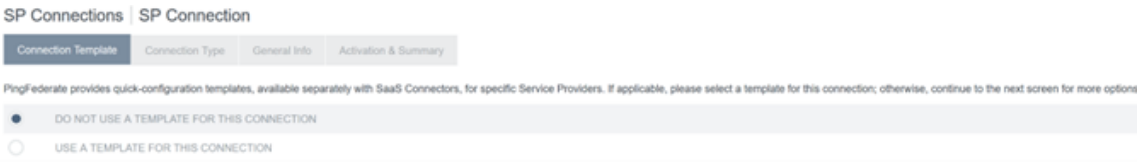
- Les demandes d'authentification SAML envoyées depuis la console d'administration Workspace/Citrix Cloud DOIVENT être signées.
- Les liaisons HTTP POST SAML seront utilisées pour les requêtes SSO et SLO.
- La déconnexion unique (SLO) est une exigence au sein de votre organisation. Lorsqu'un utilisateur final se déconnecte de Workspace ou de la console d'administration Citrix Cloud, une demande SLO SAML est envoyée par Citrix Cloud au fournisseur SAML (fournisseur d'identité) pour déconnecter l'utilisateur.
- PingFederate nécessite des requêtes HTTP POST signées pour démarrer la déconnexion. Le fournisseur SAML nécessite des requêtes SLO signées.



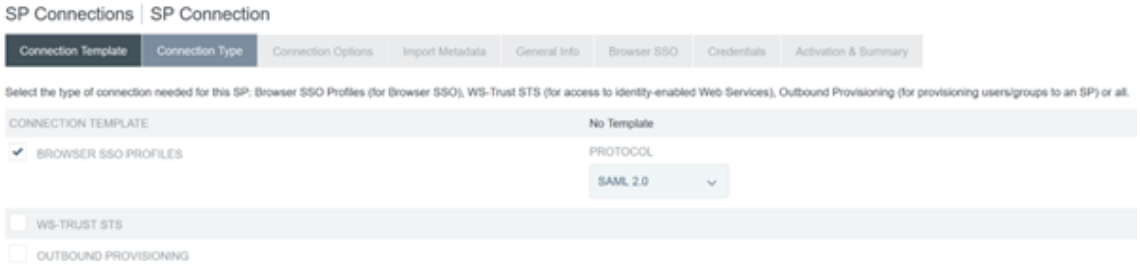
Pour plus d'informations, consultez Gestion des fournisseurs de services PingFederate

Procédure

1. Configurez le **modèle de connexion**.

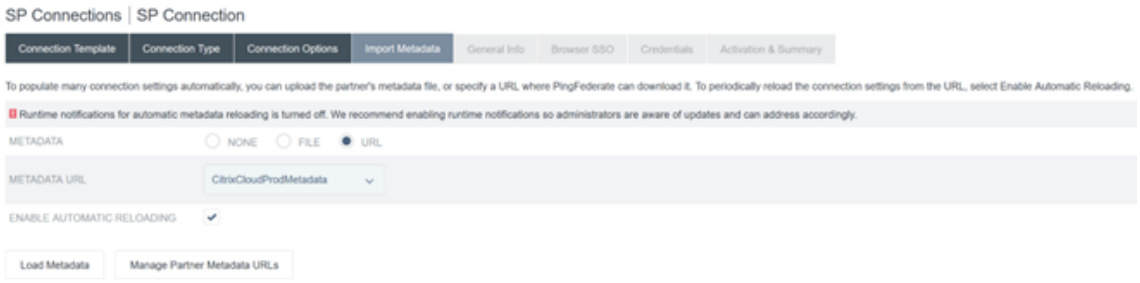


2. Configurez le **type de connexion** et sélectionnez **Profils d'authentification unique du navigateur et SAML 2.0.**



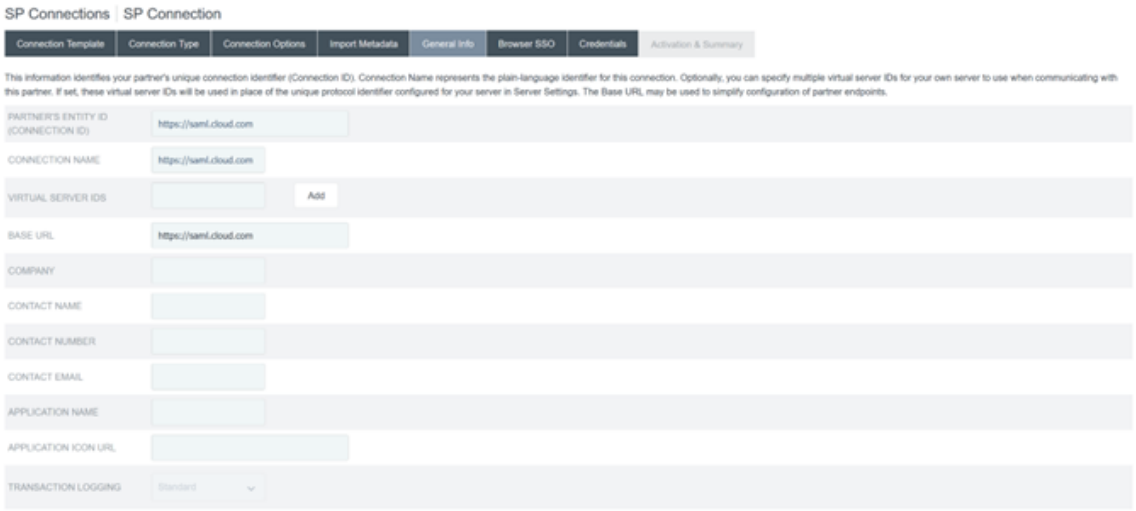
3. Configurez les **options de connexion**.

4. Importez les métadonnées Citrix Cloud. Sélectionnez l'URL et l'URL `CitrixCloudProdMetadata` que vous avez créée précédemment, puis cliquez sur **Charger les métadonnées**

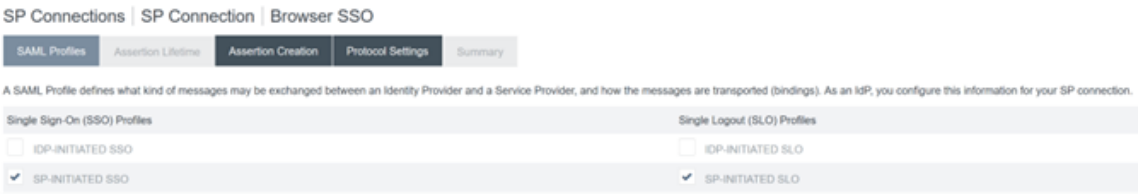


5. Configurez les **informations générales**. Définissez l'ID de l'entité de connexion du fournisseur de services, l'URL de base et le nom de connexion sur le point de terminaison Citrix Cloud SAML pour votre région client Citrix Cloud.

    - https://saml.cloud.com - Régions commerciales d'Europe, des États-Unis et de l'Asie-Pacifique Sud
    - https://saml.citrixcloud.jp - Japon
    - https://saml.cloud.us - Gouvernement



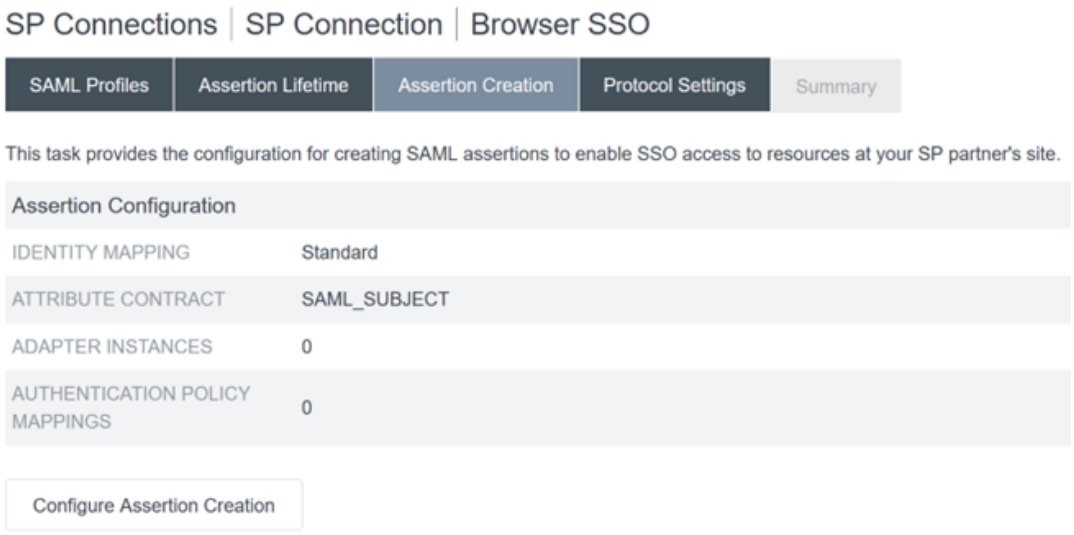
6. Configurez les **paramètres du protocole**.



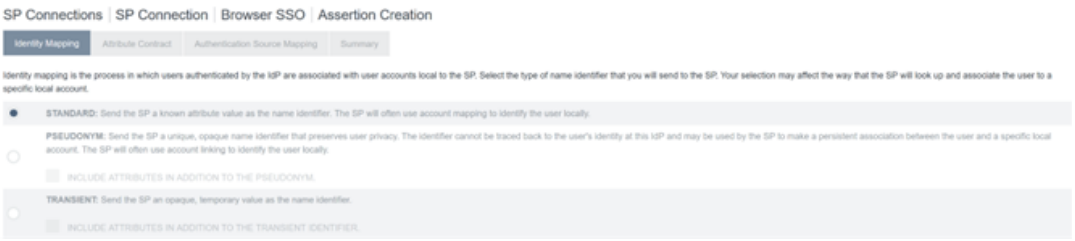
7. Utilisez les paramètres de **durée de vie des assertions** par défaut.

8. Configurez la création d'assertions SAML.

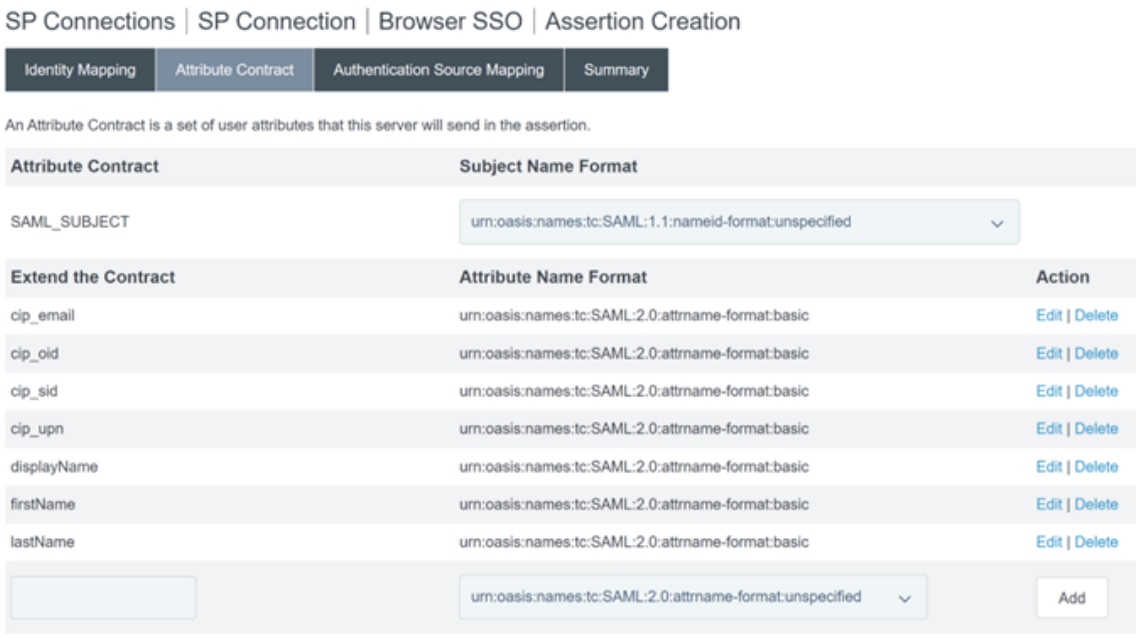
   a) Cliquez sur **Configurer la création d'assertions**



   b) Sélectionnez **Standard**.

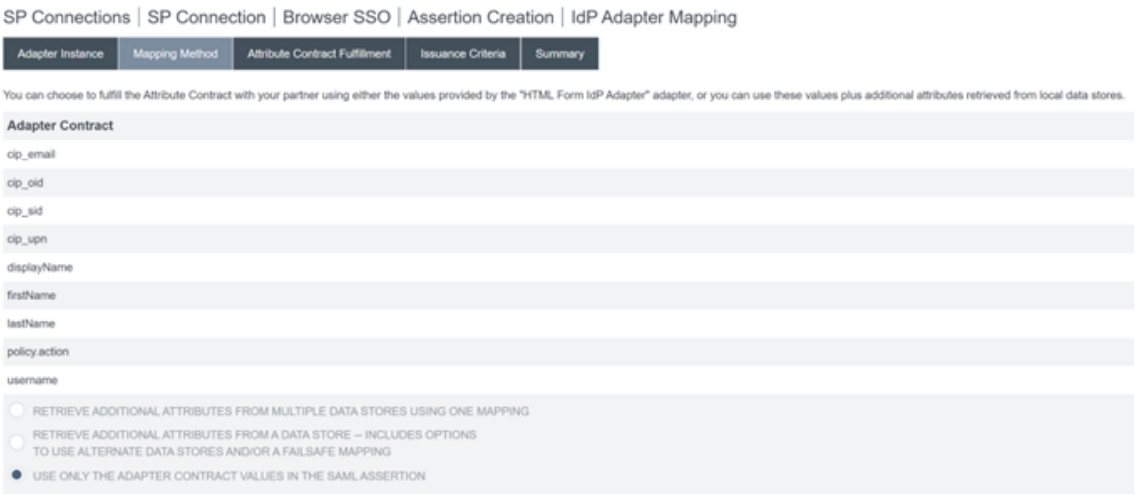


9. Configurez le **contrat d'attribut**.

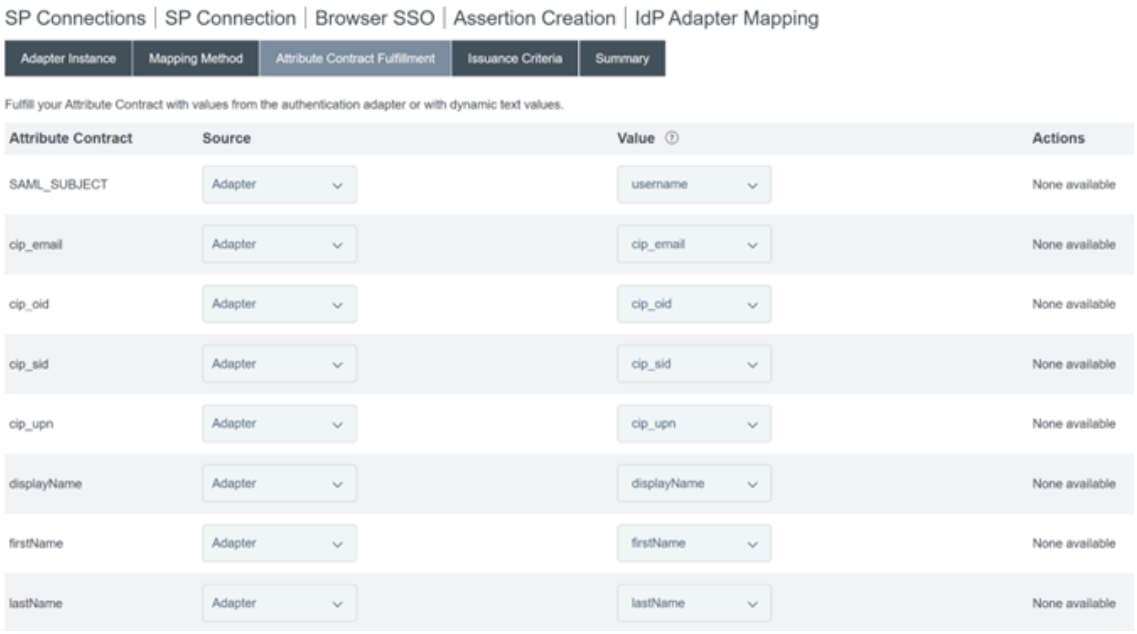


10. Configurez l'**instance d'adaptateur**.

11. Configurez la **méthode de mappage**.



12. Configurez l'**exécution des contrats d'attribut**.

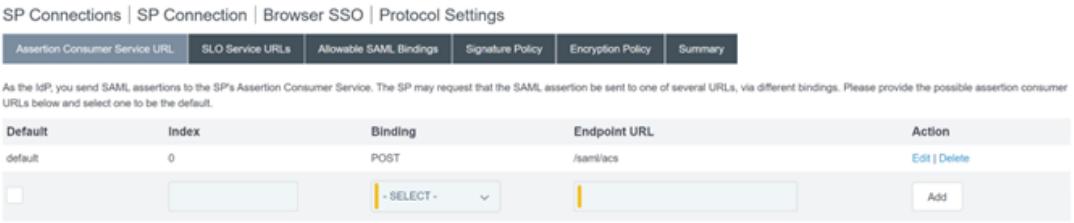


13. Configurez les **critères d'émission de certificats** en tant que valeurs par défaut, sans aucune condition.

14. Le **mappage d'adaptateur IDP** terminé apparaît comme suit :
15. Configurez les **paramètres du protocole**. Les chemins SAML requis par Citrix Cloud seront ajoutés à l'URL de base de votre serveur PingFederate. Il est possible de remplacer l'URL de

base en saisissant un chemin complet dans le champ URL du point de terminaison, mais cela est généralement inutile et non souhaitable.
URL de base - https://youpingfederateserver.domain.com

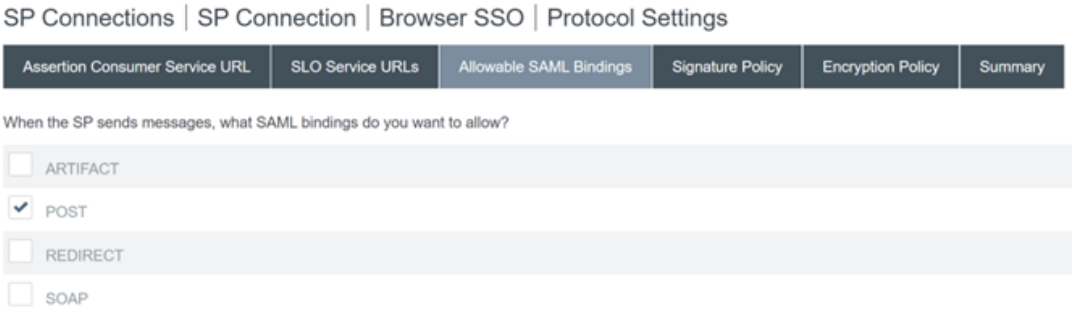
a) Configurez l'URL ACS qui ajoute le chemin SAML à l'URL de base du serveur PingFederate. URL du point de terminaison - /saml/acs



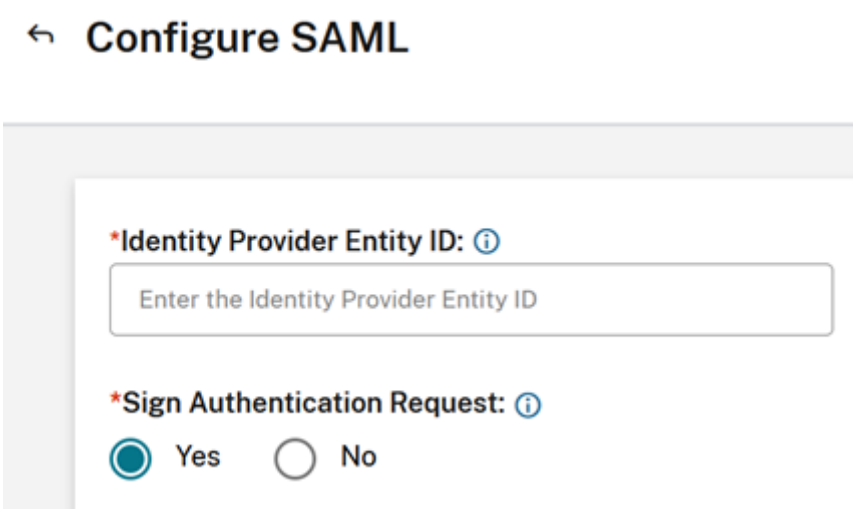
b) Configurez l'**URL du service SLO**. URL du point de terminaison - /saml/logout/callback

> **Important :**
>
> La connexion SAML Citrix Cloud nécessite la configuration d'une URL de déconnexion PingFederate correspondante si vous souhaitez effectuer une SLO lorsque vous vous déconnectez de Workspace ou de Citrix Cloud. Si vous ne configurez pas l'URL de déconnexion dans votre connexion SAML, les utilisateurs finaux se déconnecteront simplement de Workspace, mais pas de PingFederate.

a) Configurez les **liaisons SAML autorisées**.

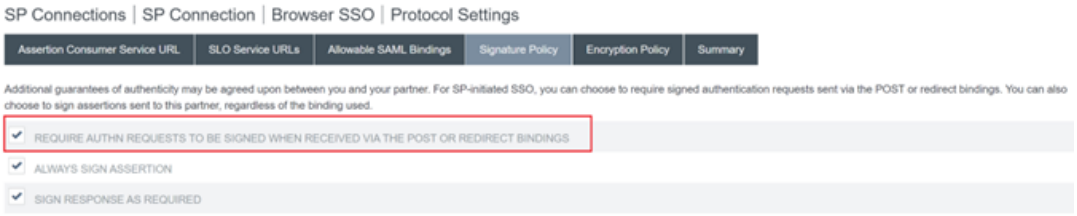


b) Configurez la **stratégie de signature**.

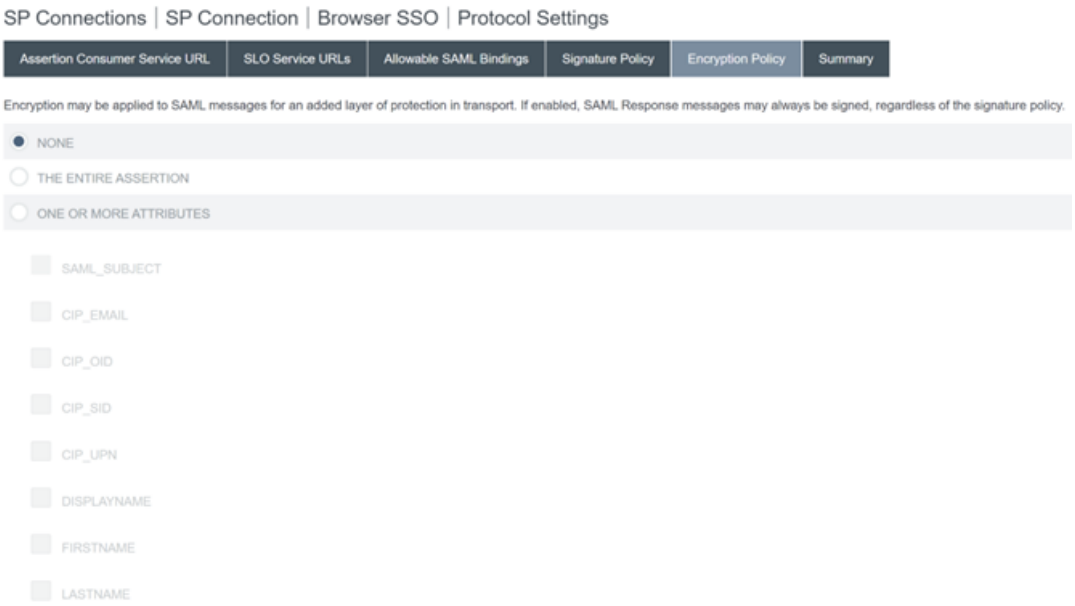


> **Important :**
>
> Les paramètres de signature SAML doivent être configurés de manière cohérente des deux côtés de la connexion SAML. Workspace ou Citrix Cloud (SP) doivent être configurés pour envoyer des demandes SSO et SLO signées.

a) PingFederate (IDP) doit être configuré pour appliquer les demandes signées à l'aide du certificat de vérification de signature SAML de Citrix Cloud.

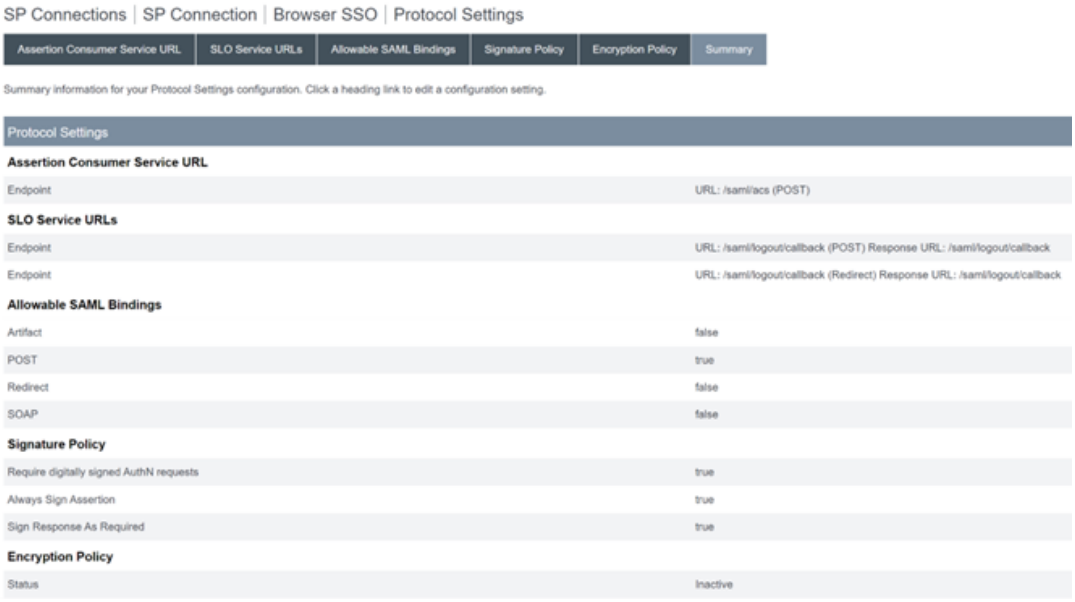


b) Configurez la **stratégie de cryptage**.

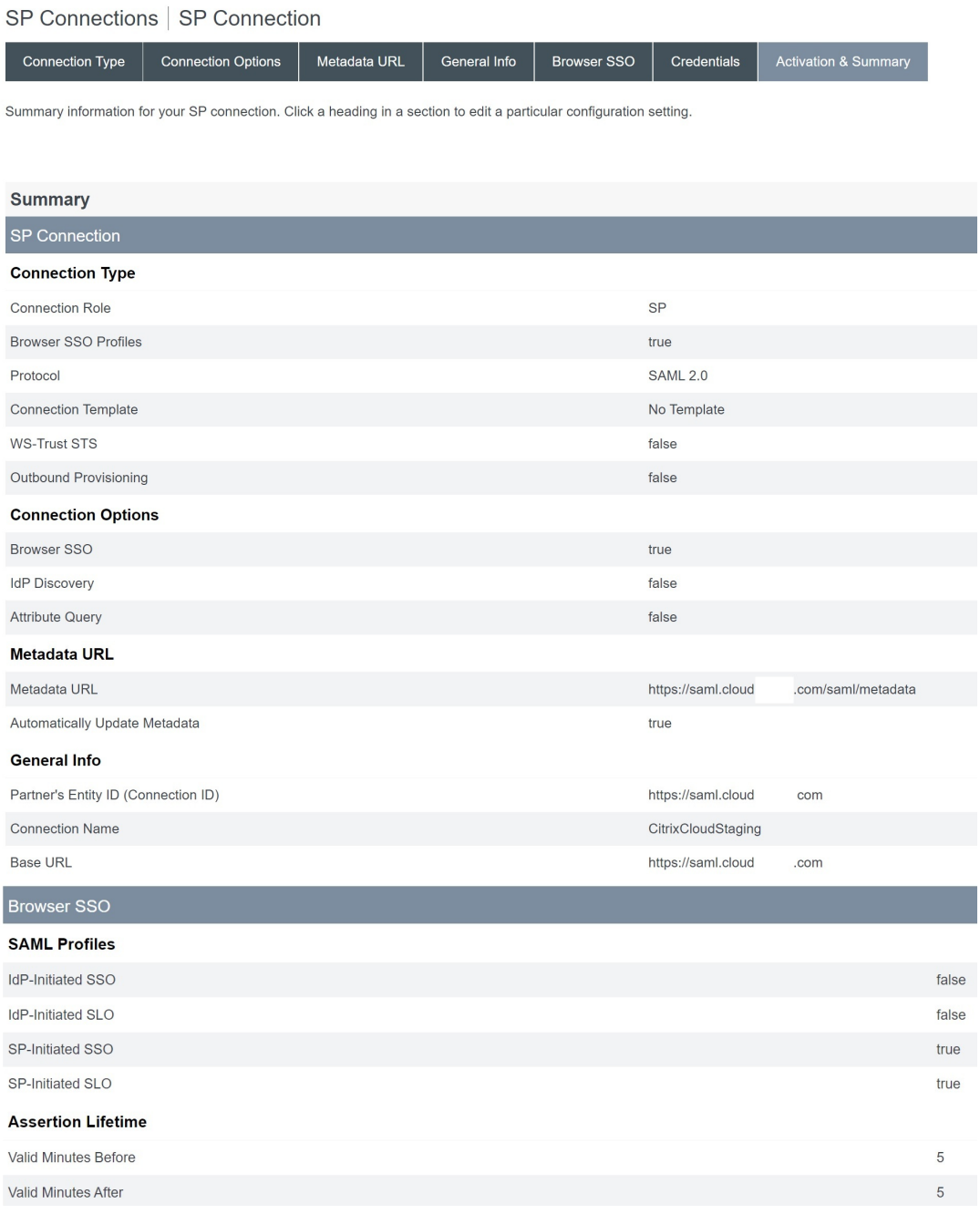


> **Remarque :**
>
> Il est recommandé de définir le cryptage sur **AUCUN** lors de la configuration initiale et les tests afin de pouvoir déboguer tout problème lié à des attributs SAML manquants ou incorrects dans l'assertion. Si vous avez besoin d'assertions cryptées, il est recommandé d'activer le cryptage après avoir prouvé que la connexion à Workspace ou à Citrix Cloud est réussie et que toutes les ressources ont été correctement énumérées et peuvent être lancées. Le débogage des problèmes avec SAML lorsque le cryptage est activé sera impossible si vous ne pouvez pas afficher le contenu en texte brut de l'assertion SAML.

c) Consultez l'onglet **Résumé**.



d) Vérifiez la **connexion au fournisseur de services Citrix Cloud**. Une fois la **connexion au fournisseur de services Citrix Cloud** configurée, elle devrait ressembler à cet exemple :



SP Connections | SP Connection

Connection Type | Connection Options | Metadata URL | General Info | Browser SSO | Credentials | Activation & Summary

Summary information for your SP connection. Click a heading in a section to edit a particular configuration setting.

Summary

SP Connection	
Connection Type	
Connection Role	SP
Browser SSO Profiles	true
Protocol	SAML 2.0
Connection Template	No Template
WS-Trust STS	false
Outbound Provisioning	false
Connection Options	
Browser SSO	true
IdP Discovery	false
Attribute Query	false
Metadata URL	
Metadata URL	https://saml.cloud .com/saml/metadata
Automatically Update Metadata	true
General Info	
Partner's Entity ID (Connection ID)	https://saml.cloud com
Connection Name	CitrixCloudStaging
Base URL	https://saml.cloud .com

Browser SSO	
SAML Profiles	
IdP-Initiated SSO	false
IdP-Initiated SLO	false
SP-Initiated SSO	true
SP-Initiated SLO	true
Assertion Lifetime	
Valid Minutes Before	5
Valid Minutes After	5

Assertion Creation	
Identity Mapping	
Enable Standard Identifier	true
Attribute Contract	
Attribute	SAML_SUBJECT
Subject Name Format	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
Attribute	cip_email
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Attribute	cip_oid
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Attribute	cip_sid
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Attribute	cip_upn
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Attribute	displayName
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Attribute	firstName
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Attribute	lastName
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Authentication Source Mapping	
Adapter instance name	CitrixCloudStagingIDPAdaptor
Adapter Instance	
Selected adapter	CitrixCloudStagingIDPAdaptor
Mapping Method	
Adapter	HTML Form IdP Adapter
Mapping Method	Use only the Adapter Contract values in the mapping
Attribute Contract Fulfillment	
SAML_SUBJECT	username (Adapter)
cip_email	cip_email (Adapter)
cip_oid	cip_oid (Adapter)
cip_sid	cip_sid (Adapter)
cip_upn	cip_upn (Adapter)
displayName	displayName (Adapter)
firstName	firstName (Adapter)
lastName	lastName (Adapter)
Issuance Criteria	
Criterion	(None)

Protocol Settings	
Assertion Consumer Service URL	
Endpoint	URL: /saml/acs (POST)
SLO Service URLs	
Endpoint	URL: /saml/logout/callback (POST) Response URL: /saml/logout/callback
Endpoint	URL: /saml/logout/callback (Redirect) Response URL: /saml/logout/callback
Allowable SAML Bindings	
Artifact	false
POST	true
Redirect	false
SOAP	false
Signature Policy	
Require digitally signed AuthN requests	true
Always Sign Assertion	true
Sign Response As Required	true
Encryption Policy	
Status	Inactive

Credentials	
Digital Signature Settings	
Selected Certificate	CN=*. .com, O="Citrix Systems, Inc.", L=Fort Lauderdale, ST=Florida, C=US (0C:BE:67:B8:63:15:D4:D4:8B:3A:17:65:0F:71:0A:FD | Exp: Sep 19, 2024)
Include Certificate in KeyInfo	false
Selected Signing Algorithm	RSA SHA256

Signature Verification	
Trust Model	
Trust Model	Unanchored
Signature Verification Certificate	
Active Certificate 1	CN=samlsigning.cloud .com, O="Citrix Systems, Inc.", L=Fort Lauderdale, ST=Florida, C=US (03:48:4A:61:BF:59:EB:13:9C:20:FE:F1:5B:3A:83:29 | Exp: May 11, 2024)
Active Certificate 2	CN=samlsigning.cloud .com, O="Citrix Systems, Inc.", L=Fort Lauderdale, ST=Florida, C=US (0B:5F:B5:43:89:16:B0:2F:98:45:58:D1:DA:D1:B1:1D | Exp: Mar 11, 2025)

> **Conseil utile :**
>
> Utilisez la page Activation et résumé de la connexion au fournisseur de services pour passer en revue votre application SAML et à des fins de débogage, car elle permet d'apporter des modifications de configuration rapides et faciles. La page Activation et résumé de la connexion au fournisseur de services vous permet d'accéder à l'une des sous-sections de configuration SAML en cliquant sur le titre de cette section. Cliquez sur l'un des titres surlignés en rouge pour mettre à jour ces paramètres.

Protocol Settings	
Assertion Consumer Service URL	
Endpoint	URL: /saml/acs (POST)
SLO Service URLs	
Endpoint	URL: /saml/logout/callback (POST)
Allowable SAML Bindings	
Artifact	false
POST	true
Redirect	true
SOAP	false
Signature Policy	
Require digitally signed AuthN requests	false
Always Sign Assertion	true
Sign Response As Required	true

16. La **connexion au fournisseur de services Citrix Cloud** terminée devrait apparaître dans la liste comme suit.

17. Il est possible d'exporter la connexion au fournisseur de services sous la forme d'un fichier XML. Citrix recommande d'effectuer une sauvegarde de votre connexion au fournisseur de services une fois que vous l'avez testée avec Citrix Cloud et Workspace.

Mettre à jour le certificat de signature SAML du fournisseur d'identité

May 31, 2024

Author:
Mark Dear

Les connexions SAML qui utilisent des demandes et des réponses signées dépendent de deux certificats de signature SAML différents. Un pour chaque côté de la connexion SAML.

Certificat de signature du fournisseur SAML

Ce certificat est fourni par votre fournisseur SAML et chargé dans Citrix Cloud lorsque vous configurez la connexion SAML.

Les certificats de signature SAML doivent faire l'objet d'une rotation avant leur date d'expiration afin de donner aux administrateurs de Citrix Cloud le temps de préparer le déploiement. La rotation des certificats est requise à la fois par les fournisseurs de services et les fournisseurs d'identité afin de garantir l'alignement et d'éviter tout temps d'arrêt.

Questions fréquentes

À quoi sert le certificat du fournisseur SAML ?

Le certificat du fournisseur SAML est utilisé pour vérifier la signature des réponses SAML envoyées par le fournisseur SAML à Citrix Cloud lors du processus d'authentification.

Où puis-je obtenir une copie du dernier certificat de signature du fournisseur d'identité ?

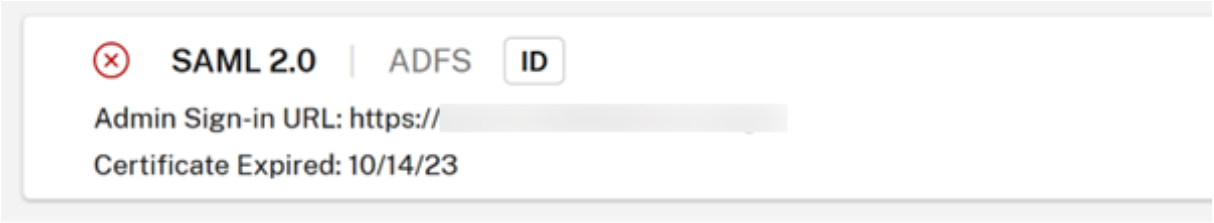
Ce certificat est fourni par votre fournisseur SAML tel qu'Azure AD, Okta, PingFederate ou ADFS. Citrix ne contrôle pas la rotation ni la mise à jour de ce certificat. Ce certificat est chargé dans Citrix Cloud lors de la création initiale de la connexion SAML. La date d'expiration des **certificats de signature du fournisseur d'identité** est généralement longue. Il peut être nécessaire de les remplacer après quelques années et à une fréquence inférieure à celle du **certificat de signature du fournisseur de services**

Comment savoir si mon certificat de signature du fournisseur SAML est sur le point d'expirer et si cela a un impact sur ma connexion SAML Citrix Cloud ?

Citrix Cloud affichera des avertissements 30 jours avant l'approche de la date d'expiration de votre certificat de signature du fournisseur SAML.

```
Certificate Expiring Soon: <certExpirationDate>
```

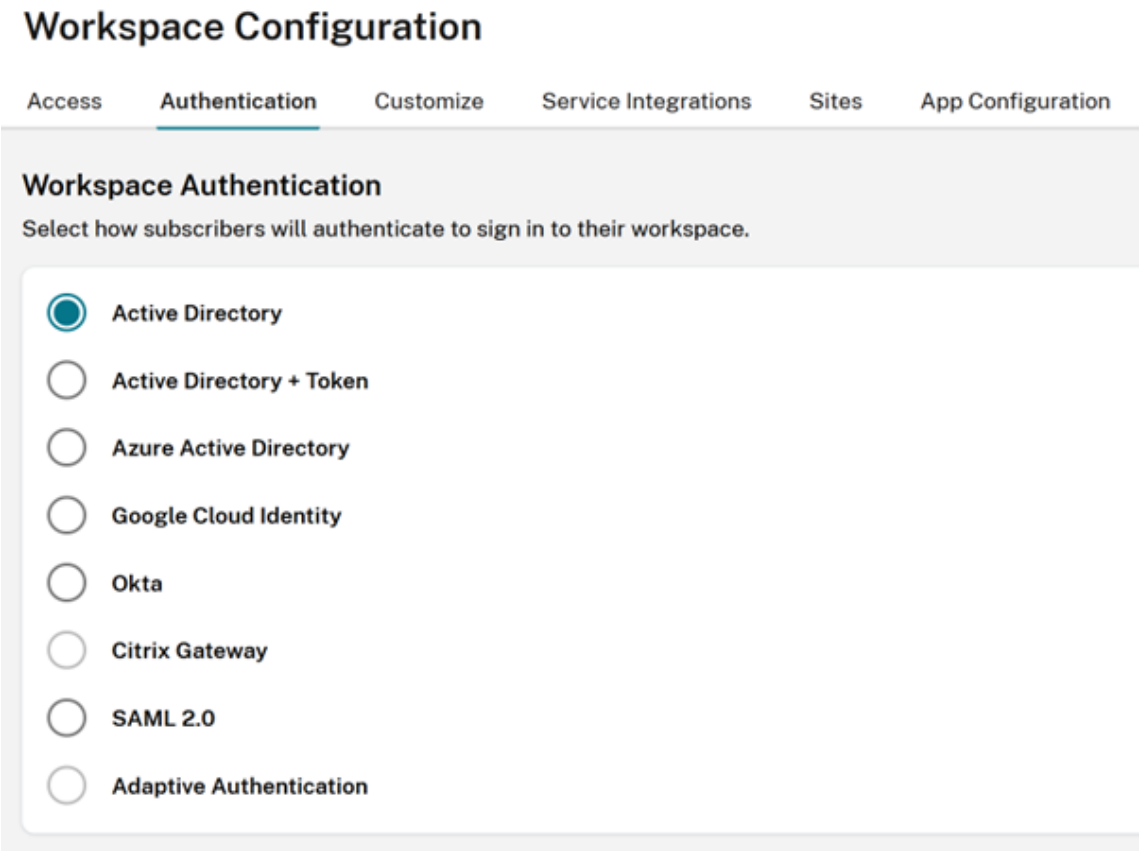
Une erreur s'affichera également une fois que le certificat aura effectivement expiré, comme indiqué ci-dessous.



Puis-je mettre à jour le certificat du fournisseur SAML tout en utilisant la connexion SAML sans temps d'arrêt ?

Non. Il est nécessaire d'effectuer une déconnexion et une reconnexion SAML pendant une fenêtre de maintenance planifiée.
Mettre à jour le certificat de signature du fournisseur d'identité

1. Sélectionnez un autre fournisseur d'identité dans **Configuration de l'espace de travail**, puis sélectionnez **Authentification** pendant que vous effectuez l'opération de déconnexion/reconnexion SAML, telle qu'Active Directory.



2. Sauvegardez votre URL GO existante, telle que celle utilisée pour la connexion SAML à Citrix Cloud : `https://citrix.cloud.com/go/<yourgourl>`.

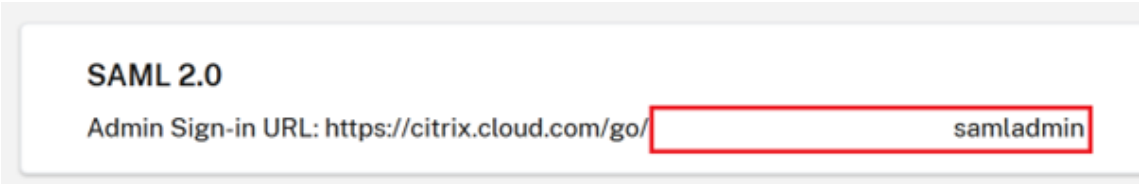
3. Effectuez une sauvegarde de vos points de terminaison SAML existants. Vous pouvez les copier depuis la console Citrix Cloud. Sauvegardez les points de terminaison SAML suivants depuis votre connexion SAML existante.

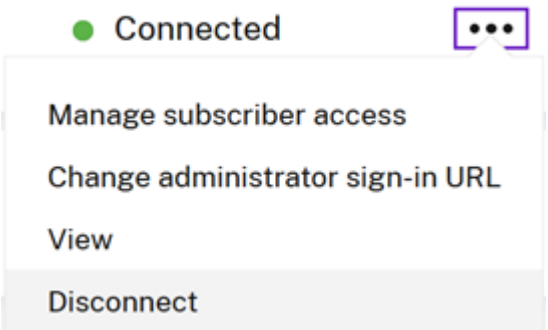
    - ID d'entité du fournisseur d'identité
    - URL du service SSO du fournisseur d'identité
    - URL de déconnexion du fournisseur d'identité

    Sauvegardez l'EntityID, l'URL SSO et l'URL de déconnexion.

> **Important :**
>
> Assurez-vous de disposer d'une copie du certificat de signature du fournisseur d'identité existant et du certificat de signature du fournisseur d'identité de remplacement avant de procéder à la déconnexion. Cela vous permet de revenir à l'ancien certificat si le nouveau certificat du fournisseur SAML n'est pas valide et entraîne des problèmes de connexion. Vous ne pourrez pas obtenir de copie de l'ancien certificat depuis l'interface utilisateur de Citrix Cloud avant d'effectuer la déconnexion. Vous devrez l'obtenir à partir de votre application SAML.

1. Déconnectez SAML dans la **Gestion des identités et des accès**, accédez à **Authentification**, puis sélectionnez la connexion SAML. Cliquez sur l'ellipse et sélectionnez **Déconnecter**
2. Reconnectez SAML dans la **Gestion des identités et des accès**, puis cliquez sur **Authentification**





3. Acceptez tous les paramètres de connexion SAML par défaut.
4. Entrez à nouveau tous les points de terminaison de l'application SAML que vous avez sauvegardés précédemment ou récupérez-les pour votre application SAML depuis l'interface utilisateur de votre fournisseur SAML.

- ID d'entité du fournisseur d'identité
- URL du service SSO du fournisseur d'identité
- URL de déconnexion du fournisseur d'identité

> **Important :**
>
> Si vous utilisez la fonctionnalité Scoped EntityID, vous devrez également mettre à jour votre application SAML avec le nouvel ID d'étendue après avoir effectué la déconnection/reconnexion SAML. Pour plus d'informations sur la fonctionnalité Scoped EntityID, consultez Configurer une application SAML avec un ID d'entité étendue dans Citrix Cloud. Copiez l'ID d'étendue nouvellement généré depuis l'interface utilisateur SAML de Citrix Cloud et mettez à jour l'ID d'entité de votre application SAML avec l'ID d'étendue de remplacement.
> EntityID doit être défini sur `https://saml.cloud.com/<new scope ID after reconnect>`.

Mettre à jour le certificat de signature SAML du fournisseur de services

May 31, 2024

Author:
Mark Dear

Les connexions SAML qui utilisent des demandes et des réponses signées dépendent de deux certificats de signature SAML différents. Un pour chaque côté de la connexion SAML.

Certificat de signature du fournisseur de services

Ce certificat est fourni périodiquement par Citrix et chargé dans votre application SAML ou obtenu via les métadonnées SAML de Citrix Cloud.

Les certificats de signature SAML doivent faire l'objet d'une rotation avant leur date d'expiration afin de donner aux administrateurs de Citrix Cloud le temps de préparer le déploiement. La rotation des certificats est requise à la fois par les fournisseurs de services et les fournisseurs d'identité afin de garantir l'alignement et d'éviter tout temps d'arrêt.

Si un fournisseur SAML sélectionné ne prend pas en charge la rotation automatique du certificat de signature SAML de fournisseur de services, une rotation manuelle du certificat de signature SAML au sein de votre fournisseur SAML doit être effectuée afin de remplacer le certificat expirant.

> **Important :**
>
> Tous les guides existants dans cette section eDoc SAML incluent des détails sur la façon de configurer la signature des deux côtés de la connexion SAML. Citrix recommande uniquement les configurations SAML signées, car elles sont plus sécurisées et sont requises par certains fournisseurs SAML pour que la déconnexion (SLO) réussisse.

Questions fréquentes

Qu'est-ce que la signature SAML ?

Les certificats de signature SAML sont des certificats X.509 utilisés pour vérifier les données envoyées entre le fournisseur de services et le fournisseur SAML (fournisseur d'identité). Votre fournisseur SAML (fournisseur d'identité) utilise le certificat de signature SAML Citrix Cloud pour vérifier la signature envoyée par Citrix Cloud dans sa demande d'authentification SAML. Citrix Cloud utilise le certificat de signature du fournisseur SAML pour vérifier que la réponse SAML provient d'un fournisseur d'identité fiable et connecté.

Qu'est-ce que l'application des demandes signées SAML ?

La configuration de Citrix Cloud pour envoyer des demandes signées ne garantit pas que le fournisseur SAML appliquera l'utilisation des signatures et rejettera toutes les demandes SAML entrantes non signées. La plupart des fournisseurs SAML disposent d'une option permettant d'appliquer les demandes signées, ce qui signifie que si une demande non signée de connexion au fournisseur SAML est reçue, la connexion échouera. Il est de la responsabilité de l'administrateur du fournisseur SAML de vérifier l'état de la configuration du fournisseur d'identité. Le support Citrix ne contrôle pas et n'a aucune visibilité sur l'application des demandes signées dans votre application SAML.

À quelle fréquence Citrix effectue-t-il une rotation de son certificat de signature SAML du fournisseur de services ?

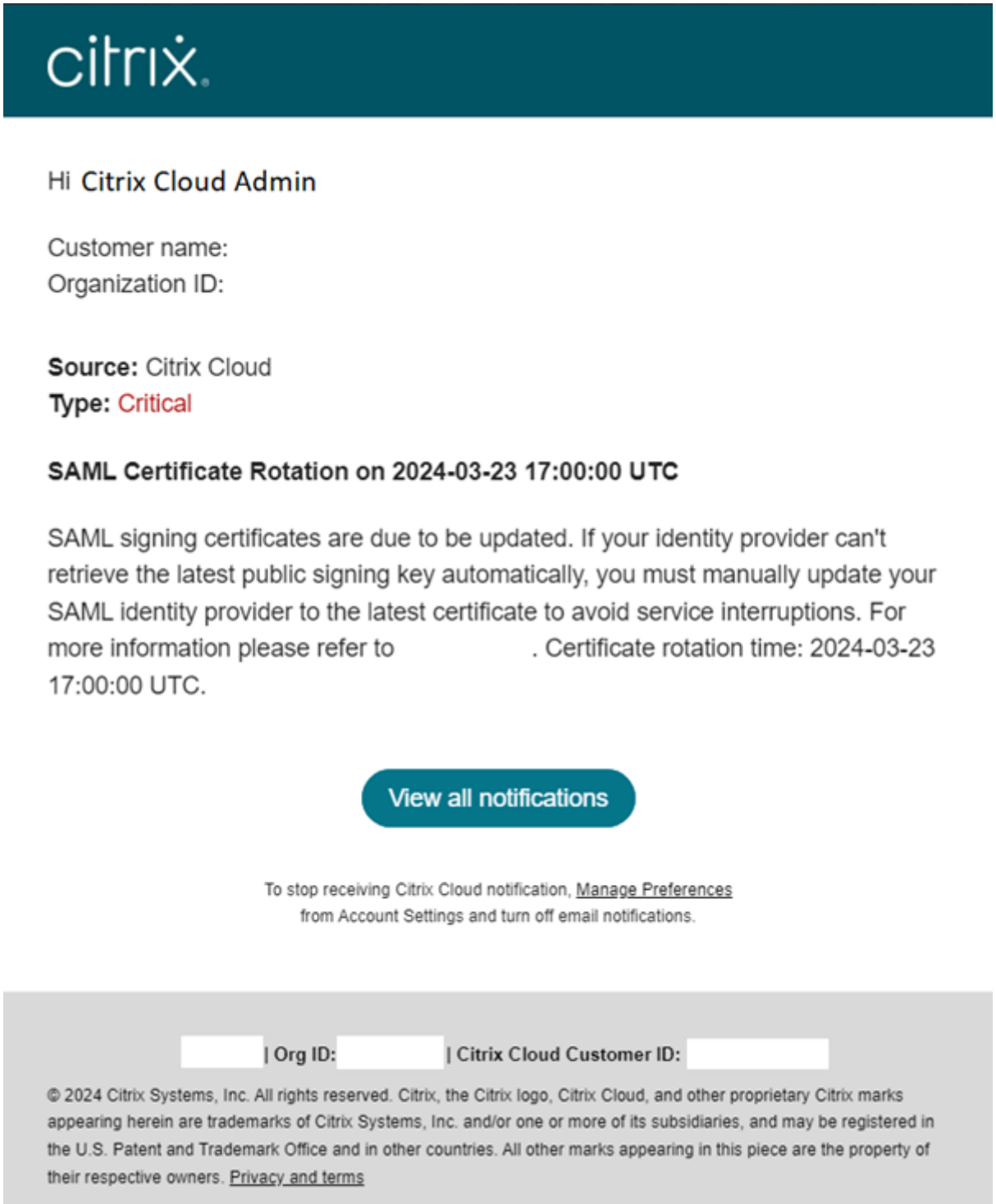
Afin de permettre un chevauchement important entre le certificat de signature du fournisseur de services actif et le certificat nouvellement émis, Citrix fait alterner le certificat de signature du fournisseur de services environ tous les 11 mois. Cela permet de garantir qu'un certificat valide est disponible pour les clients de Citrix Cloud 30 jours avant l'expiration du certificat existant.

En quoi consiste la phase d'annonce du certificat de signature SAML du fournisseur de services ?

Pendant la phase d'annonce, les certificats de signature SAML actuels et de remplacement seront présents dans les métadonnées Citrix Cloud. Seul le certificat actif peut être utilisé pour la vérification des demandes SAML jusqu'à la date et à l'heure de la rotation.

Pourquoi ai-je reçu une notification par e-mail et dans la console d'administration Citrix Cloud indiquant que le certificat de signature SAML Citrix Cloud actuel est sur le point d'expirer et doit être remplacé ?

Les fournisseurs SAML (fournisseur d'identité) ont besoin d'un certificat valide et à jour pour vérifier la signature des demandes SAML entrantes provenant de fournisseurs de services tels que Workspace et la console d'administration Citrix Cloud. Les clients Citrix Cloud utilisant SAML pour la connexion à Workspace ou à la console d'administration Citrix Cloud seront contactés pour les informer d'une rotation imminente des certificats de signature SAML.



citrix.

Hi **Citrix Cloud Admin**

Customer name:
Organization ID:

Source: Citrix Cloud
Type: Critical

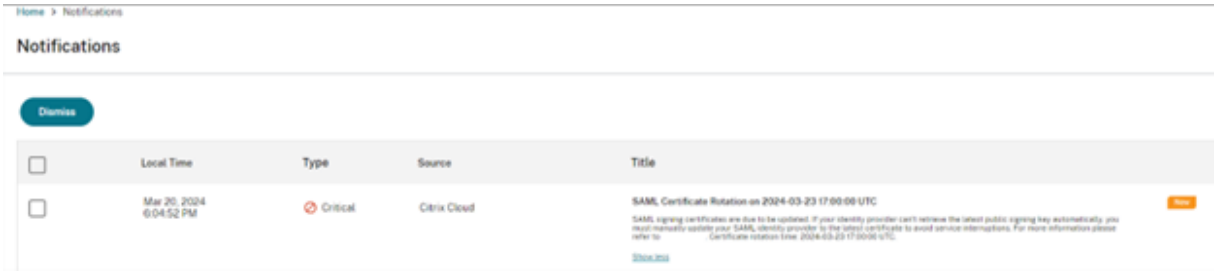
SAML Certificate Rotation on 2024-03-23 17:00:00 UTC

SAML signing certificates are due to be updated. If your identity provider can't retrieve the latest public signing key automatically, you must manually update your SAML identity provider to the latest certificate to avoid service interruptions. For more information please refer to . Certificate rotation time: 2024-03-23 17:00:00 UTC.

View all notifications

To stop receiving Citrix Cloud notification, Manage Preferences from Account Settings and turn off email notifications.

| Org ID: | Citrix Cloud Customer ID:



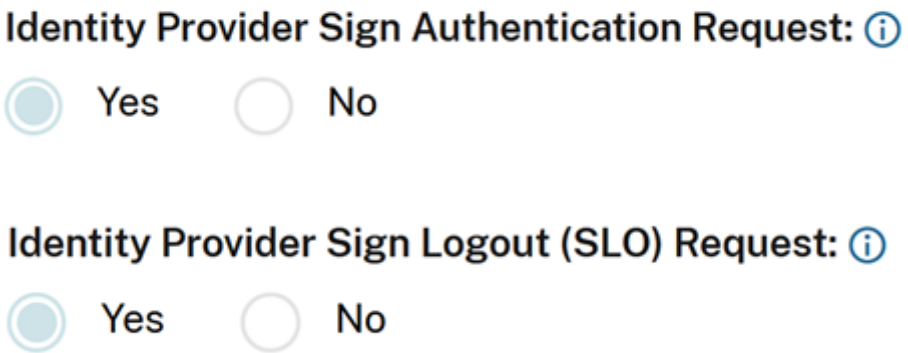
Comment savoir si mon client Citrix Cloud est concerné par la rotation des certificats de signature SAML de Citrix Cloud ?

Cela affectera les clients Citrix Cloud dotés de la configuration SAML suivante.

- Votre connexion SAML au sein de Citrix Cloud est configurée avec **Signer demande d'authentification = Oui**
- Vous avez configuré votre fournisseur SAML tel qu'Azure Active Directory, ADFS ou Okta pour rejeter les demandes SAML non signées (application des demandes signées).
- La déconnexion unique (SLO) est configurée dans votre connexion SAML Citrix Cloud et dans votre fournisseur SAML. Votre fournisseur SAML peut exiger la signature des demandes SLO, par exemple pour Okta et PingFederate.

Comment vérifier la configuration de signature de ma connexion SAML Citrix Cloud ?

Accédez à **Gestion des identités et des accès** > **SAML 2.0** > **Afficher** pour vérifier si l'option **Signer demande d'authentification** est activée dans votre connexion SAML Citrix Cloud. Toutes les nouvelles connexions SAML au sein de Citrix Cloud seront définies par défaut sur **Demande d'authentification de signature du fournisseur d'identité/Demande de déconnexion signée (SLO) du fournisseur d'identité = Oui** pour la connexion (SSO) et la déconnexion (SLO).



Comment puis-je vérifier si l'application de signature est configurée dans mon application SAML ?

Cela varie en fonction du fournisseur SAML que vous utilisez. Certains n'offrent peut-être même pas cette option. AzureAD, ADFS, Okta et PingFederate prennent tous en charge l'application de la signature. Il est essentiel que l'administrateur SAML connaisse les fonctionnalités de votre fournisseur SAML et sa configuration actuelle. Le support Citrix n'a aucun contrôle ni aucune visibilité à ce sujet.

Où puis-je obtenir une copie du dernier certificat de signature du fournisseur de services ?

Ce certificat est fourni par Citrix via les métadonnées SAML de Citrix Cloud et est mis à jour périodiquement pendant la phase d'annonce de la rotation des certificats de signature du fournisseur de services. Cela se produit au moins une fois par année civile.

États-Unis, UE et Asie-Pacifique Sud : https://saml.cloud.com/saml/metadata

Japon : https://saml.citrixcloud.jp/saml/

Gouvernement : https://saml.cloud.us/saml/metadata

Quand puis-je supprimer en toute sécurité l'ancien certificat de signature SAML de Citrix Cloud si mon application SAML prend en charge plusieurs certificats de vérification ?

Ne supprimez l'ancien certificat de signature Citrix Cloud qu'après la date et l'heure de rotation des certificats indiquées dans l'e-mail et la notification de la console d'administration Citrix Cloud.

Utilisez l'échange de métadonnées pour mettre automatiquement à jour le fournisseur SAML avec le dernier certificat de signature SAML du fournisseur de services Citrix Cloud

À l'aide de l'échange de métadonnées SAML, le fournisseur SAML consomme automatiquement les métadonnées SAML de Citrix Cloud en surveillant l'URL des métadonnées, telle que https://saml.cloud.com/saml/metadata. Si votre fournisseur SAML prend en charge l'échange de métadonnées SAML, le certificat de signature du fournisseur de services est peut-être déjà mis à jour automatiquement. Vérifiez que votre fournisseur SAML prend en charge l'échange de métadonnées. Ensuite, vous pouvez vérifier si la mise à jour a eu lieu avant l'expiration du certificat de signature SAML actuel.

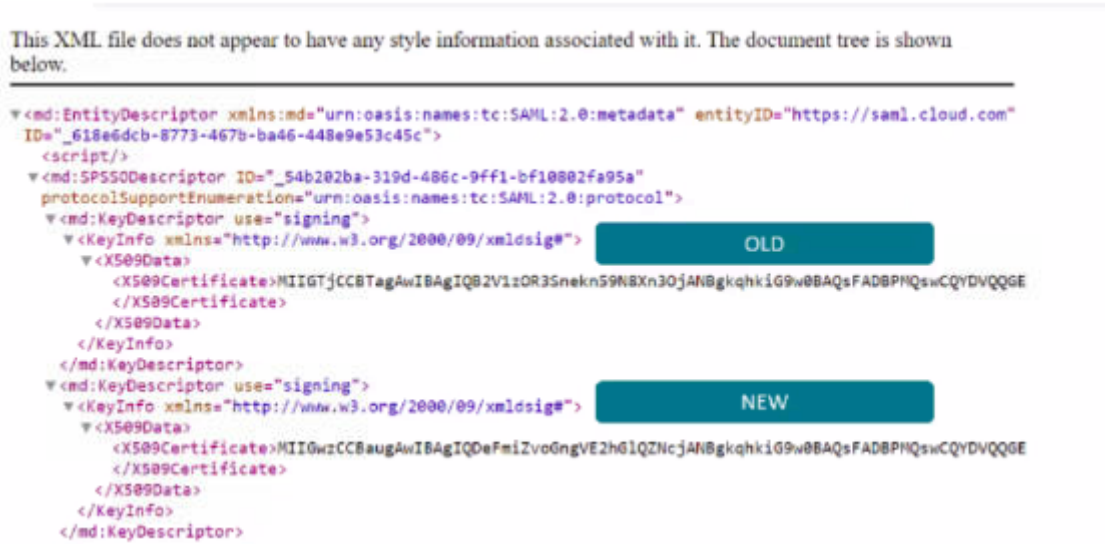
> **Important**
>
> Les fonctionnalités SAML prises en charge par chaque fournisseur SAML tiers varient considérablement. Il est de la responsabilité de l'administrateur Citrix Cloud de connaître et de comprendre les fonctionnalités et les exigences du fournisseur SAML que vous utilisez. Cela est nécessaire pour garantir que la configuration de connexion SAML (fournisseur de services) de Citrix Cloud et la configuration du fournisseur SAML (fournisseur d'identité) correspondent. Consultez la documentation de votre fournisseur SAML pour déterminer s'il prend en charge la vérification des signatures et si les demandes et réponses SAML doivent être signées.

Mettre à jour manuellement le fournisseur SAML avec le dernier certificat de signature SAML du fournisseur de services Citrix Cloud

> **Important**
>
> La rotation des certificats de fournisseur de services doit être effectuée chaque fois qu'un nouveau certificat est publié depuis Citrix Cloud, faute de quoi l'ouverture de session SAML sera affectée et vous serez confronté à un temps d'arrêt.

1. Obtenez les dernières métadonnées SAML auprès de Citrix Cloud en consultant votre connexion SAML actuelle dans **Gestion des identités et des accès**, cliquez sur **Authentification**, sélectionnez **Connexion SAML**, puis cliquez sur **Afficher**.
   L'image suivante est un exemple de ce à quoi ce fichier peut ressembler pour les régions Citrix Cloud telles que les États-Unis, l'UE et l'Asie-Pacifique Sud :

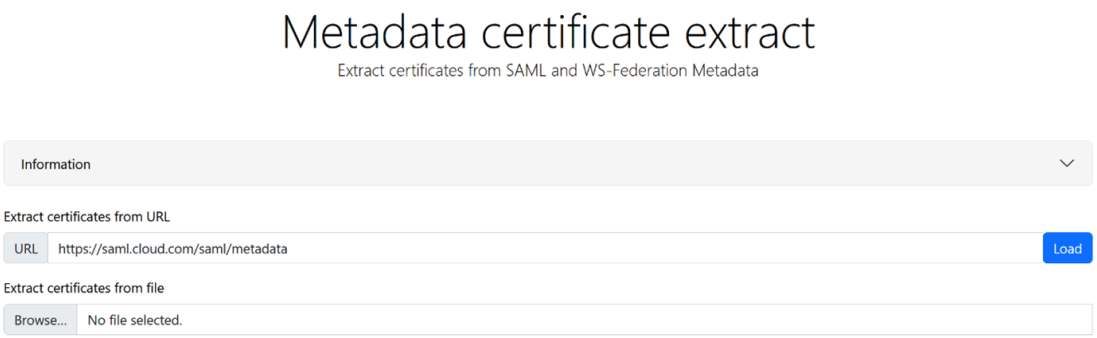
   https://saml.cloud.com/saml/metadata



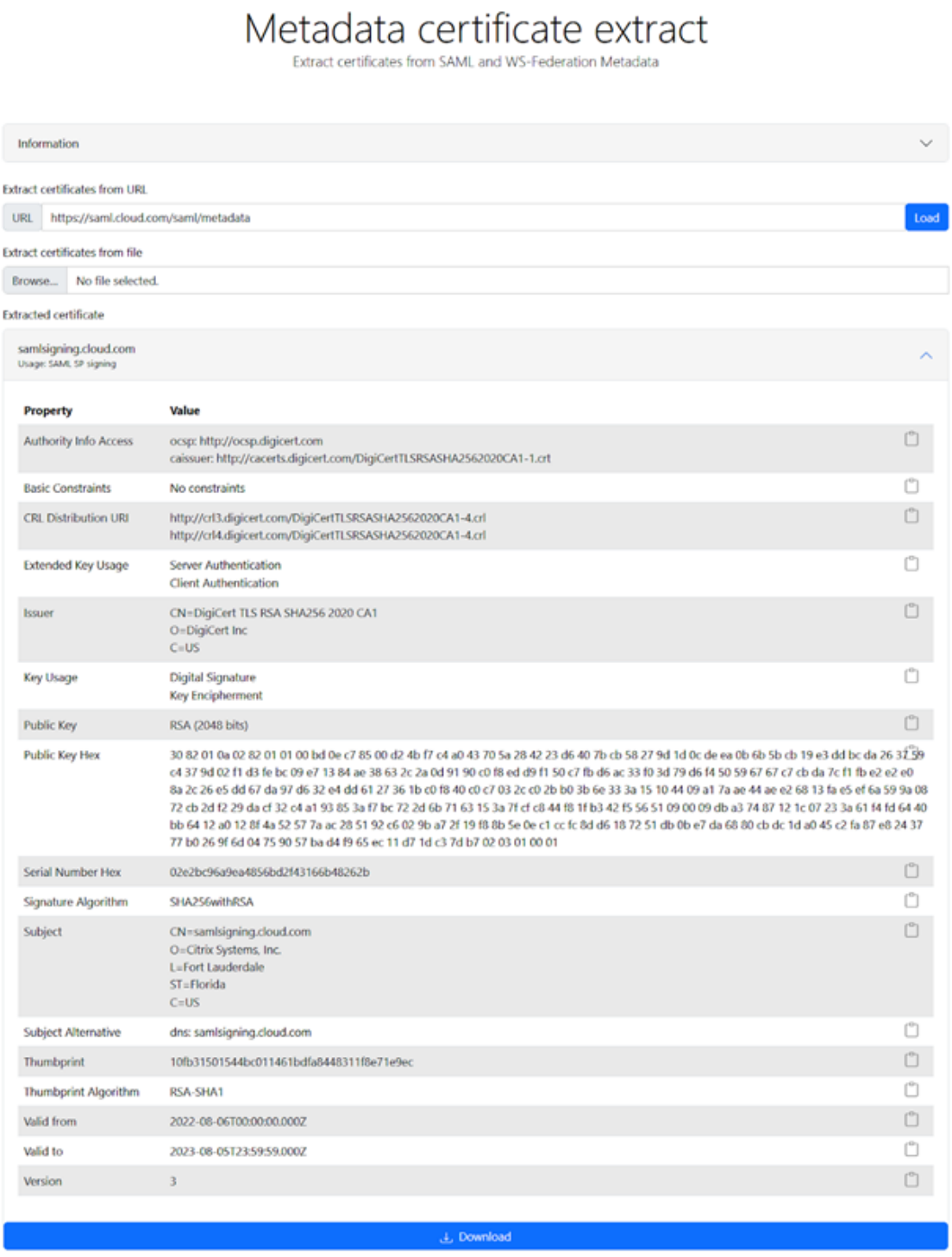
Dans cet exemple de fichier XML de métadonnées, il existe deux certificats de signature SAML Citrix Cloud x509.

2. Il est possible d'extraire le certificat x509 à partir des métadonnées en téléchargeant le fichier XML vers un outil tiers ou en fournissant l'URL des métadonnées.
3. Accéder à https://www.rcfed.com/SAMLWSFed/MetadataCertificateExtract
4. Entrez l'URL des métadonnées SAML qui correspond à la région de votre client Citrix Cloud :

    - États-Unis, UE et Asie-Pacifique Sud : https://saml.cloud.com/saml/metadata
    - Japon : https://saml.citrixcloud.jp/saml/metadata
    - Gouvernement : https://saml.cloud.us/saml/metadata



Téléchargez le certificat de signature SAML depuis https://www.rcfed.com/SAMLWSFed/MetadataCertificateExtract.



5. Téléchargez le certificat SAML du fournisseur de services Citrix Cloud récemment extrait vers votre fournisseur SAML. Ce processus sera différent pour chaque fournisseur SAML. Vérifiez la procédure de rotation des certificats de signature du fournisseur de services appropriée à l'aide de la documentation de votre fournisseur SAML spécifique.

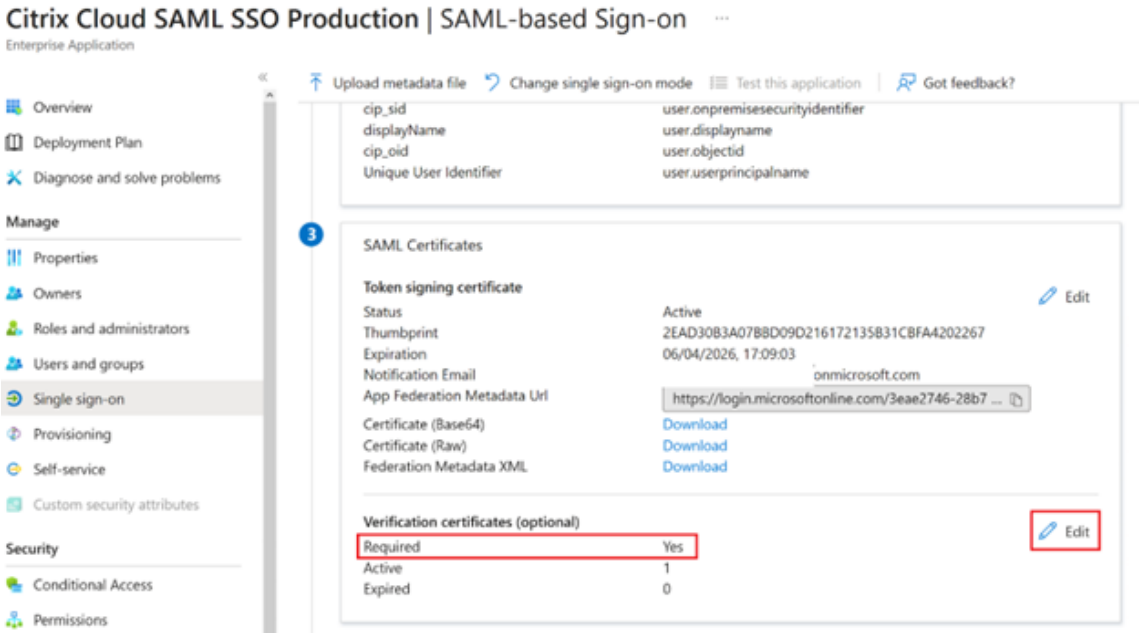
   Selon votre fournisseur SAML, le certificat de signature SAML existant devra peut-être être rem-

placé par le nouveau. Dans certains cas, le fournisseur SAML peut prendre en charge plusieurs certificats de signature du fournisseur de services en même temps. Il suffira donc de télécharger le nouveau certificat. Il est recommandé de supprimer l'ancien certificat une fois qu'il a expiré.

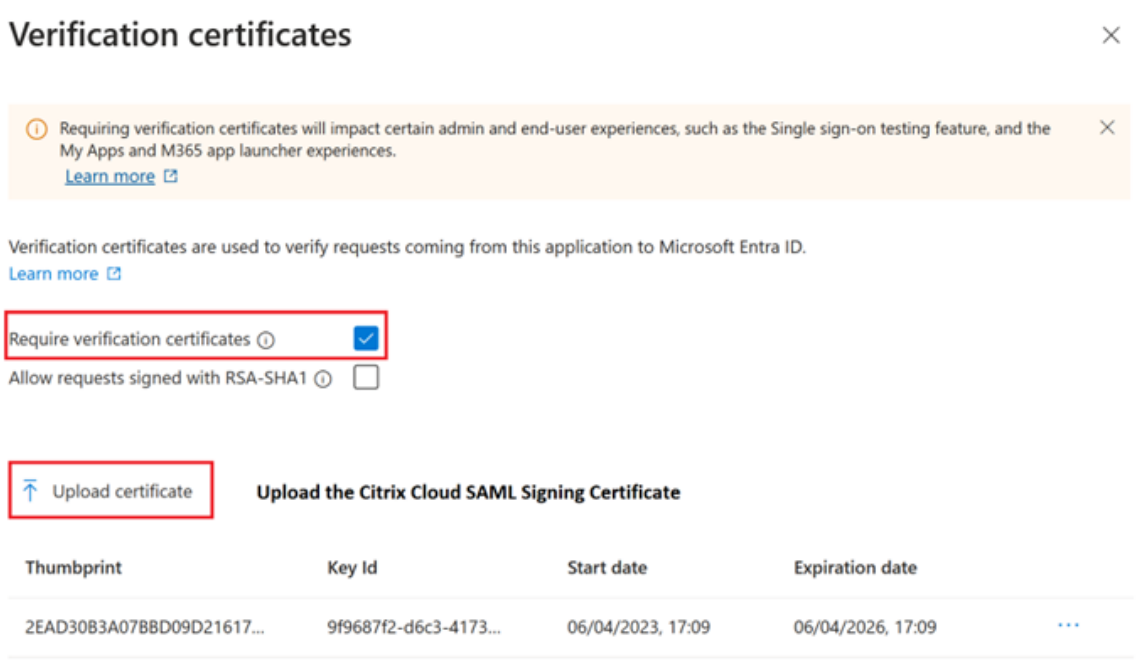
Télécharger un certificat de signature SAML Citrix Cloud de remplacement dans votre application SAML Azure Active Directory

Avant de configurer l'application SAML Azure Active Directory, consultez la section Vérification de la signature des demandes SAML pour plus d'informations.

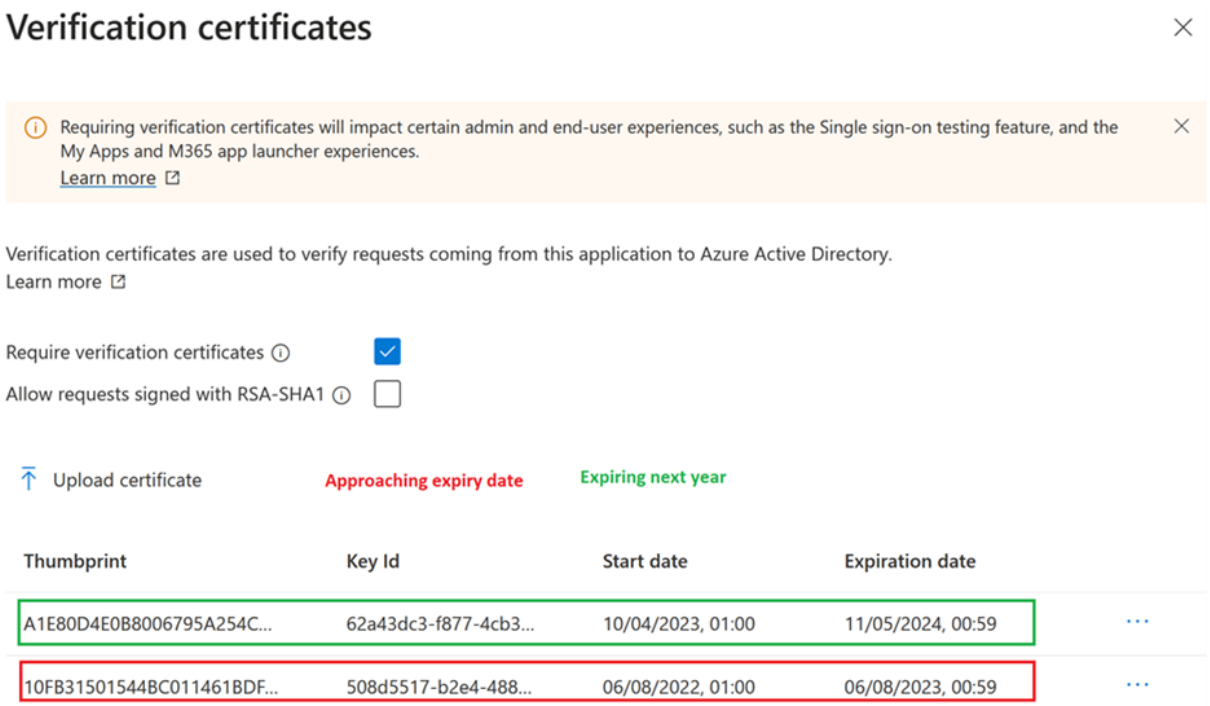
1. Accédez à **Azure Active Directory**, sélectionnez **Applications d'entreprise**, puis cliquez sur votre application SAML.
2. Localisez la section des certificats SAML dans l'application SAML.



3. Sélectionnez **Télécharger le certificat** et chargez le certificat de signature SAML Citrix Cloud de remplacement obtenu à partir des métadonnées SAML.



> **Remarque :**
>
> Les applications SAML Azure Active Directory peuvent avoir plusieurs certificats de vérification de signature configurés. Il est donc possible de télécharger un certificat de remplacement bien avant l'expiration du certificat actuel. La capture d'écran suivante montre deux certificats valides. L'un des certificats doit expirer prochainement. À condition qu'au moins un des certificats chargés soit valide et n'ait pas encore expiré, la connexion SAML à Citrix Workspace et Citrix Cloud continuera de fonctionner et vous ne rencontrerez aucune panne.

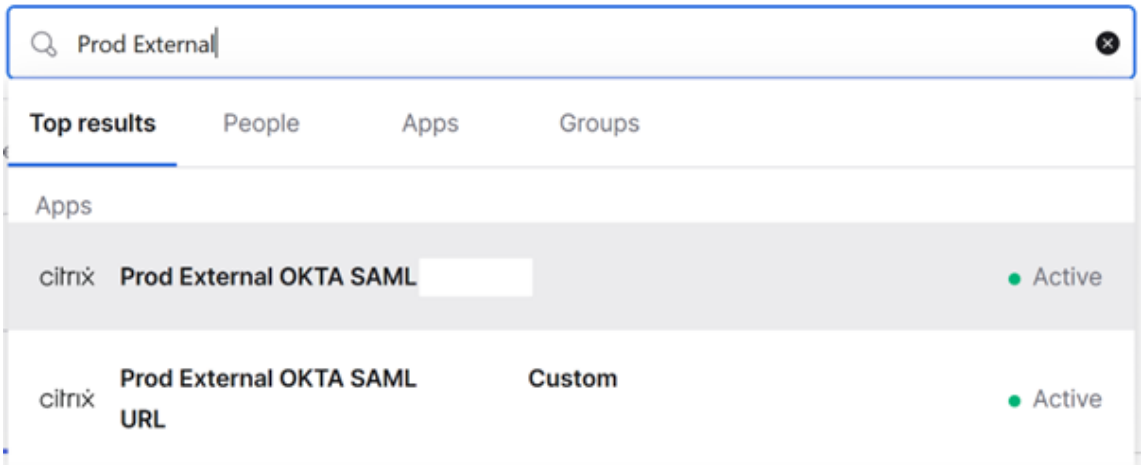


> **Important :**
>
> Ne supprimez le certificat de vérification existant qu'une fois la date et l'heure de rotation SAML indiquées dans l'e-mail et la notification de la console d'administration Citrix Cloud passées. Le nouveau certificat Citrix Cloud n'est actif qu'à la date et à l'heure indiquées dans ces deux notifications.

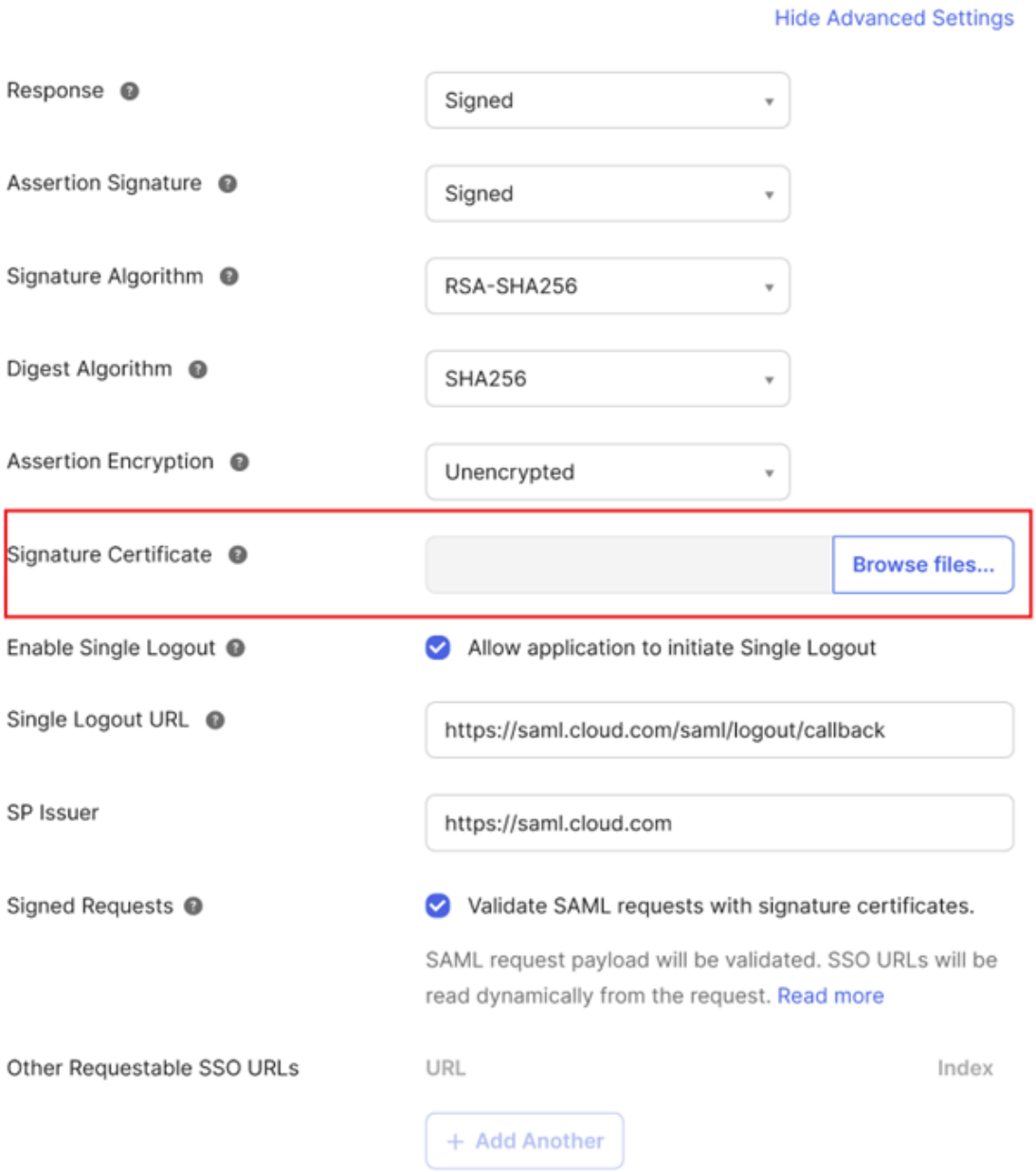
Télécharger un certificat de signature SAML Citrix Cloud de remplacement dans votre application SAML Okta

Okta ne prend pas en charge plusieurs certificats de signature SAML de fournisseur de services en même temps. Vous n'avez pas d'autre choix que de remplacer le certificat de signature du fournisseur de services Citrix Cloud que vous utilisez actuellement par le nouveau. Il est recommandé de le faire dans une fenêtre de maintenance planifiée.

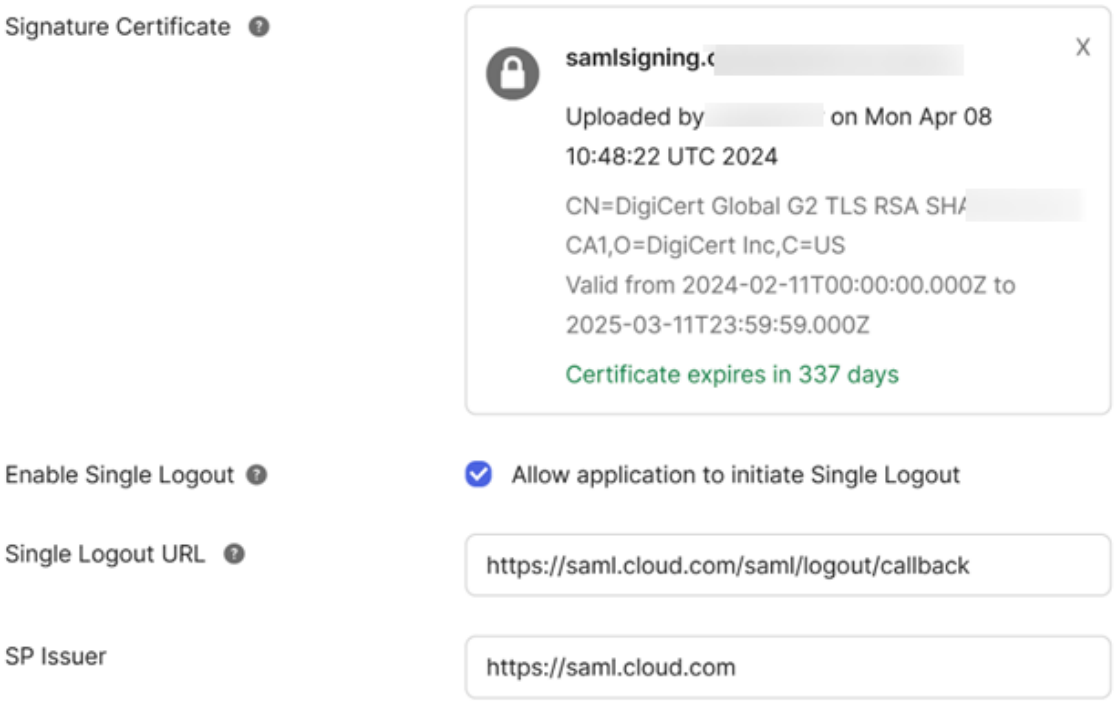
1. Accédez à **Applications**, sélectionnez **Applications**, puis recherchez votre application SAML Okta



2. Dans **Général**, accédez aux **Paramètres SAML**, cliquez sur **Modifier**, sélectionnez **Configurer SAML**, sélectionnez **Afficher les paramètres avancés**, puis cliquez sur **Certificat de signature** afin de télécharger un certificat de remplacement. Okta n'affiche pas le certificat de signature SAML Citrix Cloud actuel dans l'interface utilisateur de téléchargement. Le certificat de remplacement ne sera affiché qu'une fois celui-ci chargé.



3. Sélectionnez **Certificat de signature**, cliquez sur **Parcourir les fichiers** et téléchargez le certificat de signature SAML Citrix Cloud de remplacement obtenu à partir des métadonnées SAML Citrix Cloud.



> **Important**
>
> Ne remplacez pas le certificat de vérification existant avant la date et l'heure de rotation SAML indiquées dans l'e-mail et dans la notification de la console d'administration Citrix Cloud. Le nouveau certificat Citrix Cloud n'est actif qu'à la date et à l'heure indiquées dans ces deux notifications.

Configurer ADFS en tant que fournisseur SAML pour l'authentification de Workspace

July 2, 2024

Author:
Mark Dear

Cet article explique comment configurer l'approbation de partie de confiance requise par Citrix Cloud pour se connecter à Citrix Workspace ou Citrix Cloud à l'aide de SAML.

Une fois que vous avez suivi les étapes décrites dans cet article, vous pouvez configurer la connexion SAML entre votre serveur ADFS et Citrix Cloud comme décrit dans Connecter SAML en tant que fournisseur d'identité dans Citrix Cloud. Pour obtenir des conseils sur la saisie des valeurs ADFS correctes pour votre connexion SAML, consultez la section Configuration SAML dans Citrix Cloud dans cet article.

Pré-requis

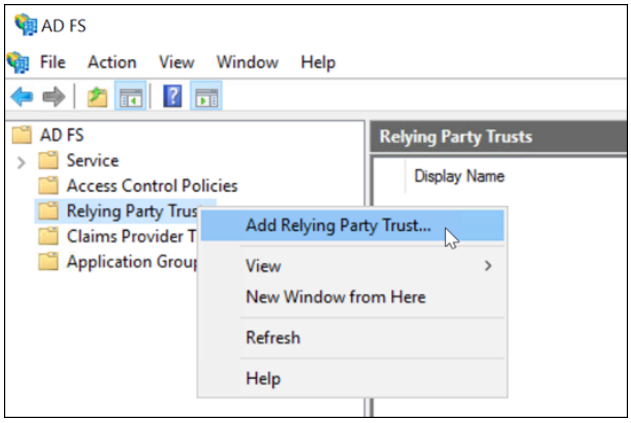
Les instructions de cet article supposent que vous disposez d'un déploiement de serveur ADFS opérationnel avec Citrix FAS dans votre environnement. Citrix FAS doit fournir une authentification unique (Single Sign-On) aux VDA lors du lancement de la session.

Pour plus d'informations, consultez les articles suivants :

- Documentation Citrix FAS :
  - Installer et configurer
  - Déploiement ADFS
- Citrix Tech Zone : Architecture de référence : Service d'authentification fédérée

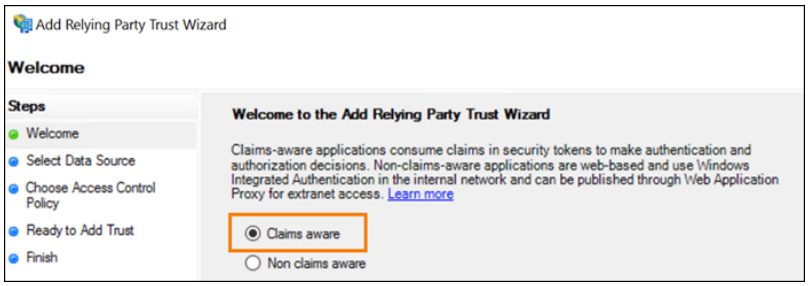
Configurer une approbation de partie de confiance pour Citrix Cloud

1. À partir de la console de gestion AD FS, développez le nœud **AD FS** dans le volet de gauche.
2. Cliquez avec le bouton droit de la souris sur **Relying Party Trust** et sélectionnez **Add Relying Party Trust**.

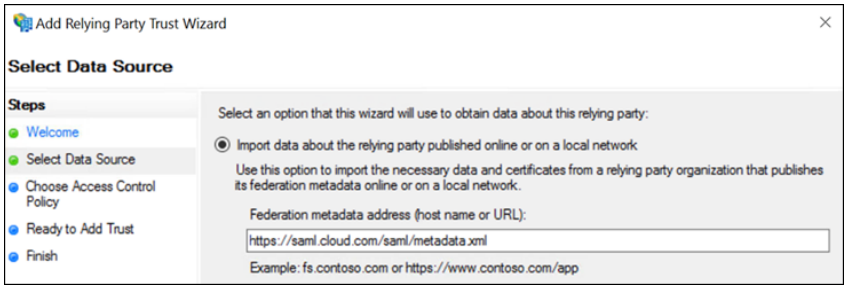


L'assistant Add Relying Party Trust apparaît.

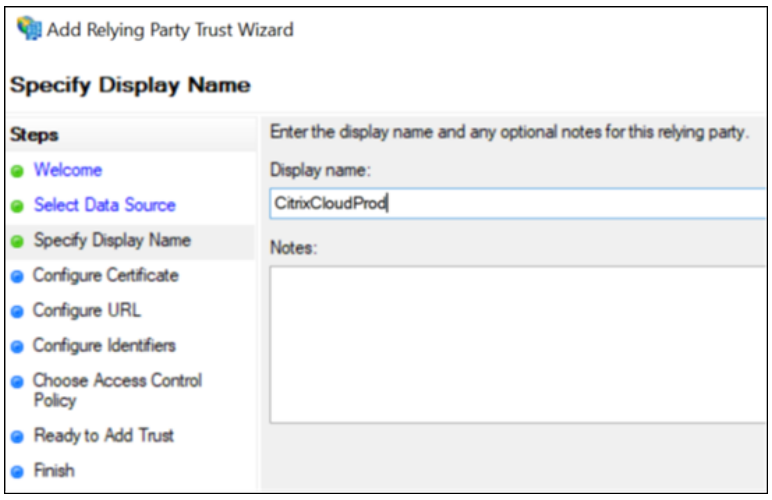
3. Sélectionnez **Claims aware**, puis cliquez sur **Next**.



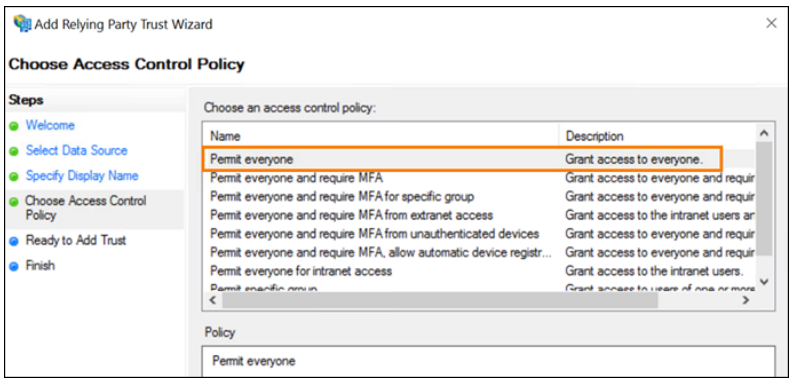
4. Dans **Federation metadata address**, entrez `https://saml.cloud.com/saml/metadata.xml`. Sélectionnez **Suivant**.



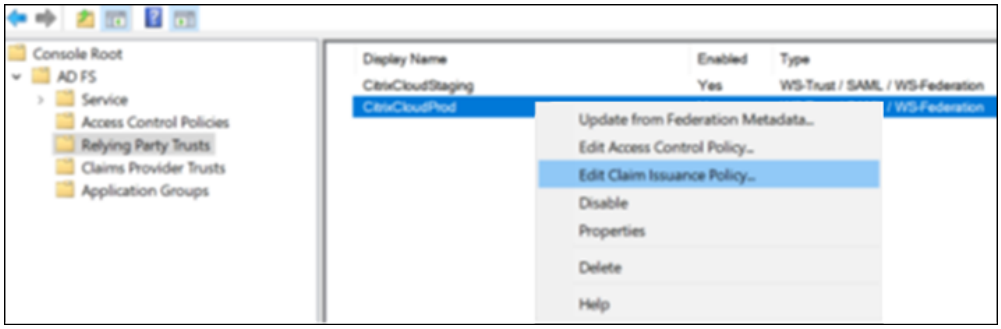
5. Pour le nom d'affichage (Display Name), entrez `CitrixCloudProd`. Sélectionnez **Suivant**.



6. Pour la stratégie de contrôle d'accès (Access Control Policy), sélectionnez **Permit everyone**. Sélectionnez **Suivant**.

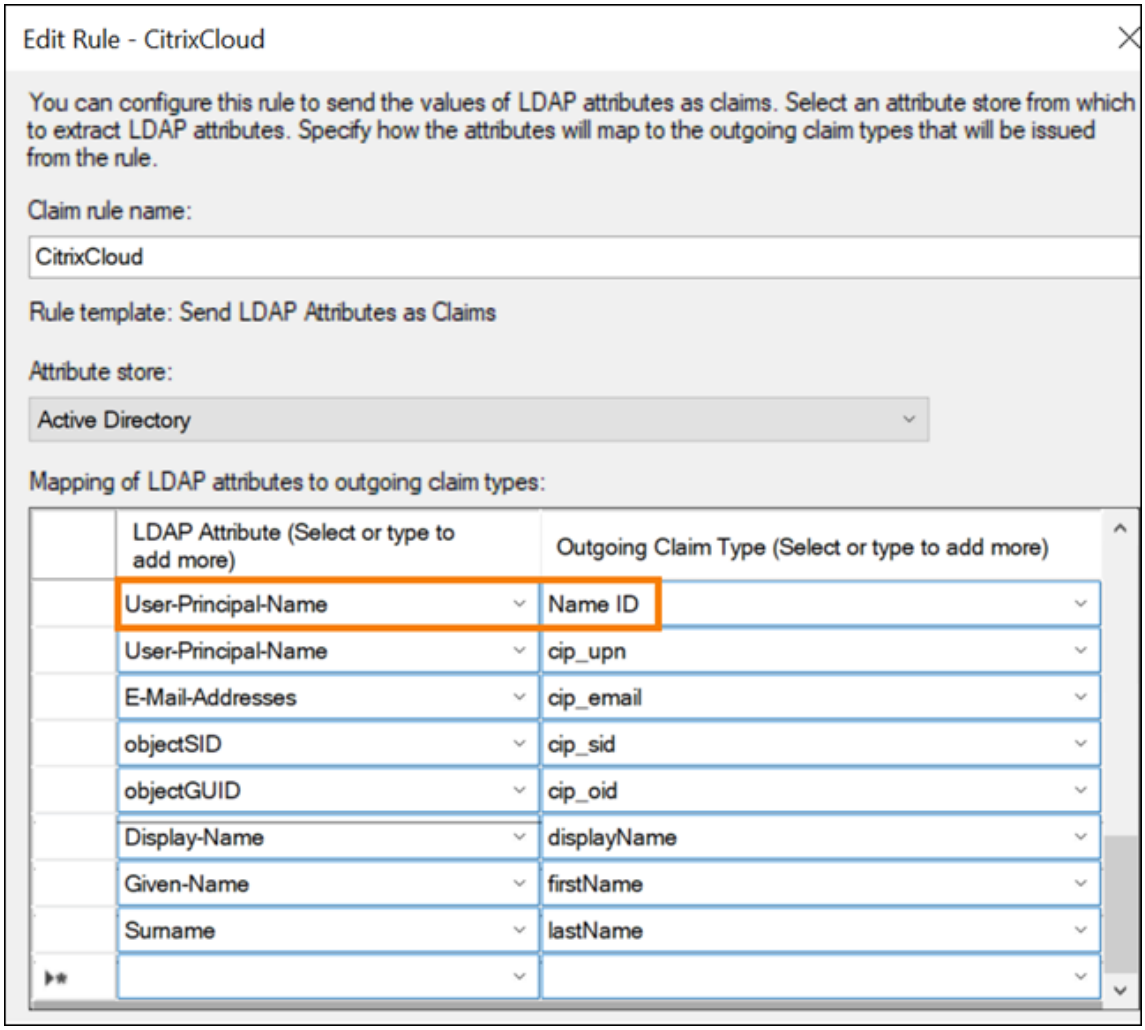


7. Sur l'écran **Ready to Add Trust**, sélectionnez **Next**.
8. Sur l'écran **Finish**, sélectionnez **Configure claims issuance policy for this application**. Sélectionnez **Suivant**.



9. Cliquez avec le bouton droit sur la nouvelle approbation de partie de confiance et sélectionnez **Edit Claim Issuance Policy**.
10. Cliquez sur **Add Rule**, puis sélectionnez **Send LDAP Attributes as Claims**. Sélectionnez **Suivant**.
11. Dans **Claim rule name**, entrez `CitrixCloud`.
12. Dans **Attribute store**, sélectionnez **Active Directory**.
13. Sous **Mapping of LDAP attributes to outgoing claim types**, ajoutez les attributs LDAP suivants, exactement comme indiqué :

Attribut LDAP	Type de revendication sortante
User-Principal-Name	Name ID
User-Principal-Name	cip_upn
E-Mail-Addresses	cip_email
objectSID	cip_sid
objectGUID	cip_oid
Display-Name	displayName
Given-Name	firstName
Surname	lastName



14. Sélectionnez **Terminer**.

Modifier une approbation de partie de confiance Citrix Cloud à l'aide de PowerShell

Si vous avez configuré votre serveur ADFS en utilisant la configuration « prête à l'emploi » par défaut, les étapes décrites dans cette section vous permettent de le mettre à jour afin qu'il réponde à la configuration recommandée par Citrix. Cette tâche est nécessaire pour résoudre ce problème : la déconnexion unique SAML depuis Citrix Cloud ou Citrix Workspace échoue si l'attribut `nameidentifier` n'est pas inclus dans le jeu de règles de revendication ou n'est pas le premier attribut SAML du jeu de règles de revendication.

> **Remarque :**
>
> Vous n'avez pas besoin d'effectuer cette tâche si vous avez créé votre jeu de règles de revendication en suivant les étapes décrites dans Configurer une approbation de partie de confiance pour Citrix Cloud dans cet article.

Pour effectuer cette tâche, vous devez remplacer le jeu de règles existant par un nouveau jeu de règles de revendication à l'aide de PowerShell. La console de gestion ADFS ne prend pas en charge ce type d'opération.

1. Sur le serveur ADFS, localisez PowerShell ISE. Cliquez avec le bouton droit et sélectionnez **Exécuter en tant qu'administrateur**.
2. Sauvegardez vos règles de revendication ADFS existantes dans un fichier texte :

```
Get-ADFSRelyingPartyTrust -name "CitrixCloudStaging" | Select-
    Object -ExpandProperty IssuanceTransformRules | Out-File "$env:
    USERPROFILE\desktop\claimrulesbackup.txt"
<!--NeedCopy-->
```

3. Téléchargez le fichier claimrules.txt fourni par Citrix à l'adresse https://github.com/citrix/sample-scripts/tree/master/citrix-cloud.
4. Copiez le fichier claimrules.txt sur votre bureau.
5. Importez les règles de revendication requises à l'aide du fichier claimrules.txt :

```
Set-ADFSRelyingPartyTrust -Name "CitrixCloudProd" `
                      -MetadataUrl "https://saml.cloud.com/saml/
                         metadata" `
                      -AutoUpdateEnabled $True `
                      -IssuanceTransformRulesFile "$env:
                         USERPROFILE\desktop\claimrules.txt" `
                      -SignedSamlRequestsRequired $True `
                      -SamlResponseSignature "MessageAndAssertion"
                          `
                      -Enabled $True
<!--NeedCopy-->
```

Mettre à jour les paramètres de signature SAML pour l'approbation de partie de confiance à l'aide de PowerShell

Par défaut, les approbations de partie de confiance ADFS ont les paramètres suivants :

- EncryptClaims : True
- SignedSamlRequestsRequired : False
- SamlResponseSignature : AssertionOnly

Pour une sécurité accrue, Citrix recommande d'utiliser des requêtes SAML signées à la fois pour l'authentification unique (SSO) et la déconnexion unique. Cette section décrit comment mettre à jour les paramètres de signature d'une approbation de partie de confiance à l'aide de PowerShell afin qu'ils répondent à la configuration recommandée par Citrix.

1. Obtenez la configuration actuelle de RelyingPartyTrust sur votre serveur ADFS.


```
Get-ADFSRelyingPartyTrust -TargetName "CitrixCloudProd"
<!--NeedCopy-->
```

2. Mettez à jour les paramètres d'approbation de partie de confiance **CitrixCloudProd**.

```
Set-ADFSRelyingPartyTrust -Name "CitrixCloudProd" `
                      -SignedSamlRequestsRequired $True `
                      -SamlResponseSignature "MessageAndAssertion"
<!--NeedCopy-->
```

3. Contactez le support Citrix et demandez à activer la fonctionnalité d'authentification **EnableSamlLogoutSigningAndPost** sur votre client Citrix Cloud. Citrix Cloud envoie alors des requêtes de déconnexion unique SAML sous forme de requêtes POST signées au lieu de requêtes de redirection non signées lorsque les utilisateurs se déconnectent de Citrix Workspace ou de Citrix Cloud. L'envoi de requêtes POST signées est obligatoire si le fournisseur SAML exige des requêtes signées pour une déconnexion unique et rejette les redirections non signées.

Configuration SAML dans Citrix Cloud

Lorsque vous configurez la connexion SAML dans Citrix Cloud (comme décrit dans Ajouter des métadonnées du fournisseur SAML à Citrix Cloud), vous entrez les valeurs pour ADFS comme suit :

Dans ce champ dans Citrix Cloud	Entrez cette valeur
ID de l'entité	`https://adfs.YourDomain.com/adfs/services/trust`, où `YourDomain.com` est le domaine de votre serveur ADFS.
Signer demande d'authentification	Oui
URL du service SSO	`https://adfs.YourDomain.com/adfs/ls`, où `YourDomain.com` est le domaine de votre serveur ADFS.
Mécanisme de liaison	Publication HTTP
Réponse SAML	Signer la réponse ou l'assertion
Contexte d'authentification	Non spécifié, Exact
URL de déconnexion	`https://adfs.YourDomain.com/adfs/ls`, où `YourDomain.com` est le domaine de votre serveur ADFS.

Se connecter à des espaces de travail avec SAML à l'aide de domaines personnalisés

November 29, 2023

Author:
Mark Dear

Si vous avez configuré un domaine personnalisé dans Citrix Workspace (par exemple `https://workspaces.yourdomain.com`), une configuration supplémentaire dans Citrix Cloud et auprès de votre fournisseur SAML peut être requise, en fonction des scénarios de connexion SAML que vous souhaitez prendre en charge dans Citrix Cloud.

Vous aurez peut-être besoin de deux applications SAML pour cette configuration. Citrix Cloud nécessite différents points de terminaison du fournisseur de services SAML, selon que l'application SAML utilise les URL cloud.com ou workspaces.yourdomain.com pour effectuer l'opération de connexion.

Pour plus d'informations sur la configuration de domaines personnalisés dans Citrix Workspace, consultez la section Configurer un domaine personnalisé dans la documentation du produit Citrix Workspace.

Considérations relatives au déploiement d'une ou deux applications SAML

Pour déterminer si vous devez déployer une solution d'application SAML unique ou double, identifiez la combinaison de scénarios de connexion SAML que votre fournisseur SAML doit prendre en charge.

Les scénarios de connexion suivants partagent la même application SAML (SAML App 1) par défaut :

- Authentification SAML pour Citrix Workspace où l'URL de connexion à l'espace de travail pour votre région (cloud.com, citrixcloud.jp, cloud.us) est configurée dans votre fournisseur SAML en tant qu'ID d'entité du fournisseur de services.
- Authentification SAML pour Citrix Cloud à l'aide de votre URL de connexion unique (par exemple, `https://citrix.cloud.com/go/mycompany`). Dans ce scénario, les administrateurs sont authentifiés auprès de Citrix Cloud à l'aide de SAML, en fonction de leur appartenance au groupe Active Directory (AD).

L'ajout de l'authentification SAML pour les utilisateurs via un domaine personnalisé (par exemple `https://workspaces.mycompany.com`) que vous définissez dans Configuration de l'espace de travail nécessite une deuxième application SAML (SAML App 2).

Le tableau suivant répertorie les combinaisons de scénarios de connexion SAML prises en charge et les applications SAML requises.

Connexion à Workspace à l'aide de l'URL de l'espace de travail	Connexion à Workspace avec une URL de domaine personnalisée	Connexion à Citrix Cloud à l'aide de l'URL de connexion SAML	Application SAML 1 requise ?	Application SAML 2 requise ?
Oui	Non	Non	Oui, utilisez les points de terminaison SAML cloud.com	Non
Non	Oui	Non	Oui, utilisez des points de terminaison SAML de domaine personnalisés	Non
Non	Non	Oui	Oui, utilisez les points de terminaison SAML cloud.com	Non
Oui	Non	Oui	Oui, utilisez les points de terminaison SAML cloud.com	Non
Non	Non	Oui	Oui, utilisez les points de terminaison SAML cloud.com	Oui, utilisez des points de terminaison SAML de domaine personnalisés
Oui	Oui	Oui	Oui, utilisez les points de terminaison SAML cloud.com	Oui, utilisez des points de terminaison SAML de domaine personnalisés

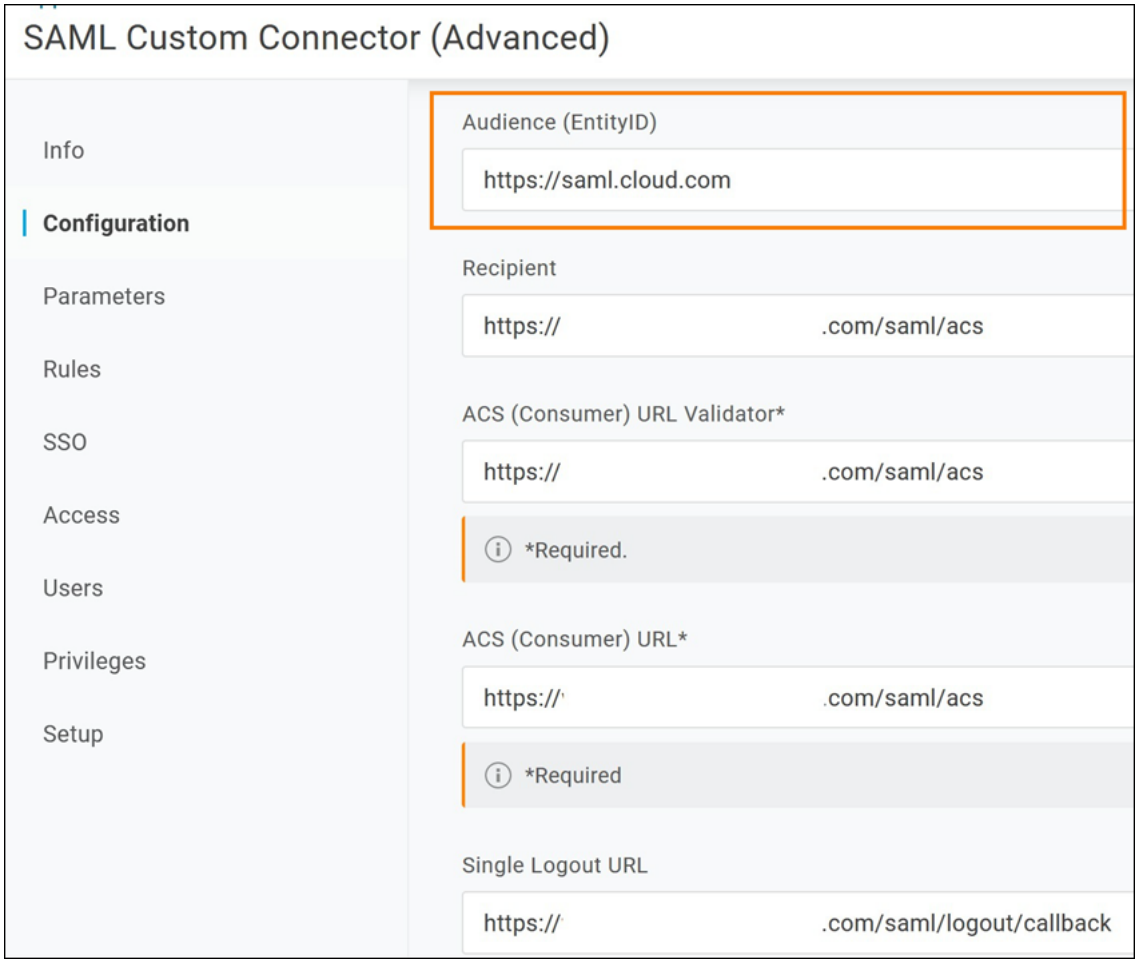
Configuration d'une application SAML unique

1. Dans Citrix Cloud, accédez à **Configuration de l'espace de travail > Accès** et configurez un domaine personnalisé. Pour plus d'informations, consultez la section Configurer un domaine personnalisé.
2. Dans la console de gestion de votre fournisseur SAML, configurez une seule application SAML en utilisant le domaine personnalisé comme points de terminaison du fournisseur de services.
3. Téléchargez le certificat de signature SAML pour l'application SAML. À une étape ultérieure, vous téléchargerez ce certificat sur Citrix Cloud.
4. Sous Entity ID, assurez-vous que `https://saml.cloud.com` est saisi. Selon votre fournisseur SAML, il se peut que ce paramètre soit intitulé **Audience**. Pour tous les autres points de terminaison, remplacez `https://saml.cloud.com` par le domaine personnalisé Workspace que vous avez configuré à l'étape 1.

   L'exemple suivant illustre la configuration du point de terminaison pour Okta, où **Audience Restriction** contient la valeur Entity ID :

   L'exemple suivant illustre la configuration du point de terminaison pour OneLogin, où **Audience** contient la valeur Entity ID :



5. Dans Citrix Cloud, accédez à **Gestion des identités et des accès > Authentification** et configurez la connexion SAML.
6. Accédez à **Configuration de l'espace de travail > Authentification** et sélectionnez **SAML 2.0**.
7. Accédez à **Configuration de l'espace de travail > URL d'espace de travail personnalisée > Modifier** et sélectionnez **Utiliser uniquement l'URL du domaine personnalisé**.
8. Sélectionnez **Enregistrer** pour enregistrer vos modifications.
9. Pour tester la configuration, connectez-vous à Citrix Workspace à l'aide de l'URL personnalisée de votre espace de travail (`https://workspaces.mycompany.com`).

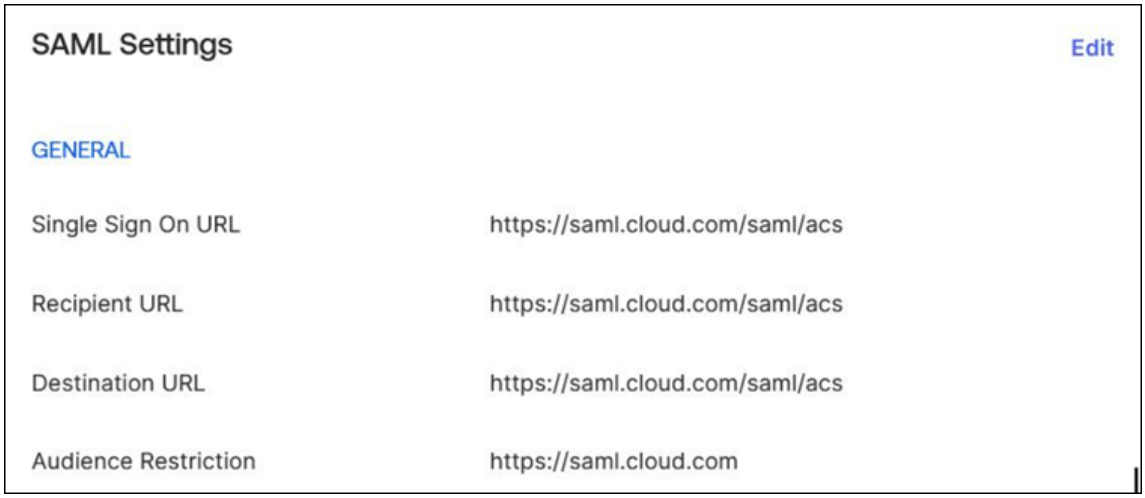
Configuration de deux applications SAML

1. Dans Citrix Cloud, accédez à **Configuration de l'espace de travail > Accès** et configurez un domaine personnalisé. Pour plus d'informations, consultez la section Configurer un domaine personnalisé.

2. Dans la console de gestion de votre fournisseur SAML, configurez deux applications SAML. Configurez ces applications de manière identique, y compris des paramètres de signature identiques pour les demandes d'authentification unique (SSO) et de déconnexion unique (SLO), le type de liaison et les paramètres de déconnexion. Si les configurations de ces applications SAML ne correspondent pas, vous pouvez rencontrer des différences de comportement au niveau de la connexion et de la déconnexion lorsque vous passez de l'URL de votre espace de travail à votre domaine personnalisé Workspace.
3. Dans la première application SAML, configurez les points de terminaison du fournisseur de services suivants :

   - Entity ID : `https://saml.cloud.com`
   - Assertion Consumer Service : `https://saml.cloud.com/saml/acs`
   - Logout : `https://saml.cloud.com/saml/logout/callback`

   L'exemple suivant montre la configuration du point de terminaison dans la console de gestion Okta :

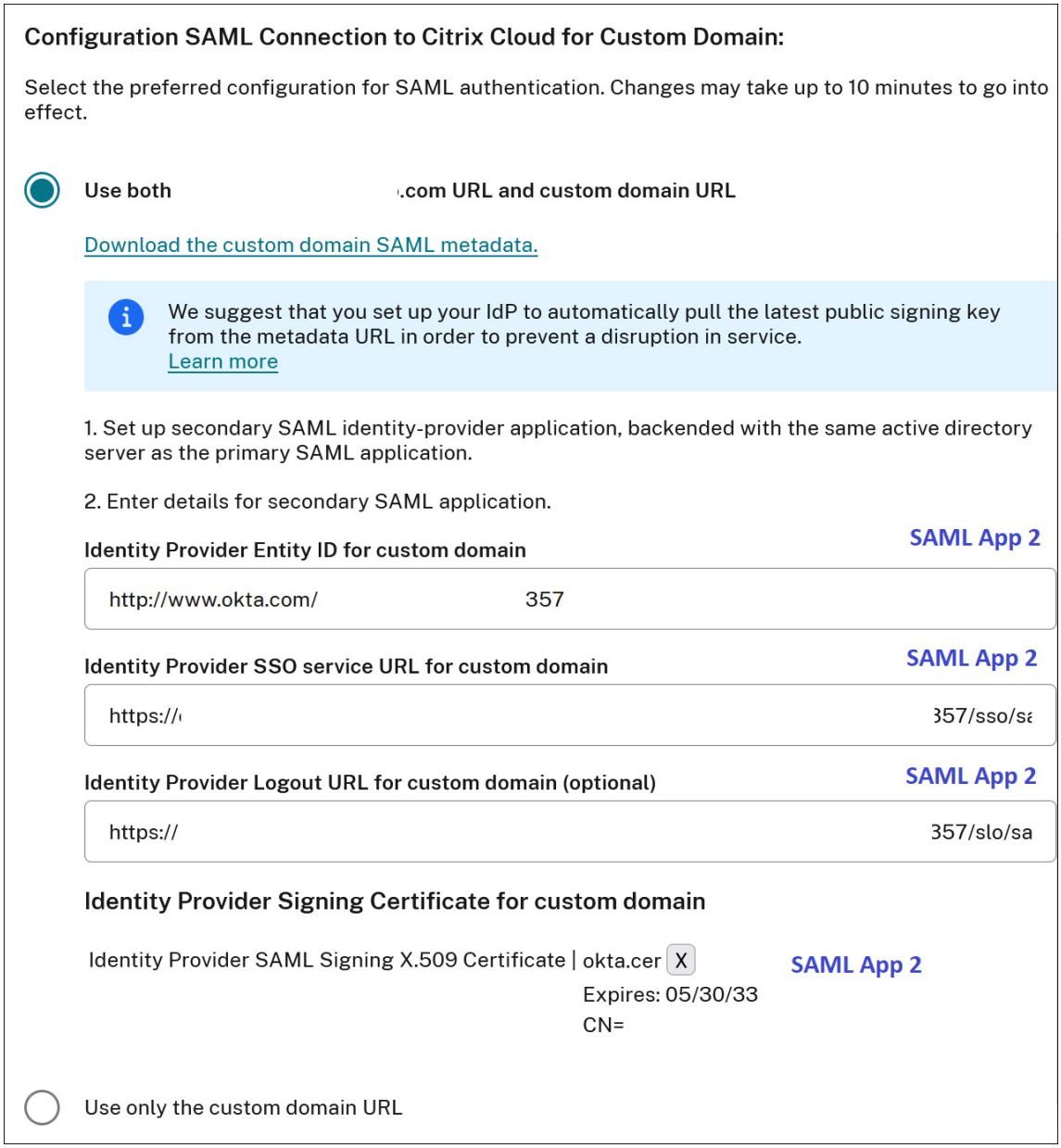
   

4. Dans la deuxième application SAML, configurez les points de terminaison du fournisseur de services suivants. Utilisez votre domaine personnalisé Workspace uniquement pour les points de terminaison Assertion Consumer Service et Logout.

   - Entity ID : `https://saml.cloud.com`
   - Assertion Consumer Service : `https://workspaces.mycompany.com/saml/acs`
   - Logout : `https://workspaces.mycompany.com/saml/logout/callback`

   L'exemple suivant montre la configuration du point de terminaison dans la console Okta. Notez que le champ **Audience Restriction** contient la valeur Entity ID.

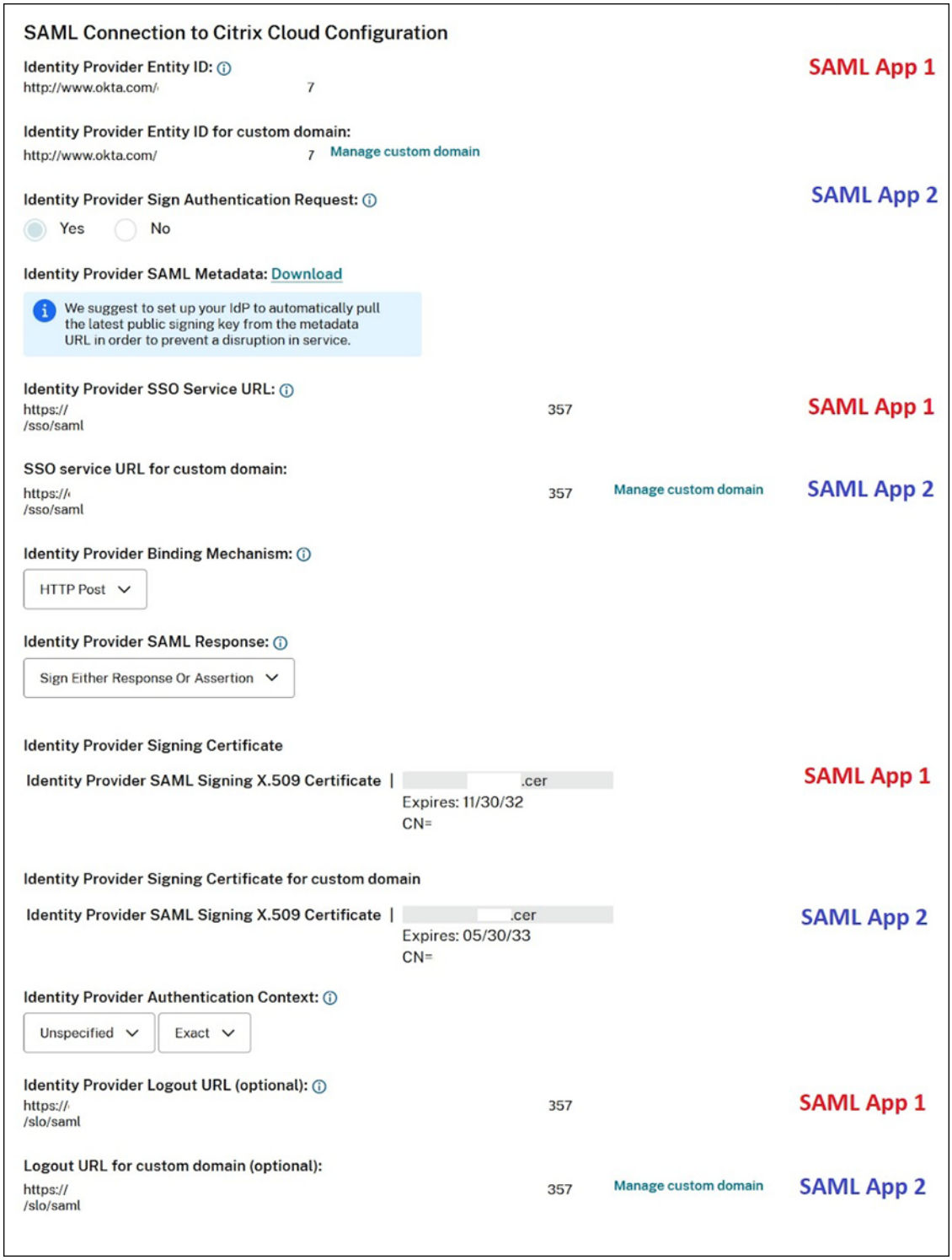
5. Téléchargez les certificats de signature SAML pour les deux applications SAML. Vous les téléchargerez sur Citrix Cloud lors d'une étape ultérieure.
6. Dans la console de gestion Citrix Cloud, configurez une connexion SAML :
    a) Dans le menu Citrix Cloud, sélectionnez **Gestion des identités et des accès**.
    b) Dans l'onglet **Authentification**, localisez **SAML 2.0**, cliquez sur le bouton des points de suspension et sélectionnez **Connecter**.
    c) Sur la page **Configurer SAML**, entrez les détails de la première application SAML que vous avez créée à l'étape 2.
7. Configurez Citrix Workspace pour utiliser la nouvelle connexion SAML :
    a) Dans le menu Citrix Cloud, sélectionnez **Configuration de l'espace de travail**.
    b) Dans l'onglet **Authentification**, sélectionnez **SAML 2.0**.
8. Dans l'onglet **Accès**, dans **URL d'espace de travail personnalisée**, sélectionnez **Modifier**.
9. Sur la page **Configurer pour SAML**, sélectionnez **Utiliser à la fois l'URL customer.cloud.com et l'URL du domaine personnalisé**.
10. Entrez les informations suivantes :
    - Sous **ID d'entité du fournisseur d'identité pour le domaine personnalisé (facultatif)**, entrez l'ID d'entité de la deuxième application SAML que vous avez créée à l'étape 2.
    - Sous **URL du service SSO pour le domaine personnalisé**, entrez l'URL SSO de la deuxième application SAML.
    - Sous **URL de déconnexion du domaine personnalisé**, entrez l'URL SLO de la deuxième application SAML.
    - Sous **Certificat de signature du fournisseur d'identité pour le domaine personnalisé**, chargez le certificat de signature SAML depuis la deuxième application SAML.



11. Sélectionnez **Enregistrer** pour enregistrer vos modifications.

Afficher les détails de la connexion SAML

Une fois la configuration effectuée, accédez à **Gestion des identités et des accès > Authentification**. Dans **SAML 2.0**, sélectionnez **Sélectionner le fournisseur SAML > Afficher** dans le menu de points de suspension. La page de configuration SAML affiche des paires de points de terminaison SAML configurés pour l'ID d'entité, l'URL SSO et l'URL de déconnexion.



Tous les autres paramètres de configuration SAML s'appliquent à la fois à la première et à la deuxième application SAML que vous avez créées.

Vérifier les connexions à Citrix Workspace

Pour vérifier le comportement de connexion et de déconnexion que vous avez configuré, effectuez les tests suivants :

- Connectez-vous à Citrix Workspace à l'aide de l'URL de votre espace de travail (`https://mycompany.cloud.com`) et de votre fournisseur SAML.
- Connectez-vous à Citrix Workspace à l'aide de votre domaine personnalisé Workspace (`https://workspace.mycompany.com`) et de votre fournisseur SAML.
- Connectez-vous à Citrix Cloud à l'aide de votre URL de connexion unique (`https://citrix.cloud.com/go/mycompany`) et de votre fournisseur SAML.

Configurer Okta en tant que fournisseur SAML pour l'authentification de l'espace de travail

March 11, 2024

Author:
Mark Dear

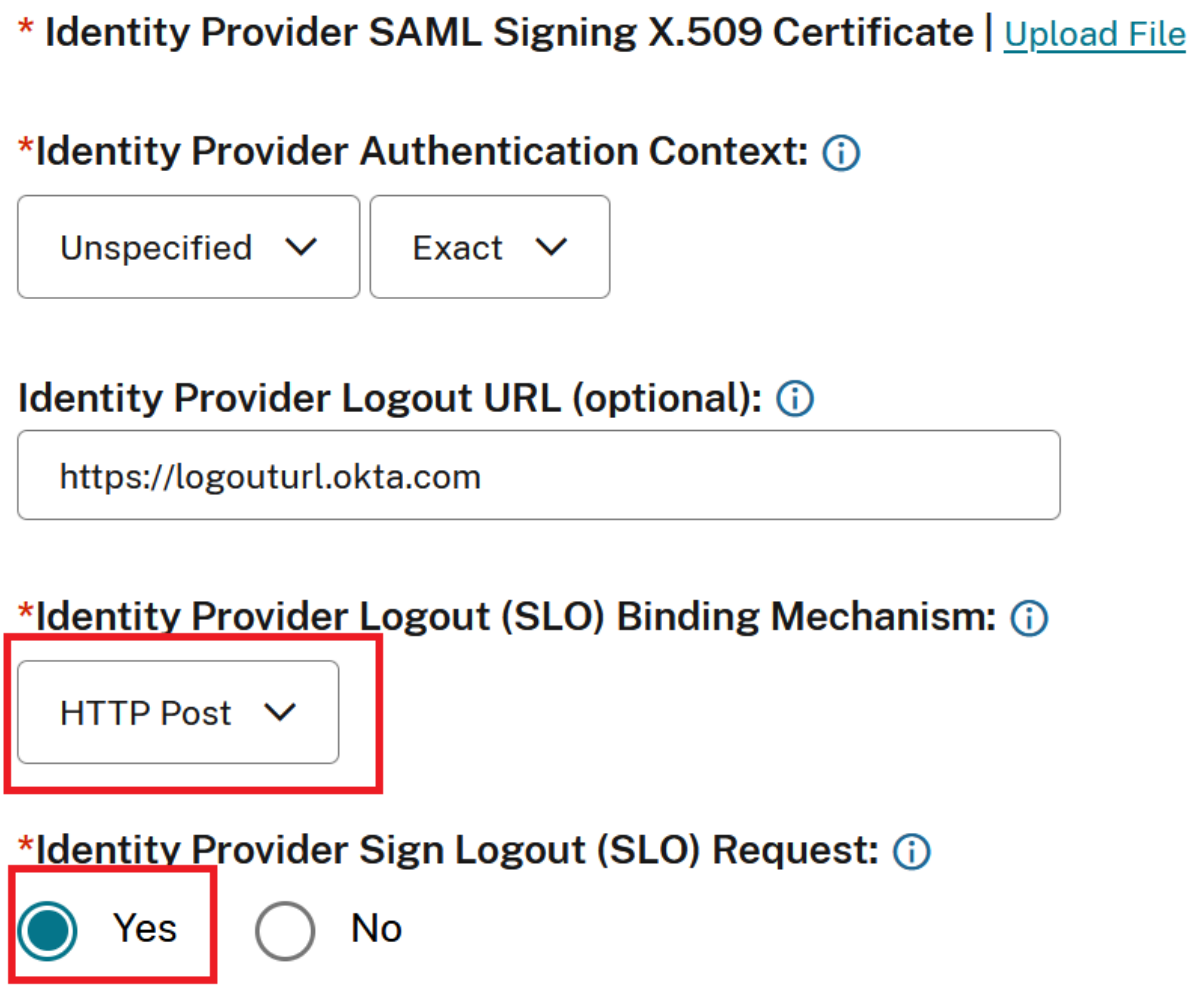
Cet article décrit les étapes requises pour configurer une application Okta SAML et une connexion entre Citrix Cloud et votre fournisseur SAML. Certaines de ces étapes décrivent les actions que vous effectuez dans la console d'administration de votre fournisseur SAML.

Logiciels requis

Avant d'effectuer les tâches décrites dans cet article, assurez-vous de remplir les conditions préalables suivantes :

- Le support Citrix a activé la fonctionnalité **SendNameIDPolicyInSAMLRequest** dans Citrix Cloud. Cette fonctionnalité est activée sur demande. Pour plus d'informations sur ces fonctionnalités, consultez la section Fonctionnalités cloud requises pour SAML avec Okta.
- Vous disposez d'une organisation Okta qui utilise l'un des domaines Okta suivants :
  - okta.com
  - okta-eu.com
  - oktapreview.com
- Vous avez synchronisé votre domaine Active Directory (AD) avec votre organisation Okta.
- Les demandes d'authentification par signature, **Sign Authentication Request**, sont activées dans votre organisation Okta.

- La **déconnexion unique (SLO) du fournisseur d'identité** est configurée dans les applications Citrix Cloud et Okta SAML. Lorsque la déconnexion unique (SLO) est configurée et que l'utilisateur se déconnecte de Citrix Workspace, il se déconnecte également d'Okta et de tous les autres fournisseurs de services qui partagent l'application Okta SAML.
- L'option **Demande de déconnexion signée (SLO) du fournisseur d'identité** est activée dans Citrix Cloud.
- L'option **Mécanisme de liaison de déconnexion (SLO) du fournisseur d'identité** est HTTP-Post dans Citrix Cloud.



Fonctionnalités cloud requises pour SAML avec Okta

Avant d'effectuer les tâches décrites dans cet article, vous devez contacter le support Citrix pour activer la fonctionnalité **SendNameIDPolicyInSAMLRequest**. Cette fonctionnalité permet à Citrix Cloud de définir la stratégie **NameID** sur **Non spécifié** dans la demande SAML adressée à votre fournisseur SAML. Cette fonctionnalité est activée pour une utilisation avec Okta uniquement.

Vous pouvez demander ces fonctionnalités en vous connectant à votre compte Citrix et en ouvrant un ticket sur le site Web de support Citrix.

Exigences

Cet article inclut une tâche dans laquelle vous créez une application SAML dans la console d'administration Okta. Cette application requiert un certificat de signature SAML pour votre région Citrix Cloud.

> **Important :**
>
> Le certificat de signature doit être encodé au format PEM. Citrix Cloud n'accepte pas la signature de certificats dans d'autres formats de codage.

Vous pouvez extraire ce certificat des métadonnées SAML Citrix Cloud de votre région à l'aide d'un outil d'extraction tel que celui disponible sur https://www.rcfed.com/SAMLWSFed/MetadataCertificateExtract. Citrix recommande d'acquérir le certificat SAML Citrix Cloud au préalable afin de pouvoir le fournir en cas de besoin.

Les étapes de cette section décrivent comment obtenir le certificat de signature à l'aide de l'outil d'extraction disponible sur https://www.rcfed.com/SAMLWSFed/MetadataCertificateExtract.

Pour obtenir les métadonnées Citrix Cloud de votre région, procédez comme suit :

1. Dans l'outil d'extraction de votre choix, entrez l'URL des métadonnées correspondant à votre région Citrix Cloud :
   - Pour les régions de l'Union européenne, des États-Unis et de l'Asie-Pacifique Sud, entrez `https://saml.cloud.com/saml/metadata`.
   - Pour la région du Japon, entrez `https://saml.citrixcloud.jp/saml/metadata`.
   - Pour la région Citrix Cloud Government, entrez `https://saml.cloud.us/saml/metadata`.
2. Cliquez sur **Load**. Le certificat extrait apparaît sous l'URL que vous avez saisie.
3. Cliquez sur **Download** pour télécharger le certificat au format PEM.

Synchroniser les comptes avec l'agent Okta AD

Pour utiliser Okta comme fournisseur SAML, vous devez d'abord intégrer votre domaine 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, consultez la page Get started with Active Directory integration sur le site Web Okta.

Vous importez ensuite vos utilisateurs et groupes AD dans Okta. Lors de l'importation, incluez les valeurs suivantes associées à vos comptes AD :

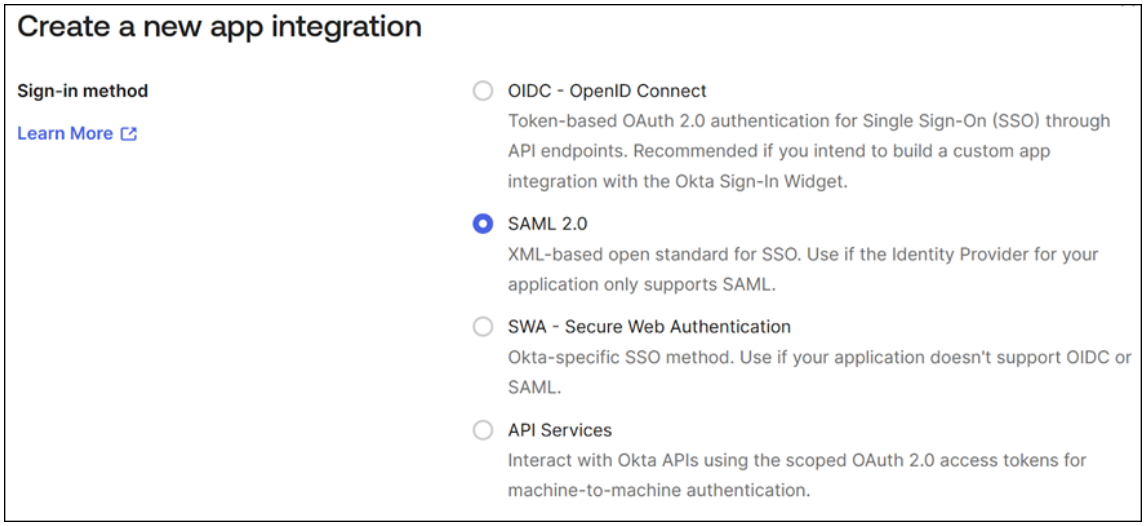
- E-mail
- SID
- UPN
- OID

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

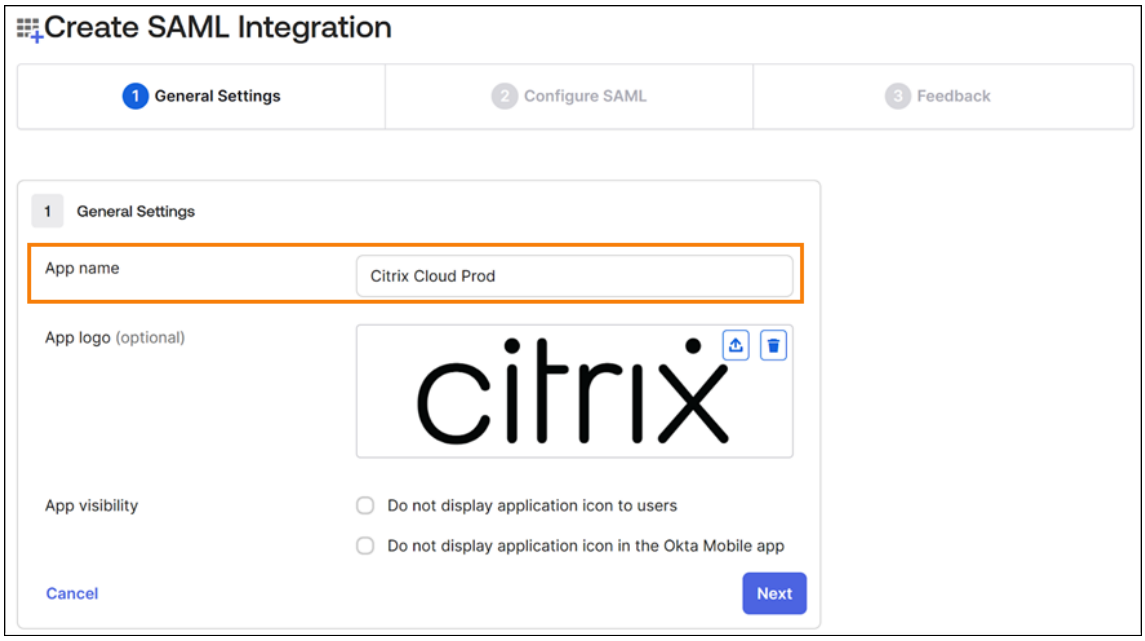
1. Installez et configurez l'agent Okta AD. Pour obtenir des instructions complètes, consultez les articles suivants sur le site Web Okta :
   - Installer l'agent Okta Active Directory
   - Configurer les paramètres d'importation et de compte Active Directory
   - Configurer les paramètres de provisioning 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 et les instructions d'importation Okta, consultez la page Manage Active Directory users and groups sur le site Web d'Okta.

Configurer une application Okta SAML pour l'authentification de l'espace de travail

1. Connectez-vous à votre organisation Okta à l'aide d'un compte administrateur autorisé à ajouter et à configurer des applications SAML.
2. Dans la console d'administration, sélectionnez **Applications > Applications > Create App Integration**, puis sélectionnez **SAML 2.0**. Sélectionnez **Suivant**.



3. Sous **App Name**, entrez un nom convivial pour l'application. Sélectionnez **Suivant**.



4. Dans la section **SAML Settings**, configurez la connexion Citrix Cloud Service Provider (SP) :

   a) Sous **Single sign-on URL**, entrez l'URL qui correspond à la région Citrix Cloud pour votre client Citrix Cloud :

   - Si votre ID client se trouve dans les régions de l'Union européenne, des États-Unis et de l'Asie-Pacifique Sud, entrez `https://saml.cloud.com/saml/acs`.
   - Si votre ID client se trouve dans la région du Japon, entrez `https://saml.citrixcloud.jp/saml/acs`.
   - Si votre ID client se trouve dans la région Citrix Cloud Government, entrez `https://saml.cloud.us/saml/acs`.

   b) Sélectionnez **Use this for Recipient and Destination URL**.

   c) Sous **Audience URI (SP Entity ID)**, entrez l'URL qui correspond à la région Citrix Cloud pour votre client Citrix Cloud :

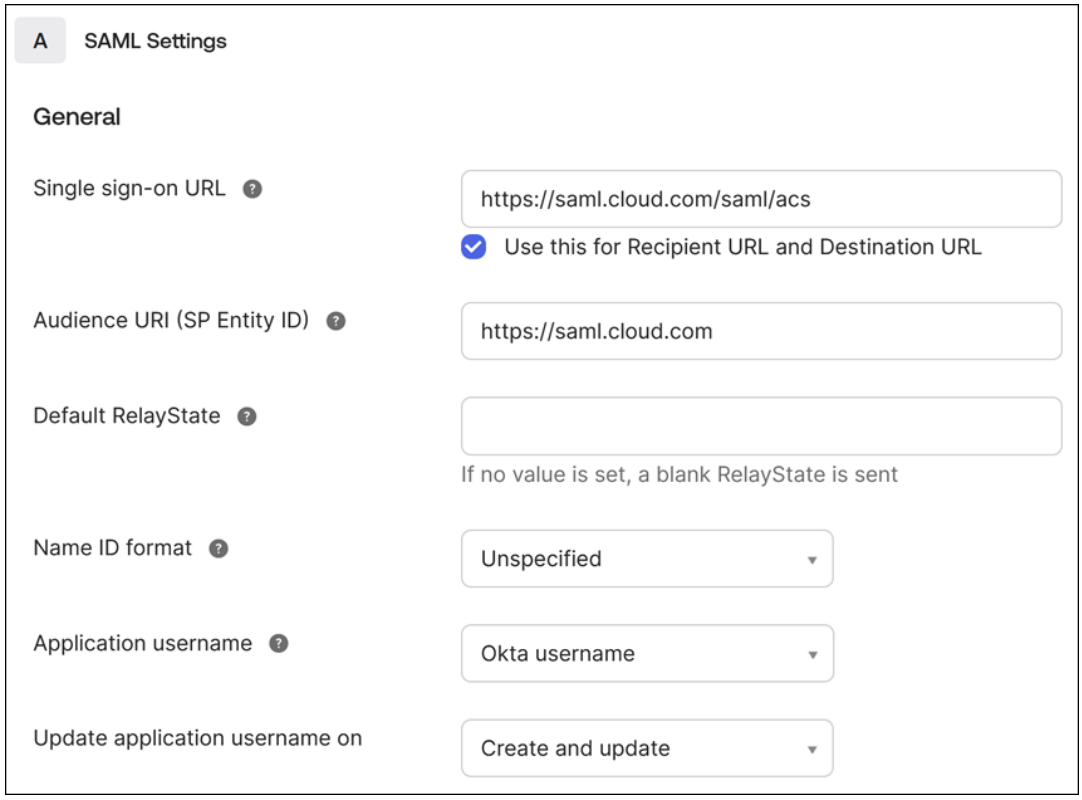
   - Si votre ID client se trouve dans les régions de l'Union européenne, des États-Unis et de l'Asie-Pacifique Sud, entrez `https://saml.cloud.com`.
   - Si votre ID client se trouve dans la région du Japon, entrez `https://saml.citrixcloud.jp`.
   - Si votre ID client se trouve dans la région Citrix Cloud Government, entrez `https://saml.cloud.us`.

   d) Sous **Name ID Format**, sélectionnez **Unspecified**. La stratégie NameID que Citrix Cloud envoie dans la requête SAML doit correspondre au format NameID spécifié dans l'application Okta SAML. Si ces éléments ne correspondent pas, l'activation de la demande d'

authentification par signature, **Sign Authentication Request**, entraîne une erreur de la part d'Okta.

e) Sous **Application username**, sélectionnez **Okta username**.

À titre d'exemple, l'image suivante illustre la configuration correcte pour les régions des États-Unis, de l'UE et de l'Asie-Pacifique Sud :



> **Important :**
>
> Le paramètre **Name ID** doit être défini sur **Unspecified**. L'utilisation d'une valeur différente pour ce paramètre entraîne l'échec de la connexion SAML.

f) Cliquez sur **Show Advanced Settings** et configurez les paramètres suivants :

- Sous **Response**, sélectionnez **Signed**.
- Sous **Assertion Signature**, sélectionnez **Signed**.
- Sous **Signature Algorithm**, sélectionnez **RSA-SHA256**.
- Sous **Assertion Encryption**, sélectionnez **Unencrypted**.

g) Sous **Signature Certificate**, chargez le certificat de signature SAML pour votre région Citrix Cloud au format PEM. Pour obtenir des instructions sur l'acquisition du certificat de signature SAML, reportez-vous à la section Exigences de cet article.

h) Sous **Enable Single Logout**, sélectionnez **Allow application to initiate Single Logout**.

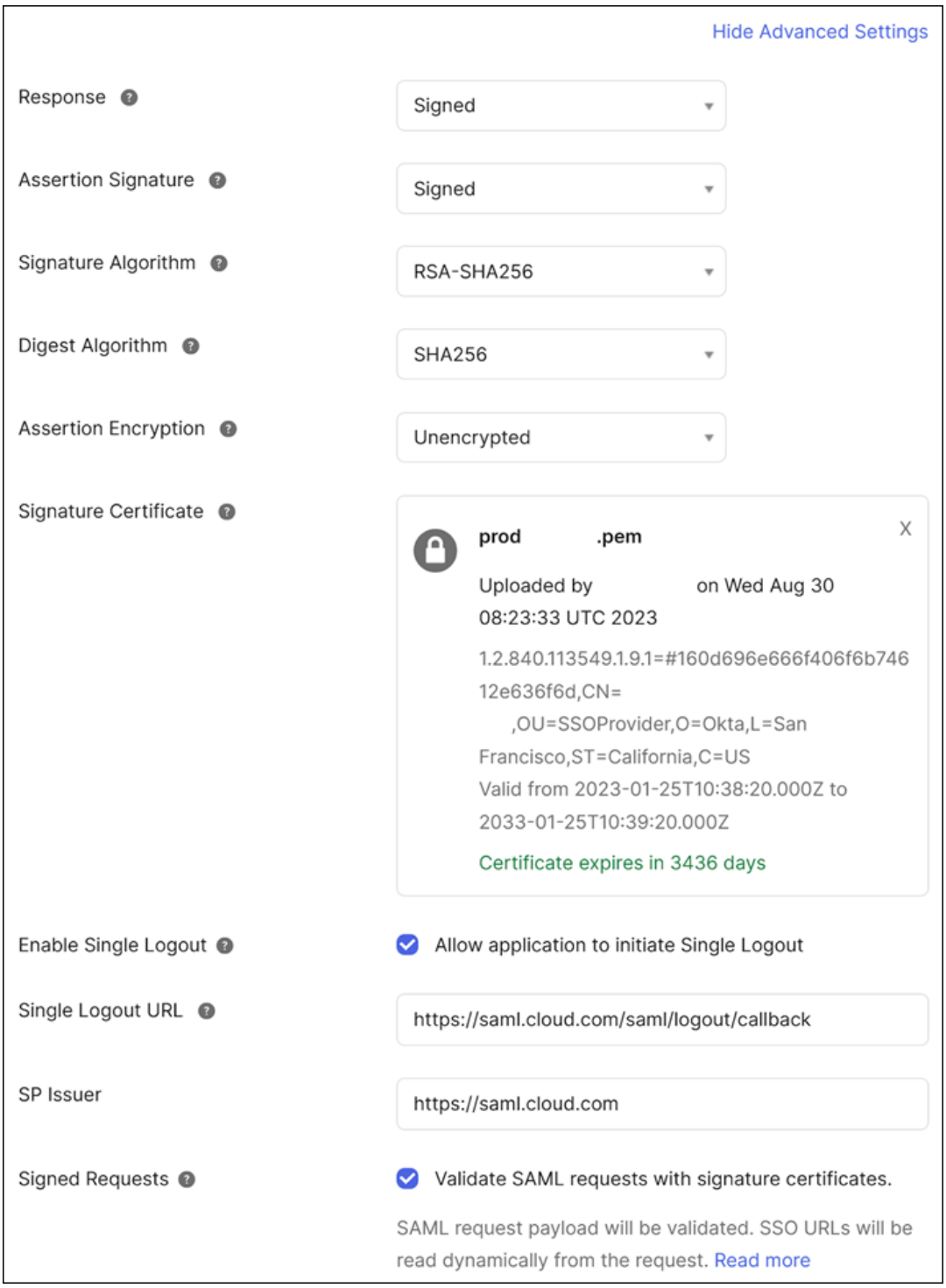
i) Sous **Single Logout URL**, entrez l'URL qui correspond à votre région Citrix Cloud :

- Pour les régions de l'Union européenne, des États-Unis et de l'Asie-Pacifique Sud, entrez `https://saml.cloud.com/saml/logout/callback`.
- Pour la région du Japon, entrez `https://saml.citrixcloud.jp/saml/saml/logout/callback`.
- Pour Citrix Cloud Government, entrez `https://saml.cloud.us/saml/logout/callback`.

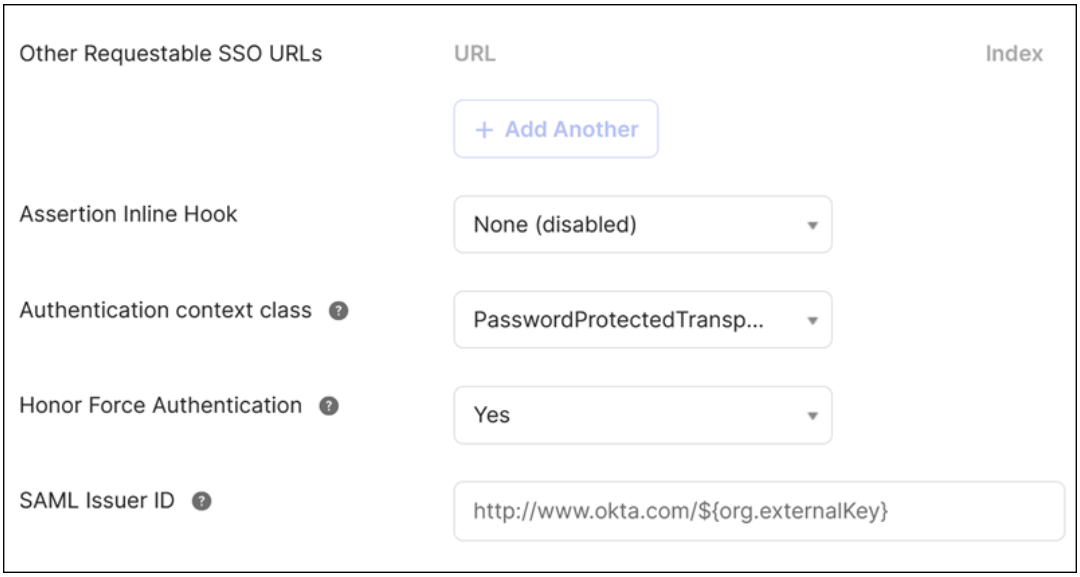
j) Sous **SP Issuer**, entrez la valeur que vous avez saisie précédemment sous **Audience URI (SP Entity ID)** (étape 4c de cette tâche).

k) Sous **Signed Requests**, sélectionnez **Validate SAML requests with signature certificates**.

L'image suivante illustre la configuration correcte pour les régions des États-Unis, de l'UE et de l'Asie-Pacifique Sud :

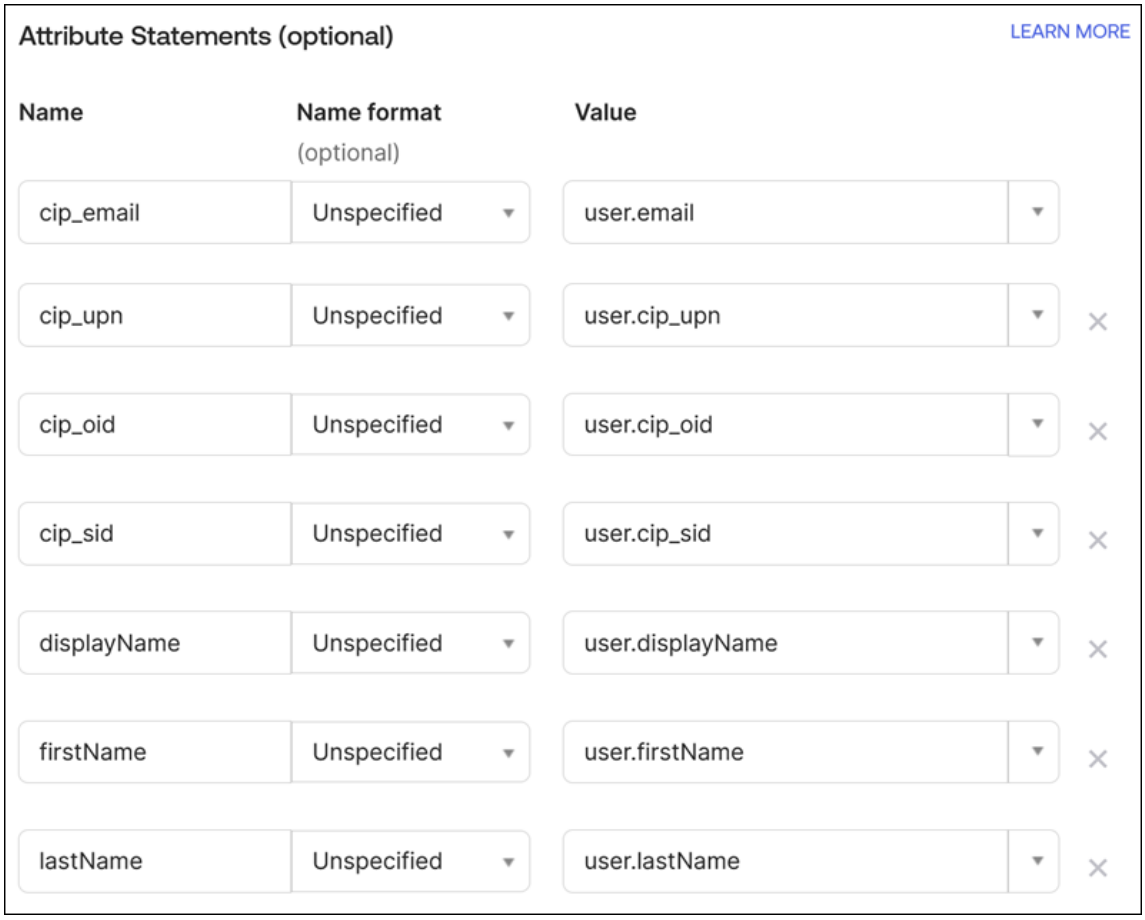


l) Pour tous les paramètres avancés restants, utilisez les valeurs par défaut.

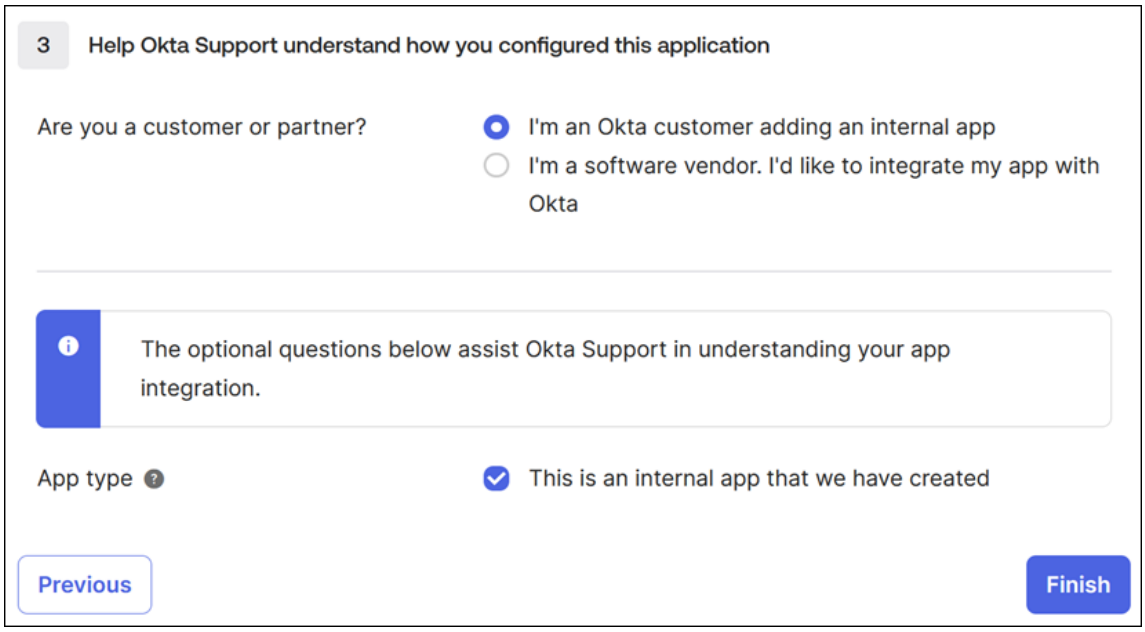


5. Sous **Attribute Statements (optional)**, entrez les valeurs pour les paramètres **Name**, **Name format** et **Value**, comme indiqué dans le tableau suivant :

Nom	Name format	Valeur
cip_email	Non spécifié	user.email
cip_upn	Non spécifié	user.cip_upn
cip_oid	Non spécifié	user.cip_oid
cip_sid	Non spécifié	user.cip_sid
displayName	Non spécifié	user.displayName
firstName	Non spécifié	user.firstName
lastName	Non spécifié	user.lastName



6. Sélectionnez **Suivant**. L'instruction de configuration Okta apparaît.



7. Sous **Are you a customer or partner?**, sélectionnez **I'm an Okta customer adding an internal app**.

8. Sous **App type**, sélectionnez **This is an internal app that we have created**.
9. Sélectionnez **Finish** pour enregistrer votre configuration. La page de profil de votre application SAML apparaît et affiche le contenu de l'onglet **Sign On**.

Après la configuration, sélectionnez l'onglet **Assignments** et attribuez des utilisateurs et des groupes à l'application SAML.

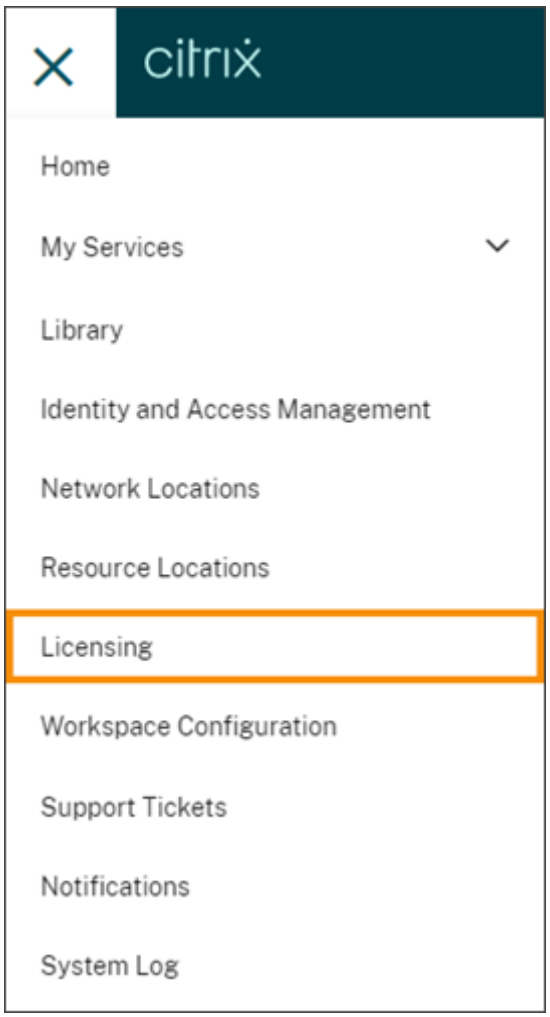
Système de licences pour Citrix Cloud

October 4, 2023

Citrix Cloud assure la surveillance des licences et de l'utilisation de certains services cloud. De plus, la surveillance des licences et de l'utilisation est disponible pour les déploiements locaux où le serveur de licences Citrix est enregistré auprès de Citrix Cloud.

Système de licences pour les clients d'entreprise

Les clients d'entreprise peuvent surveiller les attributions de licences et l'utilisation des services cloud pris en charge en sélectionnant **Système de licences** dans le menu Citrix Cloud.



Pour plus d'informations sur la surveillance des licences d'entreprise et de l'utilisation des services cloud, consultez la section Surveiller les licences et l'utilisation active pour les services cloud.

Système de licences pour les déploiements locaux

Les clients d'entreprise disposant d'un déploiement local de Citrix Virtual Apps and Desktops peuvent utiliser Citrix Cloud pour rester au courant des informations de licences et d'utilisation des modèles de licences utilisateur/appareil et simultanées. En enregistrant le serveur de licences Citrix auprès de Citrix Cloud, les clients peuvent utiliser la page **Déploiements sous licence** dans Citrix Cloud pour effectuer les tâches suivantes :

- Surveiller l'état des rapports des serveurs de licences enregistrés
- Afficher les attributions de licences et les tendances d'utilisation des déploiements utilisant le modèle de licence utilisateur/appareil
- Afficher les tendances d'utilisation maximale des licences pour les déploiements utilisant le modèle de licences simultanées

Pour plus d'informations sur la surveillance des licences et de l'utilisation pour les déploiements Virtual Apps and Desktops locaux, consultez la section Surveiller les licences et l'utilisation sur les déploiements locaux.

Système de licences pour les partenaires Citrix Service Provider (CSP)

Les partenaires Citrix Service Provider peuvent utiliser les outils suivants pour comprendre et produire des rapports sur les licences et l'utilisation des produits :

- L'outil License Usage Insights est un service gratuit dans Citrix Cloud qui collecte et agrège les informations d'utilisation des produits sur les clients mono-locataires et multi-locataires. Pour plus d'informations, consultez Système de licences pour les partenaires Citrix Service Provider.
- La fonctionnalité Système de licences de Citrix Cloud permet aux clients des partenaires CSP de surveiller leurs licences et leur utilisation pour les produits Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) pris en charge. Les partenaires Citrix Service Provider peuvent également se connecter au compte Citrix Cloud de leur client pour afficher et exporter ces informations. Pour plus d'informations, consultez les articles suivants :
  - Surveillance des licences client et de l'utilisation pour Citrix DaaS
  - Surveillance des licences client et de l'utilisation pour Citrix DaaS Standard pour Azure

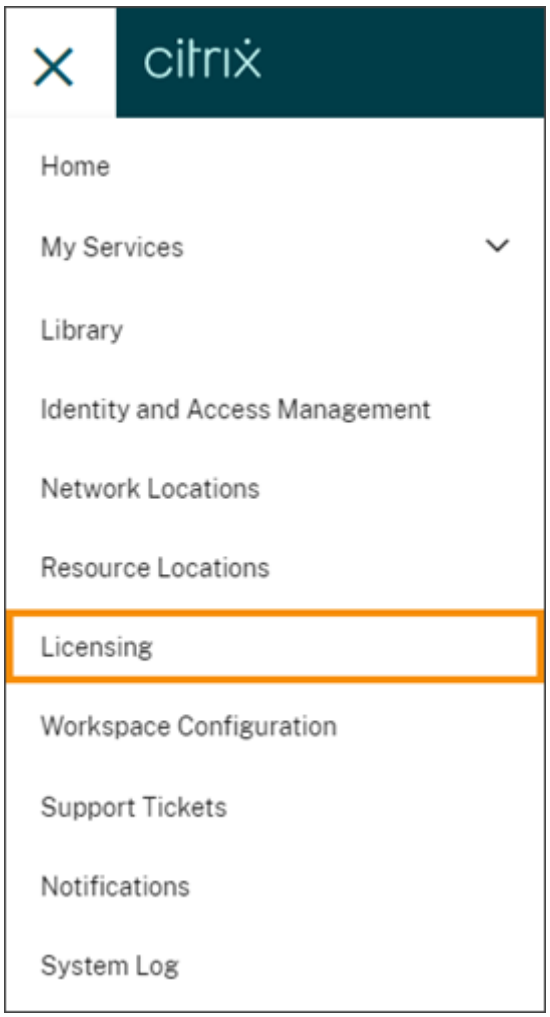
Surveiller les licences et l'utilisation active pour les services cloud

October 4, 2023

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 Citrix DaaS (utilisateur/appareil)
- Surveiller les licences et l'utilisation maximale de Citrix DaaS et Citrix DaaS Standard pour Azure (simultané)
- Surveiller les licences et l'utilisation active de Citrix DaaS Standard pour Azure (utilisateur/appareil uniquement)
- Surveiller les licences et l'utilisation active d'Endpoint Management
- Surveiller l'utilisation de la bande passante pour Gateway Service
- Surveillez les licences et l'utilisation pour Secure Private Access

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 :

- Citrix DaaS (modèles de licences utilisateur/appareil et simultanés) - anciennement Citrix Virtual Apps and Desktops Service
- Citrix DaaS Standard pour Azure (modèle de licences utilisateur/appareil) - anciennement Citrix Virtual Apps and Desktops Standard pour Azure
- Endpoint Management
- Gateway
- Secure Private Access (anciennement Secure Workspace Access)

Licences multitypes pour Citrix DaaS

Le système de licences Citrix Cloud prend en charge les licences multitypes pour Citrix DaaS. Si les deux modèles de licences, utilisateur/appareil et simultanées, sont introduits dans un seul compte Citrix Cloud, Citrix Cloud affiche l'utilisation des licences sous chaque mode de licence dans la page de la console de licences.

Citrix recommande de configurer des licences multi-types au niveau du site et du groupe de mise à disposition avant de consulter la page Système de licences. Dans le cas contraire, les informations correctes risquent de ne pas apparaître. Pour obtenir des instructions, consultez la section Licences multi-types dans la documentation de Citrix DaaS.

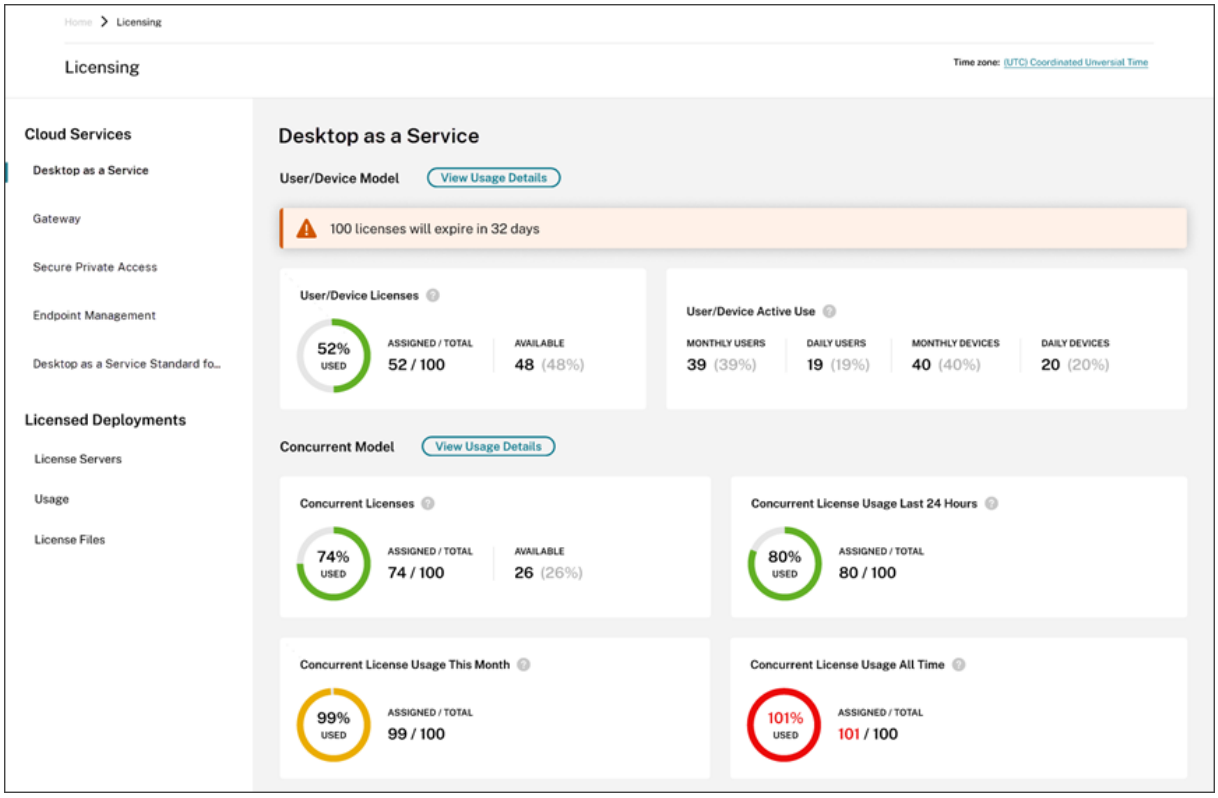
Si la page de la console Système de licences n'affiche pas l'utilisation correcte des licences multi-types après une utilisation réussie des méthodes d'installation de Web Studio ou PowerShell, vous disposez des options suivantes :

- Attendez 30 jours et libérez toutes les licences non utilisées.
- Contactez le service client Citrix.

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



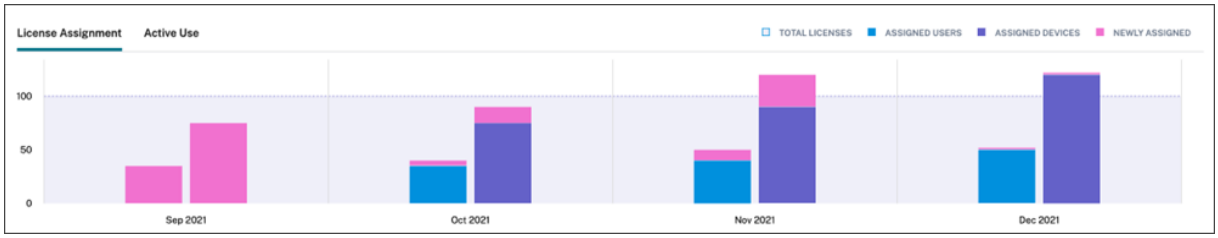
L'écran de résumé de l'option Système de licences fournit une vue d'ensemble des informations suivantes pour chaque service pris en charge :

- 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 Citrix DaaS (par exemple, en utilisant à la fois les modèles Utilisateur/appareil et Utilisateurs simultanés) ?** Oui. Consultez la section Licences multi-types dans cet article pour plus d'informations.
- **Les licences multi-éditions sont-elles prises en charge pour Citrix DaaS ? 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 Citrix DaaS ne peut détenir de licence que pour une seule édition. Si vous souhaitez utiliser plusieurs instances Citrix DaaS sur le même compte Citrix Cloud, elles doivent être de la même 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 licences recherche le caractère unique des appareils lorsque les sessions sont lancées. Le rapport de monitoring ne tient pas compte des appareils uniques.
- **Après avoir migré les utilisateurs vers une nouvelle instance de service cloud (par exemple, j'ai modifié le nom de domaine de mon organisation), pourquoi mes licences en cours d'utilisation sont-elles comptées deux fois pour les mêmes utilisateurs ?-* Citrix Cloud utilise le nom d'utilisateur principal (UPN) pour compter les utilisateurs uniques. Si un utilisateur a accédé au service cloud avant et après la migration, Citrix Cloud capture deux noms d'utilisateur principal uniques pour l'utilisateur, chacun avec un nom de domaine différent. Par conséquent, Citrix Cloud compte deux fois le même utilisateur. Vous pouvez libérer l'ancienne attribution de licence après 30 jours, en supposant que l'utilisateur n'accède pas au service sous l'ancien nom de domaine. Citrix n'empêche le lancement d'aucun service en cas de dépassement du nombre de licences cloud que vous achetées.
- **Pourquoi des licences dupliquées sont-elles affichées pour le même utilisateur ou appareil ?-* Cela est dû à la conception de l'application Workspace pour HTML5 et de l'application Workspace installée localement. Les lancements via l'application Workspace pour HTML5 consomment une licence utilisateur/machine. De même, les lancements via l'application Workspace installée localement consomment une licence utilisateur/machine. Ainsi, si un utilisateur lance des applications via l'application Workspace pour HTML5, puis via une version installée localement de l'application Workspace ultérieurement, Citrix Cloud indique que l'utilisateur a consommé deux licences. Ce comportement n'affecte pas la connectivité des utilisateurs, mais peut entraîner une augmentation artificielle des rapports d'utilisation des licences des machines dans la console du système de licences. Citrix n'empêche le lancement d'aucun service en cas de

dépassement du nombre de licences cloud que vous achetées.

Surveiller les licences et l'utilisation active de Citrix DaaS (utilisateur/appareil)

November 6, 2023

Cet article explique comment gérer les attributions de licences de service cloud et surveiller l'utilisation active à l'aide de la console Système de licences de Citrix Cloud.

Si vous avez acheté Citrix Azure Consumption Fund pour l'utiliser avec votre déploiement de service, consultez la section Surveiller la consommation des ressources Citrix Managed Azure pour Citrix DaaS pour plus d'informations.

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.

Troncation du nom de domaine

Si vous hébergez plusieurs domaines et que des utilisateurs disposent de comptes similaires dans ces domaines (par exemple, `johnsmith@company.com` et `johnsmith@mycompany.com`), vous pouvez autoriser Citrix Cloud à ignorer le domaine du compte et à n'utiliser que le nom d'utilisateur du compte (par exemple, johnsmith). Ce processus est connu sous le nom de *troncation du nom de domaine*. Par défaut, la troncation du nom de domaine est désactivée.

Lorsque la troncation du nom de domaine est activée, le calcul des utilisateurs uniques par Citrix Cloud change. Au lieu de compter `johnsmith@company.com` et `johnsmith@mycompany.com` en tant que deux utilisateurs uniques, Citrix Cloud compte uniquement johnsmith en tant qu'utilisateur unique. Ce changement de calcul affecte les données de licence suivantes :

- Attribution de licence
- Utilisation active
- Tendances d'utilisation des licences au fil du temps
- Licences pouvant être libérées

Ces modifications des données de licence sont également prises en compte lorsque vous exportez des données vers un fichier CSV depuis la console de licences.

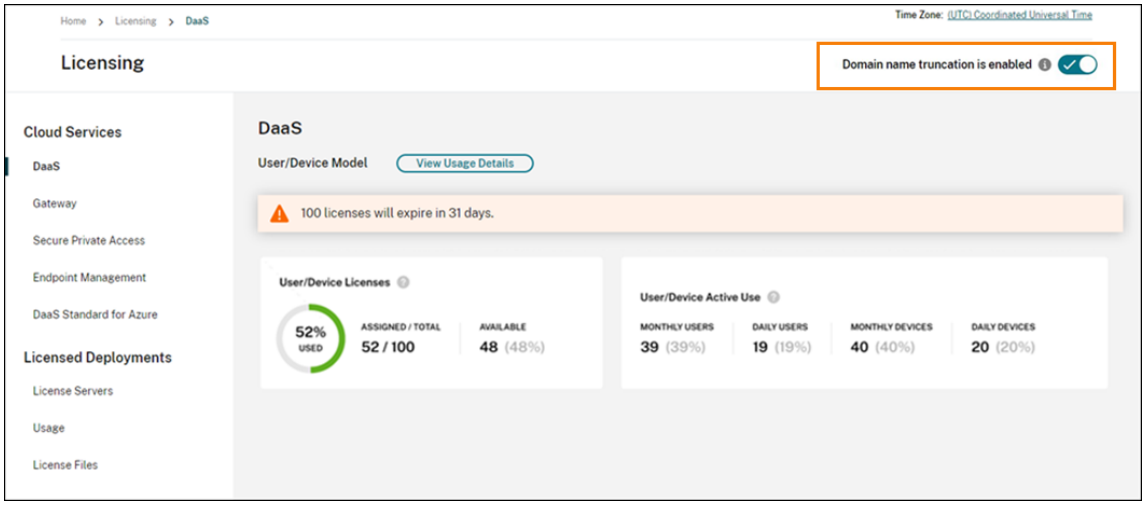
> **Remarque :**
>
> Si vous hébergez plusieurs domaines avec des comptes similaires dont le nom d'utilisateur est légèrement différent (par exemple, un utilisateur individuel disposant des comptes `johnsmith@company.com` et `jsmith@newcompany.com`), la troncation du nom de domaine n'a aucun effet sur les calculs de Citrix Cloud. Citrix Cloud considère toujours johnsmith et jsmith comme des utilisateurs uniques, même s'ils sont associés à la même personne.

Activer ou désactiver la troncation du nom de domaine

Par défaut, la troncation du nom de domaine est désactivée. La troncation du nom de domaine a un effet sur les données d'utilisation des licences utilisateur/appareil à partir du moment où vous activez ou désactivez la fonctionnalité. Par exemple, si vous activez la troncation des noms de domaine au cours d'un mois donné, les données enregistrées par Citrix Cloud au cours de ce mois sont affectées. Toutefois, les données historiques des mois précédents, lorsque la fonctionnalité était désactivée, restent inchangées. De même, si vous désactivez la troncation du nom de domaine au cours d'un mois donné, les données enregistrées par Citrix Cloud au cours de ce mois sont affectées. Cependant, les données historiques des mois pendant lesquels la fonctionnalité a été activée restent intactes.

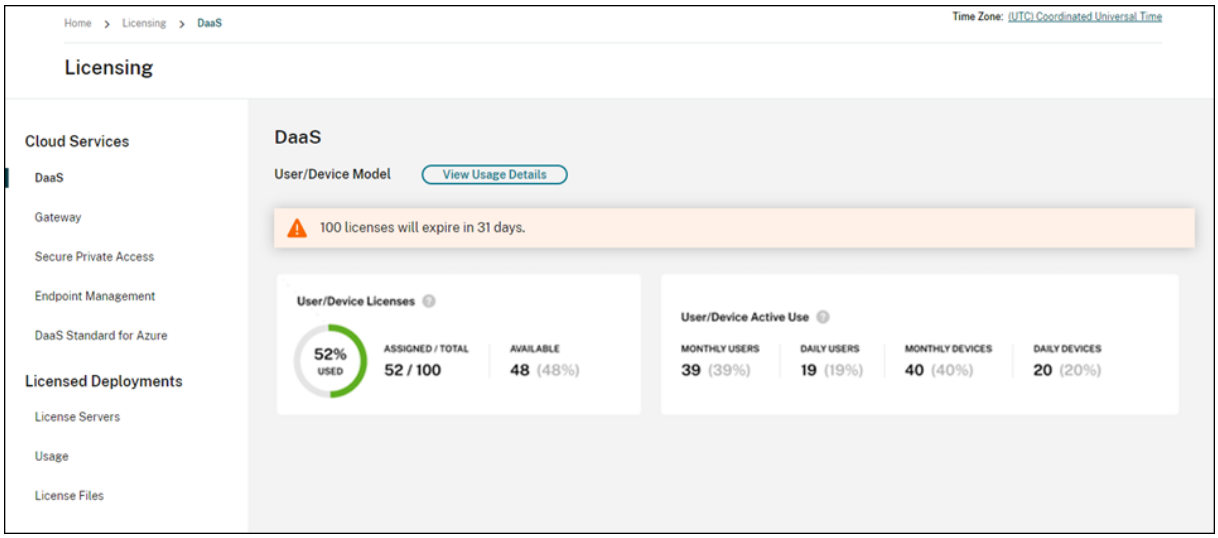
Pour activer ou désactiver la troncation du nom de domaine, procédez comme suit :

1. Cliquez sur le bouton situé en haut à droite de la console de gestion des licences.



2. Lorsque vous êtes invité à confirmer votre action, sélectionnez **Oui, je comprends**.

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.

  La quantité totale de licences achetées correspond à la somme des licences achetées pour les éditions Citrix DaaS qui utilisent le modèle de licence utilisateur/appareil.
- 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.
  - 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.
- 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 Citrix DaaS, Citrix Cloud compte le nombre d'utilisateurs uniques et d'appareils uniques qui ont utilisé le service. Pour mesurer les licences attribuées, Citrix Cloud utilise la valeur la moins élevée. Pour mesurer l'utilisation active, Citrix Cloud utilise chaque valeur comme quantité d'utilisateurs actifs et d'appareils actifs au cours d'une période donnée.

Exemple de calcul des licences attribuées

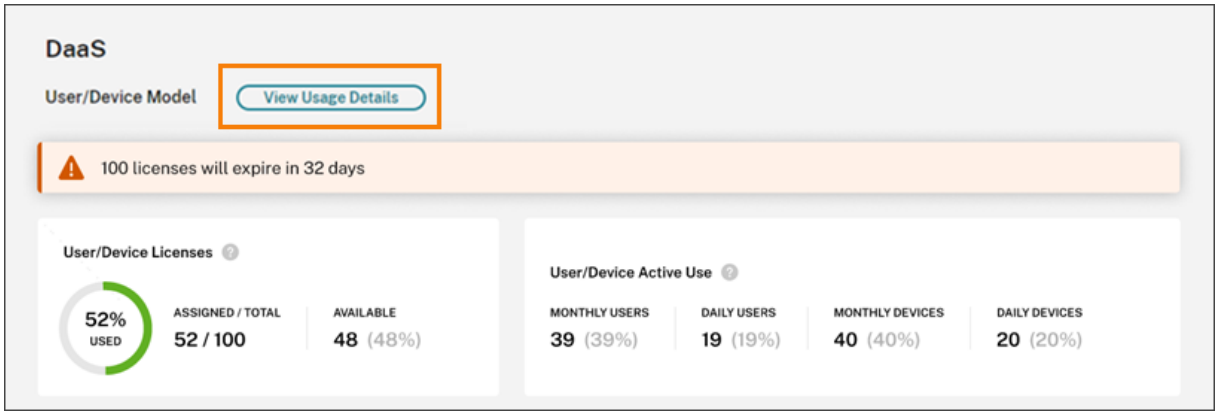
Si 100 utilisateurs uniques et 50 appareils uniques ont utilisé le service, Citrix Cloud utilise le nombre inférieur (50) pour déterminer le nombre de licences attribuées. Le pourcentage de licences utilisées et le nombre de licences disponibles sont basés sur ces 50 licences attribuées.

Exemple de calcul de l'utilisation active

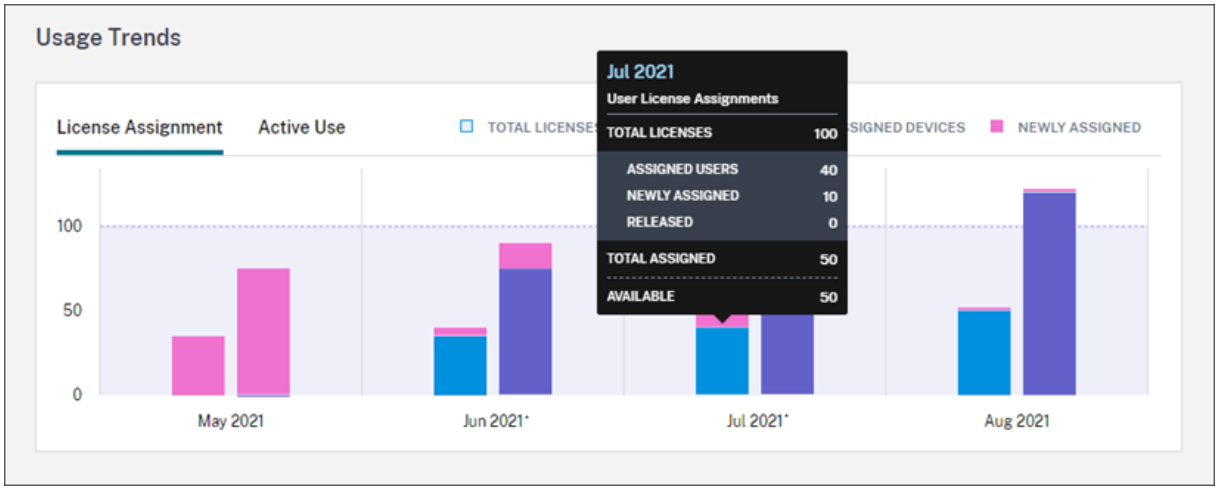
Si 10 utilisateurs uniques et 20 appareils uniques ont utilisé le service au cours des 30 derniers jours, Citrix Cloud détermine que l'utilisation active mensuelle comprend 10 utilisateurs actifs et 20 appareils actifs. De même, si 30 utilisateurs uniques et 15 appareils uniques ont été comptés au cours des dernières 24 heures, Citrix Cloud détermine que l'utilisation active quotidienne comprend 30 utilisateurs actifs et 15 appareils actifs.

Tendances d'utilisation

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



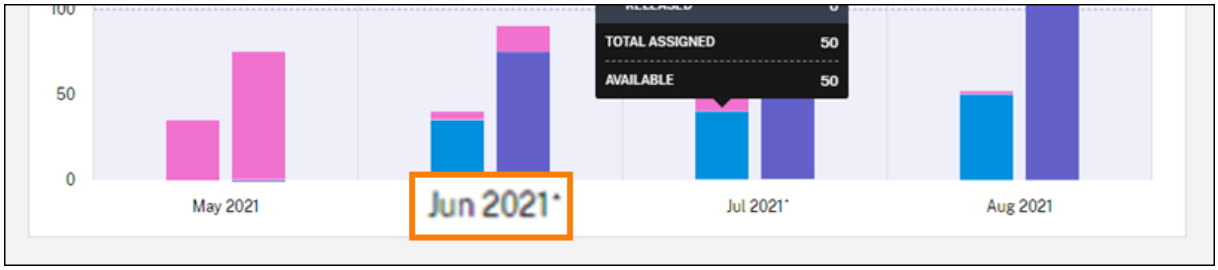
La section **Tendances d'utilisation** affiche cette répartition sous forme de graphique.



Sur le graphique **Attribution de licences**, vous pouvez pointer vers la barre d'un mois ou d'un jour spécifique pour afficher les informations suivantes :

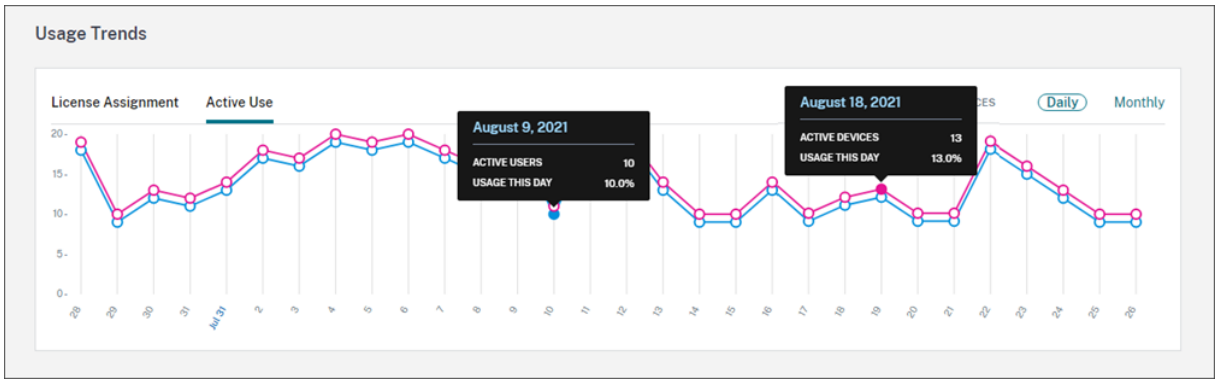
- **Nombre total de licences :** nombre total de licences achetées pour le service cloud pour toutes les prestations.
- **Utilisateurs attribués :** nombre cumulé de licences attribuées aux utilisateurs jusqu'au mois en cours.
- **Appareils attribués :** nombre cumulé de licences attribuées aux appareils 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 installée localement.
- **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.
- **Libérée :** nombre de licences éligibles qui ont été libérées chaque mois. Par exemple, si 20 licences étaient éligibles pour une libération et que vous en avez libéré 10 en juillet, le nombre de licences libérées pour juillet est de 10.

Les intervalles de temps pendant lesquels la troncation de domaine est activée sont marqués d'un astérisque.



Sur le graphique **Utilisation active**, vous pouvez afficher les utilisateurs et les appareils actifs au cours

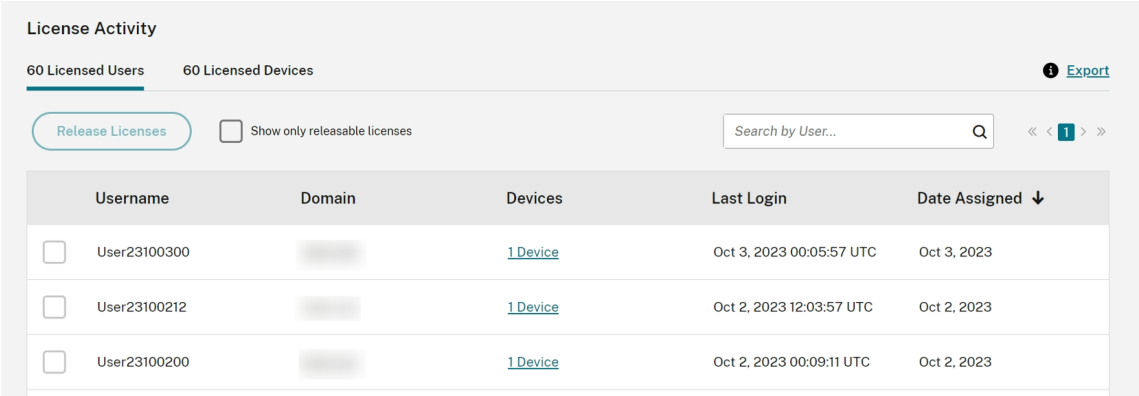
du mois calendaire et de l'année calendaire précédents, respectivement. Vous pouvez pointer vers un intervalle spécifique du graphique pour afficher le nombre d'utilisateurs ou d'appareils actifs et le pourcentage d'utilisation.



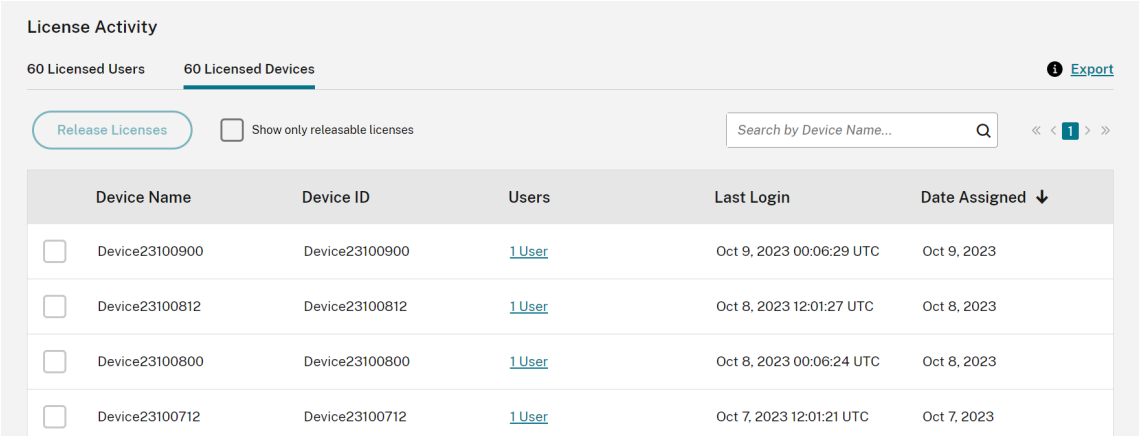
Activité des licences

La section **Activité des licences** affiche 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

Vous pouvez également filtrer la liste pour n'afficher que les licences pouvant être libérées. Consultez la section Pour libérer des licences attribuées dans cet article.

Libérer des licences attribuées

Lorsqu'une licence est attribuée, la période d'attribution est de 90 jours à compter de l'établissement d'une connexion au service. Si un utilisateur ou un appareil n'a pas lancé d'application ou de bureau pendant 90 jours, ces licences sont considérées comme des licences non utilisées et elles sont libérées par Citrix Cloud au bout de 90 jours. Ce processus est automatisé et aucune action n'est requise de la part de l'administrateur.

Après la période d'attribution (90 jours), l'administrateur est autorisé à libérer les licences manuellement dans les scénarios suivants uniquement :

- L'utilisateur n'est plus associé à l'entreprise.
- L'utilisateur est en congé prolongé.

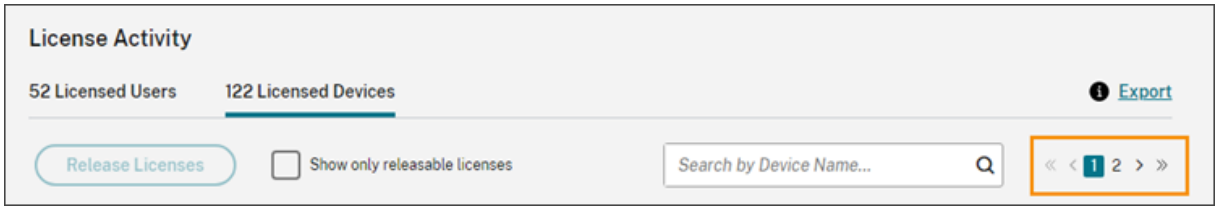
Les administrateurs ne peuvent libérer des licences associées à des machines lorsque ces dernières sont hors service.

> **Remarque :**
>
> - Il est recommandé de suivre le processus automatique de libération des licences. Toutefois, si l'administrateur a l'intention de libérer les licences avant la période de 90 jours, sauf pour les raisons mentionnées ci-dessus, cela peut constituer une violation du contrat de licence de l'utilisateur final de Citrix. Avant d'effectuer cette action, contactez Citrix.
> - L'administrateur peut libérer manuellement une seule licence via l'interface utilisateur. L'administrateur peut également choisir de libérer des licences à l'aide de l'API Cloud Licensing. Pour plus d'informations, consultez la page APIs to manage Citrix cloud licensing.

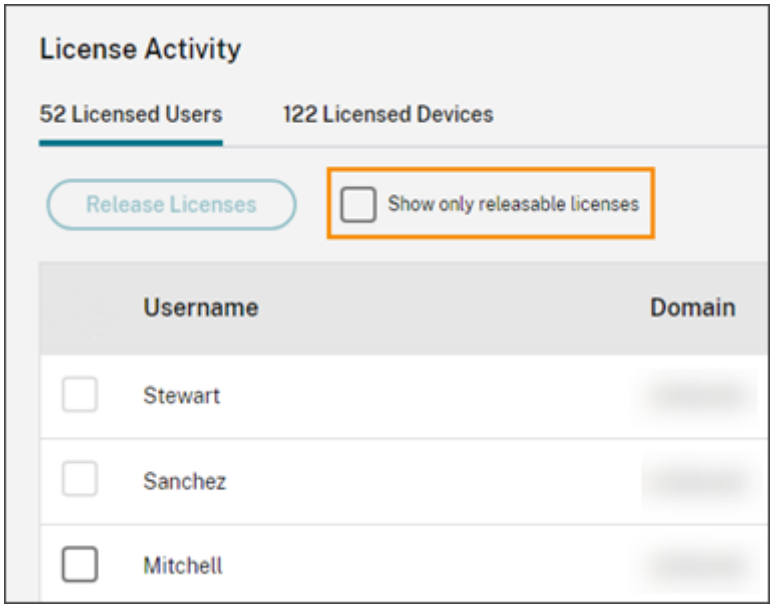
Rechercher des licences pouvant être libérées

Si l'utilisateur ou l'appareil n'a pas lancé d'application ou de bureau après 30 jours, Citrix Cloud modifie l'état de la licence et celle-ci peut être libérée. Les licences pouvant être libérées apparaissent dans la liste des utilisateurs sous licence ou des appareils sous licence avec une case à cocher gris foncé que vous pouvez sélectionner. Les licences qui ne peuvent pas être libérées affichent une case à cocher gris clair indiquant que la licence ne peut pas être sélectionnée.

La liste qui apparaît dans la section **Activité des licences** affiche jusqu'à 100 licences attribuées à la fois. Si vous disposez de plus de 100 licences, utilisez les contrôles de page pour parcourir la liste.



Pour afficher rapidement les licences pouvant être libérées, cliquez sur **Afficher uniquement les licences pouvant être libérées**, à côté du bouton **Libérer licences**. Cette action masque les licences attribuées qui ne sont pas encore autorisées à être libérées.



Sélectionner des licences pouvant être libérées

Cochez la case gris foncé en regard de chaque licence pour la sélectionner afin de la libérer. Lorsque vous sélectionnez une licence dans la liste, le bouton **Libérer licences** devient actif.

Vous pouvez sélectionner toutes les licences pouvant être libérées une par une et cliquer sur **Libérer licences**.

Pour libérer des licences attribuées

1. Sous **Activité des licences**, cliquez sur l'onglet **Utilisateurs sous licence** ou **Appareils sous licence**.
2. Si nécessaire, cliquez sur **Afficher uniquement les licences pouvant être libérées** pour afficher uniquement les utilisateurs disposant de licences pouvant être libérées.
3. Sélectionnez les utilisateurs ou les appareils que vous souhaitez gérer, puis cliquez sur **Libérer licences**.

4. Vérifiez les utilisateurs ou les appareils que vous avez sélectionnés, puis cliquez sur **Libérer licences**.

Surveiller les licences et l'utilisation maximale de Citrix DaaS (utilisateurs simultanés)

October 4, 2023

Cet article décrit comment gérer les licences d'utilisateurs simultanés pour **Citrix DaaS** uniquement.

Pour plus d'informations sur les licences utilisateur/appareil pour Citrix DaaS, consultez la section Surveiller les licences et l'utilisation active de Citrix DaaS (utilisateur/appareil).

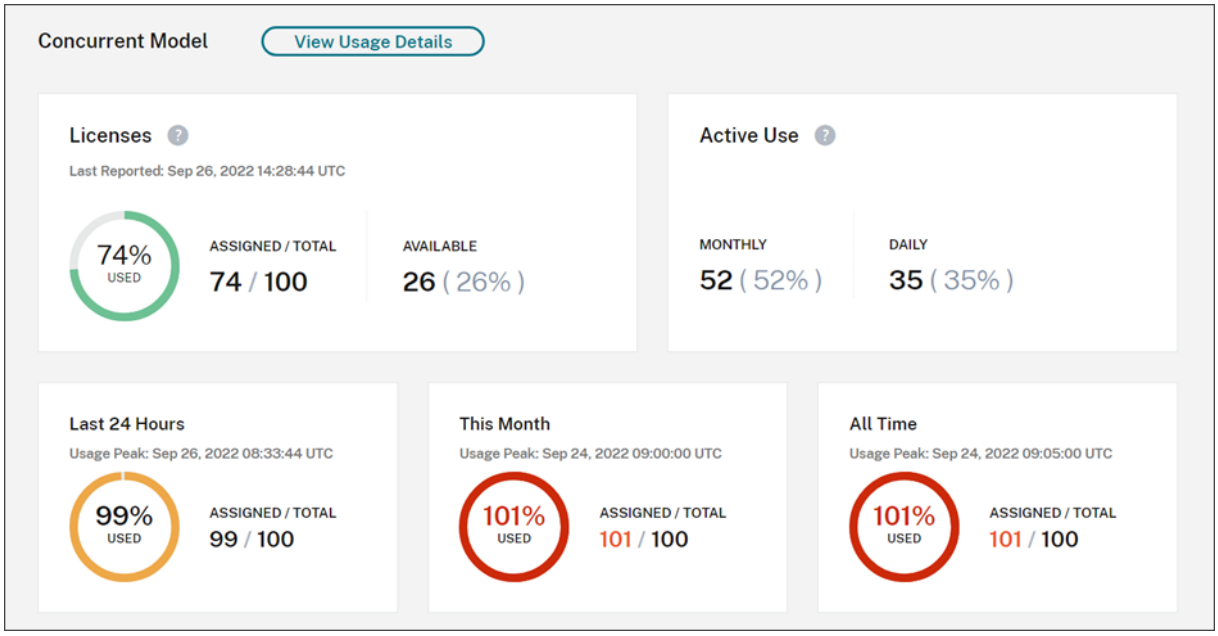
Pour plus d'informations sur les licences utilisateur/appareil et utilisateur simultané pour Citrix DaaS Standard pour Azure, consultez la section Surveiller les licences et l'utilisation de Citrix DaaS Standard pour Azure.

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 d'utilisateurs simultanés, consultez la section Licences simultanées dans la documentation relative au système de licences Citrix.

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. La quantité totale de licences achetées correspond à la somme des licences achetées pour les éditions Citrix DaaS qui utilisent le modèle de licences d'utilisateurs simultanés.
- 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.

- Statistiques d'utilisation active. Citrix Cloud affiche le nombre total de connexions uniques pour les périodes suivantes :
  - **Mensuel :** nombre total de connexions pour le mois calendaire précédent.
  - **Quotidien :** nombre total de connexions au cours des 24 heures précédentes.
    Ces chiffres sont également représentés sous forme de pourcentages du nombre total de licences détenues au cours de ces périodes.

Calcul du nombre maximal de licences utilisées

Pour refléter avec précision le modèle de licence d'utilisateurs simultanés, 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 d'utilisateurs simultanés utilisées. Pour plus d'informations sur les différences entre les rapports de monitoring et les rapports de licence, consultez Questions fréquentes.

Calcul de l'utilisation active mensuelle

Au début de chaque mois, Citrix Cloud prend un instantané du mois calendaire précédent. Citrix Cloud affiche le nombre total de connexions uniques qui se sont produites au cours de ce mois calendaire.

Calcul de l'utilisation active quotidienne

Chaque jour, à la même heure, Citrix Cloud prend un instantané des 24 heures précédentes. Citrix Cloud affiche le nombre total de connexions uniques qui se sont produites au cours de cette période de 24 heures.

Tendances d'utilisation et activité des licences

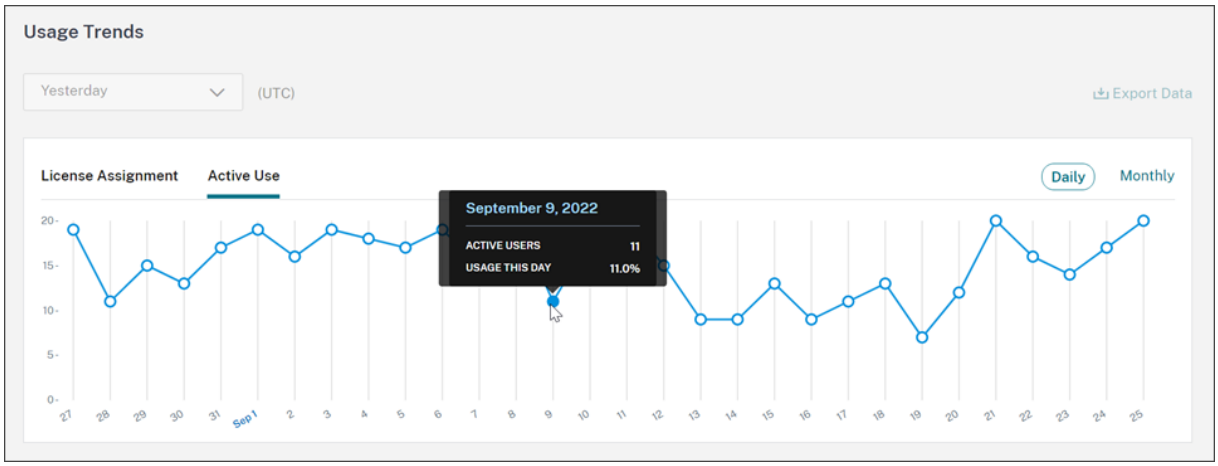
Pour afficher l'historique de vos licences, cliquez sur **Afficher détails d'utilisation**.

La section **Tendances d'utilisation** affiche les informations suivantes :

- La section **Attribution de licence** affiche un tableau contenant les informations suivantes :
  - **Nombre total de licences :** nombre total de licences d'utilisateurs simultanés 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 déroulant.

  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.
- **Utilisation active** affiche un graphique contenant les informations suivantes :
  - **Quotidien :** nombre total de connexions par jour au cours des 30 jours précédents.
  - **Mensuel :** nombre total de connexions pour chaque mois au cours de l'année calendaire précédente.

Le fait de pointer sur un intervalle dans les graphiques **Attribution de licences** ou **Utilisation active** permet d'afficher les détails de cet intervalle.



Libérer les licences

Les licences d'utilisateurs simultanés sont libérées automatiquement lorsque les utilisateurs ferment ou se déconnectent de leur session. Vous n'avez pas besoin de libérer ces licences manuellement.

Surveiller les licences et l'utilisation de Citrix DaaS Standard pour Azure

November 6, 2023

Cet article décrit l'expérience de gestion des attributions de licence pour les modèles de licence utilisateur/appareil et utilisateur simultané.

Citrix Azure Consumption Fund (utilisateur/appareil uniquement)

Si vous avez acheté Citrix Azure Consumption Fund pour l'utiliser avec votre déploiement de service, consultez la section Surveiller la consommation des ressources Citrix Managed Azure pour Citrix DaaS pour plus d'informations sur les rapports de consommation pour les ressources gérées par Citrix.

Attribution de licence

Modèle de licence utilisateur/appareil : Citrix Cloud attribue une licence lorsqu'un utilisateur ou un appareil unique lance un bureau pour la première fois.

Modèle de licences d'utilisateurs simultanés : 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 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 la section Licences simultanées dans la documentation relative au système de licences Citrix.

Calcul du nombre maximal de licences utilisées

Pour refléter avec précision le modèle de licences simultanées, 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.

Troncation du nom de domaine

Cette fonctionnalité est prise en charge uniquement pour le modèle de licence **utilisateur/appareil**.

Si vous hébergez plusieurs domaines et que des utilisateurs disposent de comptes similaires dans ces domaines (par exemple, `johnsmith@company.com` et `johnsmith@mycompany.com`), vous pouvez autoriser Citrix Cloud à ignorer le domaine du compte et à n'utiliser que le nom d'utilisateur du compte (par exemple, johnsmith). Ce processus est connu sous le nom de *troncation du nom de domaine*. Par défaut, la troncation du nom de domaine est désactivée.

Lorsque la troncation du nom de domaine est activée, le calcul des utilisateurs uniques par Citrix Cloud change. Au lieu de compter `johnsmith@company.com` et `johnsmith@mycompany.com` en tant que deux utilisateurs uniques, Citrix Cloud compte uniquement johnsmith en tant qu'utilisateur unique. Ce changement de calcul affecte les données de licence suivantes :

- Attribution de licence
- Utilisation active
- Tendances d'utilisation des licences au fil du temps
- Licences pouvant être libérées

Ces modifications des données de licence sont également prises en compte lorsque vous exportez des données vers un fichier CSV depuis la console de licences.

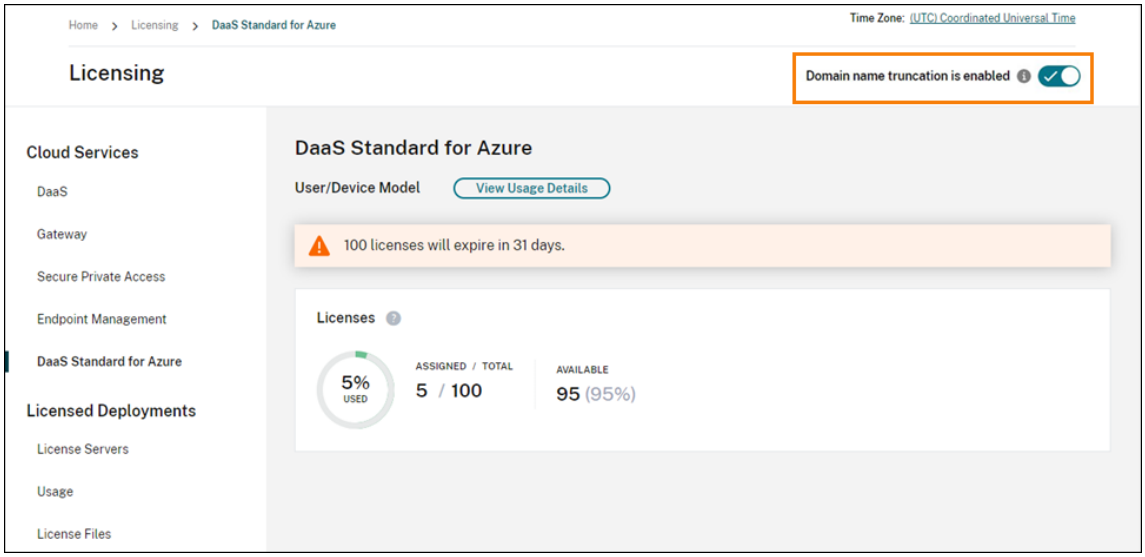
> **Remarque :**
>
> Si vous hébergez plusieurs domaines avec des comptes similaires dont le nom d'utilisateur est légèrement différent (par exemple, un utilisateur individuel disposant des comptes `johnsmith@company.com` et `jsmith@newcompany.com`), la troncation du nom de domaine n'a aucun effet sur les calculs de Citrix Cloud. Citrix Cloud considère toujours johnsmith et jsmith comme des utilisateurs uniques, même s'ils sont associés à la même personne.

Activer ou désactiver la troncation du nom de domaine

Par défaut, la troncation du nom de domaine est désactivée. La troncation du nom de domaine a un effet sur les données d'utilisation des licences utilisateur/appareil à partir du moment où vous activez ou désactivez la fonctionnalité. Par exemple, si vous activez la troncation des noms de domaine au cours d'un mois donné, les données enregistrées par Citrix Cloud au cours de ce mois sont affectées. Toutefois, les données historiques des mois précédents, lorsque la fonctionnalité était désactivée, restent inchangées. De même, si vous désactivez la troncation du nom de domaine au cours d'un mois donné, les données enregistrées par Citrix Cloud au cours de ce mois sont affectées. Cependant, les données historiques des mois pendant lesquels la fonctionnalité a été activée restent intactes.

Pour activer ou désactiver la troncation du nom de domaine, procédez comme suit :

1. Cliquez sur le bouton situé en haut à droite de la console de gestion des licences.



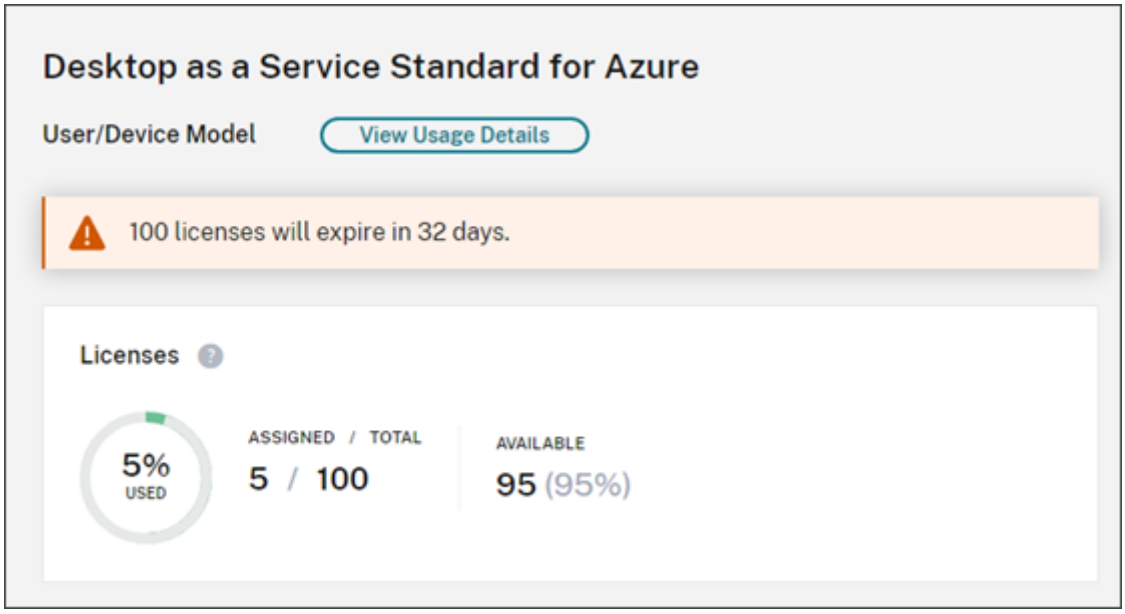
2. Lorsque vous êtes invité à confirmer votre action, sélectionnez **Oui, je comprends**.

Résumé de l'option Système de licences

Citrix Cloud affiche des vues récapitulatives des licences utilisées dans le cadre des modèles de licence utilisateur/appareil et utilisateur simultané.

Résumé pour le modèle utilisateur/appareil

Pour le modèle utilisateur/appareil, le résumé des licences affiche les licences utilisées par rapport au nombre total de licences que vous possédez.

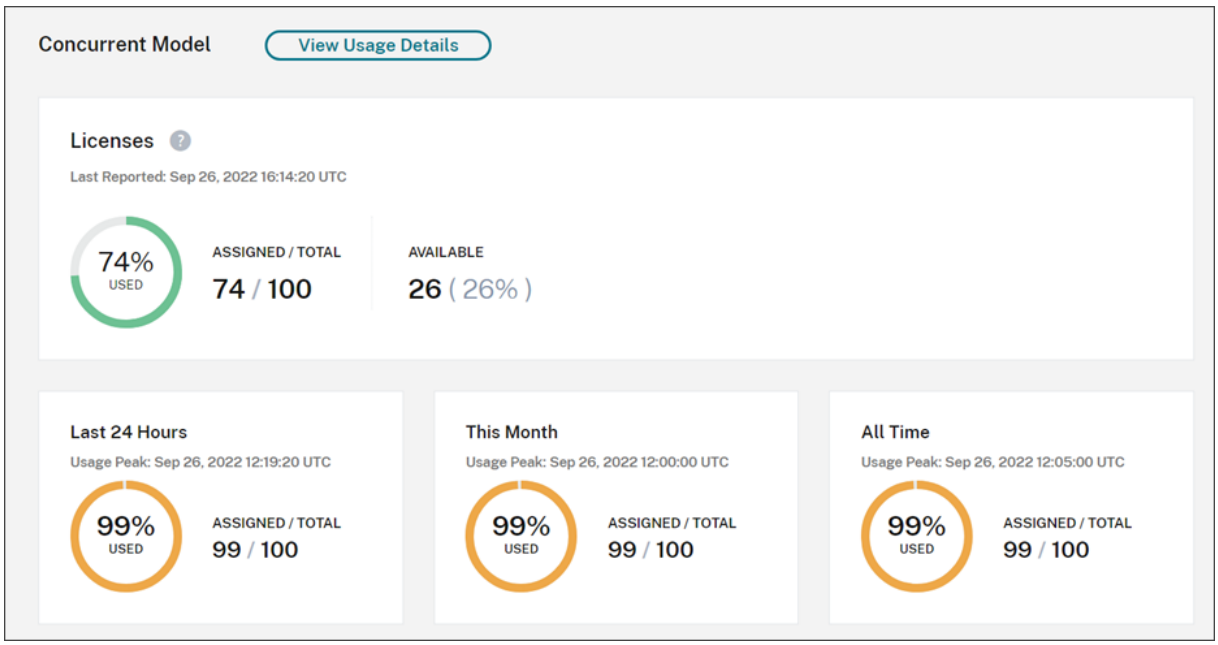


Lorsque le pourcentage approche 100 %, le pourcentage passe du vert au jaune. Si le pourcentage dépasse 100 %, il devient rouge.

Citrix Cloud affiche également le ratio entre les licences attribuées et les licences achetées, ainsi que le nombre de licences disponibles restantes.

Résumé pour le modèle de licences d'utilisateurs simultanés

Pour le modèle de licences simultanées, le résumé des licences fournit une vue d'ensemble des informations suivantes :



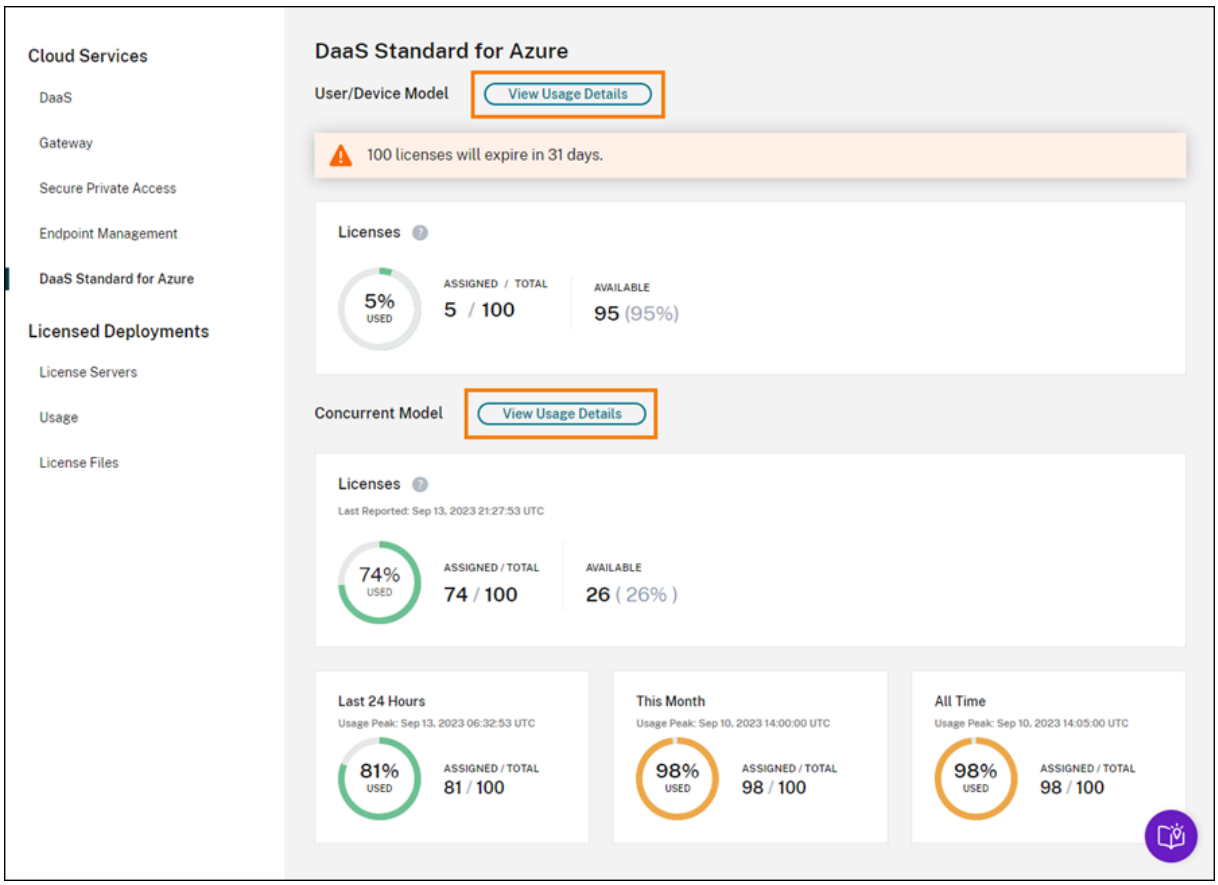
- Pourcentage du nombre total de licences achetées actuellement utilisées lors de la dernière évaluation par Citrix Cloud des licences utilisées. Citrix Cloud calcule ce pourcentage toutes les cinq minutes en fonction des appareils uniques disposant de connexions actives au service. La quantité totale de licences achetées correspond à la somme des licences achetées pour les éditions Citrix DaaS Standard pour Azure qui utilisent le modèle de licences simultanées.
- 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.

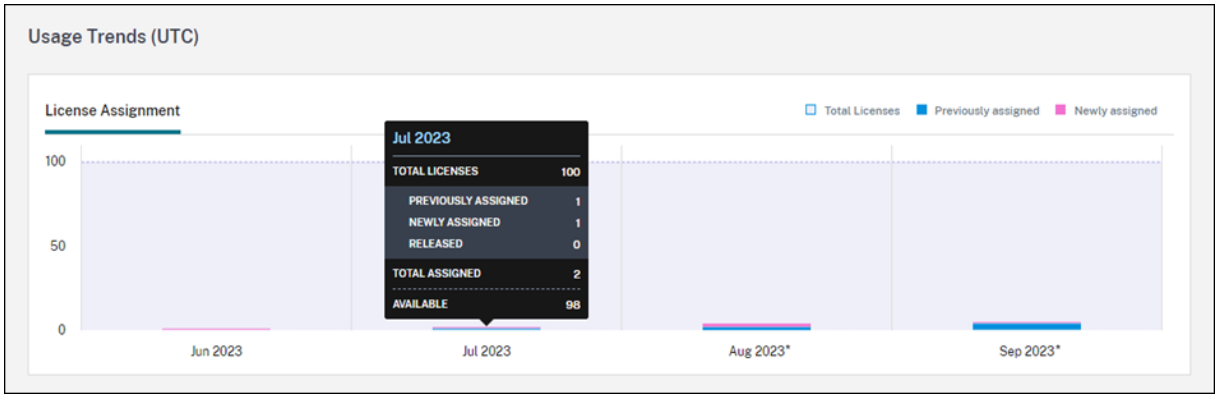
Tendances d'utilisation

Citrix Cloud affiche une répartition des tendances d'utilisation pour les licences utilisateur/appareil ou utilisateurs simultanés. Pour consulter cette répartition, sélectionnez **Afficher détails d'utilisation** sur la page récapitulative des licences.



Tendances pour le modèle utilisateur/appareil

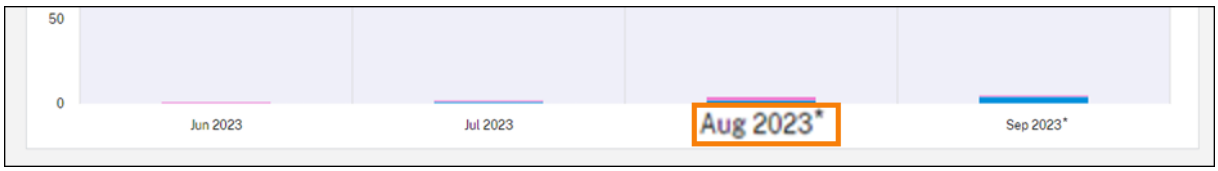
Pour les licences utilisateur/appareils, la section **Tendances d'utilisation** présente la répartition des licences attribuées sous forme de graphique.



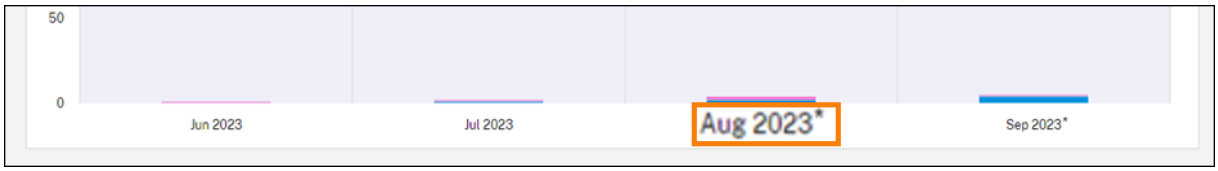
Si vous pointez sur un intervalle sur le graphique, les informations suivantes s'affichent :

- **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.

Les intervalles de temps pendant lesquels la troncation de domaine est activée sont marqués d'un astérisque.



Les intervalles de temps pendant lesquels la troncation de domaine est activée sont marqués d'un astérisque.



Tendances pour les utilisateurs simultanés

Pour les licences d'utilisateurs simultanés, la section **Tendances d'utilisation** présente les informations suivantes :

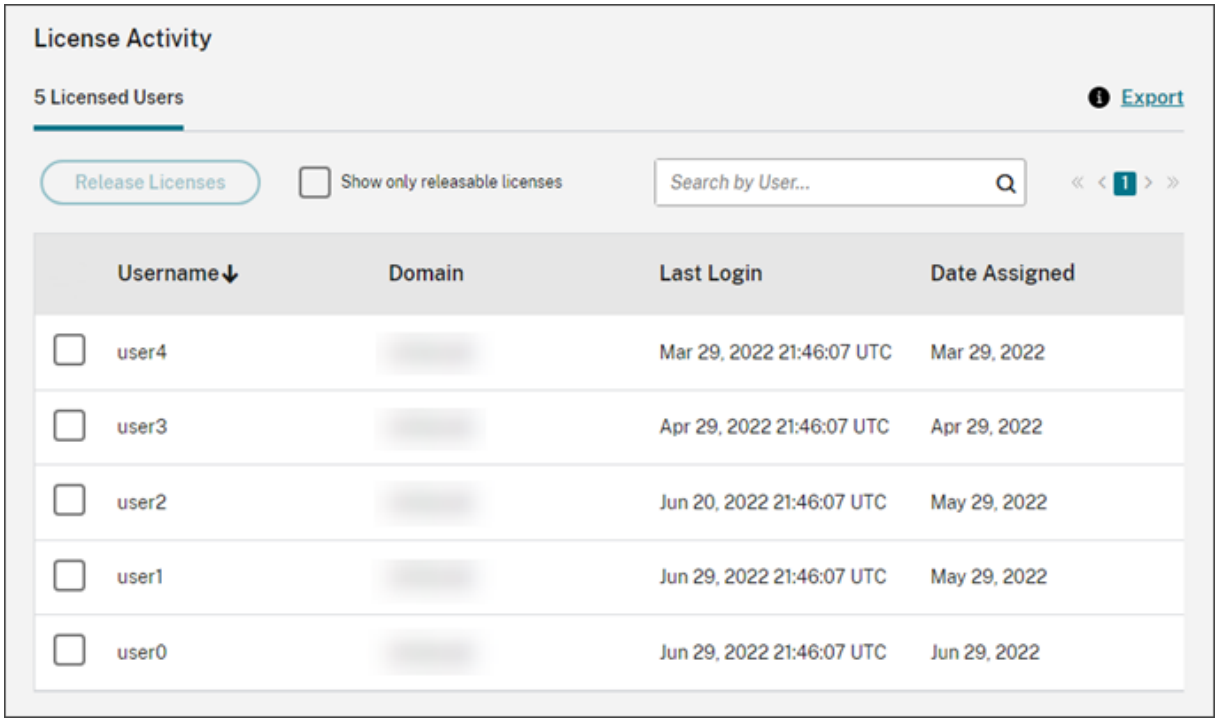
- **Nombre total de licences :** nombre total de licences simultanées achetées.
- **Nombre maximal de licences utilisées :** nombre maximal de licences attribuées pour la plage de dates que vous sélectionnez. Par défaut, Citrix Cloud affiche les pics d'utilisation pour chaque mois de l'année civile en cours. Pour accéder à l'utilisation maximale mensuelle ou horaire, sélectionnez le mois ou le jour à afficher dans le menu déroulant.

  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.

Si vous pointez sur un intervalle sur le graphique, vous pouvez voir le nombre total de licences et le nombre maximal de licences utilisées pendant cet intervalle.

Activité liée aux licences pour les utilisateurs et les appareils

Pour les licences utilisateur/appareil, 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. Cette section n'est pas disponible pour les licences simultanées.



Vous pouvez également filtrer la liste pour n'afficher que les licences pouvant être libérées. Consultez la section Libérer des licences attribuées dans cet article.

Libérer des licences utilisateur/appareil

La libération de licences utilisateur/appareil éligibles varie en fonction du type d'abonnement au service.

- **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 attribuée, la période d'attribution est de 90 jours à compter de l'établissement d'une connexion au service. Si un utilisateur ou un appareil n'a pas lancé d'application ou de bureau pendant 90 jours, ces licences sont considérées comme des licences non utilisées et elles sont libérées par Citrix Cloud au bout de 90 jours. Ce processus est automatisé et aucune action n'est requise de la part de l'administrateur.

Après la période d'attribution (90 jours), l'administrateur est autorisé à libérer les licences manuellement dans les scénarios suivants uniquement :

- L'utilisateur n'est plus associé à l'entreprise.

- L'utilisateur est en congé prolongé.

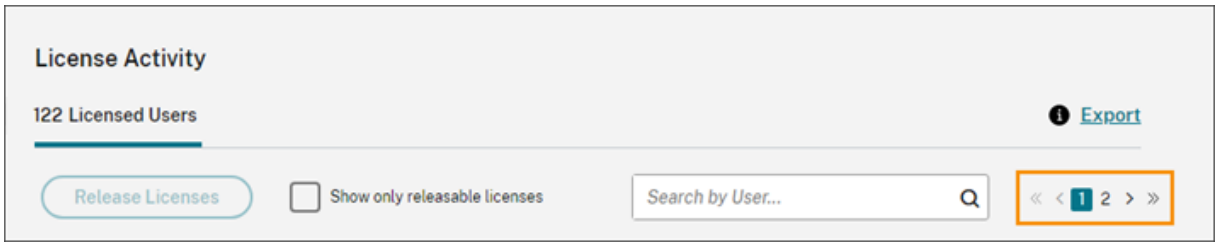
Les administrateurs ne peuvent libérer des licences associées à des machines lorsque ces dernières sont hors service.

> **Remarque :**
>
> - Il est recommandé de suivre le processus automatique de libération des licences. Toutefois, si l'administrateur a l'intention de libérer les licences avant la période de 90 jours, sauf pour les raisons mentionnées ci-dessus, cela peut constituer une violation du contrat de licence de l'utilisateur final de Citrix. Avant d'effectuer cette action, contactez Citrix.
> - L'administrateur peut libérer manuellement une seule licence via l'interface utilisateur. L'administrateur peut également choisir de libérer des licences à l'aide de l'API Cloud Licensing. Pour plus d'informations, consultez la page APIs to manage Citrix cloud licensing.

Afficher les licences pouvant être libérées

Si l'utilisateur ou l'appareil n'a pas lancé d'application ou de bureau après 30 jours, Citrix Cloud modifie l'état de la licence et celle-ci peut être libérée. Les licences pouvant être libérées apparaissent dans la liste des utilisateurs sous licence ou des appareils sous licence avec une case à cocher gris foncé que vous pouvez sélectionner. Les licences qui ne peuvent pas être libérées affichent une case à cocher gris clair indiquant que la licence ne peut pas être sélectionnée.

La liste qui apparaît dans la section **Activité des licences** affiche jusqu'à 100 licences attribuées à la fois. Si vous disposez de plus de 100 licences, utilisez les contrôles de page pour parcourir la liste.



Pour afficher rapidement les licences pouvant être libérées, sélectionnez **Afficher uniquement les licences pouvant être libérées**, à côté du bouton **Libérer licences**. Cette action masque les licences attribuées qui ne peuvent pas encore être libérées.

Sélectionner les licences pouvant être libérées

Cochez la case gris foncé en regard de chaque licence pour la sélectionner afin de la libérer. Lorsque vous sélectionnez une licence, le bouton **Libérer licences** devient actif.

Vous pouvez sélectionner toutes les licences pouvant être libérées une par une et cliquer sur **Libérer licences**.

Libérer des licences attribuées

1. Si nécessaire, cliquez sur **Afficher uniquement les licences pouvant être libérées** pour afficher uniquement les utilisateurs disposant de licences pouvant être libérées.
2. Sélectionnez les utilisateurs que vous souhaitez gérer, puis cliquez sur **Libérer licences**.
3. Vérifiez les utilisateurs que vous avez sélectionnés, puis cliquez sur **Libérer licences**.

Libérer des licences d'utilisateurs simultanés

Les licences d'utilisateurs simultanés sont libérées automatiquement lorsque les utilisateurs ferment ou se déconnectent de leur session. Vous n'avez pas besoin de libérer ces licences manuellement.

Surveiller les licences et l'utilisation active d'Endpoint Management

November 29, 2023

Attribution de licence

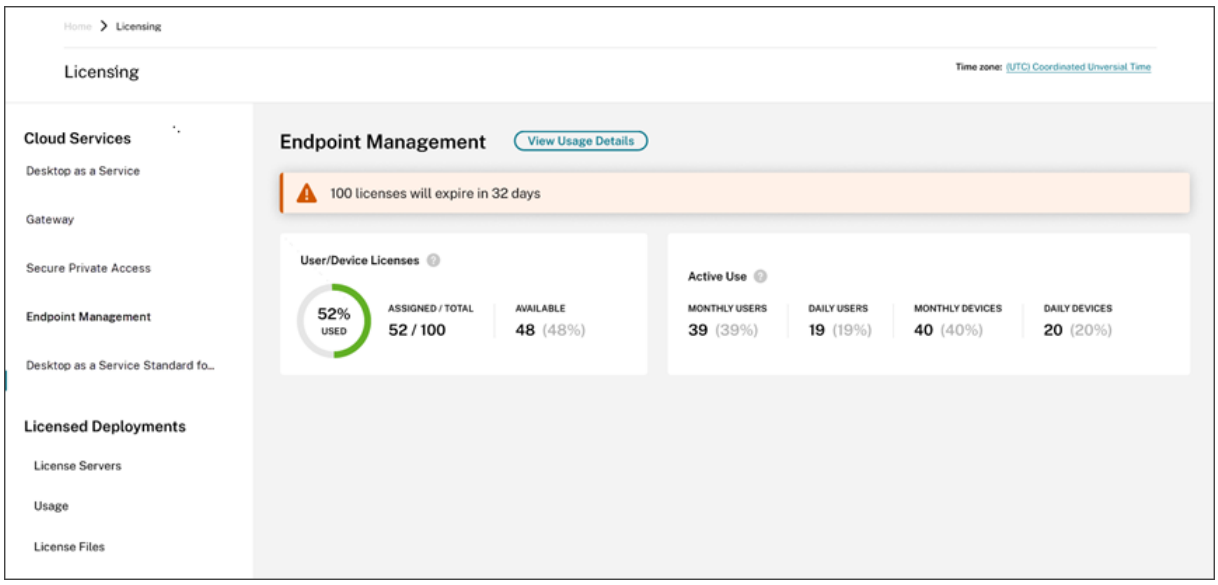
En général, les utilisateurs se voient attribuer une licence lors de la première utilisation du service cloud. Pour Endpoint Management, une licence est attribuée lorsqu'un utilisateur inscrit un appareil.

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

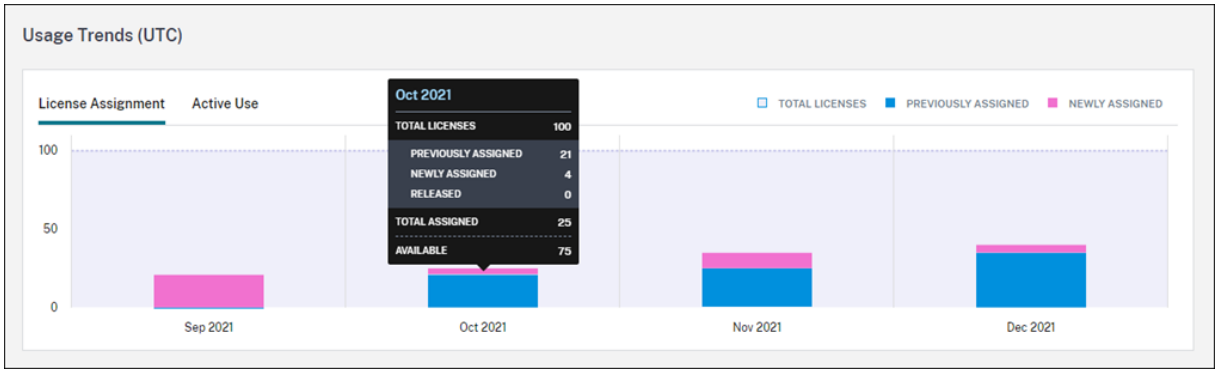


L'écran de résumé de l'option Système de licences fournit une vue d'ensemble des informations suivantes pour chaque service pris en charge :

- 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.

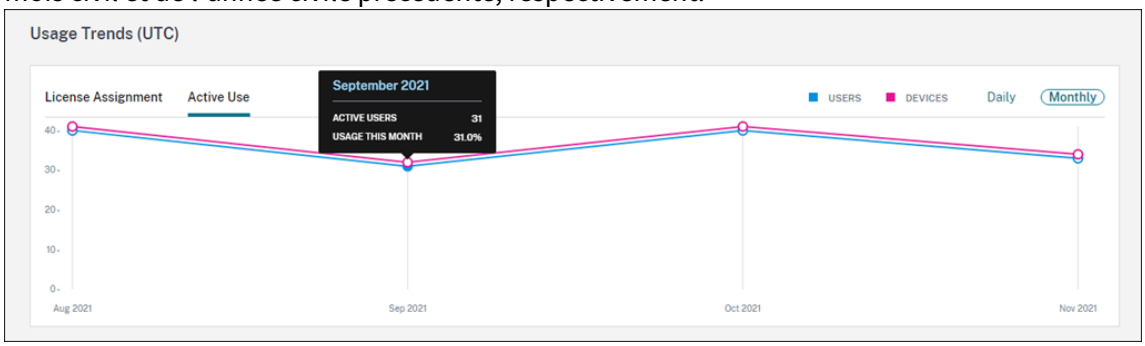
Tendances d'utilisation

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 :

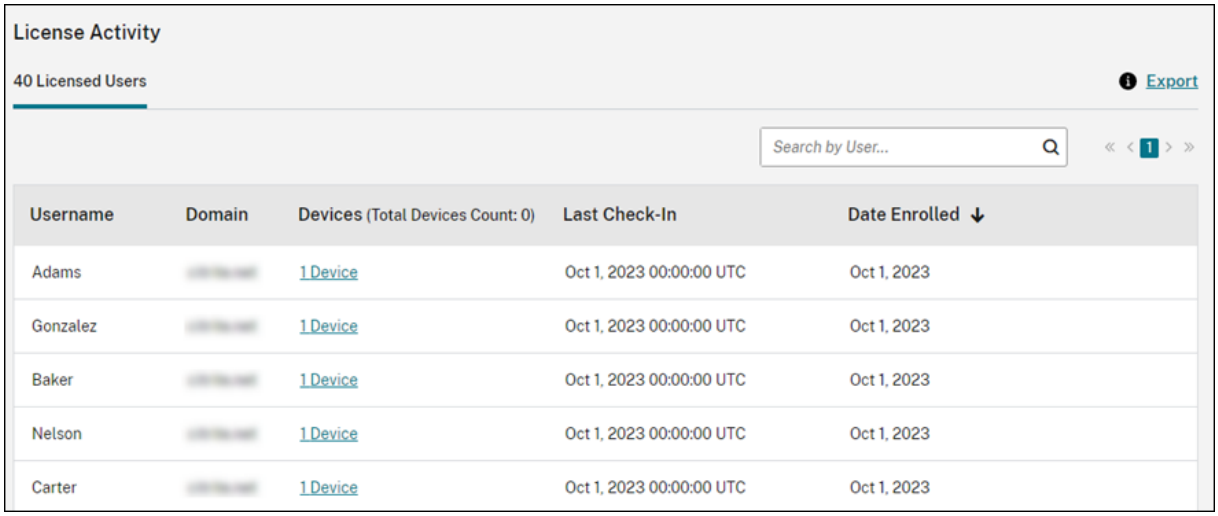
- **Nombre total de licences :** nombre total de licences achetées pour le service cloud pour toutes les prestations.
- **Précédemment attribuée :** licences de service cloud déjà attribuées au début de chaque mois. Par exemple, si une licence est attribuée à un utilisateur en juillet, cette attribution 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.



Activité des licences

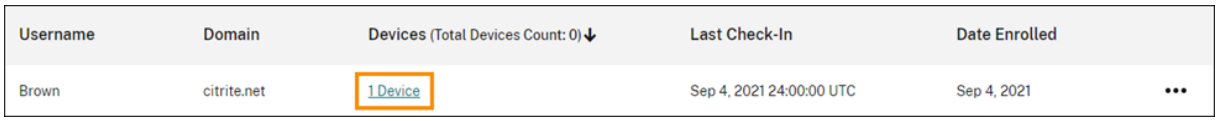
La section **Activité des licences** affiche une liste contenant les informations suivantes :

- Utilisateurs 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

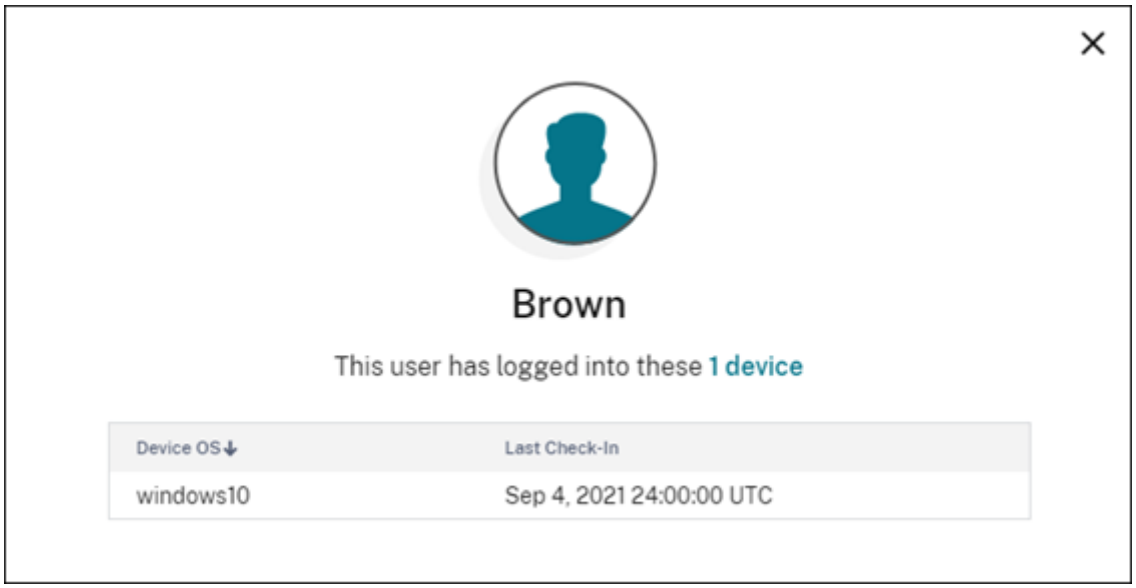


Afficher les appareils inscrits

Pour afficher le nombre d'appareils inscrits pour un utilisateur spécifique, cliquez sur le lien dans la colonne **Appareils**.



Citrix Cloud affiche la liste des appareils inscrits pour l'utilisateur et la date du dernier enregistrement pour chaque appareil.



Libérer automatiquement des licences attribuées

Citrix Cloud libère automatiquement les licences pour les utilisateurs qui répondent à **toutes** les conditions suivantes au cours des 30 derniers jours :

- L'utilisateur n'a pas inscrit de nouvel appareil.
- L'utilisateur possède déjà un appareil qui n'est pas enregistré auprès de Citrix Cloud.

Aucune autre action n'est requise pour libérer les licences éligibles.

Une fois les licences éligibles libérées, les utilisateurs peuvent acquérir une autre licence en enregistrant un appareil.

Surveiller l'utilisation de la bande passante pour Gateway Service

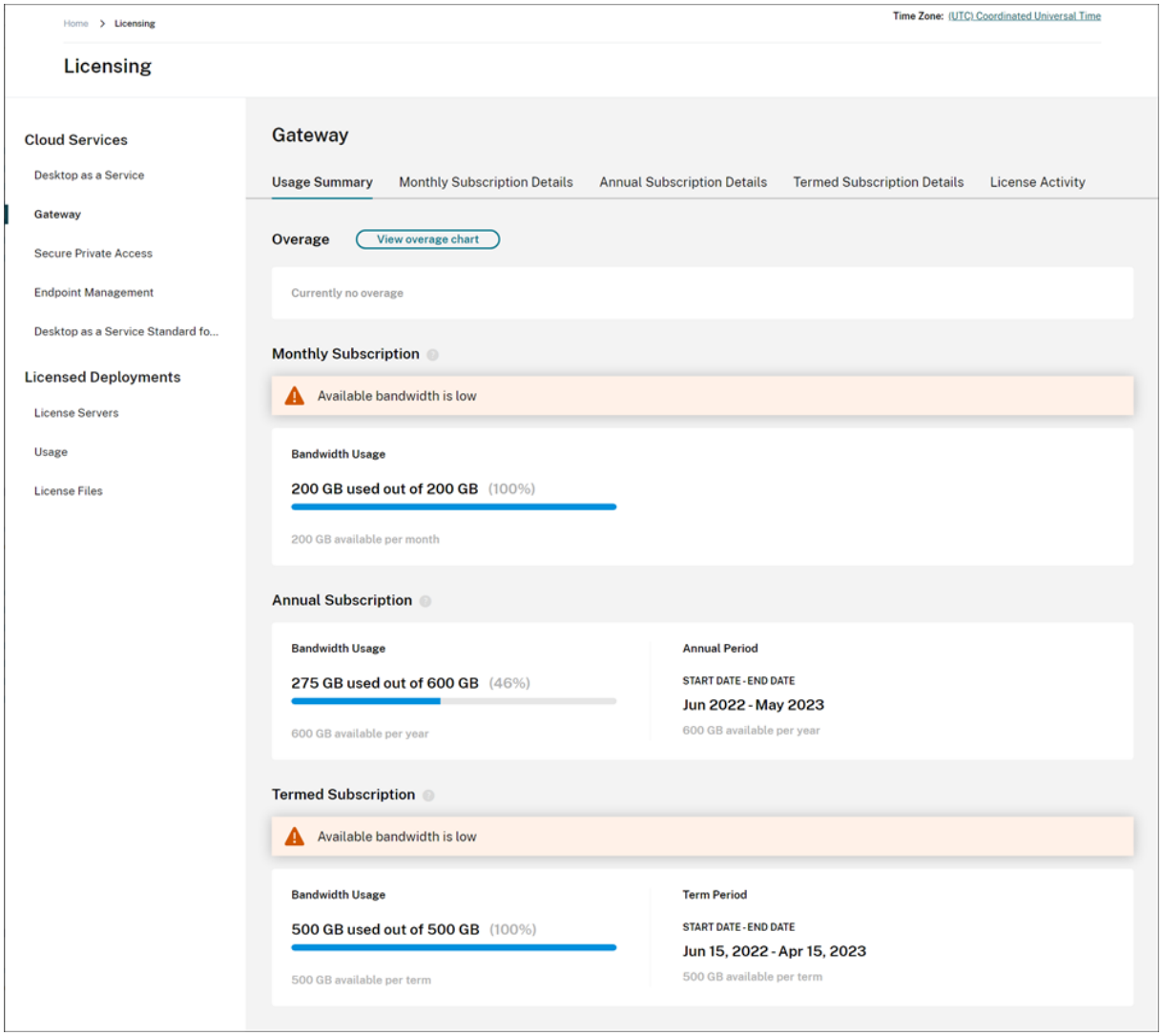
October 4, 2023

Cet article décrit l'utilisation de la bande passante via le service Gateway lorsqu'il est utilisé avec Citrix DaaS (anciennement 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.

> **Remarque :**
>
> Le système de licences pour le service Gateway vous aide à comprendre votre utilisation de la bande passante lors de l'utilisation d'applications et de bureaux virtuels. Citrix n'applique pas les attributions d'utilisation de la bande passante dans votre environnement. Si vous abusez de votre allocation de bande passante, Citrix n'interfère pas avec les charges de travail de production ou le fonctionnement du service. Si Citrix modifie la manière dont les stratégies du service Gateway et de l'utilisation de la bande passante sont appliquées, Citrix vous informe avant la mise en oeuvre de ces modifications.

Résumé de l'utilisation

Le résumé de l'utilisation fournit une vue d'ensemble de l'utilisation de la bande passante pour chaque abonnement à Gateway Service et de l'excédent total de tous vos abonnements (mensuels, annuels et à durée déterminée).



Citrix Cloud affiche la quantité totale de bande passante et la quantité de bande passante consommée pour chaque type d'abonnement.

En fonction du type d'abonnement, Citrix Cloud affiche également la période de facturation de l'abonnement :

- Abonnements mensuels : Citrix Cloud n'affiche pas la période de facturation en cours. Pour ces abonnements, la période de facturation commence le premier jour de chaque mois et se termine le dernier jour du mois.
- Abonnements annuels : Citrix Cloud affiche les dates de début et de fin de la période de facturation. Pour ces abonnements, la période de facturation est d'un an.
- Abonnements à durée déterminée : Citrix Cloud affiche les dates de début et de fin de la période de facturation. Pour ces abonnements, la période de facturation correspond à la durée pour laquelle l'abonnement a été acheté. Par exemple, si un abonnement d'une durée de trois ans est acheté, les dates de début et de fin de la période de facturation correspondent à cet

intervalle de trois ans.

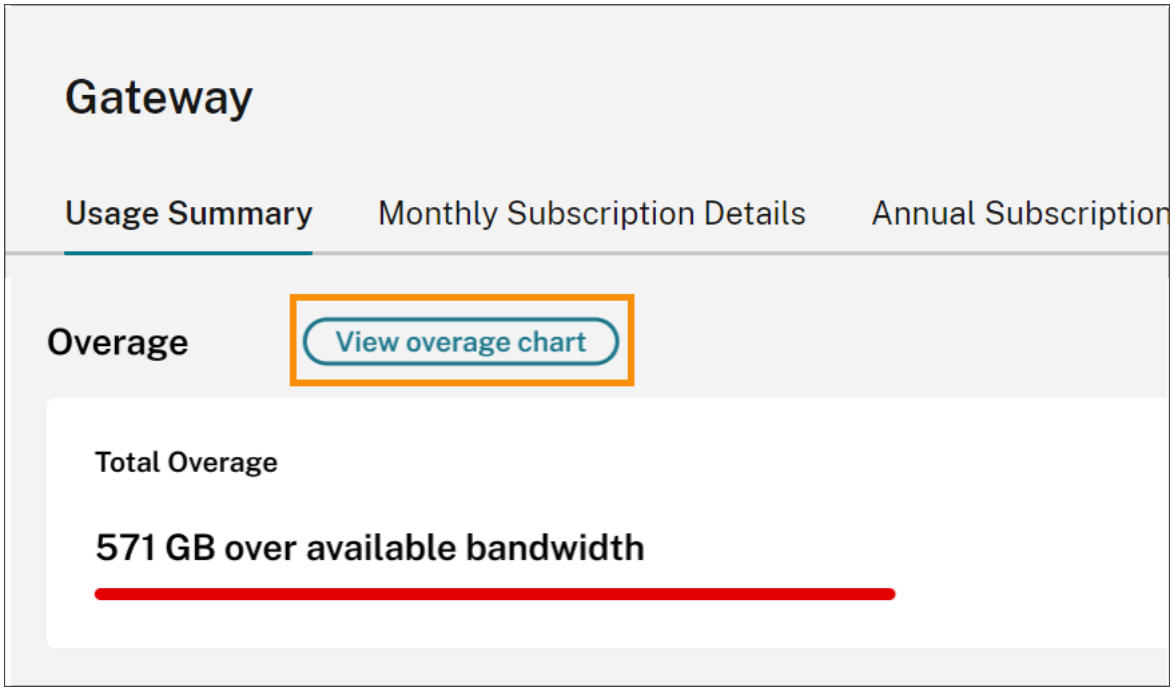
Si un abonnement expire dans les 90 jours, un message d'avertissement s'affiche pour cet abonnement.

Excédent

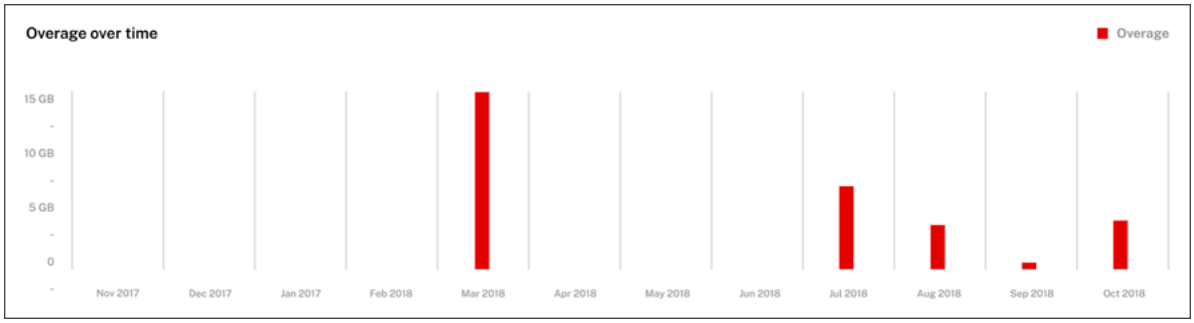
Citrix Cloud calcule l'excédent sur une base mensuelle pour tous vos abonnements. Si vous consommez plus de bande passante que vous n'en avez acheté, Citrix Cloud affiche l'excédent de bande passante comme un dépassement.

Si vous avez plusieurs abonnements, Citrix Cloud utilise l'abonnement dont la date de fin est la plus proche pour mesurer votre consommation de bande passante. Si vous épuisez la bande passante allouée dans le cadre de cet abonnement, Citrix Cloud utilise l'abonnement suivant dont la date de fin est la plus proche pour mesurer votre consommation de bande passante. Si vous épuisez la bande passante allouée dans tous vos abonnements, Citrix Cloud affiche l'utilisation excédentaire comme un dépassement.

La page Récapitulatif d'utilisation affiche l'excédent total pour le mois en cours. Pour voir l'excédent dans le temps, sélectionnez **Afficher tableau des excédents**.



Citrix Cloud affiche un graphique de votre excédent total au cours des 12 derniers mois.



L'excédent du mois en cours n'est pas reporté au mois suivant. Au début du mois suivant, l'excédent total est remis à zéro.

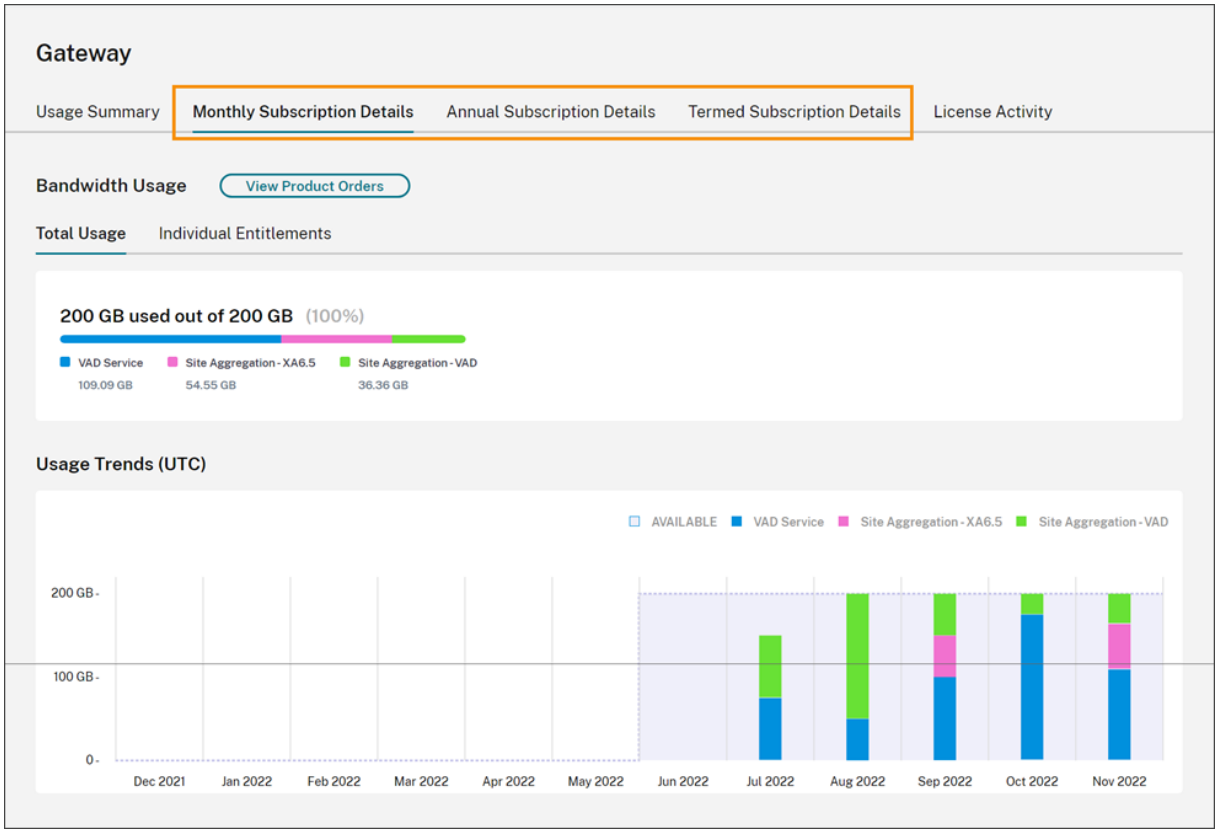
Bande passante non utilisée

Citrix Cloud réinitialise automatiquement l'utilisation de la bande passante pour un abonnement lors de la prochaine période de facturation. Si vous n'utilisez pas la totalité de la bande passante pendant une période d'abonnement donnée, Citrix Cloud ne reporte aucune bande passante inutilisée à la période de facturation suivante.

Par exemple, si votre abonnement mensuel inclut 150 Go de bande passante totale et que vous utilisez 100 Go de bande passante au cours d'un mois donné, Citrix Cloud réinitialise l'utilisation à zéro et affiche 150 Go comme quantité totale de bande passante au début du mois suivant. La bande passante non utilisée n'est pas ajoutée à votre allocation de bande passante totale.

Détails d'utilisation

Pour obtenir une vue détaillée de vos abonnements, sélectionnez les onglets de détails des abonnements mensuels, annuels ou à durée déterminée situés en haut de la console.



Pour chaque type d'abonnement, l'onglet Détails affiche les informations suivantes :

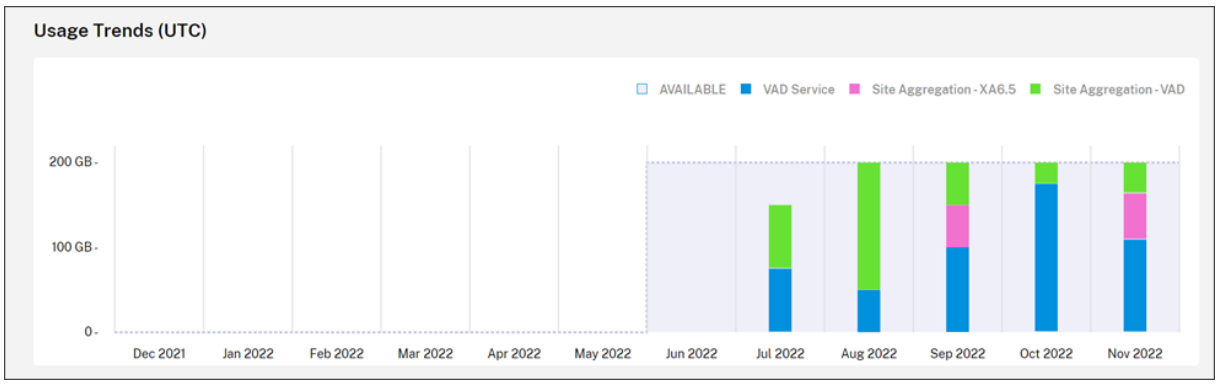
- **Utilisation totale :** quantité de bande passante consommée par rapport à la bande passante totale disponible pour tous les abonnements d'un type donné. Pour les abonnements mensuels, l'utilisation totale est indiquée pour le mois en cours. Pour les abonnements annuels et à durée déterminée, l'utilisation totale est cumulée sur tous vos abonnements annuels ou à durée déterminée.
- **Droits individuels :** quantité totale de bande passante consommée pour chaque abonnement d'un type donné. Par exemple, si vous avez plusieurs abonnements annuels, cet onglet affiche la répartition de l'utilisation pour chaque abonnement annuel séparément.

La quantité de bande passante consommée est répartie en fonction de l'accès via Citrix DaaS (**service CVAD**) ou via votre déploiement local de Virtual Apps and Desktops à l'aide de l'agrégation de sites dans Citrix Workspace.

Tendances d'utilisation

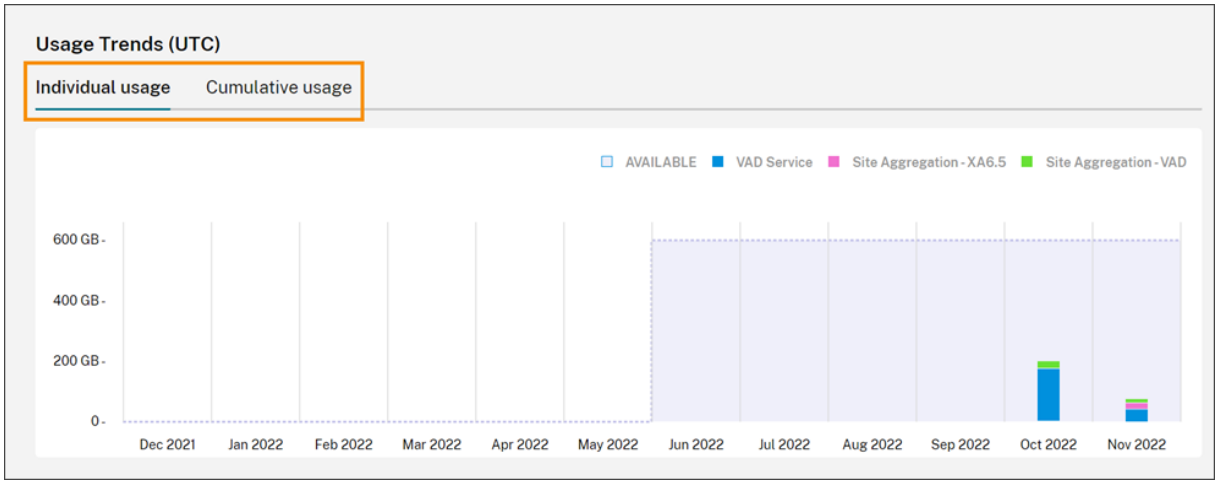
La section **Tendances d'utilisation** présente la répartition de l'utilisation au cours des 12 derniers mois.

Pour les abonnements mensuels, l'utilisation est affichée pour chaque mois au cours duquel elle a été consommée.

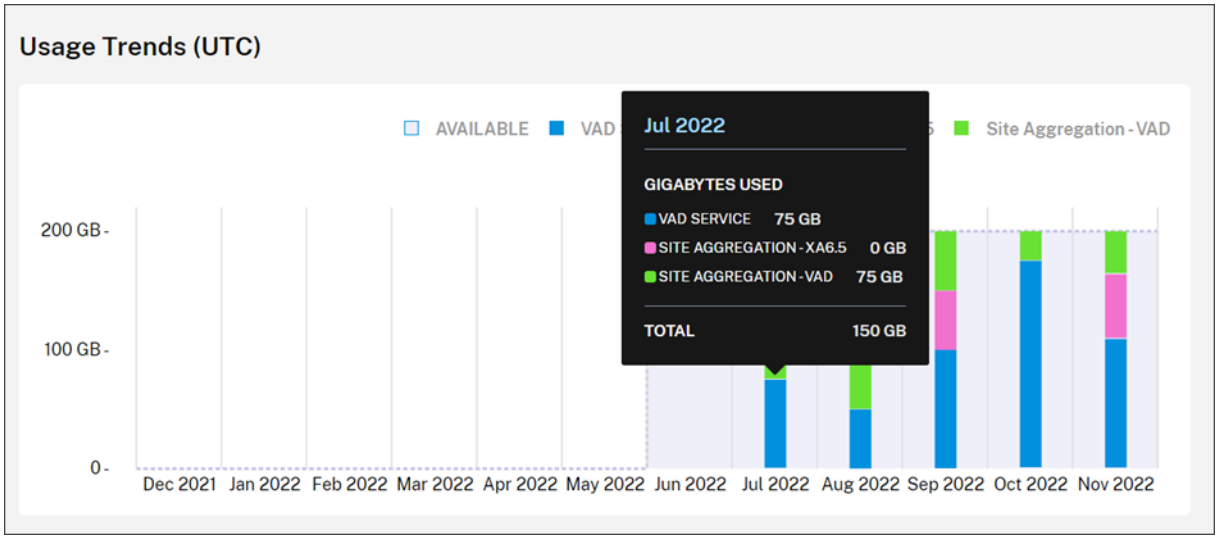


Pour les abonnements annuels et à durée déterminée, cette section inclut les vues suivantes :

- **Utilisation individuelle :** utilisation de la bande passante au cours de chaque mois durant la période de facturation en cours.
- **Utilisation cumulée :** utilisation de la bande passante cumulée chaque mois durant la période de facturation en cours.



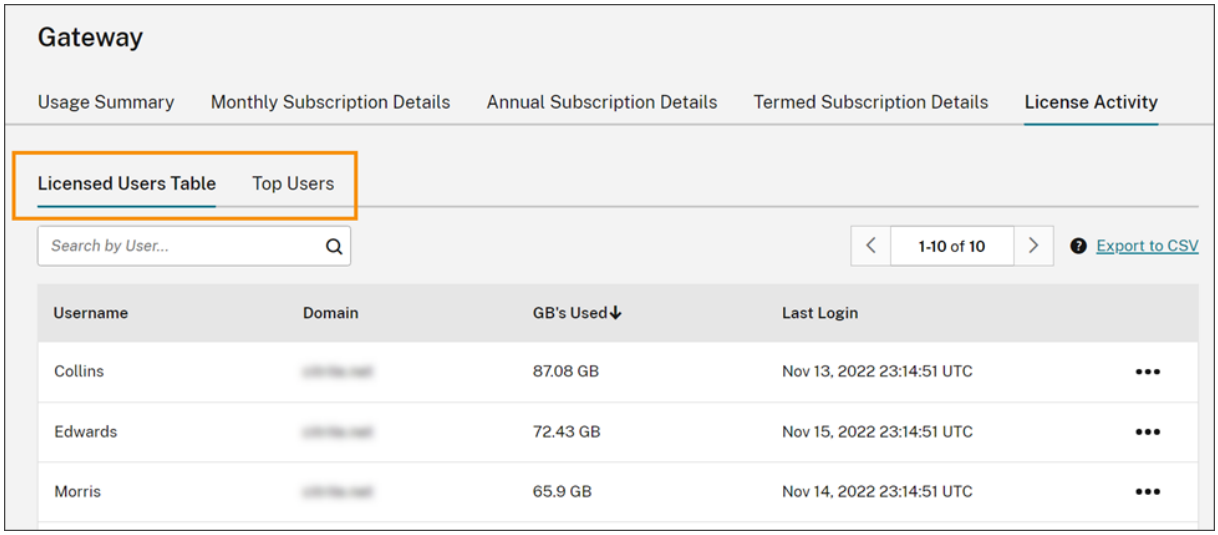
Pour tous les types d'abonnement, le fait de pointer sur une barre dans le graphique des tendances d'utilisation affiche l'utilisation de la bande passante à ce moment-là, répartie par accès.



Activité des licences

La section **Activité des licences** permet de consulter les informations suivantes :

- **Utilisateurs sous licence :** affiche la liste des utilisateurs individuels auxquels des licences ont été attribuées. Cette liste inclut le domaine auquel appartient chaque utilisateur, la quantité de bande passante utilisée au cours des 30 derniers jours et la date à laquelle l'utilisateur a utilisé pour la dernière fois un service nécessitant de la bande passante.
- **Principaux utilisateurs** : affiche la liste des 10 principaux utilisateurs en fonction de l'utilisation de la bande passante. Cette liste inclut une ventilation de l'utilisation pour chaque utilisateur au cours des 30 derniers jours en fonction du type d'accès (Citrix DaaS ou Virtual Apps and Desktops local par agrégation de sites).

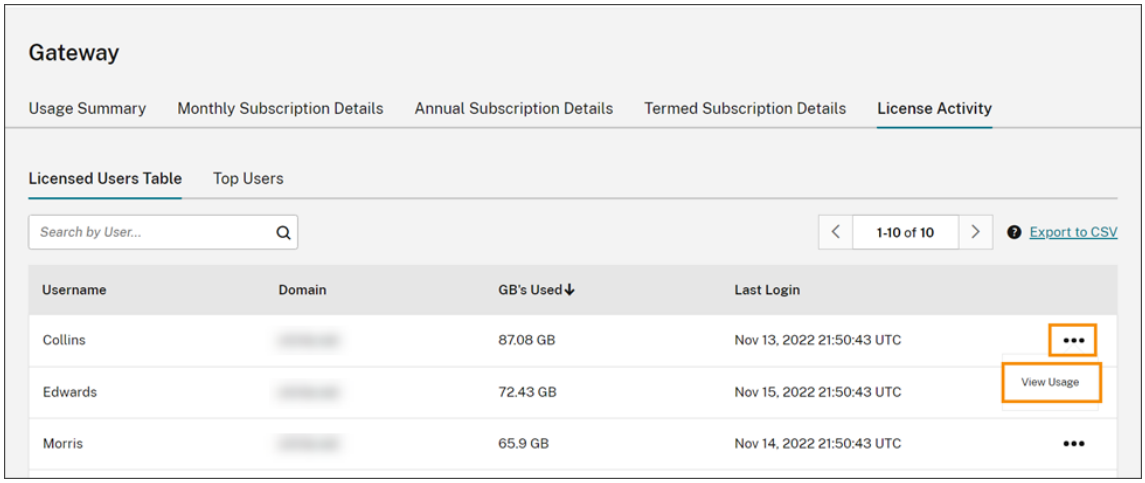


Citrix Cloud affiche l'utilisation de la bande passante au cours des 30 derniers jours pour un utilisateur

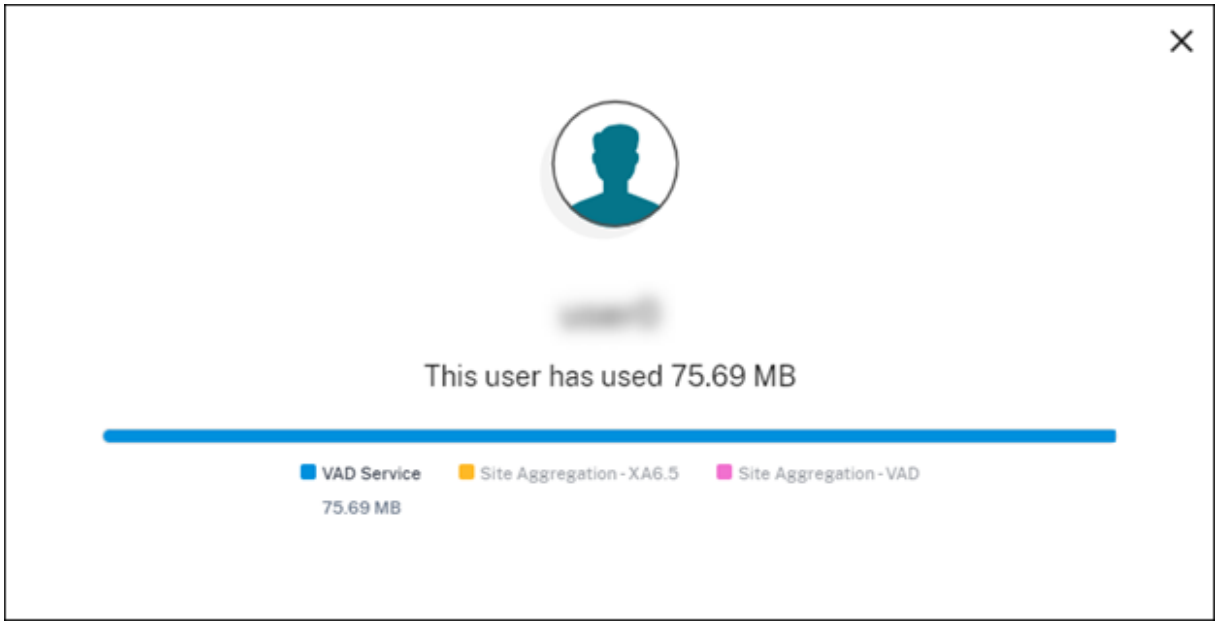
donné, même si ce dernier n'utilise plus de licence. Lorsqu'un abonnement à Gateway Service expire, Citrix Cloud affiche toujours la bande passante consommée par les utilisateurs individuels au cours de la période de 30 jours.

Afficher les détails d'utilisation d'un utilisateur spécifique

1. Sélectionnez **Tableau des utilisateurs sous licence** et recherchez un utilisateur dans la liste.
2. Sélectionnez **Afficher l'utilisation** dans le menu représentant des points de suspension situé à droite de la page.

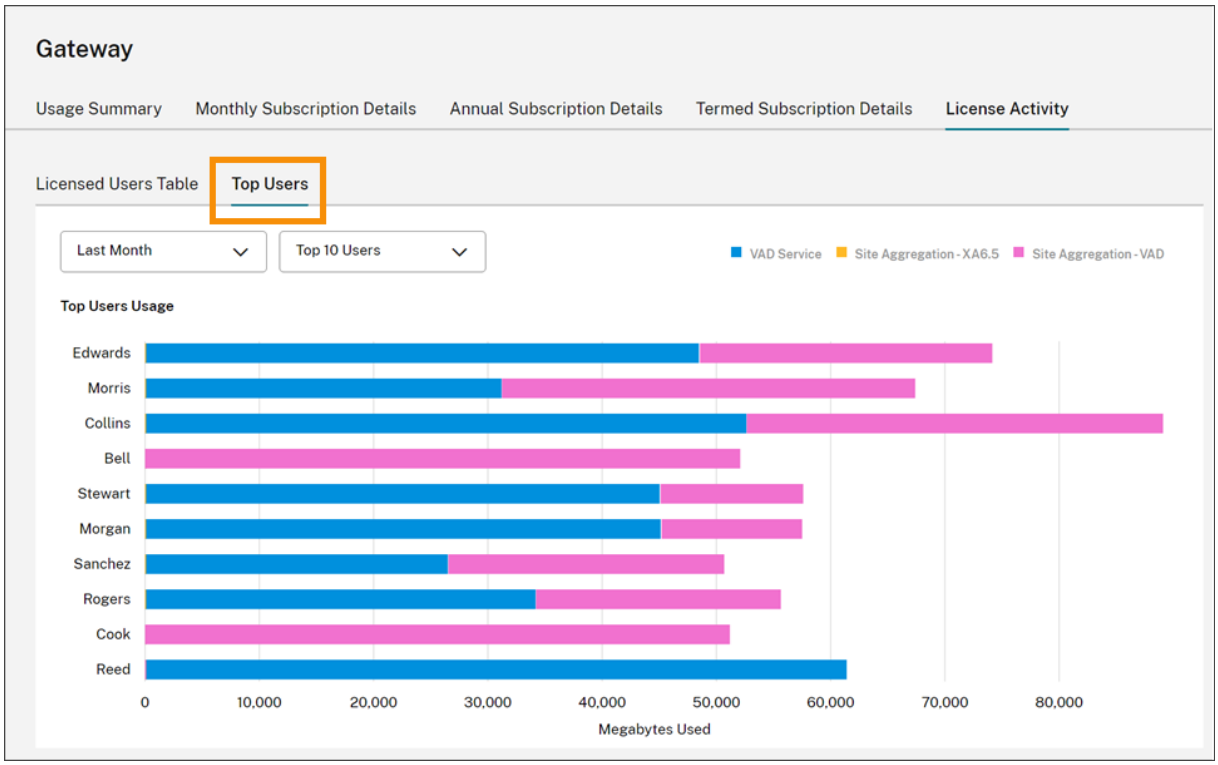


Citrix Cloud affiche la bande passante de l'utilisateur, ventilée par accès.



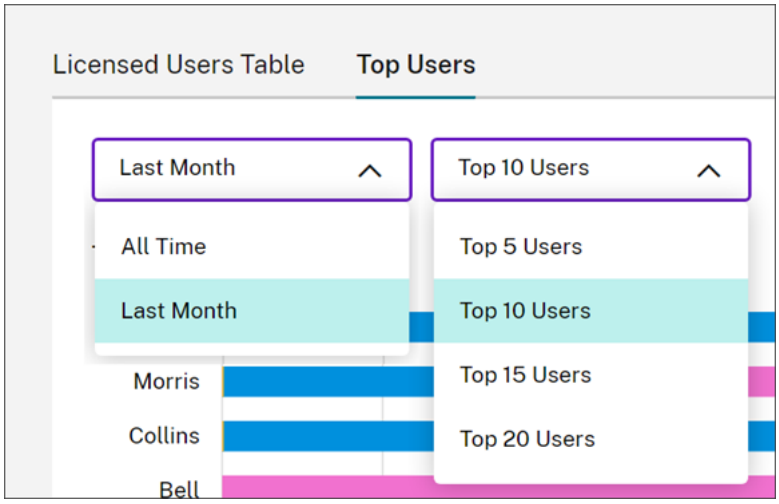
Afficher les détails d'utilisation des principaux utilisateurs

Sélectionnez **Principaux utilisateurs**.



Citrix Cloud affiche un graphique de l'utilisation de la bande passante par les principaux utilisateurs, ventilée par accès.

Par défaut, le graphique **Principaux utilisateurs** affiche les 10 utilisateurs ayant utilisé le plus de bande passante au cours des 30 derniers jours. Vous pouvez modifier cet affichage pour afficher les cinq premiers, les 15 premiers ou les 20 premiers utilisateurs. Vous pouvez également modifier la durée sur **Toute période**, ce qui permet d'afficher les principaux utilisateurs pendant la durée de votre abonnement. Pour modifier cet affichage, sélectionnez une option dans chaque menu.



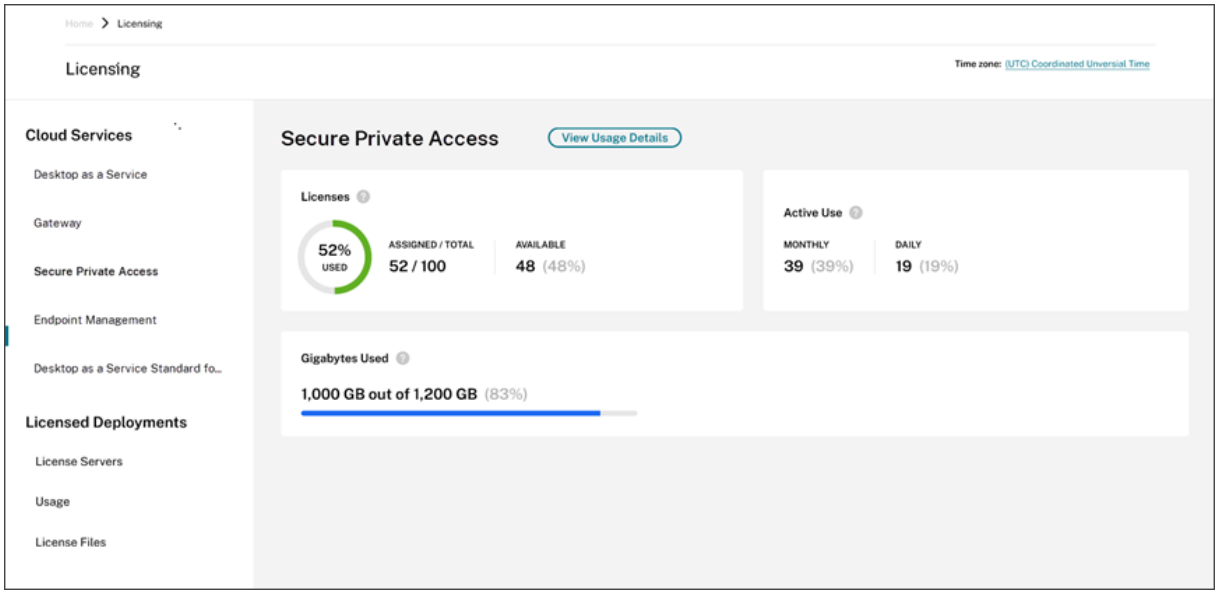
Surveillez les licences et l'utilisation pour Secure Private Access

November 29, 2023

Attribution de licence

Une licence est attribuée lorsqu'un utilisateur unique lance des application SaaS et Web ou des applications TCP et UDP pour la première fois.

Résumé de l'option Système de licences



Le résumé de l'écran Système de licences contient les 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 qui sont disponibles.
- 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.
- 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

Avec les abonnements Secure Private Access Advanced, chaque utilisateur a accès à 5 Go de bande passante par mois (60 Go par utilisateur, par an). Avec les abonnements Secure Private Access Standard, chaque utilisateur a accès à 1 Go de bande passante par mois (12 Go par utilisateur, par an). Cette bande passante est regroupée selon le nombre de licences et la période d'abonnement.

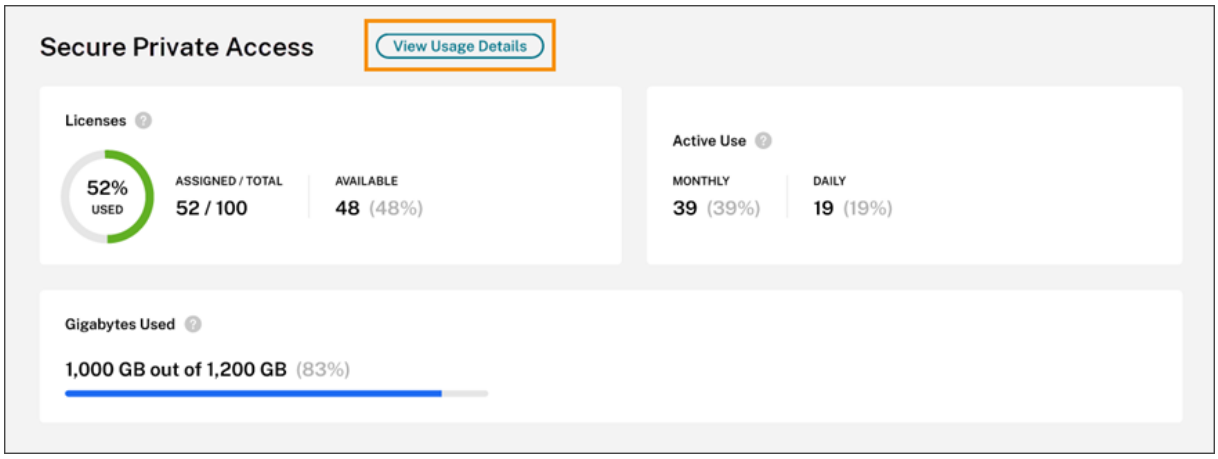
Par exemple, si vous achetez 100 licences pendant trois ans, vous disposez de 18 000 Go de bande passante totale (6 000 Go par an pendant trois ans). Cette bande passante est répartie entre tous les utilisateurs sous licence pendant la période de 3 ans. Si vous achetez des abonnements supplémentaires, Citrix Cloud affiche le nombre total de licences et de bande passante sur tous vos abonnements.

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. Si vous utilisez plus de bande passante que la quantité achetée à l'expiration de l'abonnement, la quantité de bande passante disponible reste à zéro lorsque vous renouvelez l'abonnement.

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.

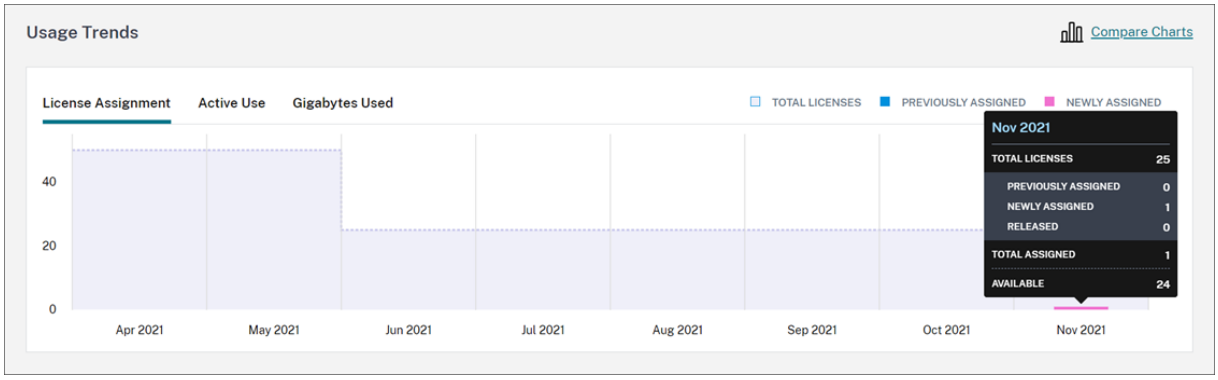
Tendances d'utilisation

Pour obtenir une vue détaillée de l'utilisation de la bande passante et des licences, cliquez sur **Afficher détails d'utilisation**.



Citrix Cloud affiche une répartition de la consommation de bande passante en fonction du type d'applications auxquelles les utilisateurs ont accès.

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



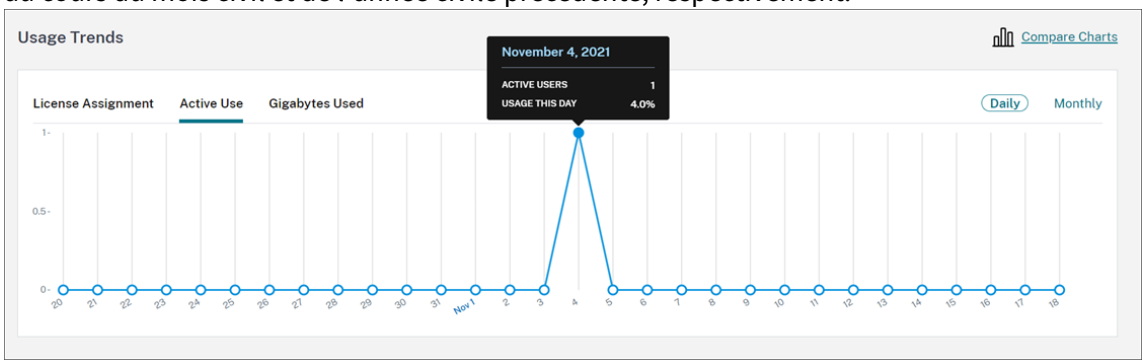
Cette répartition, sous **Tendances d'utilisation**, vous présente les informations suivantes :

- Dans l'onglet **Attribution de licences** :
  - **Nombre total de licences :** nombre total de licences achetées pour le service cloud pour

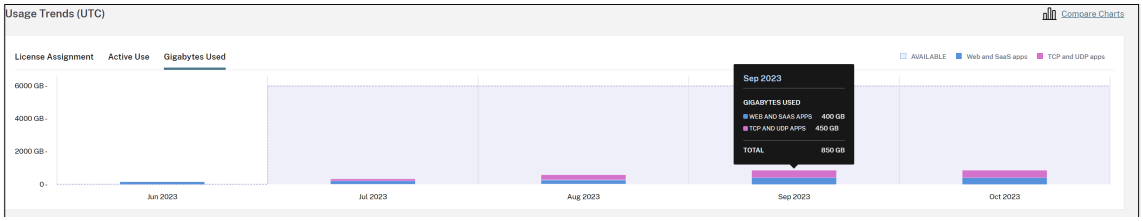
toutes les prestations.

- **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, Citrix Cloud comptabilise cette attribution dans le nombre « Précédemment attribuée » du mois d'août.
- **Nouvellement attribuées :** nombre de licences qui ont été attribuées chaque mois. Par exemple, si vous accédez au service cloud pour la première fois en juillet, une licence vous sera attribuée. Citrix Cloud comptabilise cette licence dans le nombre de licences nouvellement attribuées pour juillet.

- Dans l'onglet **Utilisation active** : tendances quotidiennes et mensuelles de l'utilisation active au cours du mois civil et de l'année civile précédente, respectivement.



- Dans l'onglet **Gigaoctets utilisés** : quantité de bande passante consommée par rapport à la bande passante totale disponible. Cet onglet affiche l'utilisation par utilisateur et les informations par application, telles que les applications Web et SaaS ou les applications TCP et UDP.



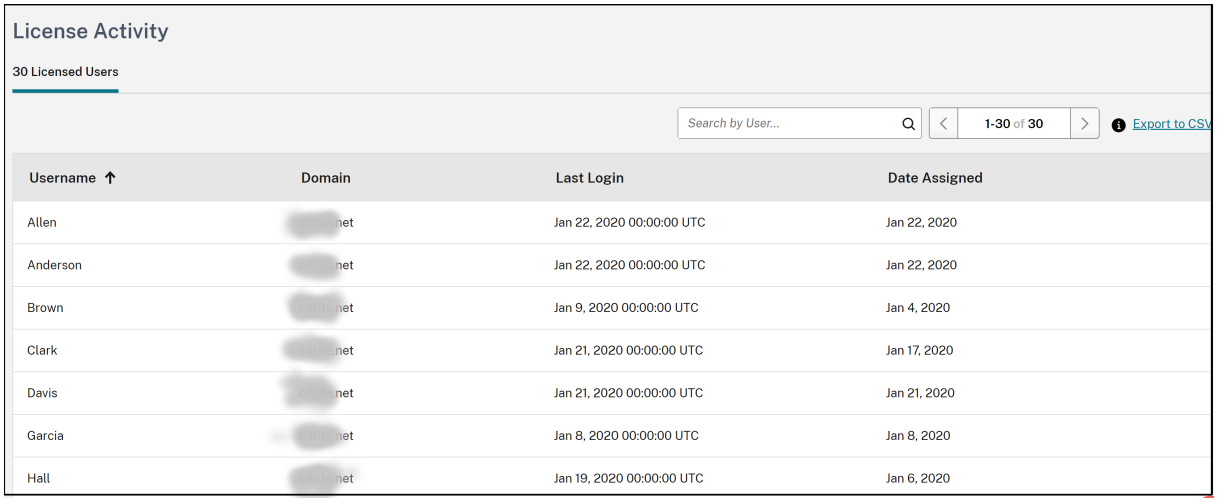
Pour comparer les tendances d'attribution des licences, d'utilisation active et d'utilisation de la bande passante, sélectionnez **Comparer les graphiques**.

Remarque :

Les tendances d'utilisation sont cumulatives pour la durée de la période d'abonnement actuelle. Lorsque vous renouvelez l'abonnement, les tendances d'utilisation sont réinitialisées au début de la nouvelle période d'abonnement.

Activité des licences

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



- Liste des utilisateurs individuels qui ont attribué des licences.
- Domaine auquel l'utilisateur appartient.
- Date à laquelle l'utilisateur a utilisé le service pour la dernière fois.
- Date à laquelle une licence a été attribuée à l'utilisateur.

Libérer des licences attribuées

Citrix Cloud libère automatiquement des licences si vous n'avez pas utilisé le service au cours des 30 derniers jours. Aucune action n'est requise de la part de l'administrateur Citrix pour libérer les licences.

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, vous pouvez acquérir une autre licence en vous connectant et en utilisant le service cloud.

Surveiller la consommation des ressources Citrix Managed Azure pour Citrix DaaS

October 4, 2023

Lorsque vous achetez un droit d'accès à Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service), vous pouvez également acheter le Citrix Azure Consumption Fund qui vous permet d'utiliser des ressources dans le cadre d'un abonnement Citrix Managed Azure. Vous pouvez utiliser

ces ressources pour mettre à disposition des applications et des bureaux pour vos utilisateurs en même temps que vos VDA locaux.

Lorsque vous achetez le Citrix Azure Consumption Fund, vous pouvez payer la consommation en utilisant l'une des méthodes suivantes :

- Paiement à l'utilisation : pour les ressources Citrix Managed Azure que vous utilisez au cours d'un mois donné, Citrix vous facture le mois suivant. Citrix Cloud affiche votre utilisation en tant que dépassement.
- Consommation prépayée : vous pouvez payer à l'avance la consommation sur une base mensuelle ou annuelle (échelonnée). Si votre utilisation dépasse la consommation prépayée, Citrix Cloud affiche cette utilisation en tant que dépassement. Pour tout dépassement au cours d'un mois donné, Citrix vous facture le mois suivant.

Chaque unité de consommation est évaluée à 1 $ US. La console de gestion des licences de Citrix Cloud vous permet de voir les unités que vous utilisez.

Pour estimer les coûts de consommation, utilisez le calculateur de consommation Citrix Managed Azure. Pour estimer la consommation et les coûts de licence pour Citrix DaaS Standard pour Azure (anciennement Citrix Virtual Apps and Desktops Standard pour Azure), utilisez le calculateur de licences et de consommation.

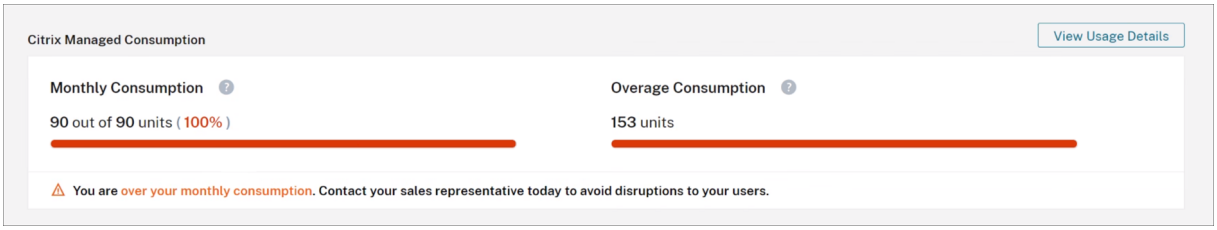
Produits pris en charge

La surveillance de la consommation est disponible pour les éditions suivantes de Citrix DaaS :

- Citrix DaaS Advanced (anciennement Virtual Apps Advanced)
- Citrix DaaS Premium (anciennement Virtual Apps Premium)
- Citrix DaaS Advanced Plus (anciennement Virtual Apps and Desktops Advanced)
- Citrix DaaS Premium (anciennement Virtual Apps and Desktops Premium)
- Citrix DaaS Standard pour Azure (anciennement Virtual Apps and Desktops Standard pour Azure)

Résumé de la consommation

La section Consommation de Citrix Managed affiche un résumé des unités que vous avez utilisées dans votre Consumption Fund.



La **consommation mensuelle** indique le nombre d'unités que vous avez consommées pour le mois en cours par rapport au nombre total d'unités Consumption Fund mensuelles que vous avez achetées. La consommation mensuelle est réinitialisée chaque mois. Les unités non consommées ne sont pas reportées au mois suivant.

La **consommation annuelle** indique le nombre d'unités que vous avez consommées par rapport au nombre total d'unités Consumption Fund annuelles que vous avez achetées. Comme pour les unités de consommation mensuelle, les unités annuelles non consommées ne sont pas reportées à l'année suivante.

La **consommation excédentaire** indique le nombre d'unités que vous avez consommées au-delà du nombre d'unités de votre Azure Consumption Fund. Si vous utilisez des ressources Citrix Managed Azure sur une base de paiement à l'utilisation, votre consommation apparaît comme excédentaire par défaut.

Comment l'excédent est mesuré

Si vous utilisez Azure Consumption Fund sur une base de paiement à l'utilisation, Citrix Cloud affiche le nombre d'unités que vous avez consommées pour le mois en cours en tant qu'excédent.

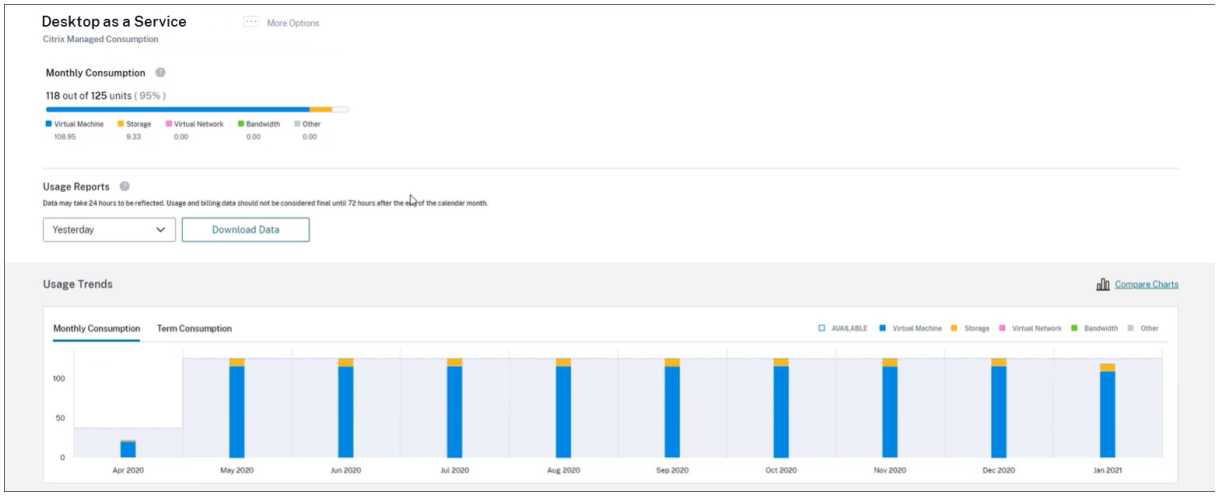
Si vous avez prépayé votre consommation sur une base mensuelle ou annuelle, Citrix Cloud affiche le nombre d'unités mensuelles ou annuelles que vous avez consommées pour le mois ou l'année en cours. Si vous consommez plus d'unités que le nombre acheté, Citrix Cloud affiche les unités excédentaires comme excédent.

Si vous avez prépayé votre consommation sur une base mensuelle et annuelle, Citrix Cloud mesure d'abord votre consommation par rapport aux unités mensuelles que vous avez achetées. Une fois ces unités consommées, Citrix Cloud mesure votre consommation par rapport à vos unités annuelles. Une fois ces unités consommées, Citrix Cloud affiche toutes les unités excédentaires que vous consommez en tant qu'excédent.

Si vous achetez des unités de consommation supplémentaires et que votre compte possède déjà un excédent, les nouvelles unités de consommation ne sont pas appliquées à l'excédent. Les nouvelles unités de consommation ne sont appliquées qu'à l'utilisation effectuée après l'achat de ces unités.

Détails sur la consommation

Pour obtenir une vue détaillée de vos unités de consommation, cliquez sur **Afficher détails d'utilisation** à l'extrême droite du résumé. La page de détails affiche la répartition de votre consommation et les tendances d'utilisation.



Rapports d'utilisation

Vous pouvez télécharger les informations d'utilisation sous forme de fichier CSV pour un intervalle que vous spécifiez. Cliquez sur **Télécharger les données** pour générer et télécharger un fichier CSV sur votre ordinateur local.

Les données peuvent prendre jusqu'à 72 heures après la fin d'un jour/mois pour refléter toutes les utilisations.

Le fichier CSV comprend les sections suivantes :

- Récapitulatif qui indique les unités de consommation disponibles avant et après la plage de dates du rapport, le total des frais d'utilisation et les excédents en attente.

Data may take 24 hours to be reflected. Usage and billing data should not be considered final until 72 hours after the end of the calendar month.			
Org ID	51938754		
Report Date	12/3/2021		
Date Start	11/1/2021		
Date End	11/30/2021		
Report Summary			
	Credits	Debits	
Monthly Consumption Units Available before 11/01/2021	$0		
Termed Consumption Units Available before 11/01/2021	$0		
Trial Consumption Units Available before 11/01/2021	$0		
Total Usage to Charge		$851.96	
Expired Consumption Commitment		$0.00	
Total	$0.00	$851.96	
Monthly Consumption Units Available after 11/30/2021	$0		
Termed Consumption Units Available after 11/30/2021	$0		
Trial Consumption Units Available after 11/30/2021	$0		
Pending Overage by 11/30/2021	$0.00		

- Récapitulatif quotidien qui indique le total des frais d'utilisation, les fonds mensuels et annuels restants et les frais d'utilisation excédentaire pour chaque jour de la plage de dates du rapport.

Daily Summary				
Date	Total Usage	Remaining Monthly Funds	Remaining Termed Funds	Overage Amount
11/1/2021	$28.40	$0	$0	$0
11/2/2021	$28.40	$0	$0	$0
11/3/2021	$28.40	$0	$0	$0
11/4/2021	$28.40	$0	$0	$0
11/5/2021	$28.39	$0	$0	$0
11/6/2021	$28.39	$0	$0	$0
11/7/2021	$28.40	$0	$0	$0
11/8/2021	$28.40	$0	$0	$0

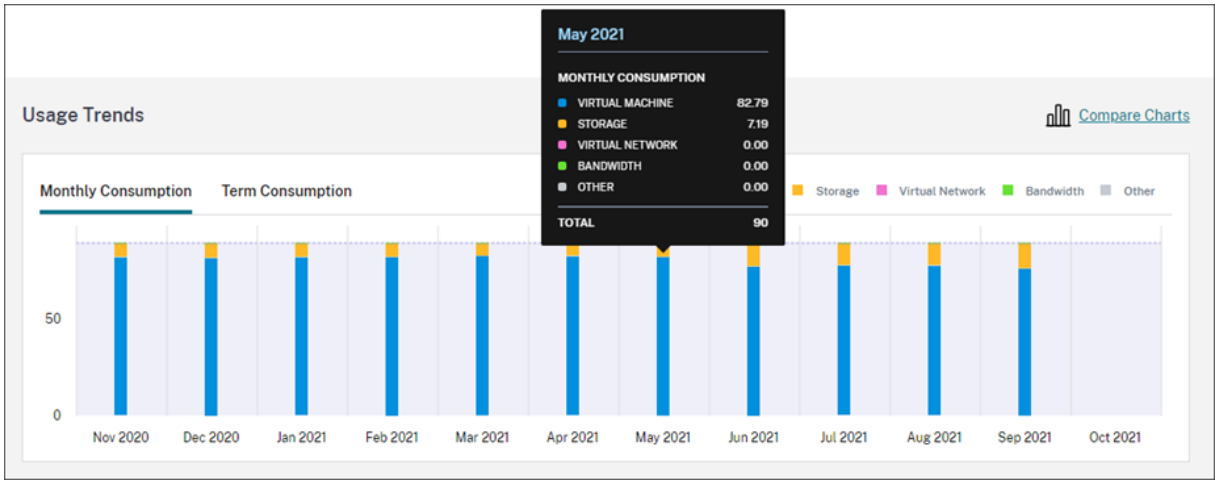
- Utilisation mesurée des machines virtuelles Azure, des connexions réseau, du stockage Azure et de la bande passante pour chaque jour de la plage de dates du rapport.

Date	Citrix Meter Name	Citrix Meter Description	Catalog Id	Catalog Name	Citrix Meter Region	Citrix Meter Category	Citrix Meter Sub Category	Citrix Meter Unit	Quantity	SRP	Total	Total Charged
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		07f1d01f-9ffb-472e-93ab-ae2d7393202a	Win-11-MS-2	None	Bandwidth		10 GB	0.0000444	$1.13	$0.00	$0.00
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		f061eeac-2507-459c-ab99-71fde94b318e	Finance desktops	None	Bandwidth		10 GB	0.0000018	$1.13	$0.00	$0.00
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		N/A	N/A	None	Bandwidth		10 GB	0.0064263	$1.13	$0.01	$0.01
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		cb7516c0-33e7-485a-9eb0-d84b7f2e9c5a	Windows-11-MultiSession	None	Bandwidth		10 GB	0.0000137	$1.13	$0.00	$0.00
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		6dbcda61-cdf6-4135-86e0-76e2f5f45204	Windows-11-SingleSession	None	Bandwidth		10 GB	0.0000015	$1.13	$0.00	$0.00
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		dfb04e0a-b08f-4f0a-af95-fff7cdd6cd83	AVD Desktops	None	Bandwidth		10 GB	0.0000073	$1.13	$0.00	$0.00
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		e86cee4e-1930-4d87-b2e5-3b189bb3e6e3	Win-11-SS-22	None	Bandwidth		10 GB	0.0000334	$1.13	$0.00	$0.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		f061eeac-2507-459c-ab99-71fde94b318e	Finance desktops	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		e86cee4e-1930-4d87-b2e5-3b189bb3e6e3	Win-11-SS-22	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		dfb04e0a-b08f-4f0a-af95-fff7cdd6cd83	AVD Desktops	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		cb7516c0-33e7-485a-9eb0-d84b7f2e9c5a	Windows-11-MultiSession	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		07f1d01f-9ffb-472e-93ab-ae2d7393202a	Win-11-MS-2	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		6dbcda61-cdf6-4135-86e0-76e2f5f45204	Windows-11-SingleSession	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Network Peering - Ingress		N/A	N/A	None	VirtualNetwork		100 GB	0.00016714	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		f061eeac-2507-459c-ab99-71fde94b318e	Finance desktops	None	VirtualNetwork		100 GB	0.00000034	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Ingress		cb7516c0-33e7-485a-9eb0-d84b7f2e9c5a	Windows-11-MultiSession	None	VirtualNetwork		100 GB	0.00000323	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Ingress		07f1d01f-9ffb-472e-93ab-ae2d7393202a	Win-11-MS-2	None	VirtualNetwork		100 GB	0.00000422	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		07f1d01f-9ffb-472e-93ab-ae2d7393202a	Win-11-MS-2	None	VirtualNetwork		100 GB	0.00000165	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Ingress		dfb04e0a-b08f-4f0a-af95-fff7cdd6cd83	AVD Desktops	None	VirtualNetwork		100 GB	0.00000307	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		e86cee4e-1930-4d87-b2e5-3b189bb3e6e3	Win-11-SS-22	None	VirtualNetwork		100 GB	0.00000129	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		cb7516c0-33e7-485a-9eb0-d84b7f2e9c5a	Windows-11-MultiSession	None	VirtualNetwork		100 GB	0.00000148	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		dfb04e0a-b08f-4f0a-af95-fff7cdd6cd83	AVD Desktops	None	VirtualNetwork		100 GB	0.00000115	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Ingress		e86cee4e-1930-4d87-b2e5-3b189bb3e6e3	Win-11-SS-22	None	VirtualNetwork		100 GB	0.00000342	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		N/A	N/A	None	VirtualNetwork		100 GB	0.00012714	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		6dbcda61-cdf6-4135-86e0-76e2f5f45204	Windows-11-SingleSession	None	VirtualNetwork		100 GB	0.00000121	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Ingress		6dbcda61-cdf6-4135-86e0-76e2f5f45204	Windows-11-SingleSession	None	VirtualNetwork		100 GB	0.00000323	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Ingress		f061eeac-2507-459c-ab99-71fde94b318e	Finance desktops	None	VirtualNetwork		100 GB	0.00000094	$1.30	$0.00	$0.00
11/1/2021	General Block Blob - Read Operations		N/A	N/A	None	Storage		100000000	0.00000016	$4.68	$0.00	$0.00
11/1/2021	Standard HDD Managed Disks - S10 - Disks - US East		N/A	N/A	US East	Storage		1 /Month	0.400032	$7.64	$3.06	$3.06
11/1/2021	Standard HDD Managed Disks - S10 - Disks - US East		dfb04e0a-b08f-4f0a-af95-fff7cdd6cd83	AVD Desktops	US East	Storage		1 /Month	0.033336	$7.64	$0.25	$0.25
11/1/2021	Standard HDD Managed Disks - S10 - Disks - US East		6dbcda61-cdf6-4135-86e0-76e2f5f45204	Windows-11-SingleSession	US East	Storage		1 /Month	0.100008	$7.64	$0.76	$0.76
11/1/2021	Virtual Machines Av2 Series - A2 v2 - US East		N/A	N/A	US East	VirtualMachine		100 Hours	0.48	$11.83	$5.68	$5.68
11/1/2021	Premium SSD Managed Disks - P10 - Disks - US East		f061eeac-2507-459c-ab99-71fde94b318e	Finance desktops	US East	Storage		1 /Month	0.033336	$19.22	$0.64	$0.64
11/2/2021	Bandwidth - Data Transfer Out - Zone 1		07f1d01f-9ffb-472e-93ab-ae2d7393202a	Win-11-MS-2	None	Bandwidth		10 GB	0.0000235	$1.13	$0.00	$0.00

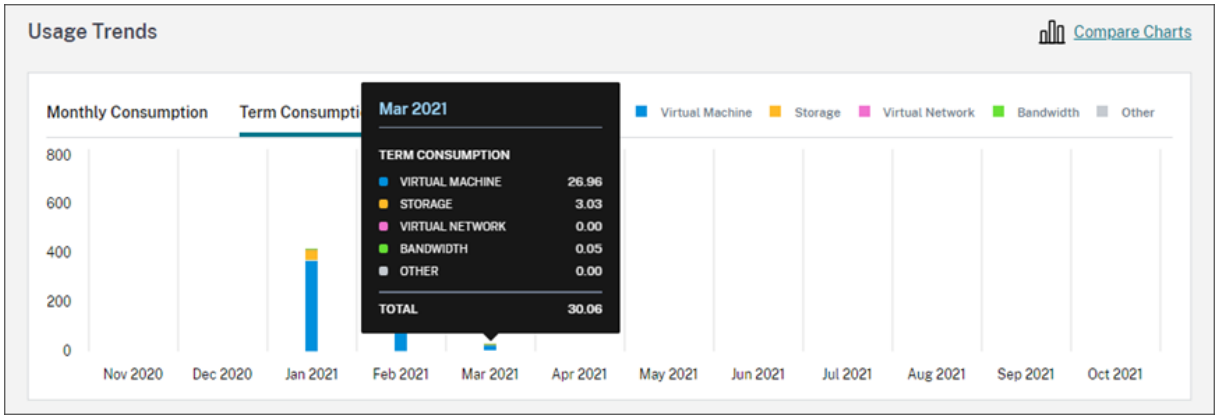
Tendances d'utilisation et activité de consommation

La section **Tendances d'utilisation** affiche un graphique des ressources Citrix Managed Azure que vous avez utilisées. Pointez sur une barre du graphique pour afficher la quantité de ressources que vous avez consommée pour ce mois, y compris les machines virtuelles, le stockage, les ressources réseau virtuelles et la bande passante.

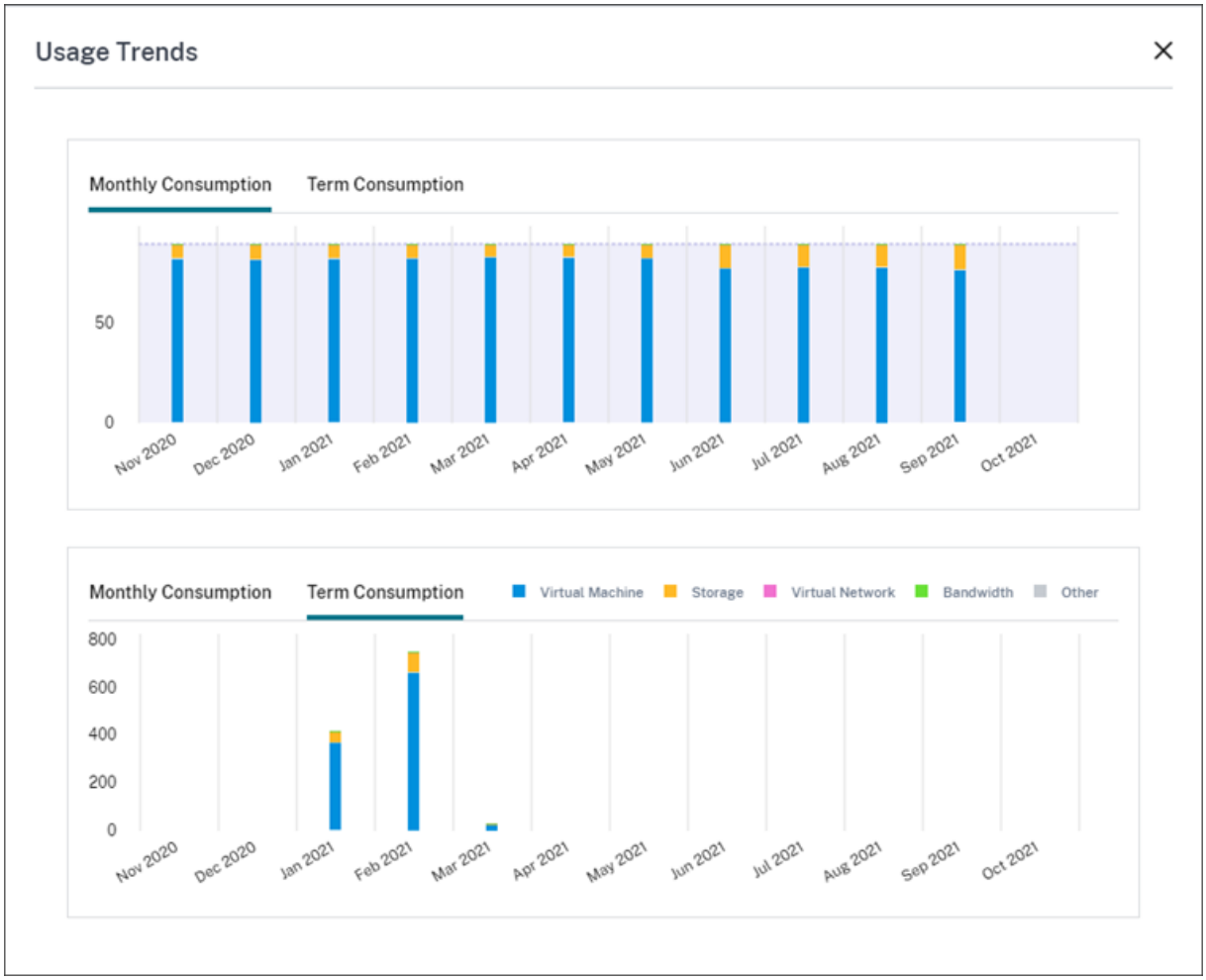
Sélectionnez **Consommation mensuelle** pour afficher votre consommation mensuelle des 12 derniers mois.



Sélectionnez **Consommation annuelle** pour afficher votre consommation pour chaque mois de l'année précédente.

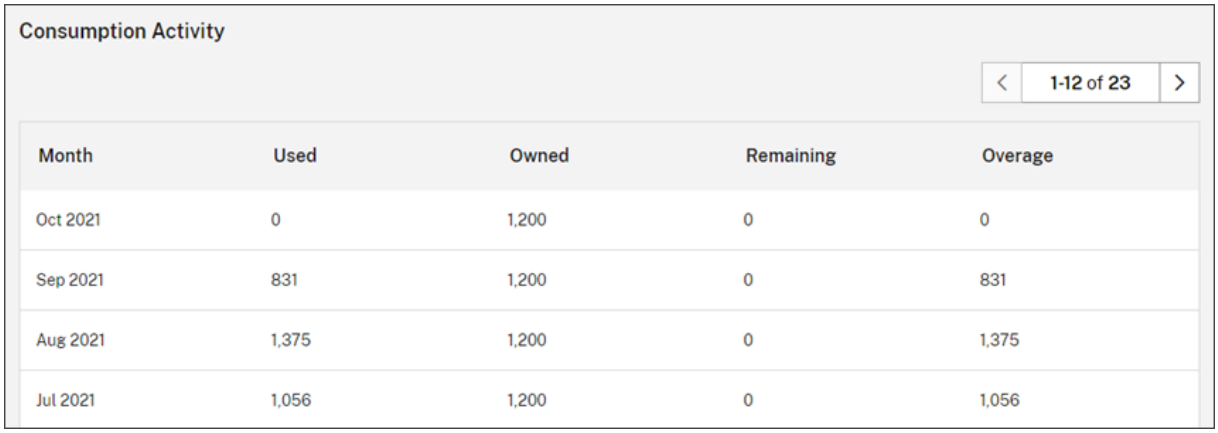


Si vous avez acheté des unités de consommation mensuelles et annuelles, sélectionnez **Comparer les graphiques** à l'extrême droite du graphique pour afficher les tendances de consommation mensuelles et annuelles dans une seule vue.



La section **Activité de consommation** affiche également une liste de vos unités de consommation

pour chaque mois.



Month	Used	Owned	Remaining	Overage
Oct 2021	0	1,200	0	0
Sep 2021	831	1,200	0	831
Aug 2021	1,375	1,200	0	1,375
Jul 2021	1,056	1,200	0	1,056

L'activité de consommation comprend les informations suivantes :

- **Utilisé :** nombre d'unités utilisées au cours de chaque mois.
- **Détenu :** nombre total d'unités achetées pour chaque mois.
- **Restant :** nombre d'unités achetées qui n'ont pas été utilisées au cours de chaque mois.
- **Excédent :** nombre d'unités consommées qui ont dépassé les unités que vous avez achetées au cours de chaque mois.

Libérer des licences attribuées

Le moment auquel les attributions de licence peuvent être libérées dépend des unités Consumption Fund que vous avez achetées.

Vous pouvez libérer des licences inactives après 30 jours si :

- Vous n'utilisez pas d'abonnement Citrix Managed Azure avec votre déploiement de service.
- Vous avez acheté des unités de consommation annuelle à utiliser avec votre déploiement de service.

Vous pouvez libérer des licences inactives au cours du mois en cours, à condition qu'aucun utilisateur ou appareil n'ait lancé d'applications ou de bureaux, si :

- Vous avez acheté des unités mensuelles Consumption Fund à utiliser avec votre déploiement de service.
- Vous avez acheté des unités mensuelles et annuelles Consumption Fund.

Pour obtenir des instructions sur la libération de licences éligibles, consultez les articles suivants :

- Citrix DaaS (modèle utilisateur/appareil) : Libérer des licences attribuées
- Citrix DaaS Standard pour Azure : Libérer des licences attribuées

Surveiller les licences et l'utilisation sur les déploiements locaux

October 4, 2023

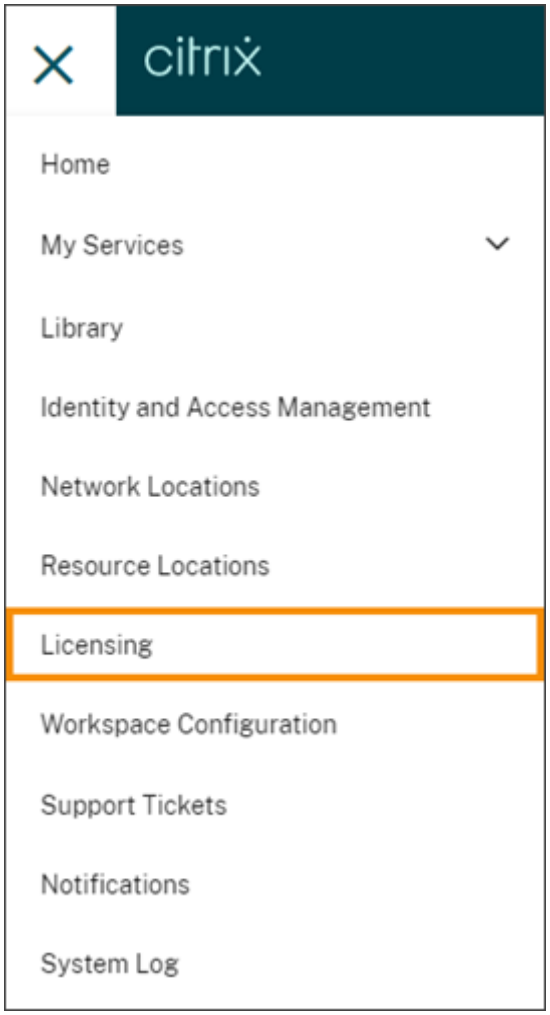
L'expérience de déploiements sous licence dans Citrix Cloud comprend les tâches suivantes :

- 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.
- 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.

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.

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

Exigences en matière de connectivité

Pour enregistrer correctement votre serveur de licences auprès de Citrix Cloud, assurez-vous que les adresses suivantes sont joignables :

- `https://citrix.cloud.com/` (pour accéder à la console d'administration pour entrer le code et afficher l'état du serveur de licences)

- 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

Se connecter à Citrix Cloud

Pour activer les informations sur l'utilisation du serveur de licences Citrix, vous devez effectuer les tâches suivantes :

1. Accédez à des insights sur l'utilisation de vos serveurs de licences à l'aide de la console Licensing Manager. Pour plus d'informations, consultez Partager les statistiques d'utilisation dans la documentation produit de Gestion des licences.
2. Passez en revue les exigences de connectivité décrites dans la section Exigences en matière de connectivité de cet article et assurez-vous que les adresses sont joignables. Si vous utilisez un serveur proxy avec le serveur de licences Citrix, assurez-vous que le serveur proxy est configuré comme décrit dans Étape 5 Configurer un serveur proxy de la documentation produit de Gestion des licences.
3. Enregistrez votre serveur de licences auprès de Citrix Cloud comme décrit dans la section Enregistrer des produits sur site avec Citrix Cloud.

Afficher l'utilisation locale des licences produit

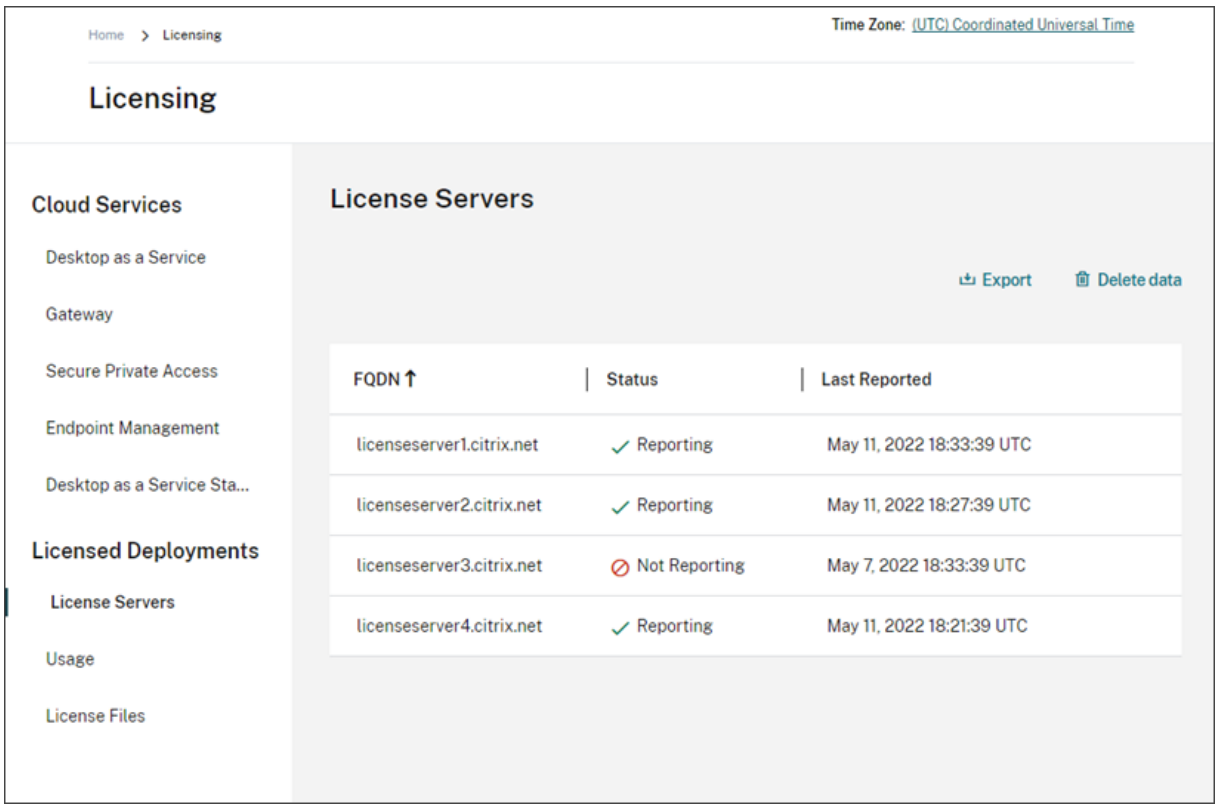
Les informations sur l'utilisation du serveur de licences Citrix fournissent une visibilité sur l'utilisation des licences dans l'ensemble de votre parc Citrix. Vous pouvez accéder aux rapports d'utilisation pour :

- 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.

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.

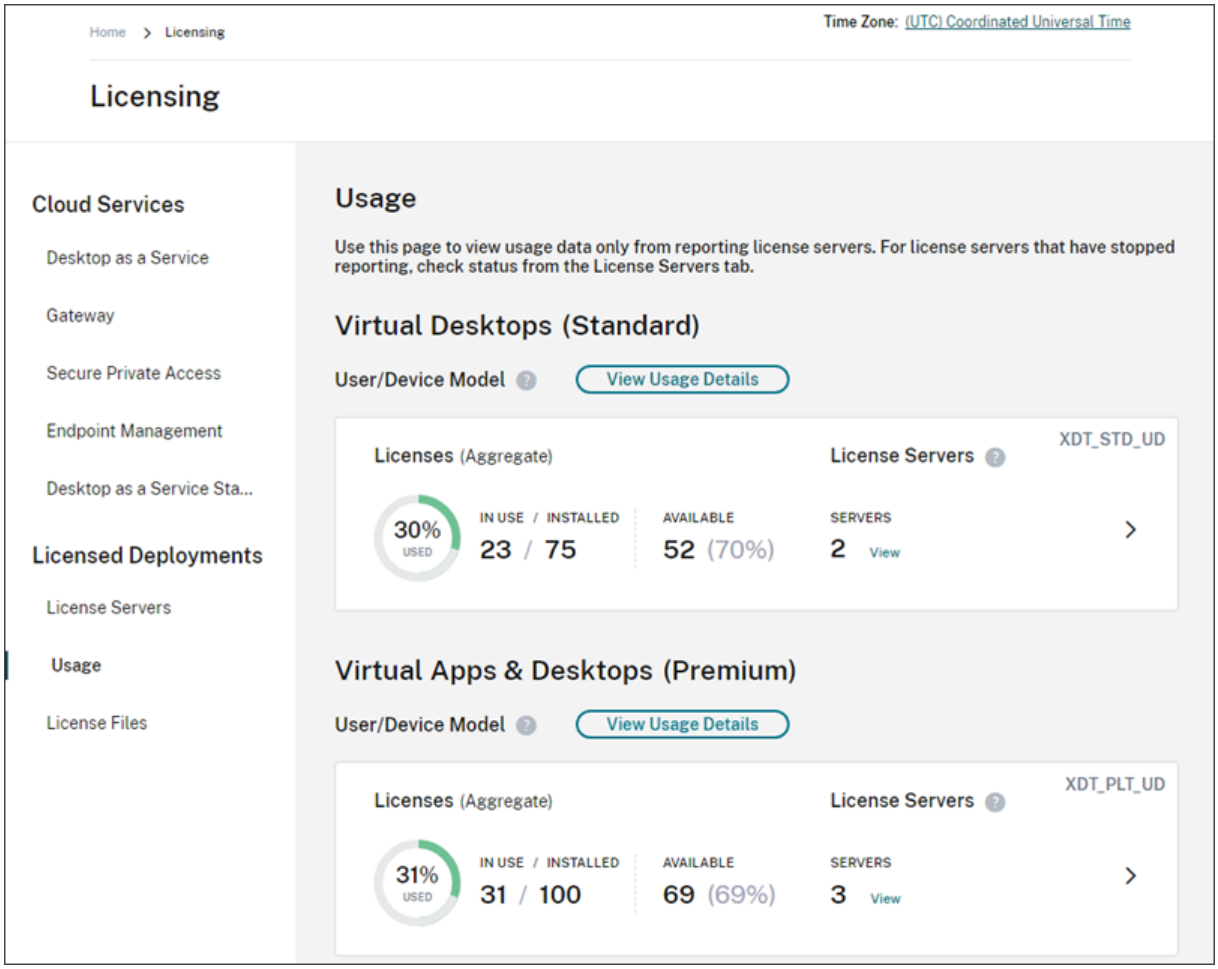
Impact de l'état du serveur de licences sur les vues d'utilisation des licences

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.

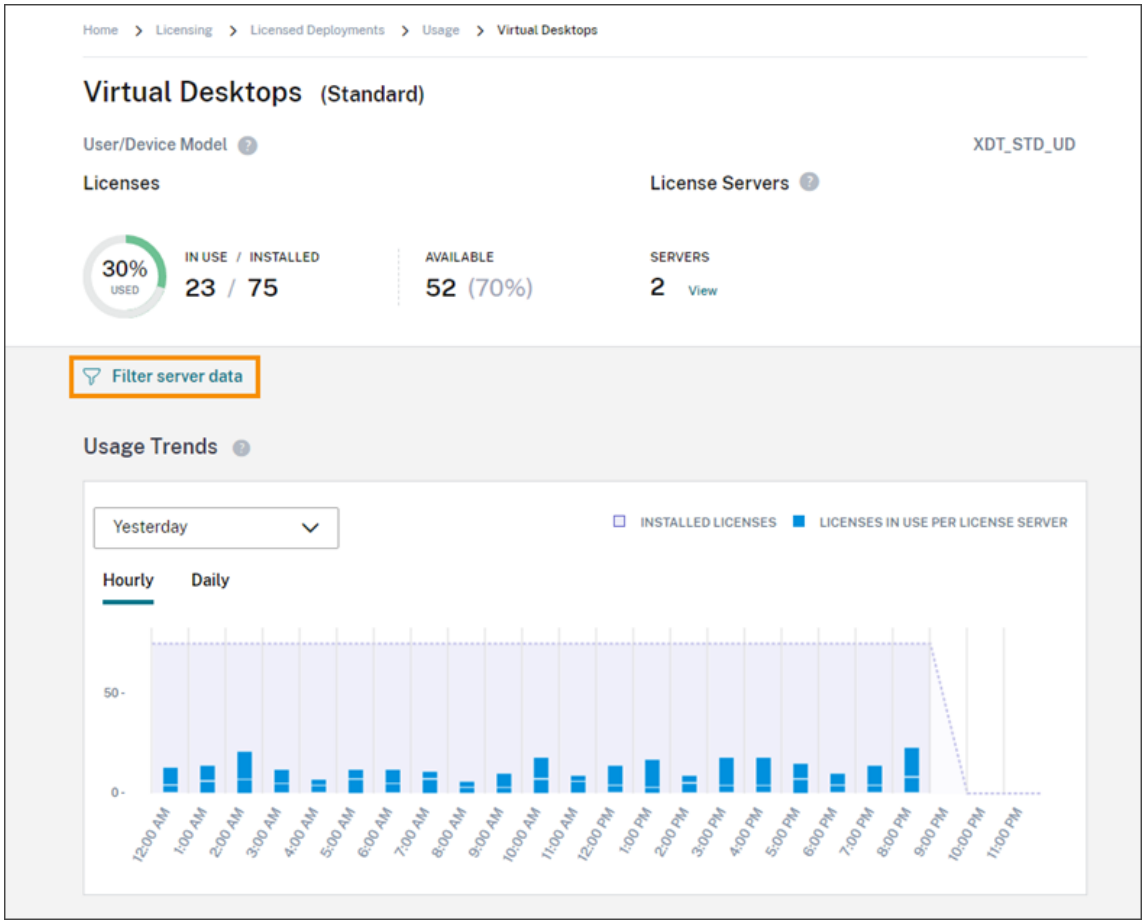


L'utilisation des licences est organisée et agrégée sur plusieurs serveurs de licences en fonction de l'édition du produit et du modèle de licence. Une fiche récapitulative de l'utilisation des licences est affichée pour chaque édition de licence unique trouvée sur tous les serveurs de licences de reporting. Une fiche récapitulative est affichée pour chaque édition de produit détectée.

Utilisation par serveur de licences

Pour afficher l'utilisation des licences de produit pour chaque serveur de licences, vous pouvez filtrer les données des serveurs.

1. Sur la page **Utilisation**, sélectionnez **Afficher détails d'utilisation** pour le produit que vous souhaitez gérer.
2. Cliquez sur **Filtrer les données du serveur**, puis sélectionnez les serveurs de licences dont vous souhaitez afficher l'utilisation. Par défaut, tous les serveurs de licences sont sélectionnés.



3. Sélectionnez **Appliquer**.

Une fois le filtre appliqué, Citrix Cloud affiche les tendances d'utilisation, la répartition des serveurs de licences et l'activité des licences uniquement pour les serveurs que vous avez sélectionnés.

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.

Supprimer l'enregistrement du serveur de licences

La suppression complète de l'enregistrement du serveur de licences de Citrix Cloud comprend les tâches suivantes :

1. Supprimer le serveur de licences enregistré auprès de Citrix Cloud à l'aide de la console Citrix Licensing Manager. Pour obtenir des instructions complètes, consultez Supprimer l'enregistrement de votre serveur de licences.
2. Supprimer toutes les données d'utilisation précédemment collectées.
3. Vérifier que Citrix Cloud n'affiche plus le serveur de licences sur la page Enregistrements de produits. Si le serveur de licences apparaît toujours dans la liste, supprimez-le comme décrit dans la section Supprimer un enregistrement de produit.

Supprimer les données d'utilisation

Lorsque vous supprimez un serveur de licences enregistré auprès de Citrix Cloud, les données d'utilisation précédemment collectées sont toujours stockées. Si vous ne souhaitez plus conserver ces données, vous pouvez les supprimer.

> **Important :**
>
> La suppression des données d'utilisation est permanente et ne peut pas être annulée. Si vous supprimez les données d'utilisation mais ne supprimez pas l'enregistrement de votre serveur de licences, Citrix Cloud continue de collecter des données d'utilisation.

1. Dans le menu Citrix Cloud, sélectionnez **Système de licences**.
2. Dans l'onglet **Serveurs de licences**, sélectionnez **Supprimer les données**.
3. Lorsque vous y êtes invité, cochez les cases pour confirmer que vous comprenez l'impact de la suppression.
4. Sélectionnez **Supprimer les données du serveur**.

Système de licences pour les partenaires Citrix Service Provider (CSP)

July 2, 2024

Le service License Usage Insights de Citrix Cloud est un service de cloud gratuit qui permet aux partenaires **Citrix Service Providers (CSP)** de comprendre et de créer des rapports sur les licences et l'utilisation des produits. Seuls les partenaires CSP ont accès à License Usage Insights.

> **Remarque :**
>
> Citrix DaaS était auparavant Citrix Virtual Apps and Desktops Service. Citrix DaaS Standard pour Azure était auparavant Citrix Virtual Apps and Desktops Standard pour Azure. Certains affichages peuvent contenir l'ancien nom.

Le service License Usage Insights vous permet de :

- Collecter et agréger automatiquement les informations sur l'utilisation des produits à partir des serveurs de licences Citrix
- Regrouper automatiquement l'utilisation et la consommation des licences cloud pour les clients mono-locataires et multi-locataires
- 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 au format CSV les données d'utilisation des licences Virtual Apps and Desktops et Citrix DaaS, les données d'allocation NetScaler VPX, ainsi que les données de consommation et de licences Citrix DaaS Standard pour Azure

Informations supplémentaires

Pour connaître les exigences et les instructions de configuration, consultez la section Prise en main de License Usage Insights.

Pour afficher l'utilisation agrégée des licences pour les clients mono-locataires et les partenaires multi-locataires, consultez Utilisation de licences et rapports Cloud Service pour les partenaires Citrix Service Provider.

Pour afficher l'utilisation des clients pour les services pris en charge à l'aide de la console Système de licences, consultez les articles suivants :

- Surveillance des licences client et de l'utilisation pour Citrix DaaS
- Surveillance des licences client et de l'utilisation pour Citrix DaaS Standard pour Azure

Prise en main de License Usage Insights

July 2, 2024

Produits Citrix pris en charge

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

- Utilisation du produit Virtual Apps and Desktops (instance locale)
- Citrix DaaS Premium (anciennement services Virtual Apps Premium et Virtual Apps and Desktops Premium)
- Citrix DaaS Standard pour Azure (anciennement Citrix Virtual Apps and Desktops Standard pour Azure)
- Allocations NetScaler Console VPX

Exigences

Pour capturer les informations de licence et d'utilisation des produits Citrix locaux, le serveur de licences Citrix 11.16.3.0 ou version ultérieure est requis. Seuls les serveurs de licences Windows et VPX sont pris en charge.

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.

Étape 1 : Mettre à jour le serveur de licences Citrix

Si vous exécutez des serveurs de licences antérieurs à la version 11.16.3.0, vous devez mettre à niveau vos serveurs de licences avant d'utiliser License Usage Insights. La mise à niveau sur place est simple et rapide. Effectuez les tâches suivantes :

1. Téléchargez la dernière version du serveur de licences. Pour de plus amples informations sur la dernière version du serveur de licences Citrix, consultez la documentation relative au système de licences Citrix.
2. Mettez à niveau votre serveur de licences actuel.
3. Répétez le processus de mise à niveau pour chacun de vos serveurs de licences.

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

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

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

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

Étape 3 (facultatif) : 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 ou Citrix DaaS 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 de License Usage Insights 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 License Usage Insights 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>
<!--NeedCopy-->
```

3. Enregistrez le fichier.

Étape 4 : Utiliser le service License Usage Insights

À partir de la console Citrix Cloud, recherchez License Usage Insights et cliquez sur **Gérer**. Pour obtenir une présentation des principales fonctionnalités du service, consultez Gérer l'utilisation des produits, les serveurs de licences et les notifications.

Détails supplémentaires

Lorsque vous utilisez le serveur de licences Citrix avec License Usage Insights, tenez compte des éléments suivants :

- Un serveur de licences récemment mis à jour peut prendre jusqu'à 24 heures avant d'apparaître dans la console de gestion License Usage Insights.
- 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 à License Usage Insights 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 ou Citrix DaaS 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 de License Usage Insights 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.

Aide et assistance

Si vous avez besoin d'aide avec License Usage Insights, ouvrez un ticket d'assistance via le portail My Support. Pour accéder à My Support depuis Citrix Cloud :

1. Connectez-vous à Citrix Cloud.
2. Cliquez sur l'icône **Aide** en haut à droite de l'écran.
3. Sélectionnez **Ouvrir un ticket**.
4. Sélectionnez **Accéder à My support** et connectez-vous avec vos informations d'identification My Citrix.
5. Remplissez le formulaire et envoyez-le.

Un membre du support technique Citrix donnera suite à votre demande.

Questions fréquemment posées

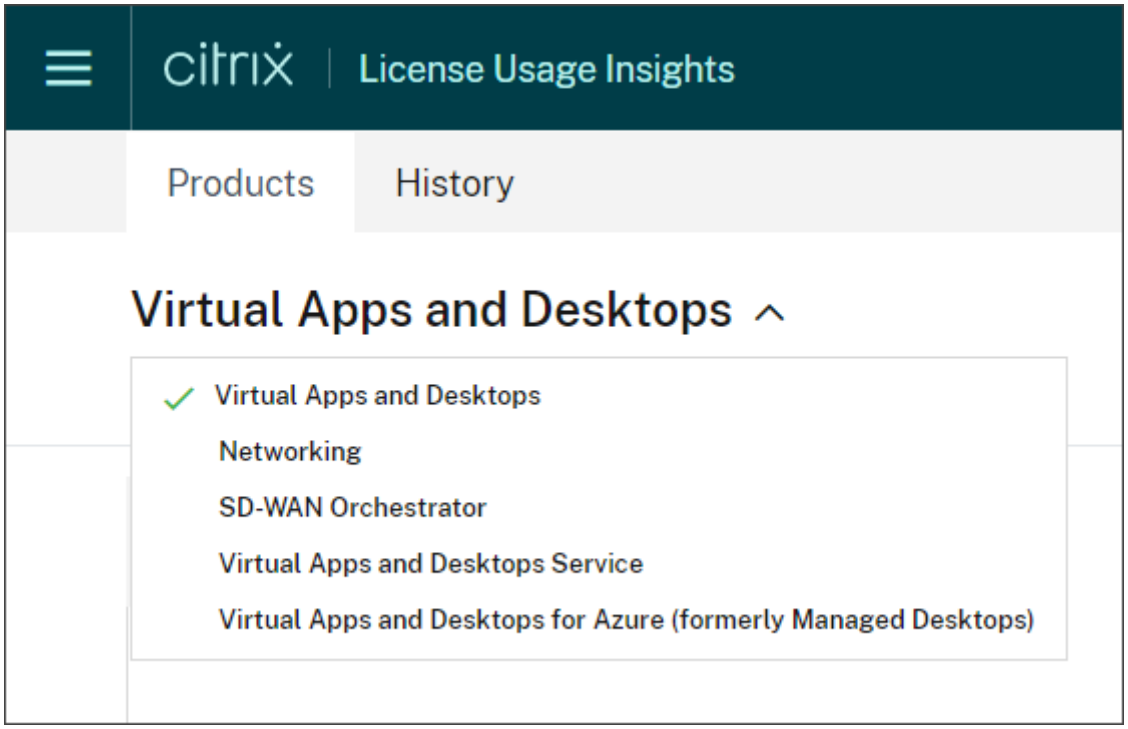
- **Quelles informations sont-elles envoyées ? Puis-je consulter les informations que mes serveurs de licences envoient à Citrix ?** Oui, vous pouvez afficher une copie des informations envoyées à Citrix. Pour plus de détails, consultez Informations sur le serveur de licences incluses dans les chargements.
- **Le service License Usage Insights est-il disponible auprès des clients ou partenaires Citrix qui ne sont pas membres du programme Citrix Service Provider (CSP) ?** Non. Le service License Usage Insights est uniquement disponible auprès des partenaires CSP qui ont rejoint ce programme de partenariat.
- **Puis-je désactiver la fonction Call Home sur le serveur de licences ?** Non. Conformément au contrat de licence Citrix Service Provider, tous les serveurs de licences sont tenus de transmettre les données d'utilisation des produits. Les partenaires souhaitant ne pas utiliser la fonction Phone Home peuvent utiliser la fonction d'anonymisation du nom d'utilisateur. Pour de plus amples informations, consultez la section Anonymiser les noms d'utilisateurs via le serveur de licences.
- **Serais-je facturé en fonction de l'utilisation du produit indiquée dans le service License Usage Insights ?** Non. Le service License Usage Insights 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.

Gérer l'utilisation des produits, les serveurs de licences et les notifications

July 2, 2024

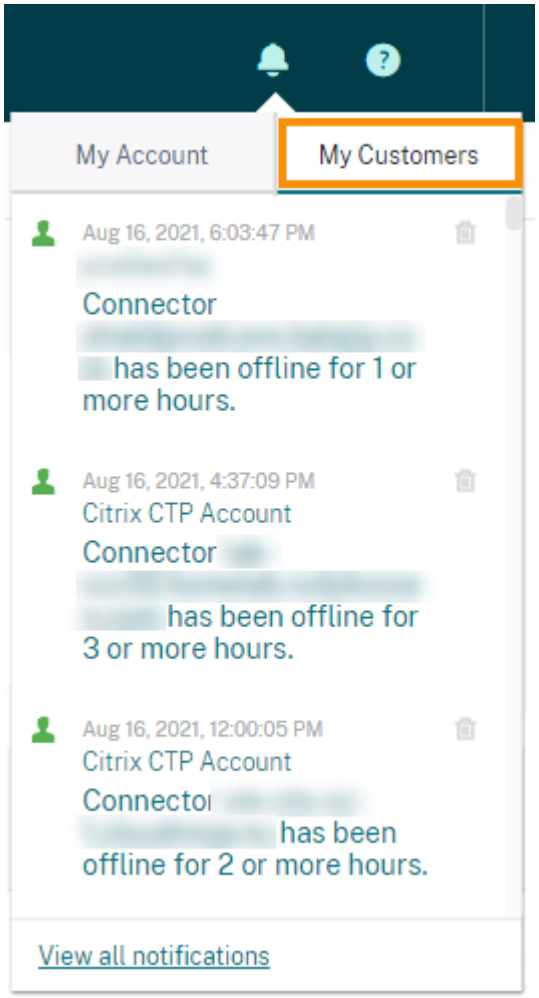
Sélection du produit

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



Notifications des clients

Surveillez l'intégrité de la solution sur de multiples 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.

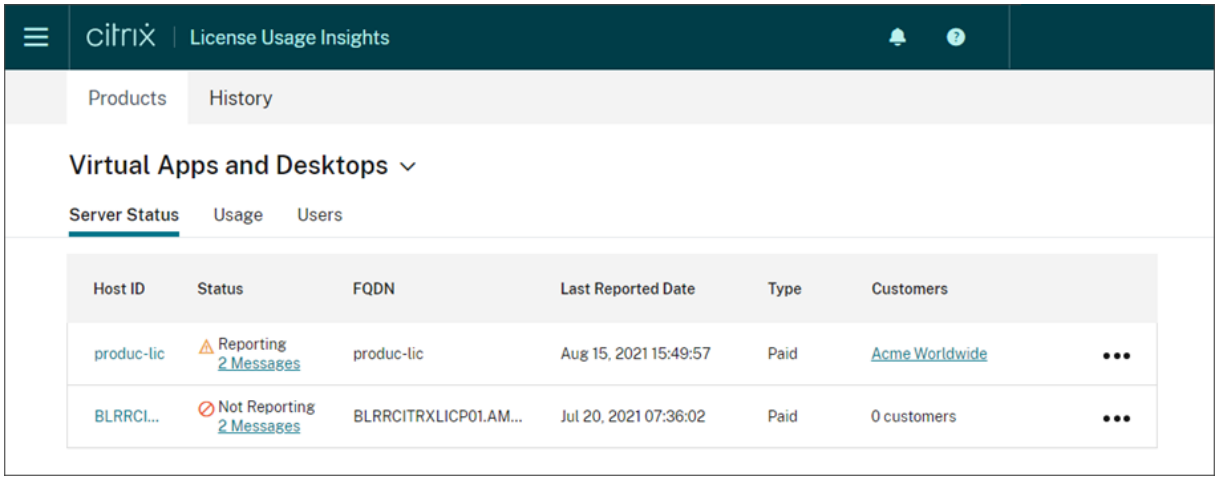


1. Dans la console de gestion Citrix Cloud, cliquez sur l'icône **Notifications**, puis sur **Mes clients**. Une liste des notifications les plus récentes apparaît.
2. Pour afficher la liste complète des notifications des clients, cliquez sur **Afficher toutes les notifications**.

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 License Usage Insights.

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, License Usage Insights affiche l'état « reporting » et comprend un horodatage du chargement plus récent.



Informations sur le serveur de licences incluses dans les chargements

Lorsque Call Home est activé sur un serveur de licences, les informations suivantes sont téléchargées quotidiennement :

- Version du serveur de licences
- Informations sur le fichier de licence :
  - 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
- 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,

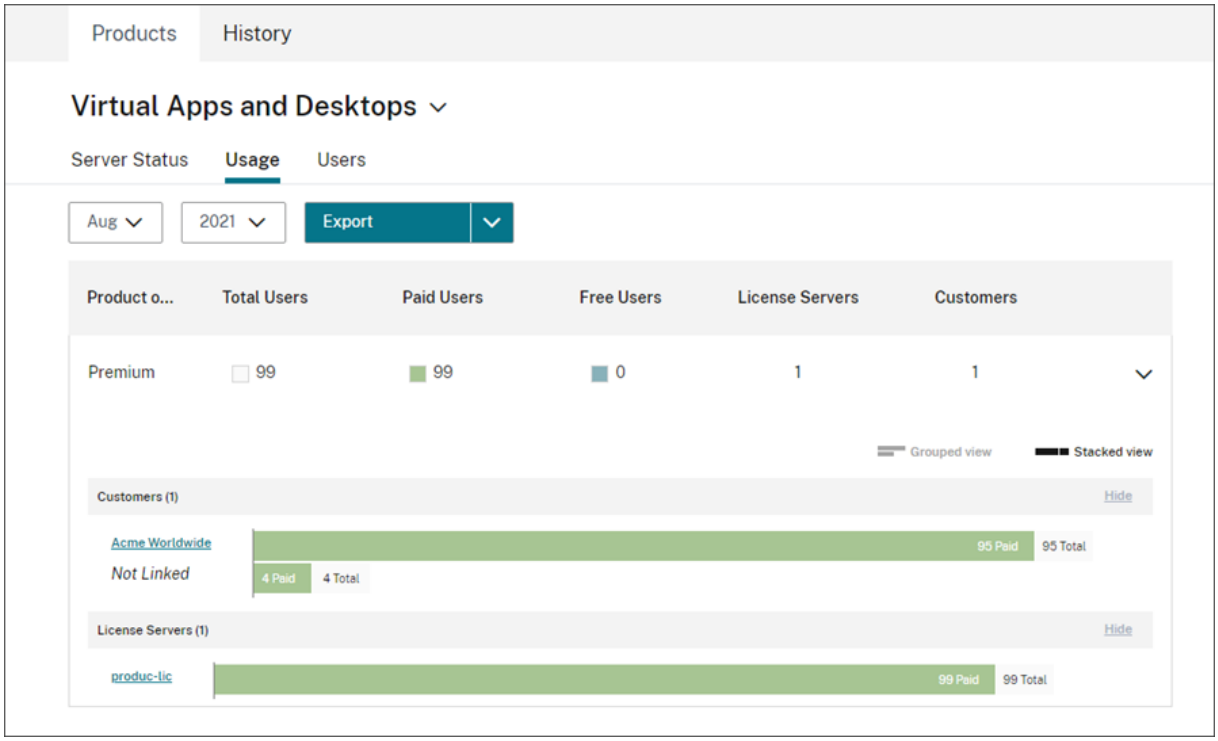
> tous les chargement sont supprimés à l'exception du dernier.

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 License Usage Insights 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.



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

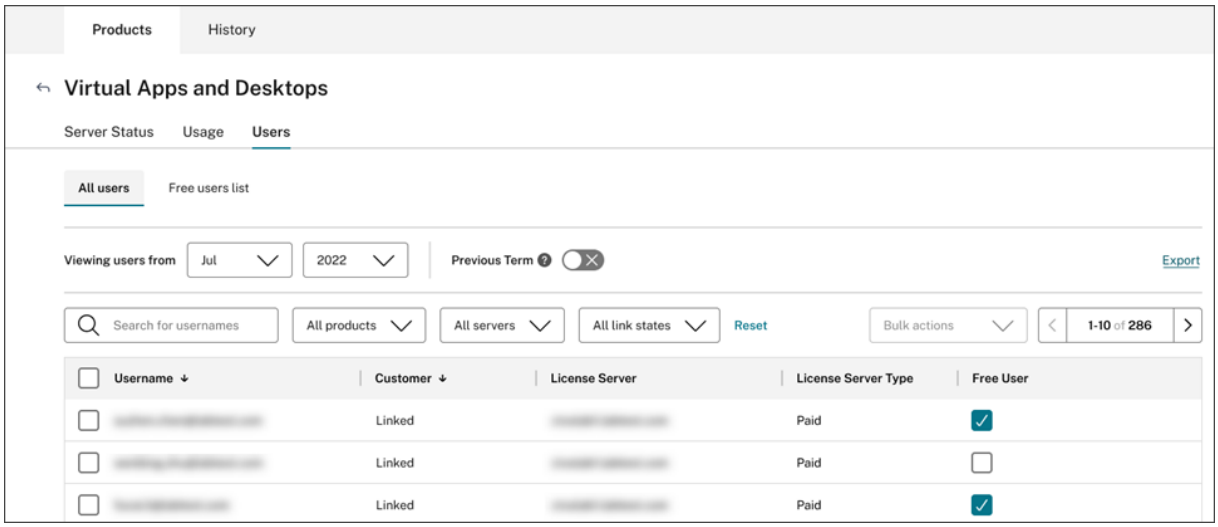
Pour détailler l'utilisation des licences par client, vous devez d'abord associer des utilisateurs aux clients ou aux locataires à qui ils appartiennent. Si aucun client n'est défini dans votre tableau de

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**.

Gestion des utilisateurs

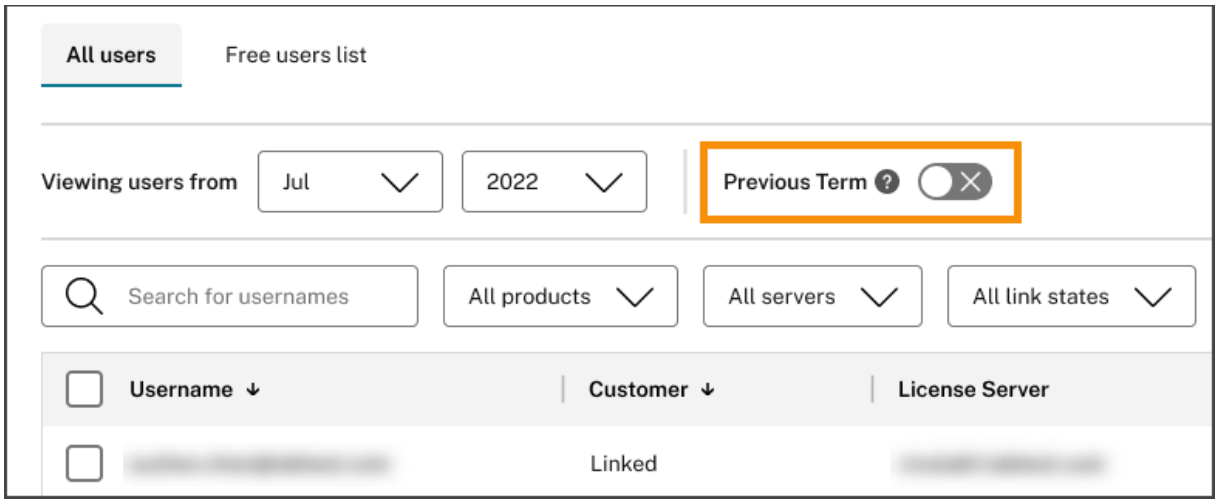
Le service License Usage Insights fournit une vue complète de l'utilisation des produits sur les déploiements tout en vous permettant de profiter pleinement du programme de licences CSP qui prend en charge les utilisateurs à des fins d'évaluation, de test et d'utilisation administrative.



Pour vous assurer que la facturation des utilisateurs payants soit effectuée de manière appropriée au cours d'un cycle de facturation donné, vous pouvez désigner certains utilisateurs comme des utilisateurs gratuits pendant ce cycle. Au cours d'un mois donné de votre cycle de facturation actuel, vous pouvez sélectionner des utilisateurs gratuits à tout moment, jusqu'au 10 du mois suivant. Par exemple, en mars, vous pouvez sélectionner des utilisateurs gratuits à tout moment jusqu'au 10 avril.

Entre le premier et le 10e jour de chaque mois, vous pouvez également sélectionner des utilisateurs gratuits pour le cycle de facturation précédent. Pendant cette période, vous pouvez activer le

paramètre **Cycle précédent** et sélectionner les utilisateurs gratuits pour ce cycle de facturation. Après le 10e jour du mois, Citrix Cloud n'affiche plus le paramètre **Cycle précédent** .



Les utilisateurs gratuits que vous sélectionnez au cours d'un mois donné sont pris en compte lorsque vous êtes facturé pour les utilisateurs payants. Lorsque vous modifiez l'état d'un utilisateur gratuit à un utilisateur payant, Citrix enregistre la date du changement et inclut cet utilisateur dans le cycle de facturation au cours duquel le changement s'est produit.

Marquage des clients d'utilisateurs

Cette fonctionnalité fournit une répartition des données d'utilisation des licences pour chaque client, y compris une assistance pour la gestion et la création de rapports sur les architectures de serveurs de licences à locataire unique et multi-locataire. Les objets de License Usage Insights sont les suivants :

- Serveur de licences : serveur de licences « produisant des rapports » ou « ne produisant pas de rapports » figurant sur la liste.
- Utilisateur : nom d'utilisateur unique figurant dans les données d'utilisation de Call Home.
- NetScaler : allocation de licence NetScaler VPX unique (VPX sur la liste VPX).

> **Remarque**
>
> La fonction de marquage des clients a le même comportement que le marquage des utilisateurs gratuit, où un CSP peut mettre à jour le marquage des clients pour le cycle de facturation en cours jusqu'au 10 du mois suivant.

Marquage des serveurs gratuits

Cette fonctionnalité apporte de la flexibilité dans la gestion des ressources au sein de l'environnement Citrix Cloud en permettant aux administrateurs d'organiser et d'identifier les serveurs en fonction de

leurs rôles spécifiques, de leur emplacement ou de tout autre critère pertinent, sans se soucier des implications en matière de licences.

> **Remarque**
>
> Un CSP peut modifier le marquage gratuit ou le marquage client pour le mois en cours exclusivement, les modifications s'appliquant à la fois au mois en cours et aux mois à venir.

Marquage des clients de serveurs

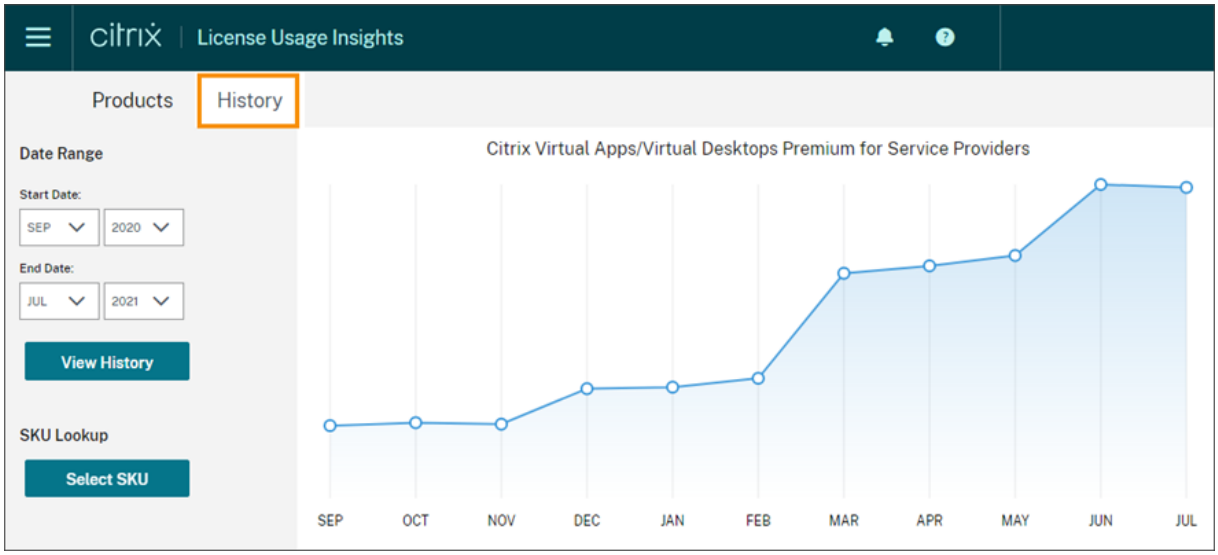
Cette fonctionnalité permet une meilleure organisation et une meilleure gestion des ressources au sein de l'environnement Citrix Cloud, en garantissant que les serveurs sont marqués en fonction des besoins spécifiques des clients. En utilisant le marquage des clients de serveurs, les administrateurs peuvent facilement identifier et suivre les ressources associées à différents clients, ce qui facilite une allocation et une gestion plus efficaces des ressources.

> **Remarque**
>
> Un CSP peut modifier le marquage gratuit ou le marquage client pour le mois en cours exclusivement, les modifications s'appliquant à la fois au mois en cours et aux mois à venir.

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 de License Usage Insights :

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

1. Sélectionnez **Virtual Apps and Desktops** ou **Mise en 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**.

Accéder aux données des licences à l'aide d'API

Citrix fournit plusieurs API que vous pouvez utiliser pour accéder aux données de vos licences en dehors de Citrix Cloud. Pour en savoir plus sur ces API, consultez la section APIs to manage Citrix cloud licensing dans la documentation Citrix Developer.

Pour utiliser ces API, vous devez d'abord créer un client sécurisé et générer un jeton porteur. Pour créer un client sécurisé, vous devez disposer de l'autorisation **Client sécurisé** dans Citrix Cloud. Pour plus d'informations, consultez la section Autorisations de la console.

Pour plus d'informations sur les tâches requises pour l'utilisation des API Citrix Cloud, consultez la section Get started with Citrix Cloud APIs dans la documentation Citrix Developer.

Accès des distributeurs aux API

Vous pouvez autoriser votre distributeur Citrix à accéder aux données de vos licences via les API Citrix Cloud sans lui accorder un accès administrateur complet à votre compte Citrix Cloud. Cela peut être utile par exemple si vous voulez que votre distributeur puisse valider vos rapports d'utilisation et garantir une facturation précise.

Pour permettre aux distributeurs d'accéder aux données de vos licences, vous créez un administrateur d'accès personnalisé autorisé uniquement à créer des clients sécurisés et à accéder à License Usage Insights Service. Ce compte dispose d'un accès limité aux API Citrix Cloud et n'a aucun accès aux autres fonctions de Citrix Cloud. Une fois le compte créé, vous pouvez partager les informations d'identification du compte avec votre distributeur afin qu'il puisse se connecter à votre compte Citrix Cloud et créer le client sécurisé requis pour utiliser les API Citrix Cloud. Vous pouvez également vous connecter en tant qu'administrateur d'accès personnalisé, créer le client sécurisé, puis partager les détails du client sécurisé avec votre distributeur.

Pour créer le compte d'accès personnalisé pour votre distributeur :

1. Créez un nouveau compte administrateur spécialement pour votre distributeur Citrix. Pour obtenir des instructions, voir Inviter des administrateurs individuels.
2. Dans **Définir l'accès**, sélectionnez **Accès personnalisé**, puis sélectionnez les autorisations suivantes :
    - **Général > Client sécurisé**
    - **License Usage Insights > License Usage Insights : accès des distributeurs**

Pour créer le client sécurisé :

1. Connectez-vous à Citrix Cloud à l'aide des informations d'identification du nouveau compte.
2. Créez un nouveau client sécurisé comme décrit dans Get started with Citrix Cloud APIs.
3. Notez l'ID client et la clé secrète client générés par Citrix Cloud. Ces informations sont des entrées obligatoires pour toutes les API Citrix Cloud.

Données de licences mises à la disposition des distributeurs

Cette section décrit les données de licences et les API auxquelles votre distributeur Citrix peut accéder à l'aide des informations du client sécurisé que vous lui fournissez. Cliquez sur les liens ci-dessous pour obtenir plus de détails sur chaque API.

Rapports du CSP sur l'utilisation mensuelle et historique des licences de Virtual Apps and Desktops (License Usage Insights) :

- Utilisation actuelle de Virtual Apps and Desktops
- Historique d'utilisation de Virtual Apps and Desktops

Rapports du CSP sur l'utilisation des licences monolocataire et multilocataire (License Usage Insights) :

- Utilisation actuelle de DaaS
- Historique de l'utilisation de DaaS

Utilisation des licences cloud du CSP (licence) :

- Utilisation actuelle de DaaS
- Historique de l'utilisation de DaaS

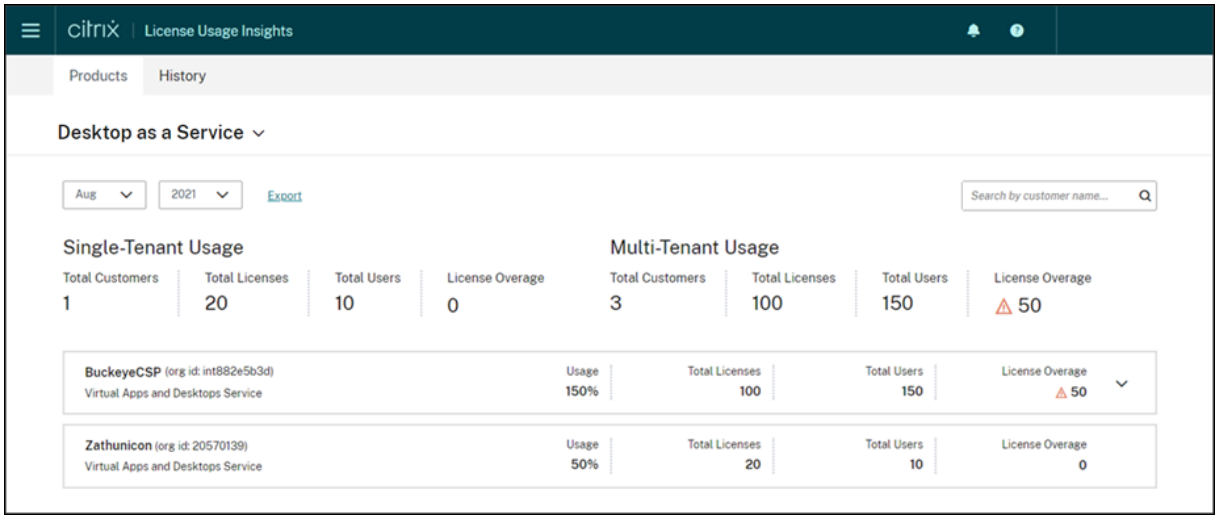
Utilisation des licences cloud par le locataire (Tableau de bord client -> Afficher les licences)

- Utilisation actuelle des CCU DaaS
- Historique de l'utilisation des CCU DaaS
- Utilisation actuelle des licences UD DaaS
- Historique de l'utilisation des licences UD DaaS

Utilisation de licences et rapports Cloud Service pour les partenaires Citrix Service Provider

October 4, 2023

Le service License Usage Insights regroupe automatiquement l'utilisation des services cloud pour fournir une vue complète sur tous les clients mono-locataires et les partenaires multi-locataires. Vous pouvez également exporter ces informations pour un mois donné vers un fichier CSV pour une analyse plus approfondie.



Services pris en charge

L'utilisation des licences à locataire unique est disponible pour Citrix DaaS Premium (anciennement Virtual Apps Premium et Virtual Apps and Desktops Premium).

L'utilisation des licences multi-locataires est disponible pour les services suivants :

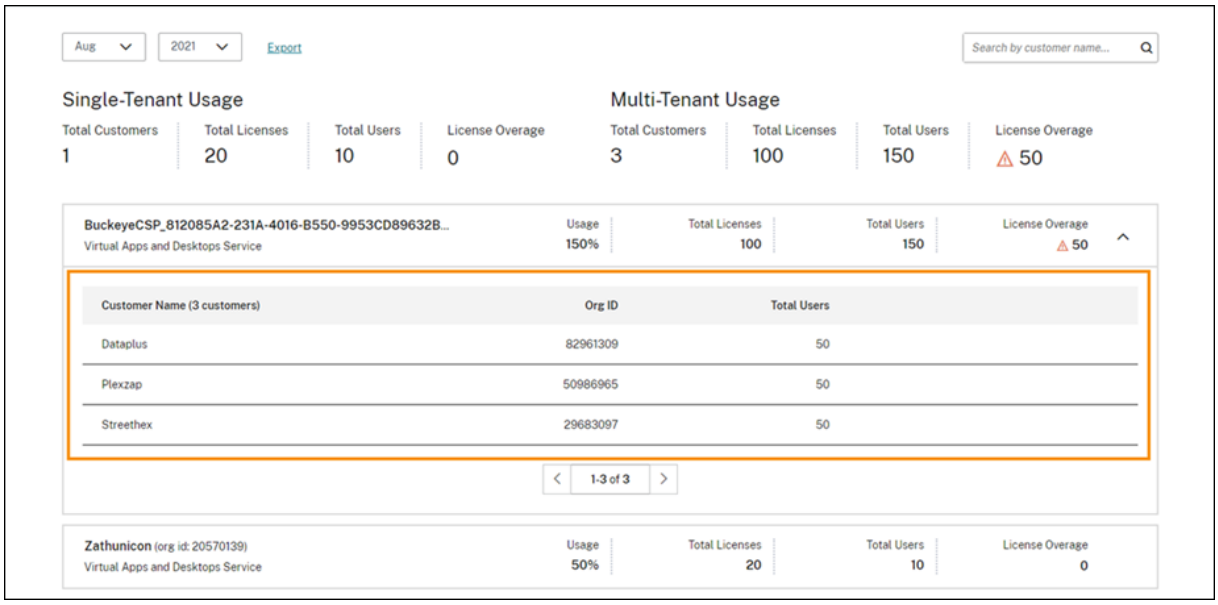
- Citrix DaaS (anciennement Virtual Apps and Desktops Service)
- Citrix DaaS Standard pour Azure (anciennement Virtual Apps and Desktops Standard pour Azure)

Résumé du système de licences

License Usage Insights fournit la répartition suivante de l'utilisation de licences pour les clients mono-locataires et multi-locataires pour Citrix Service Providers (CSP) :

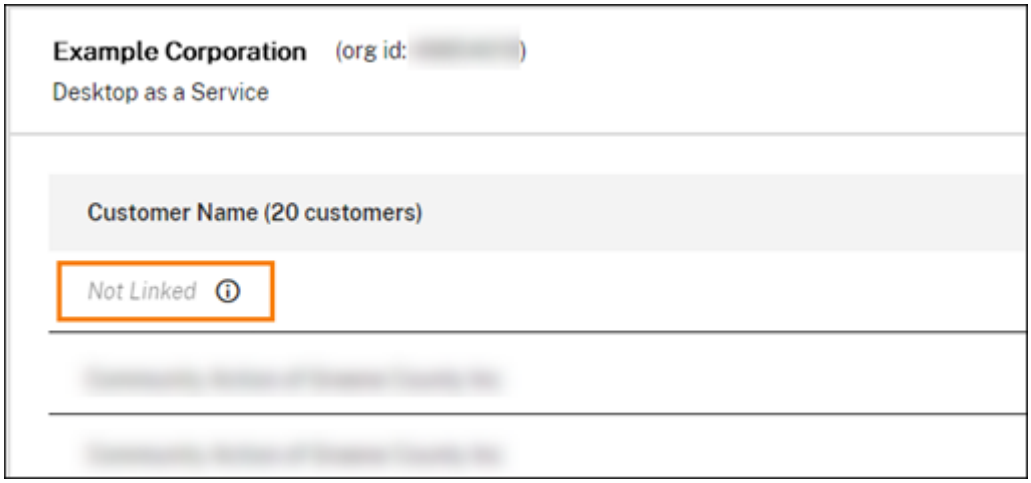
- Vue d'ensemble regroupée par type de locataire qui inclut le nombre total de clients et le nombre total de licences achetées, d'utilisateurs et de licences suraffectées sur tous les clients
- Résumé de l'utilisation pour chaque client ou partenaire qui inclut le pourcentage du nombre total de licences utilisées, le nombre total de licences achetées, d'utilisateurs et de licences suraffectées

Pour les services multi-locataires, vous pouvez développer le résumé de l'utilisation pour afficher les clients, l'ID d'organisation (OrgID) et le nombre total d'utilisateurs associés à chaque partenaire.



Clients locataires non liés

Dans certains cas, un client locataire peut être répertorié comme « Non lié ». Cet état peut se produire lorsque les utilisateurs de ce locataire accèdent à un service cloud via l'URL de l'espace de travail du CSP, plutôt que par l'URL de l'espace de travail du locataire.

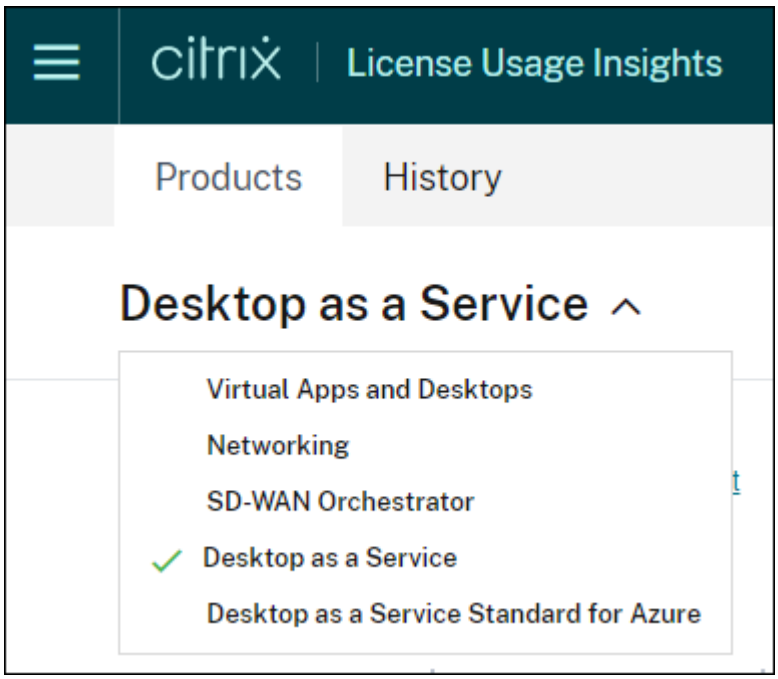


Lorsque l'utilisateur locataire accède au service via l'URL de l'espace de travail du locataire, Citrix Cloud considère l'utilisateur comme appartenant au locataire et le message « Non lié » est supprimé.

Afficher et exporter l'utilisation mensuelle

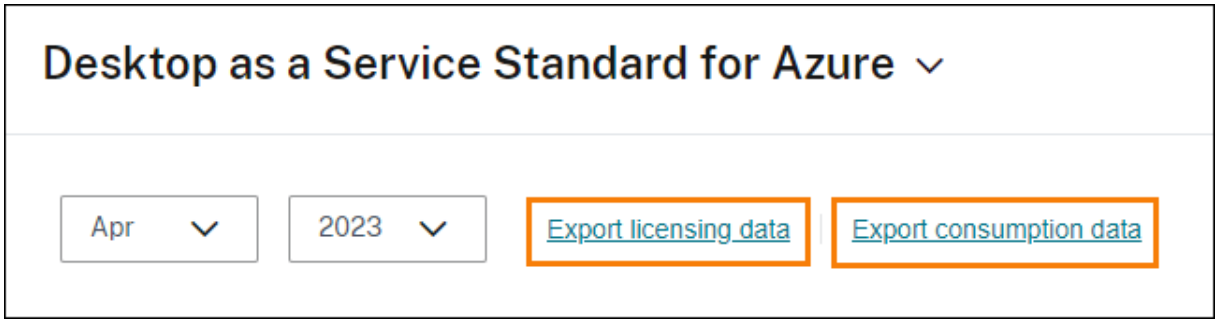
À tout moment, vous pouvez consulter l'utilisation des licences des mois précédents pour tous les clients et partenaires. Vous pouvez également exporter ces données vers un fichier CSV pour une analyse plus approfondie. Pour Citrix DaaS Standard pour Azure, vous pouvez également exporter les données de consommation mensuelles.

1. À partir du menu de produit, sélectionnez le service cloud que vous souhaitez afficher.



Pour Citrix DaaS, sélectionnez le mois et l'année que vous souhaitez afficher, puis sélectionnez **Exporter**.

Pour Citrix DaaS Standard pour Azure, sélectionnez le mois et l'année que vous souhaitez afficher, puis sélectionnez **Exporter données de licences** ou **Exporter données de consommation**.

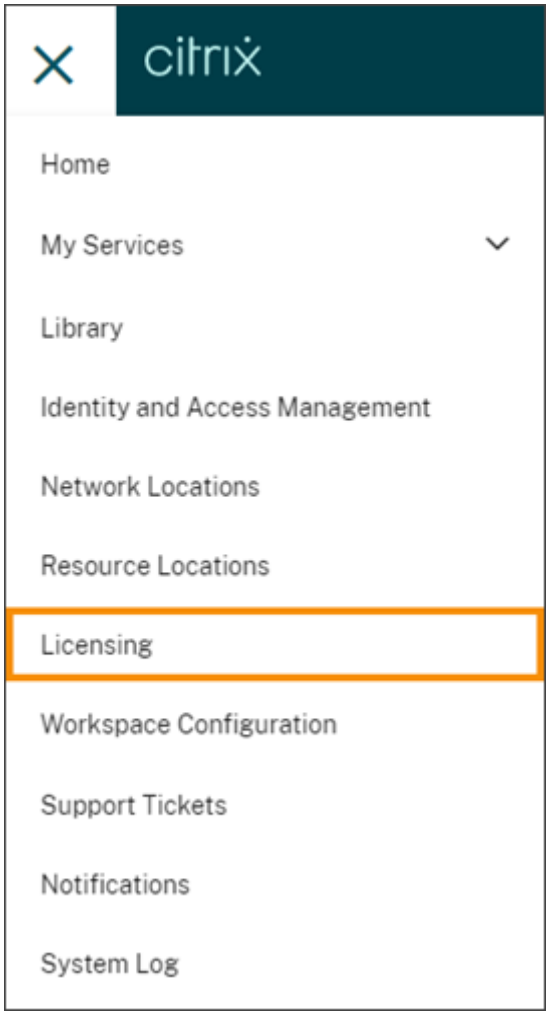


Surveillance des licences client et de l'utilisation pour Citrix DaaS

October 4, 2023

Les clients de **Citrix Service Providers (CSP)** peuvent facilement surveiller les licences de Citrix DaaS pour leurs utilisateurs dans Citrix Cloud. En tant que CSP, vous pouvez accéder à ces informations en vous connectant au compte de votre client dans Citrix Cloud. Pour afficher les informations agrégées d'utilisation des licences sur les clients mono-locataires et multi-locataires, consultez Utilisation de licences et rapports Cloud Service pour les partenaires Citrix Service Provider.

Les clients peuvent afficher leurs données de licence en sélectionnant **Système de licences** dans le menu Citrix Cloud.



Attribution de licence

Modèle de licence utilisateur/appareil : Citrix Cloud attribue une licence lorsqu'un utilisateur client unique lance une application ou un bureau pour la première fois lors du mois en cours.

Modèle de licences d'utilisateurs simultanés : 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 la section Licences simultanées dans la documentation relative au système de licences Citrix.

Résumé de l'option Système de licences

Citrix Cloud affiche des vues récapitulatives des licences utilisées dans le cadre des modèles de licence utilisateur/appareil et utilisateur simultané.

Résumé pour le modèle utilisateur/appareil

Pour le modèle utilisateur/appareil, le résumé des licences fournit une vue d'ensemble des licences utilisées par rapport au nombre total de licences que vous possédez.

Lorsque le pourcentage approche 100 %, le pourcentage passe du vert au jaune. Si le pourcentage dépasse 100 %, il devient rouge.

Citrix Cloud affiche également le ratio entre les licences attribuées et les licences achetées, ainsi que le nombre de licences disponibles restantes.

Résumé pour le modèle de licences d'utilisateurs simultanés

Pour le modèle de licences d'utilisateurs simultanés, le résumé des 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. La quantité totale de licences achetées correspond à la somme des licences achetées pour les éditions Citrix DaaS qui utilisent le modèle de licences simultanées.

- 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.
- Statistiques d'utilisation active. Citrix Cloud affiche le nombre total de connexions uniques pour les périodes suivantes :

  - **Mensuel :** nombre total de connexions pour le mois calendaire précédent.
  - **Quotidien :** nombre total de connexions au cours des 24 heures précédentes. Ces chiffres sont également représentés sous forme de pourcentages du nombre total de licences détenues au cours de ces périodes.

Calcul du nombre maximal de licences utilisées

Pour refléter avec précision le modèle de licences simultanées, 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 d'utilisateurs simul-

> tanés utilisées. Pour plus d'informations sur les différences entre les rapports de monitoring et les rapports de licence, consultez Questions fréquentes.

Calcul de l'utilisation active mensuelle

Au début de chaque mois, Citrix Cloud prend un instantané du mois calendaire précédent. Citrix Cloud affiche le nombre total de connexions uniques qui se sont produites au cours de ce mois calendaire.

Calcul de l'utilisation active quotidienne

Chaque jour, à la même heure, Citrix Cloud prend un instantané des 24 heures précédentes. Citrix Cloud affiche le nombre total de connexions uniques qui se sont produites au cours de cette période de 24 heures.

Tendances d'utilisation

Citrix Cloud affiche une répartition des tendances d'utilisation pour les licences utilisateur/appareil ou utilisateurs simultanés. Pour consulter cette répartition, sélectionnez **Afficher détails d'utilisation** sur la page récapitulative des licences.

Tendances pour le modèle utilisateur/appareil

Pour les licences utilisateur/appareils, la section **Tendances d'utilisation** présente la répartition des licences attribuées sous forme de graphique.

Si vous pointez sur un intervalle sur le graphique, les informations suivantes s'affichent :

- **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.

Tendances pour les utilisateurs simultanés

Pour les licences d'utilisateurs simultanés, la section **Tendances d'utilisation** 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 déroulant.

  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.
- **Utilisation active** affiche un graphique contenant les informations suivantes :
  - **Quotidien :** nombre total de connexions par jour au cours des 30 jours précédents.
  - **Mensuel :** nombre total de connexions pour chaque mois au cours de l'année calendaire précédente.

Le fait de pointer sur un intervalle dans les graphiques **Attribution de licences** ou **Utilisation active** permet d'afficher les détails de cet intervalle.

Utilisateurs sous licence

La section **Activité des licences** affiche la liste des utilisateurs clients individuels auxquels des licences sont attribuées au cours du mois en cours. Cette liste affiche également le domaine auquel chaque utilisateur appartient, la date à laquelle une licence a été attribuée et la dernière fois que le service a été utilisé.

Libération mensuelle des licences

Le premier jour de chaque mois, les licences attribuées du mois précédent sont libérées automatiquement. Dans ce cas, le nombre de licences attribuées est réinitialisée à zéro et la liste des utilisateurs clients sous licence est effacée. Les licences sont réattribuées lorsque les utilisateurs lancent des applications ou des bureaux pour la première fois au cours du nouveau mois.

Consulter l'historique mensuel des licences

Le premier jour de chaque mois, la liste des utilisateurs clients sous licence du mois précédent, sous **Activité des licences**, est effacée lorsque le nombre de licences attribuées est réinitialisée à zéro. Toutefois, vous pouvez accéder aux informations utilisateur des mois précédents à tout moment et les télécharger sous forme de fichier CSV, si nécessaire.

1. Dans la section **Activité des licences**, sélectionnez **Afficher l'historique des licences** à droite de la section.
2. Sélectionnez le mois que vous souhaitez afficher. La liste des détails de l'utilisateur pour le mois sélectionné s'affiche.
3. Pour exporter la liste, sélectionnez **Exporter au format CSV** à droite de la section, puis enregistrez le fichier.

Informations sur l'exportation de la licence

À tout moment, les clients peuvent exporter les informations des utilisateurs sous licence vers un fichier CSV pour une analyse plus approfondie. Le client peut ensuite utiliser le fichier CSV si nécessaire pour analyser les détails de la licence.

Pour exporter les informations du mois en cours, dans la section **Activité des licences**, sélectionnez **Exporter au format CSV** à droite de la section, puis enregistrez le fichier.

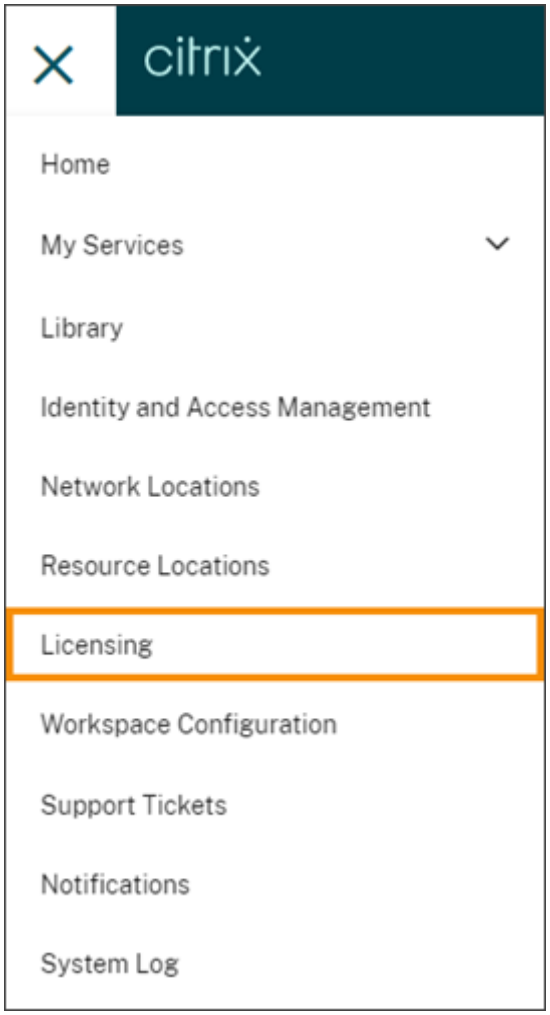
Pour exporter les informations des mois précédents, générez une liste pour un mois sélectionné, comme décrit dans Consulter l'historique mensuel des licences. Sélectionnez **Exporter au format CSV** et enregistrez le fichier.

Surveillance des licences client et de l'utilisation pour Citrix DaaS Standard pour Azure

October 4, 2023

Les clients de **Citrix Service Providers (CSP)** peuvent facilement surveiller les licences de Citrix DaaS Standard pour Azure pour leurs utilisateurs dans Citrix Cloud. En tant que CSP, vous pouvez accéder à ces informations en vous connectant au compte de votre client dans Citrix Cloud. Pour afficher les informations agrégées d'utilisation des licences sur les clients mono-locataires et multi-locataires, consultez Utilisation de licences et rapports Cloud Service pour les partenaires Citrix Service Provider.

Les clients peuvent afficher leurs données de licence en sélectionnant **Système de licences** dans le menu Citrix Cloud.



Attribution de licence

Modèle de licence utilisateur/appareil : Citrix Cloud attribue une licence lorsqu'un utilisateur ou un appareil unique lance un bureau pour la première fois.

Modèle de licences d'utilisateurs simultanés : 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 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 la section Licences simultanées dans la documentation relative au système de licences Citrix.

Résumé de l'option Système de licences

Citrix Cloud affiche des vues récapitulatives des licences utilisées dans le cadre des modèles de licence utilisateur/appareil et utilisateur simultané.

Résumé pour le modèle utilisateur/appareil

Pour le modèle utilisateur/appareil, le résumé des licences fournit une vue d'ensemble des licences utilisées par rapport au nombre total de licences que vous possédez.

Lorsque le pourcentage approche 100 %, le pourcentage passe du vert au jaune. Si le pourcentage dépasse 100 %, il devient rouge.

Citrix Cloud affiche également le ratio entre les licences attribuées et les licences achetées, ainsi que le nombre de licences disponibles restantes.

Résumé pour le modèle de licences d'utilisateurs simultanés

Pour le modèle de licences simultanées, le résumé des 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. La quantité totale de licences achetées correspond à la somme des licences achetées pour les éditions Citrix DaaS Standard pour Azure qui utilisent le modèle de licences simultanées.
- 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, 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.

Tendances d'utilisation

Citrix Cloud affiche une répartition des tendances d'utilisation pour les licences utilisateur/appareil ou utilisateurs simultanés. Pour consulter cette répartition, sélectionnez **Afficher détails d'utilisation** sur la page récapitulative des licences.

Tendances pour le modèle utilisateur/appareil

Pour les licences utilisateur/appareils, la section **Tendances d'utilisation** présente la répartition des licences attribuées sous forme de graphique.

Si vous pointez sur un intervalle sur le graphique, les informations suivantes s'affichent :

- **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.

Tendances pour les utilisateurs simultanés

Pour les licences d'utilisateurs simultanés, la section **Tendances d'utilisation** 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 déroulant.

  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.

Si vous pointez sur un intervalle sur le graphique, vous pouvez voir le nombre total de licences et le nombre maximal de licences utilisées pendant cet intervalle.

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.

Sous **Rapports d'utilisation**, sélectionnez un intervalle, puis sélectionnez **Télécharger les données** pour générer et télécharger un fichier CSV sur votre machine locale.

Utilisateurs sous licence

Pour les licences utilisateur/appareil, la section **Activité des licences** affiche la liste des utilisateurs clients individuels auxquels des licences sont attribuées au cours du mois en cours. Cette liste affiche également le domaine auquel chaque utilisateur appartient, la date à laquelle une licence a été attribuée et la dernière fois que le service a été utilisé. Cette section n'est pas disponible pour les licences d'utilisateurs simultanés.

Libération mensuelle des licences

Le premier jour de chaque mois, les licences attribuées du mois précédent sont libérées automatiquement. Dans ce cas, le nombre de licences attribuées est réinitialisée à zéro et la liste des utilisateurs clients sous licence est effacée. Les licences sont réattribuées lorsque les utilisateurs lancent des applications ou des bureaux pour la première fois au cours du nouveau mois.

Consulter l'historique mensuel des licences

Le premier jour de chaque mois, la liste des utilisateurs clients sous licence du mois précédent, sous **Activité des licences**, est effacée lorsque le nombre de licences attribuées est réinitialisée à zéro. Toutefois, vous pouvez accéder aux informations utilisateur des mois précédents à tout moment et les télécharger sous forme de fichier CSV, si nécessaire.

1. Dans la section **Activité des licences**, sélectionnez **Afficher l'historique des licences** à droite de la section.
2. Sélectionnez le mois que vous souhaitez afficher. La liste des détails de l'utilisateur pour le mois sélectionné s'affiche.
3. Pour exporter la liste, sélectionnez **Exporter au format CSV** à droite de la section, puis enregistrez le fichier.

Informations sur l'exportation de la licence

À tout moment, vous pouvez exporter les informations des utilisateurs sous licence d'un seul client vers un fichier CSV pour une analyse plus approfondie. Vous pouvez ensuite utiliser le fichier CSV si nécessaire pour analyser les détails de la licence.

Pour exporter les informations du mois en cours, dans la section **Activité des licences**, sélectionnez **Exporter au format CSV** à droite de la section, puis enregistrez le fichier.

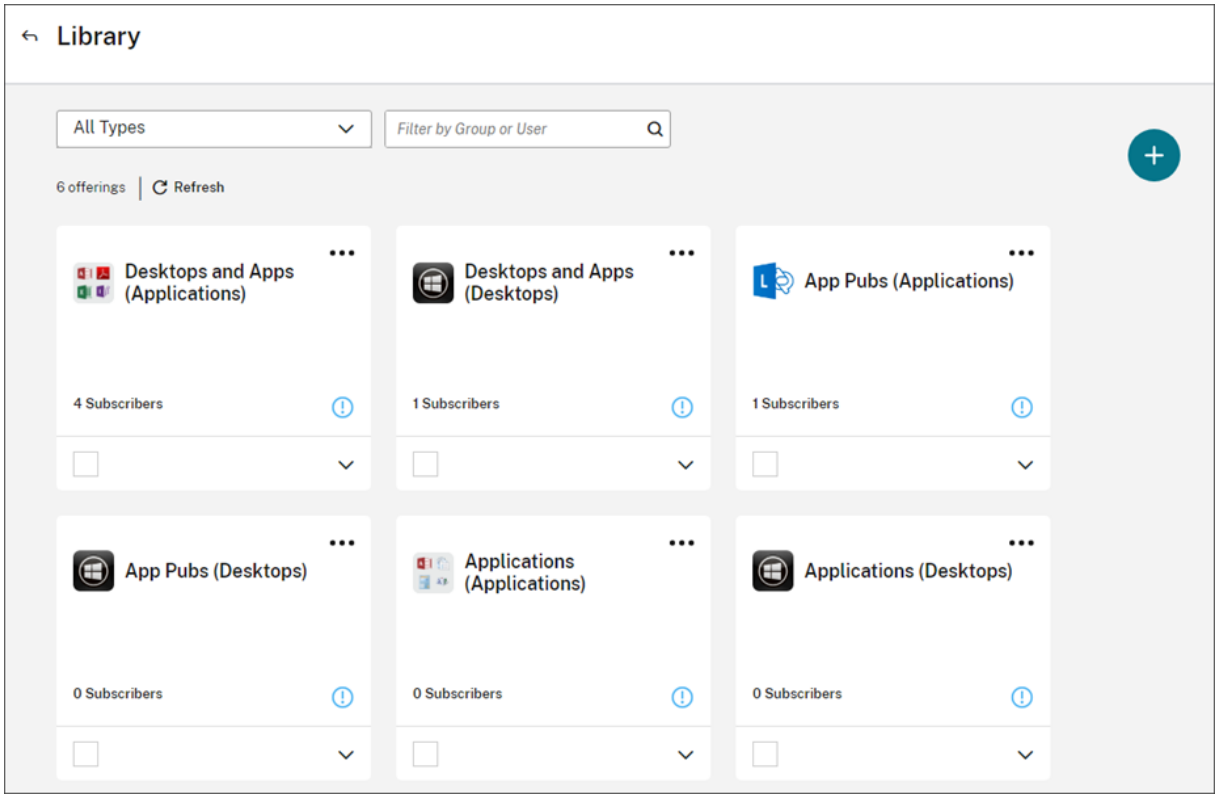
Pour exporter les informations des mois précédents, générez une liste pour un mois sélectionné, comme décrit dans Consulter l'historique mensuel des licences. Sélectionnez **Exporter au format CSV** et enregistrez le fichier.

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

April 26, 2024

> **Remarque :**
>
> Pour les groupes de mise à disposition *gérés par Citrix Cloud*, les attributions d'utilisateurs peuvent désormais être gérées directement dans la console Web Studio. Pour de plus amples informations, consultez la documentation du service DaaS. Auparavant, la gestion de ces groupes de mise à disposition était limitée à la bibliothèque, mais vous pouvez désormais utiliser les mêmes fonctionnalités de gestion dans la console Web Studio. Cette fonctionnalité est désormais disponible pour tous les clients. En juin 2024, les cas d'utilisation spécifiques au DaaS dans Cloud Library seront totalement obsolètes.

Vous pouvez attribuer des ressources ou d'autres éléments que vous configurez dans un service à vos utilisateurs et groupes Active Directory à l'aide de la bibliothèque. Les offres peuvent comporter des applications, des bureaux, 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.



Accès des administrateurs

Pour accéder à la bibliothèque, les administrateurs doivent répondre aux exigences suivantes :

- S'authentifier via le fournisseur d'identité Citrix ou Azure AD.
- Se connecter en tant qu'administrateur individuel et non en tant que membre d'un groupe d'administrateurs.

- Disposer d'un accès complet à Citrix Cloud ou d'un accès personnalisé avec le rôle de bibliothèque sélectionné.

Si vous possédez des comptes d'administrateur individuel et de groupe dans Citrix Cloud, votre accès à la bibliothèque peut dépendre des autorisations en vigueur lorsque vous vous connectez avec chaque compte. Pour plus d'informations, consultez la section Autorisations résultantes pour les administrateurs avec identités Citrix, AD, Azure AD et Google Cloud.

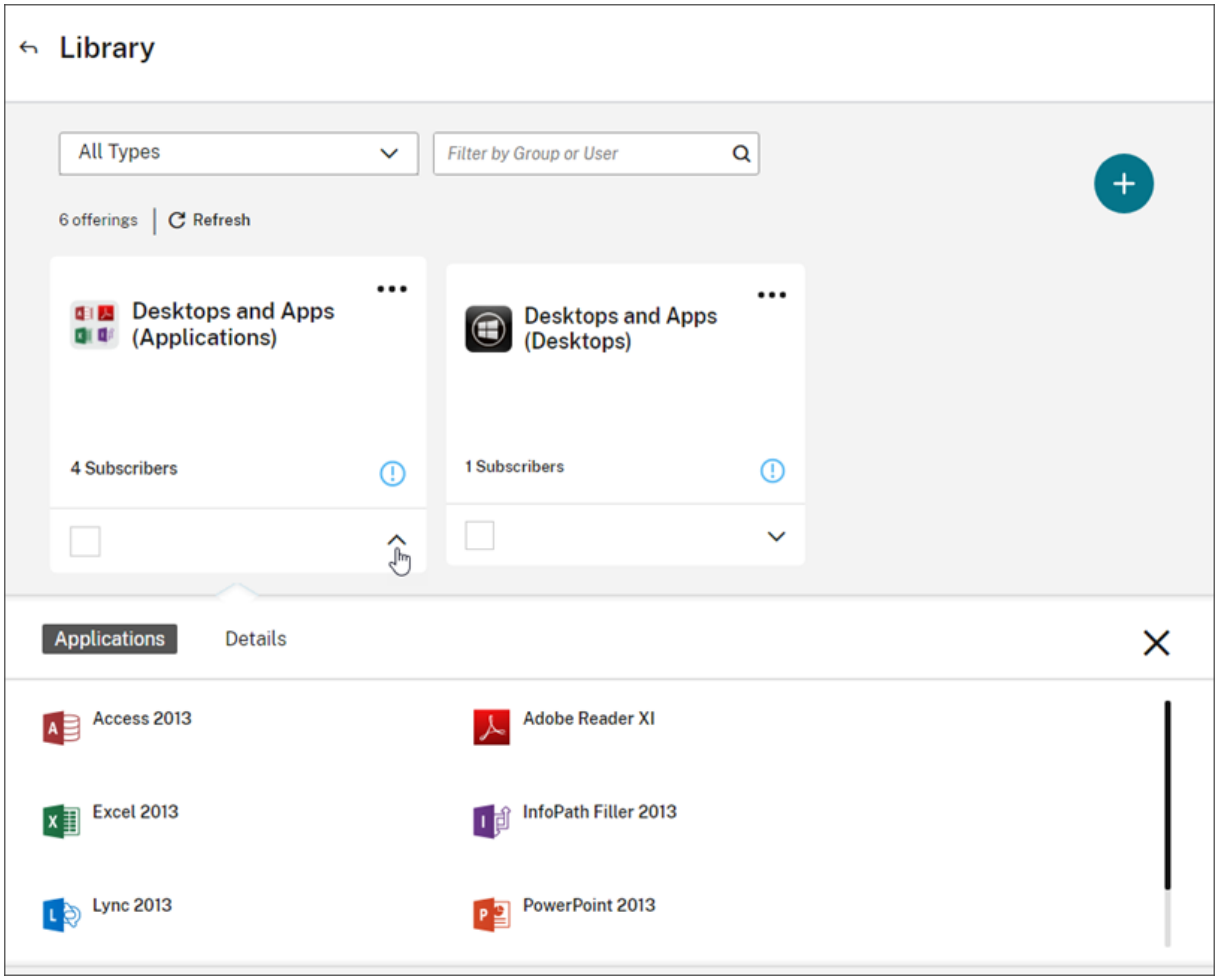
Considérations relatives à l'utilisation de StoreFront avec Citrix DaaS

Si vous utilisez une instance StoreFront locale avec Citrix DaaS, n'utilisez pas la bibliothèque pour attribuer des ressources lors de la création de groupes de mise à disposition. Utilisez plutôt Studio pour attribuer des ressources aux utilisateurs. Si vous utilisez la bibliothèque dans ce scénario, les ressources peuvent ne pas être énumérées pour les utilisateurs.

Lorsque vous créez un groupe de mise à disposition dans Studio, sur la page **Utilisateurs**, ne sélectionnez pas **Laissez Citrix Cloud se charger de la gestion des utilisateurs**. Sélectionnez plutôt une autre option (**Autoriser les utilisateurs authentifiés à utiliser ce groupe de mise à disposition** ou **Restreindre l'utilisation de ce groupe de mise à disposition aux utilisateurs suivants**).

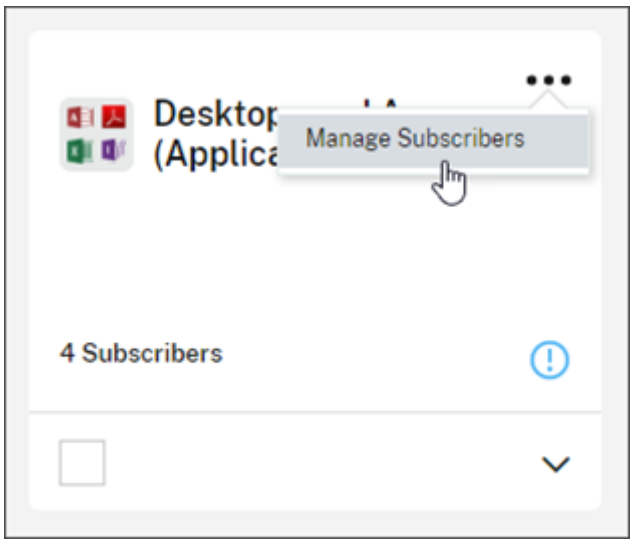
Afficher les détails d'une offre

Pour afficher les applications, les bureaux, les stratégies et toute autre information relative à l'offre, cliquez sur la flèche sur la carte d'offre.

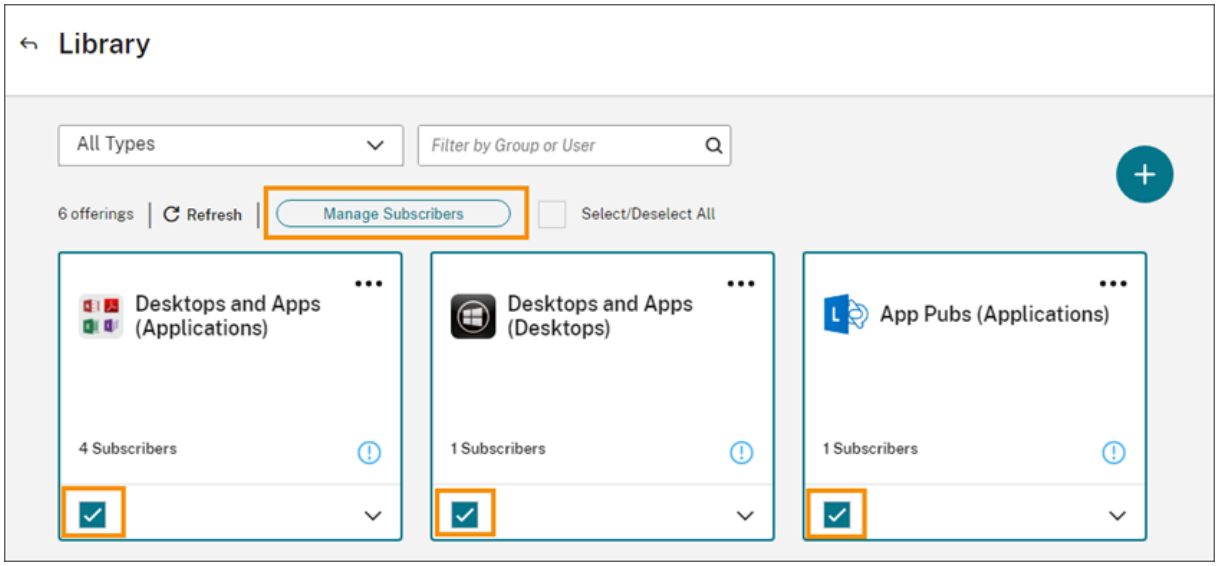


Ajouter ou supprimer des abonnés

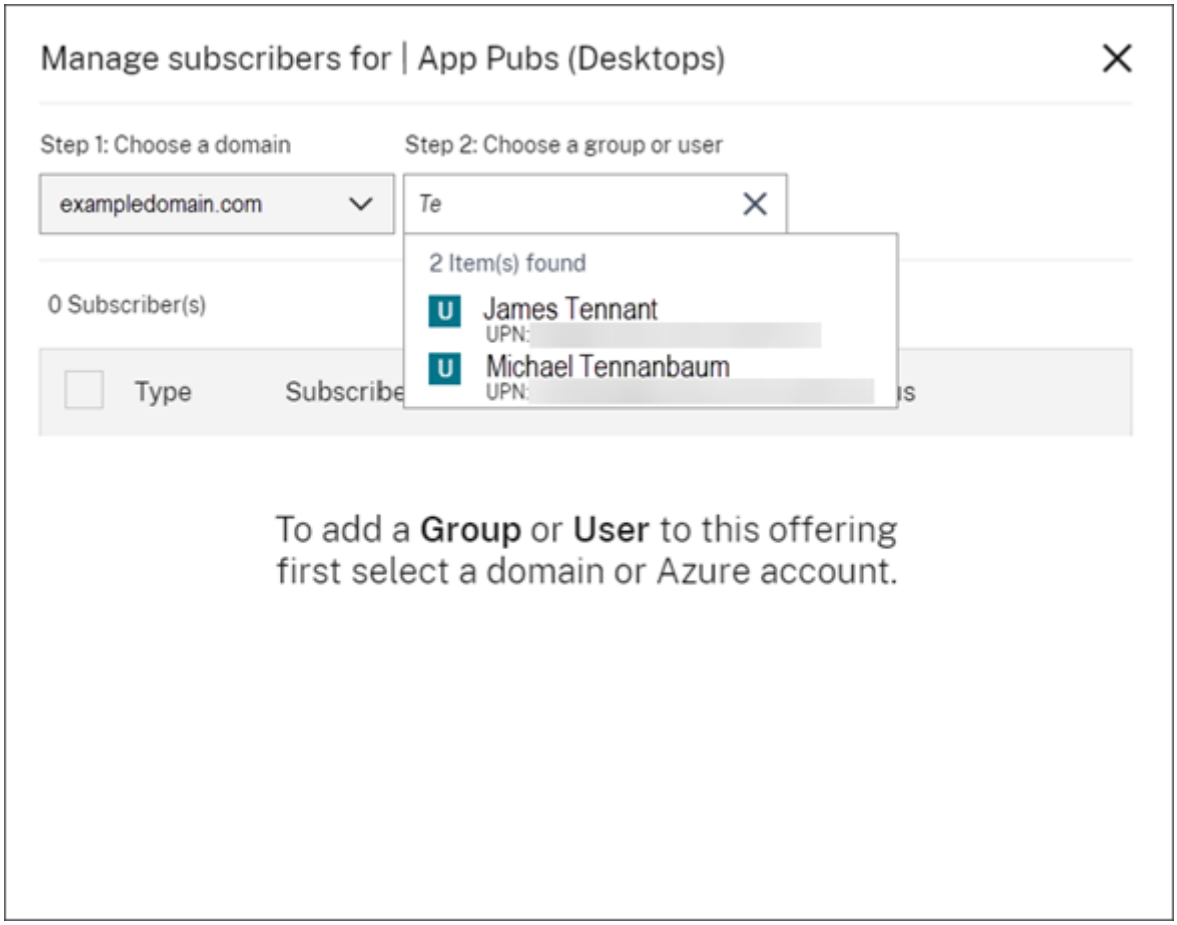
Pour gérer les utilisateurs ou groupes d'une seule offre, cliquez sur **Gérer les abonnés** dans le menu de la carte d'offre.



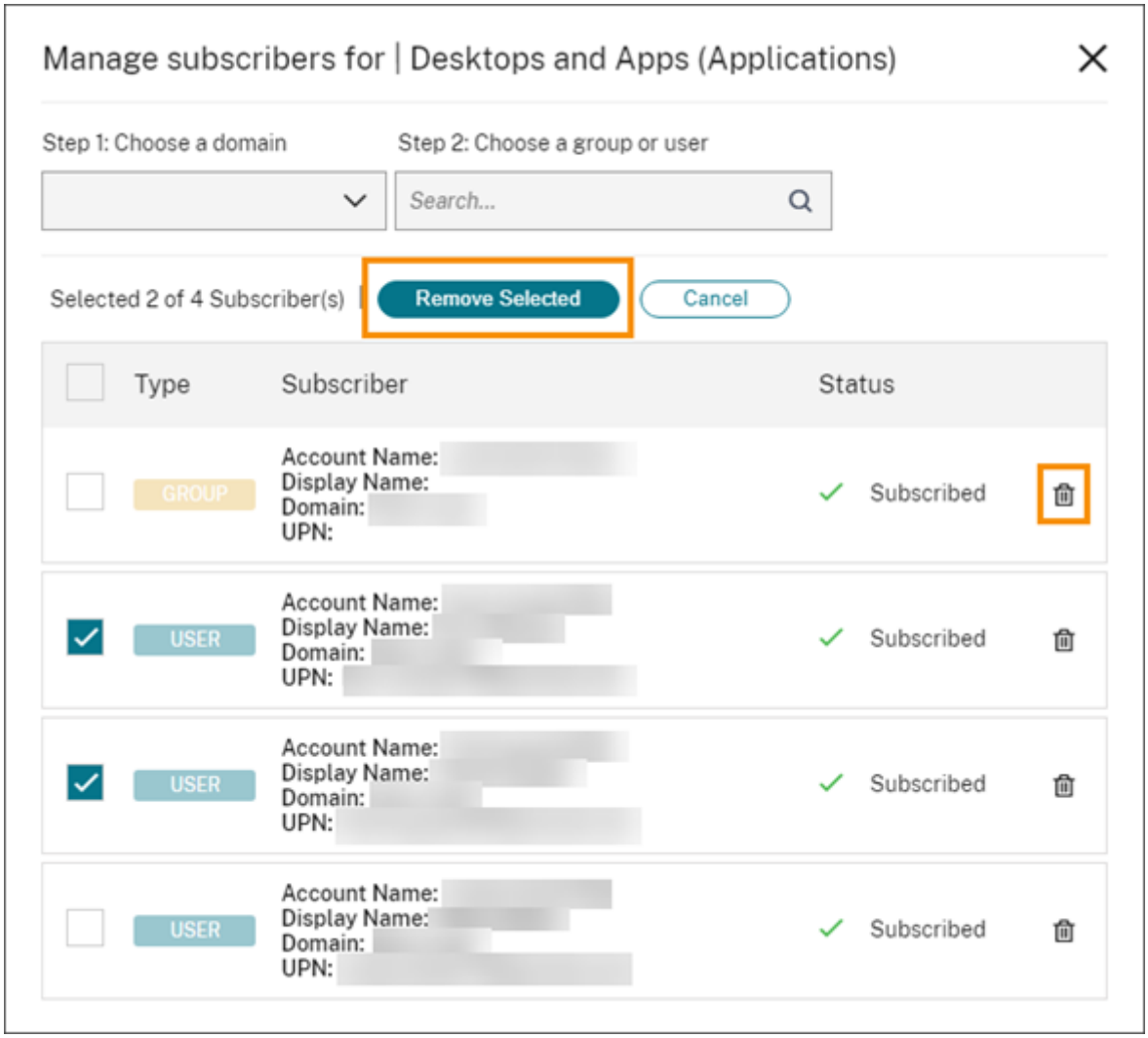
Pour gérer les abonnés pour plusieurs offres, sélectionnez la coche de chaque offre et cliquez sur **Gérer les abonnés**.



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



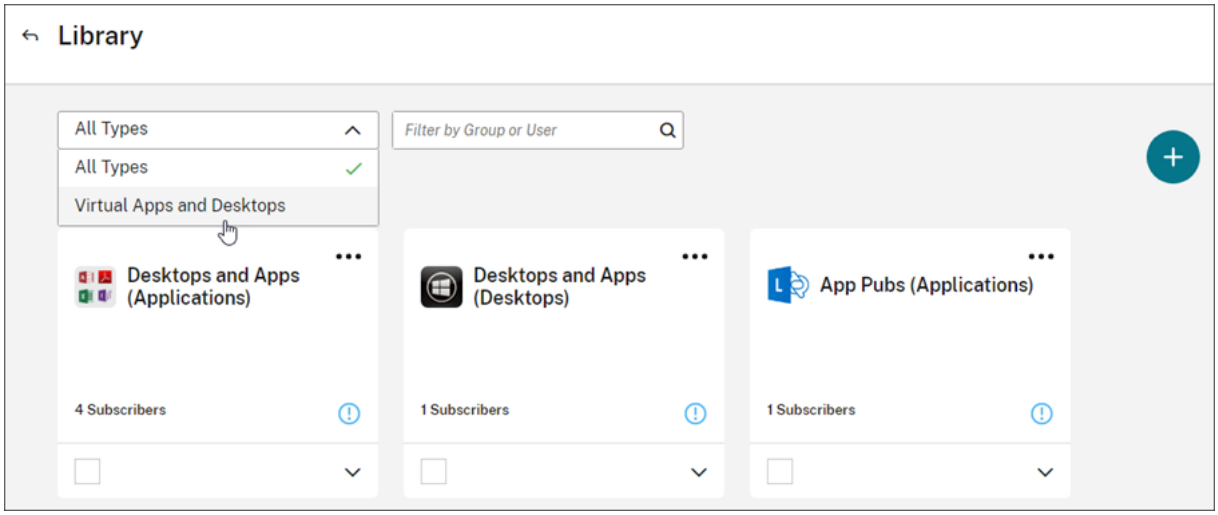
Pour supprimer un seul abonné, cliquez sur l'icône de corbeille pour un utilisateur ou groupe. Pour supprimer plusieurs abonnés, sélectionnez les utilisateurs ou groupes et cliquez sur **Supprimer la sélection**.



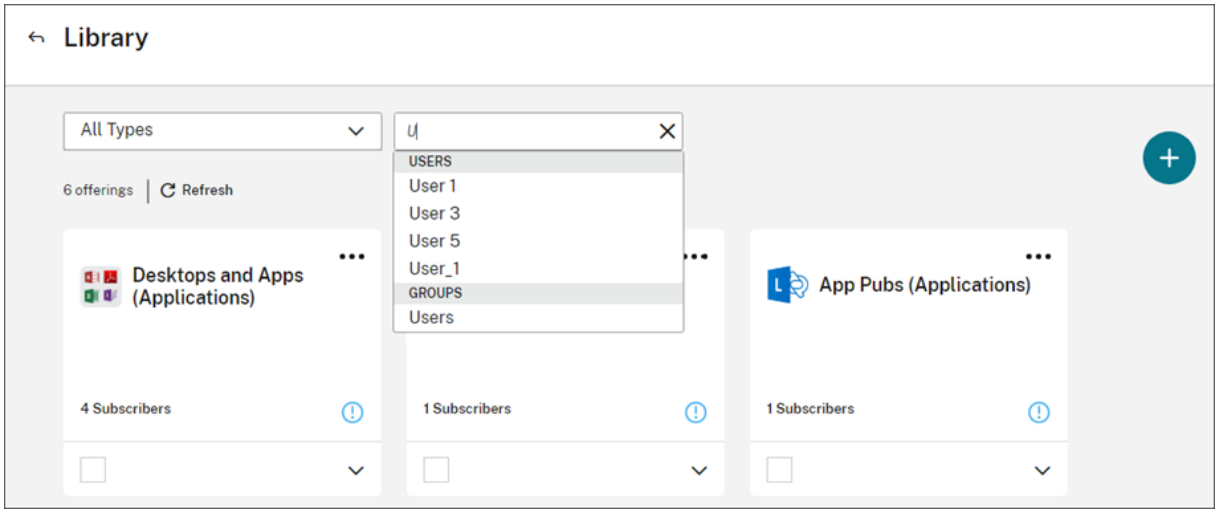
Après avoir ajouté ou supprimé des abonnés d'une offre, la carte d'offre affiche le nombre actuel d'abonnés.

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.



Page de destination personnalisée

April 5, 2024

De nombreux administrateurs accèdent à la console Cloud pour effectuer des tâches spécifiques, telles que la gestion des applications dans la console Web Studio ou l'affichage de données dans DaaS Monitor.

Cependant, ces tâches nécessitent plusieurs clics et la navigation sur plusieurs pages à chaque fois que les administrateurs se connectent, ce qui peut prendre beaucoup de temps. Cette nouvelle

fonctionnalité permet aux administrateurs de définir ou de modifier une page de destination personnalisée, ce qui permet de gagner du temps et d'améliorer l'expérience de la console.

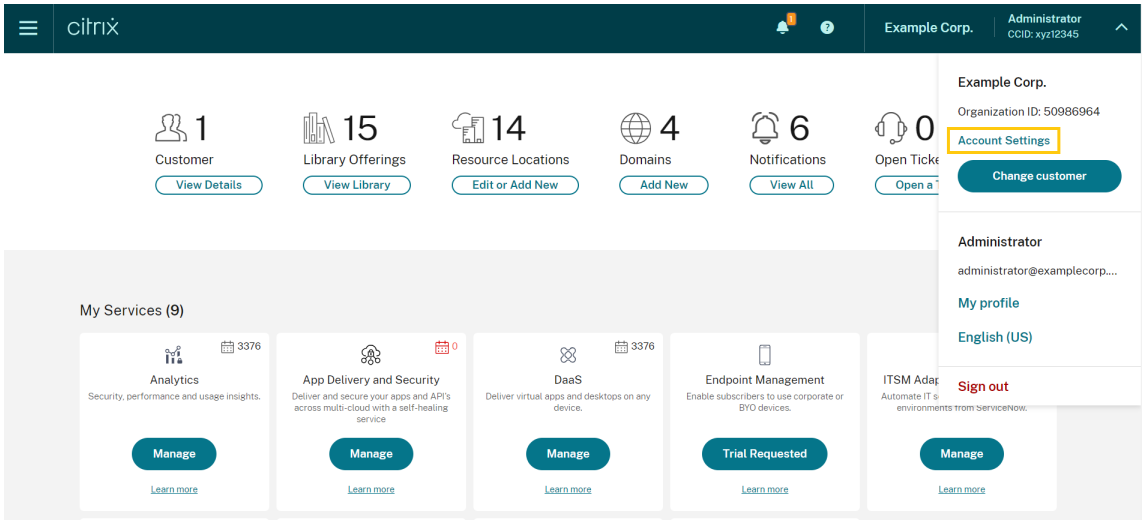
Actuellement, les pages suivantes peuvent être configurées en tant que page de destination personnalisée, et d'autres devraient être ajoutées à l'avenir :

- DaaS
- DaaS-Monitor
- Console NetScaler
- CAS
- Sécurité CAS
- Performances CAS
- WEM
- Généralités

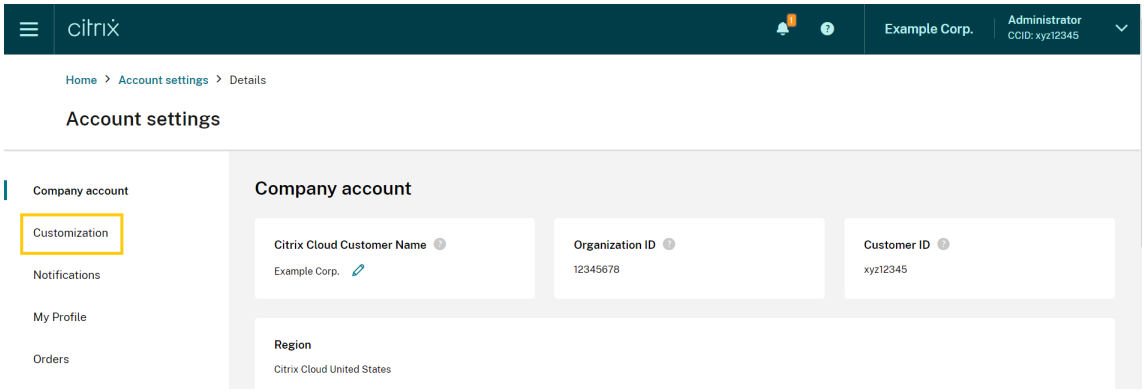
> **Remarque :**
>
> Le paramètre de page de destination personnalisée est facultatif et est défini par compte. Ainsi, chaque administrateur peut personnaliser sa propre expérience dans Citrix Cloud. Tous les administrateurs (qu'ils soient personnalisés ou complets) ont accès à cette fonctionnalité.

Configuration d'une page de destination personnalisée

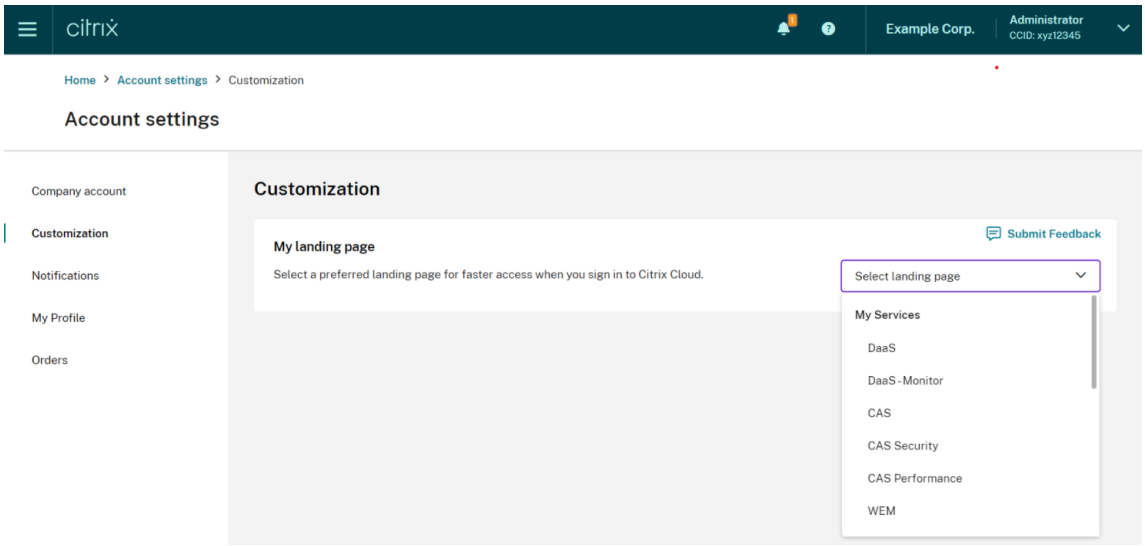
1. Cliquez sur le nom du profil et sélectionnez **Paramètres du compte**.



2. Cliquez sur **Personnalisation**.



3. Sélectionnez le service que vous souhaitez configurer comme page de destination personnalisée.



4. Cliquez sur **Appliquer**.

   Votre page de destination personnalisée est maintenant configurée.

> **Remarque :**
>
> - Vous pouvez redéfinir à tout moment la page de destination personnalisée sur votre page d'accueil Cloud par défaut en cliquant sur **Rétablir valeurs par défaut**.
> - Si vous vous reconnectez sur la même page que celle de laquelle vous venez de vous déconnecter, vous serez redirigé vers la dernière page consultée au lieu de votre nouvelle page de destination.

Autoriser les clients à supprimer leur compte Citrix Cloud et à se réintégrer

April 26, 2024

Citrix Cloud permet aux clients de supprimer leur compte Citrix Cloud en toute sécurité et de se réintégrer facilement si nécessaire.

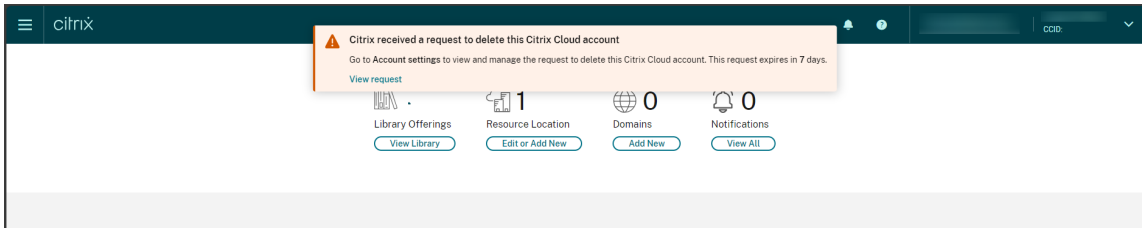
Logiciels requis

- Si votre compte possède des droits DaaS actifs et que votre environnement DaaS est provisionné, contactez le support technique de Citrix pour exécuter une désactivation rapide avant de continuer. Consultez l'article Studio Console Shows "Enable DaaS"for First Time Use pour plus de détails sur la manière de vérifier si votre environnement DaaS est provisionné.
- Supprimez tous les composants Cloud Connector et Connector Appliance.

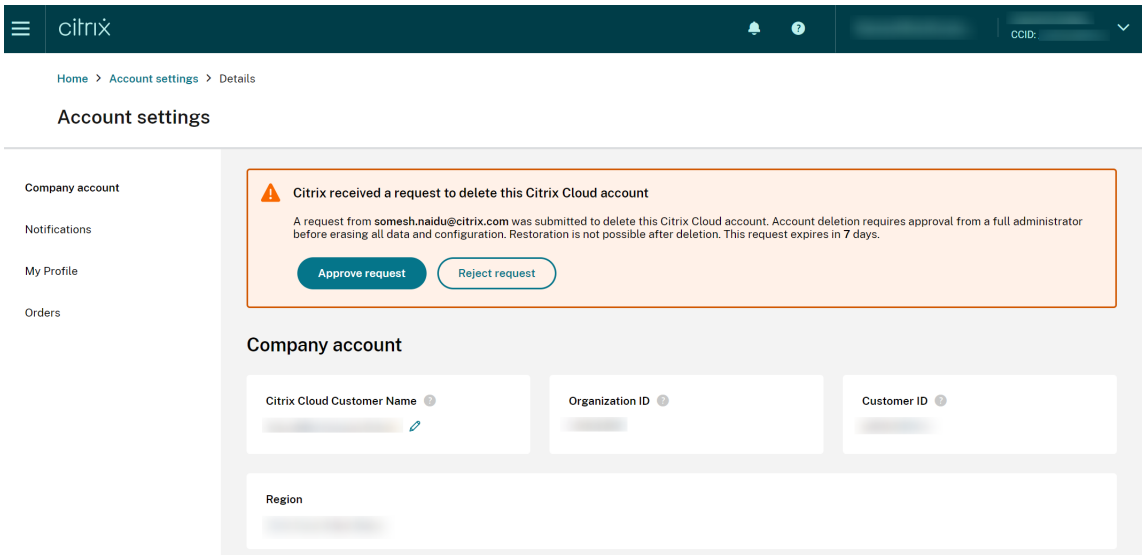
> **Important**
>
> Avant de supprimer un compte Citrix Cloud, prenez en compte les points suivants :
>
> - Toutes les données client sont supprimées des bases de données Citrix.
> - Toutes les ressources relatives aux services Citrix Cloud, y compris les VM gérées et provisionnées par Citrix dans votre environnement cloud, seront supprimées. Consultez services Citrix Cloud pour obtenir la description des composants gérés par Citrix et inclus dans des services Citrix Cloud spécifiques.
> - L'accès des administrateurs et des utilisateurs à Citrix Cloud et aux services est désactivé.
> - Les administrateurs ou les utilisateurs qui utilisent activement le service seront confrontés à une interruption de service.
> - Cette action est irréversible. Une fois les données supprimées, elles ne peuvent plus être récupérées.

Étapes

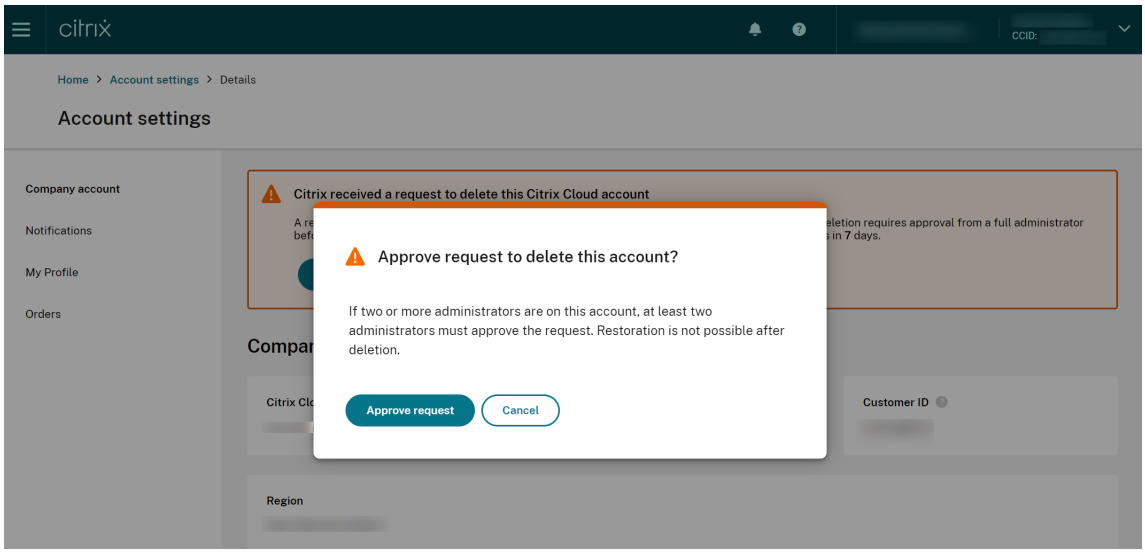
1. Contactez le service client Citrix pour soumettre une demande de suppression. Cette demande doit être soumise par un *administrateur complet* du compte Citrix Cloud.
2. Une fois la demande initiée, connectez-vous à votre compte Citrix Cloud. Vous y verrez le workflow de suppression de compte Citrix Cloud.



3. Suivez les instructions à l'écran pour approuver ou rejeter cette demande.



4. Pour approuver cette demande de suppression, connectez-vous au compte, accédez aux **paramètres du compte** et cliquez sur **Approuver la demande** dans la bannière du workflow d'approbation.



Pour annuler la demande de suppression, connectez-vous au compte, accédez aux **paramètres du compte** et cliquez sur **Rejeter et supprimer la demande** dans la bannière du workflow d'approbation de suppression.

> **Remarque :**
>
> - Si deux administrateurs ou plus sont associés à ce compte, au moins deux administrateurs doivent approuver la demande.
> - Cette demande expire si les approbations requises ne sont pas reçues dans les 7 jours.

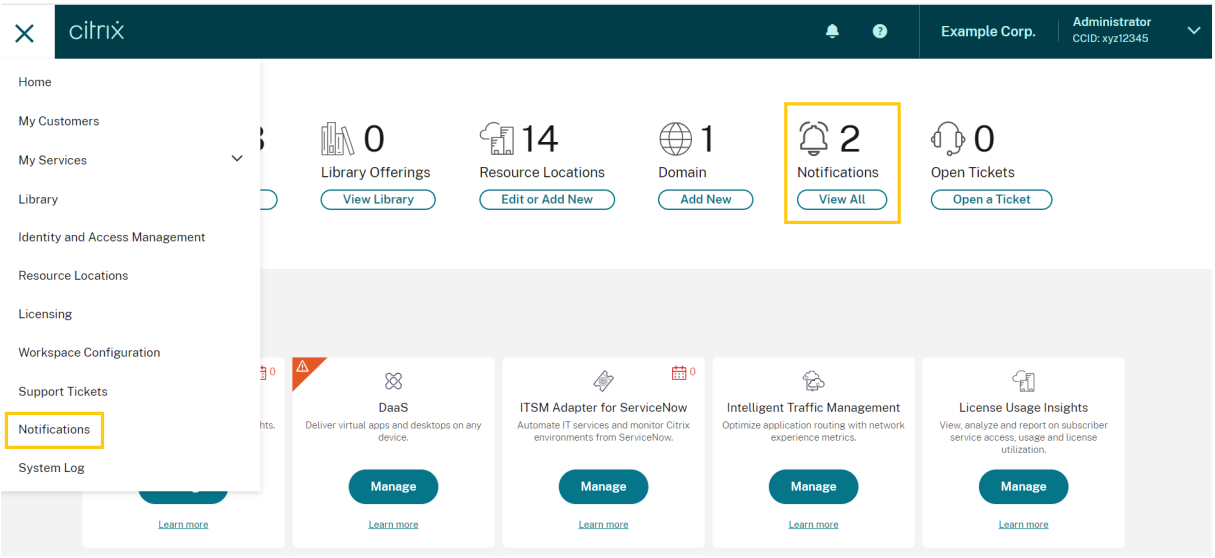
Notifications

October 4, 2023

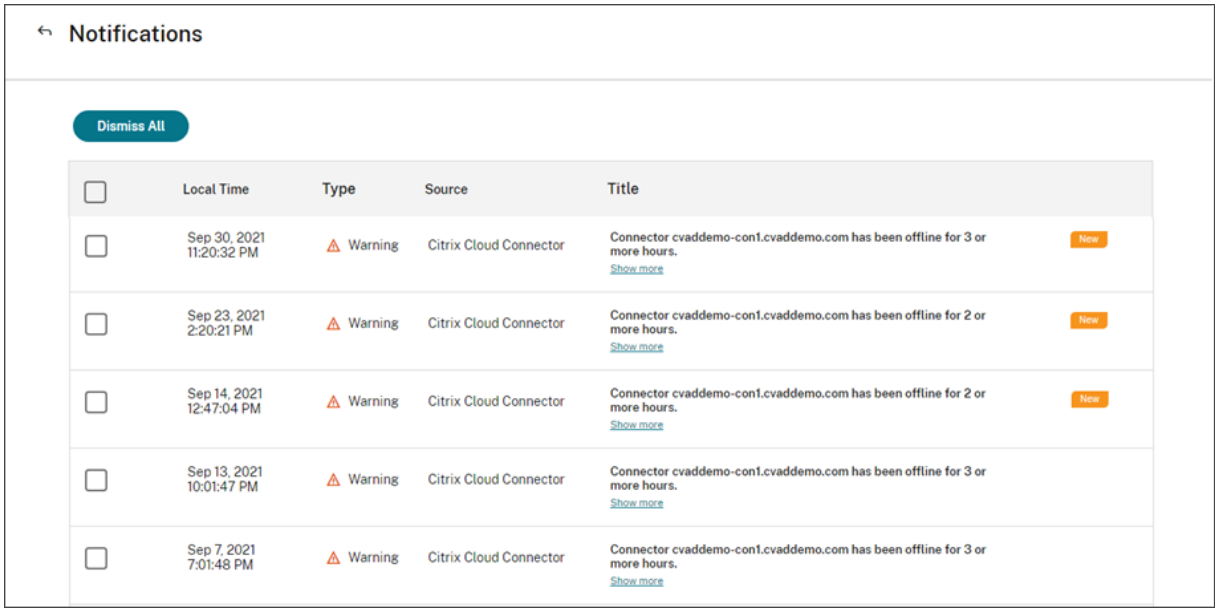
Les notifications fournissent des informations sur des problèmes ou événements susceptibles d'intéresser les administrateurs, tels que de nouvelles fonctionnalités Citrix Cloud ou des problèmes rencontrés sur une machine dans un emplacement de ressources. Les notifications peuvent provenir de n'importe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



La page Notifications affiche les notifications que vous recevez. Les notifications les plus récentes sont affichées en haut de la liste.

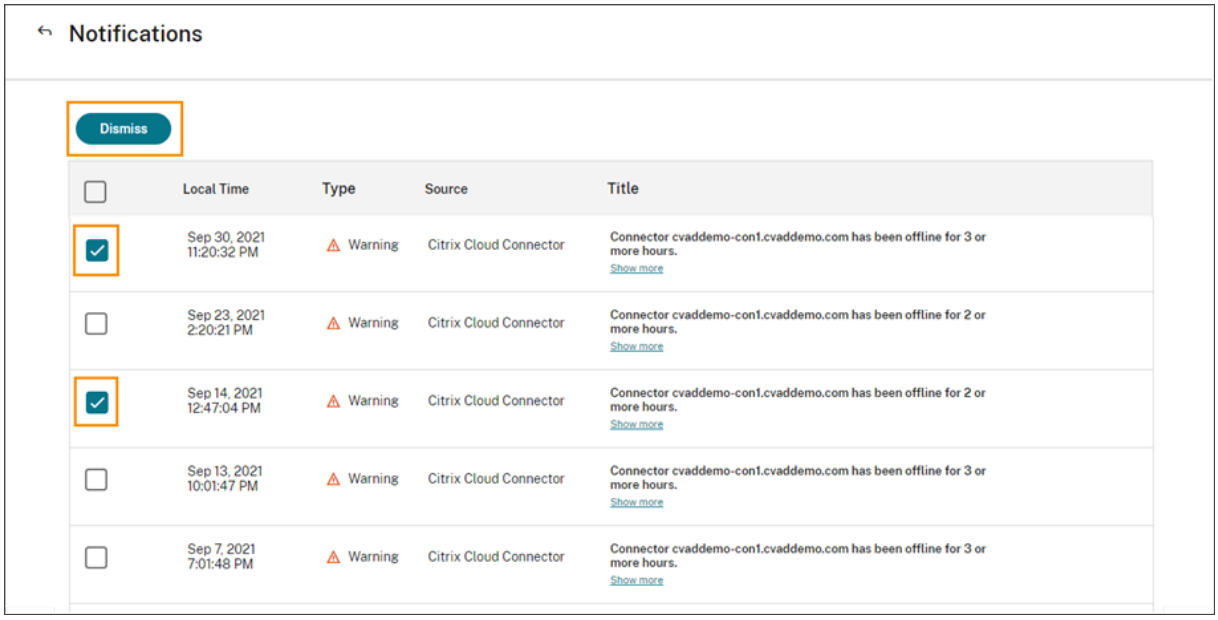


Ignorer les notifications

Les notifications sont gérées par administrateur. Lorsque vous ignorez des notifications, le rejet se produit sous votre propre identité d'administrateur dans Citrix Cloud. Les autres administrateurs peuvent toujours consulter et ignorer leurs propres notifications, même si vous les ignorez toutes.

Pour ignorer toutes les notifications que vous avez reçues, sélectionnez **Tout ignorer** en haut de la page.

Pour ignorer des notifications individuelles, sélectionnez chaque notification, puis sélectionnez **Ignorer**.



Recevoir des notifications par e-mail

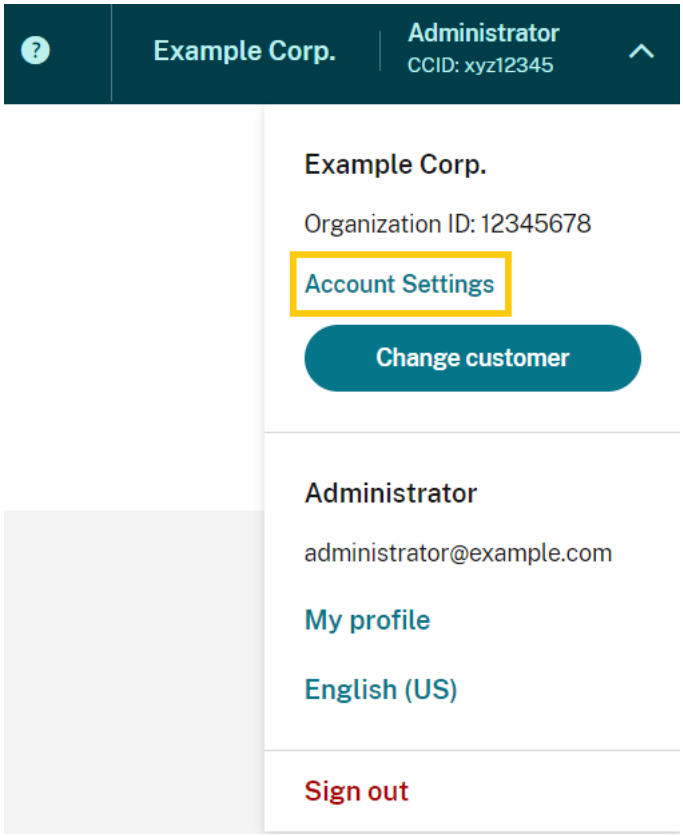
Vous pouvez choisir de recevoir des notifications par e-mail au lieu de vous connecter pour les voir. Par défaut, les notifications par e-mail sont désactivées.

Vous pouvez également activer les notifications par e-mail pour d'autres participants qui ne disposent pas d'un accès administrateur à votre compte Citrix Cloud, tels que les membres des équipes de sécurité et d'audit de votre organisation.

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.

Pour activer les notifications par e-mail pour vous-même

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



2. Sélectionnez **Notifications**.
3. Activez le paramètre **Mes notifications par e-mail**.
4. Sous **Gérer mes paramètres de notification**, sélectionnez les types de notifications que vous souhaitez recevoir. Par défaut, tous les types de notification sont sélectionnés.

5. Cliquez sur **Appliquer** pour enregistrer vos paramètres.

Pour activer les notifications par e-mail pour les non-administrateurs

Suivez les étapes de cette section pour ajouter des non-administrateurs en tant que contacts pour les notifications par e-mail. Si vous tentez d'ajouter un administrateur existant en tant que contact, Citrix Cloud affiche une erreur.

1. Dans la console de gestion de Citrix Cloud, cliquez sur **Paramètres de compte**.
2. Sélectionnez **Notifications**.
3. Sous **Gestion des contacts**, sélectionnez **Ajouter un contact**.
4. Entrez le nom, l'adresse e-mail et la langue préférée du contact.
5. Sous **Gérer les paramètres de notification**, sélectionnez les types de notifications à envoyer.
6. Sélectionnez **Ajouter un contact** pour enregistrer les informations du contact.

Modifier les paramètres de notification

En tant qu'administrateur, vous pouvez modifier les types de notifications que vous recevez en cochant ou en décochant les cases sous **Gérer mes paramètres de notification**. La modification de vos notifications n'a aucune incidence sur les notifications que reçoivent les autres administrateurs.

Vous pouvez également modifier les notifications que les non-administrateurs reçoivent.

Pour modifier les notifications destinées aux non-administrateurs

1. Dans la console de gestion de Citrix Cloud, cliquez sur **Paramètres de compte**.
2. Sélectionnez **Notifications**.
3. Sous **Gestion des contacts**, localisez le contact que vous souhaitez gérer.
4. Pointez vers le contact, puis sélectionnez l'icône en forme de crayon.
5. Sous **Gérer les paramètres de notification**, cochez ou décochez les cases correspondant à chaque type de notification.

Pour modifier l'adresse e-mail d'un contact, vous devez d'abord supprimer le contact, puis l'ajouter en tant que nouveau contact avec sa nouvelle adresse e-mail.

Désactiver les notifications par e-mail

En tant qu'administrateur, vous pouvez désactiver vos propres notifications par e-mail à tout moment en désactivant le paramètre **Mes notifications par e-mail**.

Les non-administrateurs peuvent arrêter de recevoir des notifications en cliquant sur le lien de désabonnement qui apparaît dans chaque e-mail de notification. Les contacts qui se sont désabonnés ont le statut de notification **Désabonné** dans le tableau de la section **Gestion des contacts**.

Pour désactiver les notifications pour les non-administrateurs, vous pouvez procéder comme suit :

- Décochez toutes les cases dans **Gérer les paramètres de notification** pour le contact.
- Supprimez le contact du tableau situé sous **Gestion des contacts**.

Supprimer les contacts non-administrateurs

1. Dans la console de gestion de Citrix Cloud, cliquez sur **Paramètres de compte**.
2. Sélectionnez **Notifications**.
3. Sous **Gestion des contacts**, localisez le contact que vous souhaitez gérer.
4. Pointez vers le contact, puis sélectionnez l'icône de la corbeille.

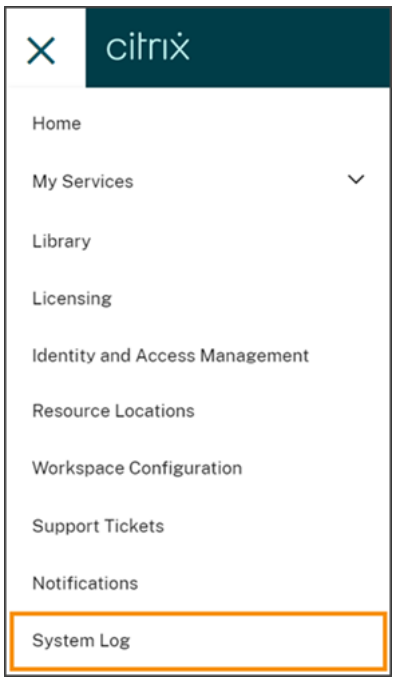
Citrix Cloud supprime le contact du tableau.

Journal du système

October 4, 2023

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.

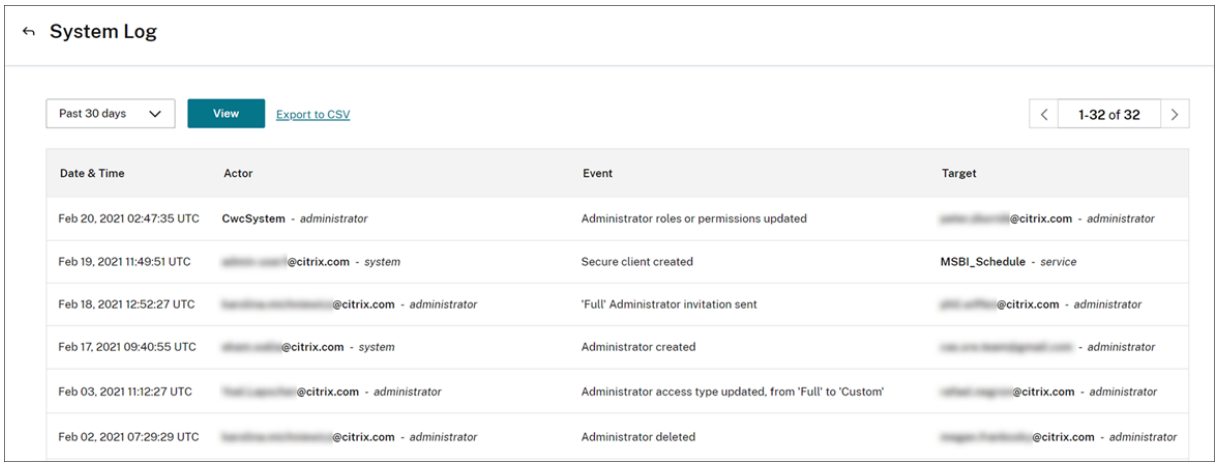


Pour plus d'informations sur la rétention des données dans les journaux système, consultez Rétention des données dans cet article.

Événements enregistrés

Le journal système capture les événements pour certaines opérations de la plate-forme Citrix Cloud et des services cloud. Pour obtenir la liste complète de ces événements et la description des données capturées, voir Référence des événements du journal système.

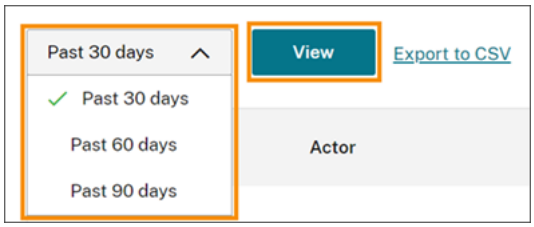
Par défaut, le journal système affiche les événements survenus au cours des 30 derniers jours. Les événements les plus récents sont affichés en premier.



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.

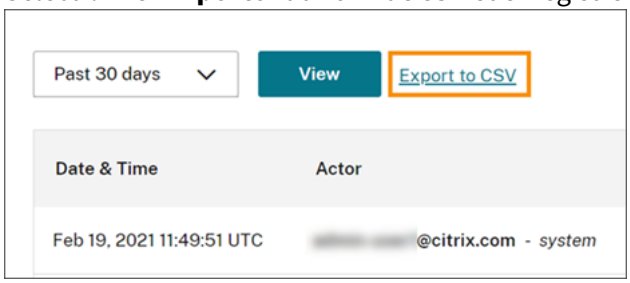


Pour récupérer des événements plus anciens survenus pendant une période spécifiée, vous pouvez utiliser l'API SystemLog. Pour plus d'informations, consultez la section Récupérer des événements pour une période spécifique dans cet article.

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 Citrix Cloud - SystemLog sur le site Web Citrix Developer.

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.

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.

Référence des événements du journal système

October 4, 2023

Pour afficher toutes les données des événements du journal système pour votre compte Citrix Cloud, vous pouvez :

- Télécharger un fichier CSV de tous les événements survenus au cours des 30, 60 ou 90 derniers jours.
- Utiliser l'API SystemLog pour récupérer les événements d'une période spécifique.

Consultez la section Descriptions des données d'événements de cet article pour obtenir une description des données capturées lorsque vous récupérez les événements du journal système. Consultez la section Composants et services cloud qui génèrent des événements pour connaître les valeurs spécifiques à un événement, telles que le texte du message d'événement, les types d'événement et si les données de champ d'objet sont enregistrées avant et après la survenue d'événements.

Composants et services cloud qui génèrent des événements

Le journal système enregistre les événements pour les entités, composants et services Citrix Cloud suivants :

- Plateforme Citrix Cloud : événements liés aux fonctions de la plateforme Citrix Cloud, telles que la gestion des administrateurs, de la réinitialisation des appareils pour les abonnés à Workspace, des locataires Azure AD et la gestion des domaines et des emplacements réseau.
- Connecteurs : événements liés à l'enregistrement et à la mise à jour des Citrix Cloud Connector et des appliances Connector.
- Licences : événements liés à l'enregistrement de serveurs de licences locaux, à la gestion des licences attribuées pour les services cloud et à l'exportation des données de licence.
- Service Secure Private Access : événements liés aux configurations du service Secure Private Access.
- Citrix Workspace : événements liés aux paramètres de configuration de l'espace de travail.

Description des données d'événements

Lorsque vous téléchargez des événements du journal système ou que vous les récupérez à l'aide de l'API SystemLog, les données suivantes sont incluses :

- **RecordID :** identifiant unique pour l'événement.
- **UtcTimestamp :** date et heure UTC auxquelles l'événement s'est produit.
- **CustomerId :** identifiant unique de l'organisation du compte Citrix Cloud.
- **EventType :** identifiant du type d'événement enregistré. Le type d'événement est enregistré au format `OriginatingService/Actor/Action`. Par exemple, le type d'événement permettant de créer un administrateur est `platform/administrator/create`.
- **TargetID :** ID de l'objet système qui a été affecté ou modifié.

- **TargetDisplayName :** nom d'affichage de l'objet système qui a été affecté ou modifié. Par exemple, le nom d'un administrateur qui a été créé.
- **TargetEmail :** adresse e-mail de l'objet système. Par exemple, l'adresse e-mail d'un administrateur qui a été créé.
- **TargetUserID :** ID utilisateur de l'objet système qui a été affecté ou modifié. Par exemple, lors de la création d'un administrateur, l'ID utilisateur cible est l'ID utilisateur de l'administrateur qui a été créé.
- **TargetType :** catégorie cible pour l'événement.
- **BeforeChanges** et **AfterChanges :** contenu des champs d'objet avant et après l'événement, respectivement. Pour certains événements, ces champs d'objet incluent :
  - CustomerID
  - Principal utilisateur
  - UserID
  - Type d'accès administrateur, tel que Custom ou Full
  - CreatedDate
  - UpdatedDate
  - DisplayName
- **AgentID :** catégorie d'événement.
- **ActorID :** ID de l'objet système qui a initié l'événement. Par exemple, pour créer un administrateur, il s'agit de l'ID d'objet de l'administrateur qui a invité un autre utilisateur sur le compte Citrix Cloud.
- **ActorDisplayName :** nom complet de la personne ou de l'entité qui a initié l'événement. Par exemple, le nom de l'administrateur qui a invité un autre utilisateur sur le compte Citrix Cloud.
- **ActorType :** service qui a généré l'événement.
- **EventMessage :** brève description de l'événement qui s'est produit.

Événements du journal système pour la plate-forme Citrix Cloud

July 11, 2023

Cet article décrit les données d'événement capturées par le journal système pour la plate-forme Citrix Cloud. Pour plus d'informations sur les données d'événement du journal système, reportez-vous à la section Référence des événements du journal système.

Pour en savoir plus sur le journal système, reportez-vous à la section Journal système.

Locataires Azure AD

Message de l'événement	Type d'événement	Type de cible	Type d'acteur	ID de l'acteur	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Locataire Azure AD connecté	platform/identityprovider/azuread/connect	identityprovider	administrateur		Oui	Non
Locataire Azure AD déconnecté	platform/identityprovider/azuread/disconnect	identityprovider	administrateur		Oui	Non
Nom de domaine d'authentification Azure AD modifié	platform/identityprovider/azuread/authdomain/update	identityprovider	administrateur	CustomDomainName	Non	Non
Échec de la modification du nom de domaine d'authentification Azure AD	platform/identityprovider/azuread/authdomain/update	identityprovider	administrateur	CustomDomainName	Non	Non

Administrateurs Citrix Cloud et clients sécurisés

Message de l'événement	Type d'événement	Type de cible	Type d'acteur	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Administrateur créé	platform/administrator/create	administrateur	system	Non	Oui
Invitation d'administrateur envoyée	platform/administrator/invite	administrateur	administrateur	Non	Oui
Rôles ou autorisations d'administrateur mis à jour	platform/administrator/update	administrateur	administrateur	Oui	Oui
Administrateur supprimé	platform/administrator/delete	administrateur	administrateur	Non	Oui
Client sécurisé créé	platform/clientadministrator/create	service	system	Non	Oui
Client sécurisé supprimé	platform/clientadministrator/delete	service	administrateur	Oui	Non
Groupe d'administrateurs créé	platform/administrator/group/create	administrateur	administrateur	Non	Oui
Rôles ou autorisations du groupe d'administrateurs mis à jour	platform/administrator/group/update	administrateur	administrateur	Oui	Oui
Groupe d'administrateurs supprimé	platform/administrator/group/delete	administrateur	administrateur	Oui	Non

Réinitialisation de l'appareil pour Active Directory + jeton

Message de l'événement	Type d'événement	Type de cible	Type d'acteur	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Réinitialisation du jeton de l'appareil de l'abonné terminée	platform/authentication/device/delete	subscriber	administrateur	Non	Oui

Gestion des domaines

Message de l'événement	Type d'événement	Type de cible	Type d'acteur	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Domaine supprimé	platform/domain/remove	service	administrateur	Non	Non

Emplacements réseau

Message de l'événement	Type d'événement	ID de la cible	ID de l'acteur	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Emplacement réseau créé	sdwan/networklocation/create	ID de l'emplacement réseau qui a été créé	Nom de l'administrateur qui a ajouté l'emplacement réseau	Non	Oui

Message de l'événement	Type d'événement	ID de la cible	ID de l'acteur	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Emplacement réseau mis à jour	sdwan/networklocation/edit	ID de l'emplacement réseau qui a été modifié	Nom de l'administrateur qui a modifié l'emplacement réseau	Oui	Oui
Emplacement réseau supprimé	sdwan/networklocation/delete	ID de l'emplacement réseau qui a été supprimé	Nom de l'administrateur qui a supprimé l'emplacement réseau	Oui	Non

Emplacements des ressources

Message de l'événement	Type d'événement	ID de la cible	ID de l'acteur	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Emplacement des ressources créé	platform/resourcelocation/create	ID de l'emplacement des ressources qui a été créé	Nom de l'administrateur qui a créé l'emplacement des ressources	Oui	Oui

Message de l'événement	Type d'événement	ID de la cible	ID de l'acteur	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Emplacement des ressources mis à jour	platform/resourcelocation/update	Nom de l'emplacement des ressources qui a été modifié	Nom de l'administrateur qui a modifié l'emplacement des ressources	Oui	Oui
Emplacement des ressources supprimé	platform/resourcelocation/delete	Nom de l'emplacement des ressources qui a été supprimé	Nom de l'administrateur qui a supprimé l'emplacement des ressources	Oui	Oui

Événements du journal système pour les connecteurs

May 3, 2022

Cet article décrit les données d'événement capturées par le journal système pour Citrix Cloud Connector et appliance Connector for Cloud Services. Pour plus d'informations sur les données d'événement du journal système, reportez-vous à la section Référence des événements du journal système.

Pour en savoir plus sur le journal système, reportez-vous à la section Journal système.

Enregistrement du connecteur

Message de l'événement	Type d'événement	Type de cible	ID de l'acteur	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Connecteur enregistré	platform/edgeservice/create	**Cloud Connector** ou **Appliance Connector**	Administrateur qui a enregistré le connecteur	Oui	Oui
Connecteur supprimé	platform/edgeservice/delete	**Cloud Connector** ou **Appliance Connector**	Administrateur qui a supprimé le connecteur	Oui	Oui

Mises à jour de Connector

Message de l'événement	Type d'événement	ID de la cible	ID de l'acteur	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Période de maintenance de l'emplacement des ressources mise à jour	platform/resourcelocation/maintenancewindow	Nom de l'emplacement des ressources qui a été modifié	Administrateur qui a modifié la configuration	Oui	Oui
Mise à niveau du connecteur déclenchée par l'administrateur	platform/edgeservice/manualupgrade	**Cloud Connector** ou **Appliance Connector**	Administrateur qui a initié la mise à jour	Non	Non

Message de l'événement	Type d'événement	ID de la cible	ID de l'acteur	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Mise à niveau du connecteur démarrée	platform/edgeservice/upgradestarted	**Cloud Connector** ou **Appliance Connector**	**Automatique** ou administrateur qui a initié la mise à jour	Oui	Non
Mise à niveau du connecteur terminée	platform/edgeservice/upgradecompleted	**Cloud Connector** ou **Appliance Connector**	**Automatique** ou administrateur qui a initié la mise à jour	Non	Oui

Clés publiques de connecteur

Message de l'événement	Type d'événement	ID de la cible	ID de l'acteur	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Clé publique ajoutée à la confiance	platform/authentication/createedgeservicekey		Administrateur qui a effectué l'opération	Non	Non
Clé publique supprimée de la confiance	platform/authentication/deleteedgeservicekey		Administrateur qui a effectué l'opération	Non	Non

Événements du journal système pour les licences dans Citrix Cloud

May 3, 2022

Cet article décrit les données d'événement capturées par le journal système pour l'enregistrement du système de licences Citrix local auprès de Citrix Cloud. Pour plus d'informations sur les données d'événement du journal système, reportez-vous à la section Référence des événements du journal système.

Pour en savoir plus sur le journal système, reportez-vous à la section Journal système.

Serveurs de licences locaux

Message de l'événement	Type d'événement	Type de cible	ID de l'acteur	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Serveurs de licences locaux supprimés	lui/onpremlicenseservers/delete	Gestion des licences	Administrateur qui a supprimé le serveur de licences	Non	Non
Échec de la suppression des serveurs de licences locaux	lui/onpremlicenseservers/deletefailed	Gestion des licences	Administrateur qui a essayé de supprimer le serveur de licences	Non	Non

Gestion des licences du service cloud

Message de l'événement	Type d'événement	Type de cible	ID de l'acteur	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Licences du service Citrix Cloud libérées	lui/cloudlicense/release	CloudLicense	Administrateur qui a publié les licences pour le service cloud	Non	Non
Échec de la libération des licences du service Citrix Cloud	lui/cloudlicense/releasefailed	CloudLicense	Administrateur qui a essayé de libérer des licences pour le service cloud	Non	Non

Informations sur l'utilisation des licences pour Citrix Service Provider

Message de l'événement	Type d'événement	Type de cible	ID de l'acteur	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Données de la liste d'utilisateurs locaux des partenaires exportées	lui/csp/userlistdataexported	Gestion des licences	Administrateur qui a exporté les données de la liste d'utilisateurs des partenaires	Non	Non

Message de l'événement	Type d'événement	Type de cible	ID de l'acteur	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Échec de l'exportation des données de la liste d'utilisateurs locaux des partenaires	lui/csp/userlistdataexportfailed	Gestion des licences	Administrateur qui a essayé d'exporter les données de la liste des utilisateurs partenaires	Non	Non

Utilisation des licences pour les services cloud et les produits sur site

Message de l'événement	Type d'événement	Type de cible	ID de l'acteur	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Données d'utilisation des licences exportées	lui/cloudlicense/usagedataexport	CloudLicensing ou Licensing	Administrateur qui a exporté les données d'utilisation des licences	Non	Non
Échec de l'exportation des données d'utilisation des licences	lui/cloudlicense/usagedataexportfailed	CloudLicensing ou Licensing	Administrateur qui a essayé d'exporter les données d'utilisation des licences	Non	Non

Événements du journal système pour Secure Private Access

October 13, 2022

Cet article décrit les données d'événement capturées par le journal système pour le service Secure Private Access. Pour plus d'informations sur les données d'événement du journal système, reportez-vous à la section Référence des événements du journal système.

Pour en savoir plus sur le journal système, reportez-vous à la section Journal système.

Applications Web et SaaS

Message de l'événement	Type d'événement	Type de cible	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Application Web/SaaS créée	swa/websaasppplicationcreated	web/saasapplication	Non	Oui
Web/SaaS application updated	swa/websaasppplicationupdated	web/saasapplication	Oui	Oui
Web/SaaS application deleted	swa/websaasppplicationdeleted	web/saasapplication	Oui	Non
Échec de la création de l'application Web/SaaS	swa/websaasppplicationcreatefailed	web/saasapplication	Non	Non
Échec de la mise à jour de l'application Web/SaaS	swa/websaasppplicationupdatefailed	web/saasapplication	Oui	Oui
Échec de la suppression de l'application Web/SaaS	swa/websaasppplicationdeletefailed	web/saasapplication	Oui	Oui

Abonnements utilisateur et groupe

Message de l'événement	Type d'événement	Type de cible	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Abonnement utilisateur/groupe ajouté	swa/websaaspplicationsubscription/subscribe	websaasapplicationsubscriptions	Non	Oui
Abonnement utilisateur/groupe supprimé	swa/websaaspplicationsubscription/unsubscribe	websaasapplicationsubscriptions	Oui	Non
Échec de l'abonnement utilisateur/groupe	swa/websaaspplicationsubscription/subscribefailed	websaasapplicationsubscriptions	Non	Non
Échec d'annulation de l'abonnement utilisateur/groupe	swa/websaaspplicationsubscription/unsubscribefailed	websaasapplicationsubscriptions	Non	Non

Stratégies contextuelles

Message de l'événement	Type d'événement	Type de cible	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Stratégie contextuelle créée	swa/contextualpolicy/create	contextualpolicy	Non	Oui
Stratégie contextuelle mise à jour	swa/contextualpolicy/update	contextualpolicy	Oui	Oui
Stratégie contextuelle supprimée	swa/contextualpolicy/delete	contextualpolicy	Oui	Non

Message de l'événement	Type d'événement	Type de cible	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Échec de la création de la stratégie contextuelle	swa/contextualpolicy/createfailed	contextualpolicy	Non	Non
Échec de la mise à jour de la stratégie contextuelle	swa/contextualpolicy/updatefailed	contextualpolicy	Non	Non
Échec de la suppression de la stratégie contextuelle	swa/contextualpolicy/deletefailed	contextualpolicy	Oui	Non

Domaines d'application

Message de l'événement	Type d'événement	Type de cible	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Domaine d'application créé	swa/applicationdomain/create	applicationdomain	Non	Oui
Domaine d'application mis à jour	swa/applicationdomain/update	applicationdomain	Oui	Oui
Domaine d'application supprimé	swa/applicationdomain/delete	applicationdomain	Oui	Non
Échec de la création du domaine d'application	swa/applicationdomain/createfailed	applicationdomain	Non	Non

Message de l'événement	Type d'événement	Type de cible	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Échec de la mise à jour du domaine d'application	swa/applicationdomain/update/failed	applicationdomain	Oui	Non
Échec de la suppression du domaine d'application	swa/applicationdomain/delete/failed	applicationdomain	Oui	Non

Paramètres d'extension du navigateur

Message de l'événement	Type d'événement	Type de cible	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Paramètres d'extension du navigateur mis à jour	swa/browserextensionsettings/update/success	browserextensionsettings	Oui	Oui
Échec de la mise à jour des paramètres d'extension du navigateur	swa/browserextensionsettings/update/failed	browserextensionsettings	Oui	Non

Listes et catégories de filtres d'URL de sites Web

Message de l'événement	Type d'événement	Type de cible	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Listes et catégories de filtres de sites Web activées	swa/website/filterlists/webfilterlistcategory/featureenabled/update	webfilterlistcategoryfeature	Oui	Oui
Listes de filtres de sites Web activées et catégories de filtres désactivées	swa/website/filterlists/webfilterlistcategory/featuredisabled/update	webfilterlistcategoryfeature	Oui	Oui
Listes de filtres de sites Web désactivées et catégories de filtres activées	swa/website/filterlists/webfilterlistcategory/featureenabled/update	webfilterlistcategoryfeature	Oui	Oui
Listes et catégories de filtres de sites Web désactivées	swa/website/filterlists/webfilterlistcategory/featuredisabled/update	webfilterlistcategoryfeature	Oui	Oui
Échec de l'activation des listes de filtres et des catégories de sites Web	swa/website/filterlists/webfilterlistcategory/featureenabled/update	webfilterlistcategoryfeature	Oui	Failed
Échec de l'activation des listes de filtres de sites Web et de la désactivation des catégories de filtres	swa/website/filterlists/webfilterlistcategory/featuredisabled/update	webfilterlistcategoryfeature	Oui	Failed

Message de l'événement	Type d'événement	Type de cible	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Échec de la désactivation des listes de filtres de sites Web et de l'activation des catégories de filtres	swa/website/filterlists/websitefilterlistcategory/disable/updatefailed	websitefilterlistcategory	Oui	Oui
Échec de la désactivation des listes de filtres et des catégories de sites Web	swa/website/filterlists/websitefilterlistcategory/disable/updatefailed	websitefilterlistcategory	Oui	Oui
Liste d'URL de sites Web créée	swa/websiteurlfilteringlist/create	websiteurlfilteringlist	Non	Oui
Liste d'URL de sites Web mise à jour	swa/websiteurlfilteringlist/update	websiteurlfilteringlist	Oui	Oui
Liste d'URL de site Web supprimée	swa/websiteurlfilteringlist/delete	websiteurlfilteringlist	Oui	Non
Échec de la création de la liste d'URL de site Web	swa/websiteurlfilteringlist/createfailed	websiteurlfilteringlist	Non	Non
Échec de la mise à jour de la liste d'URL de sites Web	swa/websiteurlfilteringlist/updatefailed	websiteurlfilteringlist	Oui	Non
Échec de la suppression de la liste d'URL de site Web	swa/websiteurlfilteringlist/deletefailed	websiteurlfilteringlist	Oui	Non
Catégorie de filtre d'URL de site Web créée	swa/websiteurlfiltercategory/create	websiteurlfiltercategory	Non	Oui

Message de l'événement	Type d'événement	Type de cible	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Catégorie de filtrage d'URL de sites Web mise à jour	swa/websiteurlfiltercategory/updatecategory	websiteurlfiltercategory	Oui	Oui
Catégorie de filtre d'URL de site Web supprimée	swa/websiteurlfiltercategory/deletecategory	websiteurlfiltercategory	Non	Non
Échec de la création de la catégorie de filtre d'URL de site Web	swa/websiteurlfiltercategory/createfailedcategory	websiteurlfiltercategory	Non	Non
Échec de la mise à jour de la catégorie de filtrage d'URL de sites Web	swa/websiteurlfiltercategory/updatefailedcategory	websiteurlfiltercategory	Oui	Non
Échec de la suppression de la catégorie de filtre d'URL du site Web	swa/websiteurlfiltercategory/deletefailedcategory	websiteurlfiltercategory	Oui	Non

Présélections de catégorie de filtre de site

Message de l'événement	Type d'événement	Type de cible	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Présélection de la catégorie de filtre de sites Web mise à jour	swa/website urlfiltercatego-rypreset/update	websiteurlfiltercategorypreset	Oui	Oui

Message de l'événement	Type d'événement	Type de cible	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Échec de la mise à jour de la préselection de catégorie de filtre des sites Web	swa/websiteurlfilter/categoryfilter/categoryset/failed	category filter/category set	Objet	Oui

Listes et catégories de filtres d'URL de sites Web bloqués

Message de l'événement	Type d'événement	Type de cible	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Liste d'URL de sites Web bloqués créée	swa/websiteurlfilter/websitefiltering/blockedurllist/created	website filtering/blocked url list	Non	Oui
Liste d'URL de sites Web bloqués mise à jour	swa/websiteurlfilter/websitefiltering/blockedurllist/updated	website filtering/blocked url list	Non	Oui
Liste d'URL de sites Web bloqués supprimée	swa/websiteurlfilter/websitefiltering/blockedurllist/deleted	website filtering/blocked url list	Non	Oui
Échec de la création de la liste d'URL de sites Web bloquées	swa/websiteurlfilter/websitefiltering/blockedurllist/createfailed	website filtering/blocked url list	Non	Oui
Échec de la mise à jour de la liste d'URL de sites Web bloqués	swa/websiteurlfilter/websitefiltering/blockedurllist/updatefailed	website filtering/blocked url list	Non	Oui

Message de l'événement	Type d'événement	Type de cible	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Échec de la suppression de la liste d'URL de sites Web bloqués	swa/websiteurlfilterwebsite/blocked/listfailed	website/blocked/list	Failed	Oui
Catégorie de filtre d'URL de sites Web bloqués créée	swa/websiteurlfilterwebsite/blocked/list	website/blocked/list	None	Oui
Catégorie de filtre d'URL de sites Web bloqués mise à jour	swa/websiteurlfilterwebsite/blocked/list	website/blocked/list	None	Oui
Catégorie de filtre d'URL de sites Web bloqués supprimée	swa/websiteurlfilterwebsite/blocked/list	website/blocked/list	None	Oui
Échec de la création de la catégorie de filtre d'URL de sites Web bloqués	swa/websiteurlfilterwebsite/blocked/list	website/blocked/list	failed	Oui
Échec de la mise à jour de la catégorie de filtre d'URL de sites Web bloqués	swa/websiteurlfilterwebsite/blocked/list	website/blocked/list	None	failed
Échec de la suppression de la catégorie de filtre d'URL de sites Web bloqués	swa/websiteurlfilterwebsite/blocked/list	website/blocked/list	failed	Oui

Listes et catégories de filtres d'URL de sites Web autorisés

Message de l'événement	Type d'événement	Type de cible	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Liste d'URL de sites Web autorisés créée	swa/websiteurlfilterwebsiteallowedlist/create	websiteallowedlist	Non	Oui
Liste d'URL de sites Web autorisés mise à jour	swa/websiteurlfilterwebsiteallowedlist/update	websiteallowedlist	Non	Oui
Liste d'URL de sites Web autorisés supprimée	swa/websiteurlfilterwebsiteallowedlist/delete	websiteallowedlist	Non	Oui
Échec de la création de la liste d'URL de sites Web autorisés	swa/websiteurlfilterwebsiteallowedlist/createfail	websiteallowedlist	Non	Oui
Échec de la mise à jour de la liste d'URL de sites Web autorisés	swa/websiteurlfilterwebsiteallowedlist/updatefail	websiteallowedlist	Non	Oui
Échec de la suppression de la liste d'URL de sites Web autorisés	swa/websiteurlfilterwebsiteallowedlist/deletefail	websiteallowedlist	Non	Oui
Catégorie de filtre d'URL de sites Web autorisés créée	swa/websiteurlfiltercategoryallowedlist/create	categoryallowedlist	Non	Oui
Catégorie de filtre d'URL de sites Web autorisés mise à jour	swa/websiteurlfiltercategoryallowedlist/update	categoryallowedlist	Non	Oui

Message de l'événement	Type d'événement	Type de cible	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Catégorie de filtre d'URL de sites Web autorisés supprimée	swa/websiteurlfiltercategory/allowedlist/delete	category/allowedlist		Oui
Échec de la création de la catégorie de filtre d'URL de sites Web autorisés	swa/websiteurlfiltercategory/allowedlist/create	category/allowedlist	failed	Oui
Échec de la mise à jour de la catégorie de filtre d'URL de sites Web autorisés	swa/websiteurlfiltercategory/allowedlist/update	category/allowedlist	failed	Oui
Échec de la suppression de la catégorie de filtre d'URL de sites Web autorisés	swa/websiteurlfiltercategory/allowedlist/delete	category/allowedlist	failed	Oui

Listes et catégories de filtres d'URL de sites Web redirigés vers Remote Browser Isolation (anciennement Secure Browser)

Message de l'événement	Type d'événement	Type de cible	Type d'acteur	ID d'agent	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Liste d'URL de sites Web redirigés vers Secure Browser créée	swa/websiteurlfilteringlist/redirected/create	website
Liste d'URL de sites Web redirigés vers Secure Browser mise à jour	swa/websiteurlfilteringlist/redirected/update	w
Liste d'URL de sites Web redirigés vers Secure Browser supprimée	swa/websiteurlfilteringlist/redirected/delete	we
Échec de la création de liste d'URL de sites Web redirigés vers Secure Browser	swa/websiteurlfilteringlist/redirecte
Échec de la mise à jour de la liste d'URL de sites Web redirigés vers Secure Browser	swa/websiteurlfilteringlist/redir
Échec de la suppression de la liste d'URL de sites Web redirigés vers Secure Browser	swa/websiteurlfilteringlist/red
Catégorie de filtre d'URL de sites Web redirigés vers Secure Browser créée	swa/websiteurlfiltercategory/redirected

|Catégorie de filtre d'URL de sites Web redirigés vers Secure Browser mise à jour|swa/websiteurlfiltercategory/redir
|Catégorie de filtre d'URL de sites Web redirigés vers Secure Browser supprimée|swa/websiteurlfiltercategory/redir
|Échec de la création de catégorie de filtre d'URL de sites Web redirigés vers Secure Browser|swa/websiteurlfiltercat
|Échec de la mise à jour de la catégorie de filtre d'URL de sites Web redirigés vers Secure Browser|swa/websiteurlfiltercategory/redirected/updatefailed|websiteurlfilteringlist|Non|Oui|
|Échec de la suppression de la catégorie de filtre d'URL de sites Web redirigés vers Secure Browser|swa/websiteurlfiltercategory/redirected/deletefailed|websiteurlfilteringlist|Non|Oui|

Événements du journal système pour Citrix Workspace

May 3, 2022

Cet article décrit les données d'événement capturées par le journal système pour Citrix Workspace. Pour plus d'informations sur les données d'événement du journal système, reportez-vous à la section Référence des événements du journal système.

Pour en savoir plus sur le journal système, reportez-vous à la section Journal système.

URL de l'espace de travail

Message de l'événement	Type d'événement	Type de cible	ID de l'acteur	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
URL de l'espace de travail mise à jour	wxp/url/update	subscriber	Administrateur qui a mis à jour l'URL	Oui	Oui
Échec de la mise à jour de l'URL de l'espace de travail	wxp/url/updatefailed	subscriber	Administrateur qui a tenté de mettre à jour l'URL	Oui	Oui

Message de l'événement	Type d'événement	Type de cible	ID de l'acteur	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
URL de l'espace de travail activée	wxp/url/enable	subscriber	Administrateur qui a activé la personnalisation de l'URL de l'espace de travail	Non	Oui
Échec de l'activation de l'URL de l'espace de travail	wxp/url/enablefailed	subscriber	Administrateur qui a tenté d'activer la personnalisation de l'URL de l'espace de travail	Non	Oui
URL de l'espace de travail désactivée	wxp/url/disable	subscriber	Administrateur qui a désactivé la personnalisation de l'URL de l'espace de travail	Non	Oui
Échec de la désactivation de l'URL de l'espace de travail	wxp/url/disablefailed	subscriber	Administrateur qui a tenté de désactiver la personnalisation de l'URL de l'espace de travail	Non	Oui

Authentification de Workspace

Message de l'événement	Type d'événement	Type de cible	ID de l'acteur	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Fournisseur d'identité de l'espace de travail mis à jour	wxp/identityprovider/update	subscriber	Administrateur qui a mis à jour la méthode d'authentification de l'espace de travail	Oui	Oui
Échec de la mise à jour du fournisseur d'identité de l'espace de travail	wxp/identityprovider/updatefailed	subscriber	Administrateur qui a tenté de mettre à jour la méthode d'authentification de l'espace de travail	Oui	Oui

Service d'authentification fédérée de Citrix

Message de l'événement	Type d'événement	Type de cible	ID de l'acteur	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Service d'authentification fédérée (FAS) de l'espace de travail activé	wxp/fas/enable	subscriber	Administrateur qui a activé FAS	Non	Oui

Message de l'événement	Type d'événement	Type de cible	ID de l'acteur	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Échec de l'activation du service d'authentification fédérée (FAS) de l'espace de travail	wxp/fas/enablefailed	subscriber	Administrateur qui a tenté d'activer FAS	Non	Oui
Service d'authentification fédérée (FAS) de l'espace de travail désactivé	wxp/fas/disable	subscriber	Administrateur qui a désactivé FAS	Non	Oui
Impossible de désactiver le service d'authentification fédérée (FAS) de l'espace de travail	wxp/fas/disablefailed	subscriber	Administrateur qui a tenté de désactiver FAS	Non	Oui

Favoris

Message de l'événement	Type d'événement	Type de cible	ID de l'acteur	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Favoris de Workspace activés	wxp/favorites/enable	subscriber	Administrateur qui a activé les favoris	Non	Oui

Message de l'événement	Type d'événement	Type de cible	ID de l'acteur	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Impossible d'activer les favoris de Workspace	wxp/favorites/enablefailed	subscriber	Administrateur qui a tenté d'activer les favoris	Non	Oui
Favoris de Workspace désactivés	wxp/favorites/disable	subscriber	Administrateur qui a désactivé les favoris	Non	Oui
Impossible de désactiver les favoris de Workspace	wxp/favorites/disablefailed	subscriber	Administrateur qui a tenté de désactiver les favoris	Non	Oui

Modifier le mot de passe

Message de l'événement	Type d'événement	Type de cible	ID de l'acteur	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Stratégie Options de modification du mot de passe de l'espace de travail mise à jour	wxp/changepasswordoptions/update	workspaceconfiguration	Administrateur qui a mis à jour la stratégie de modification du mot de passe dans Citrix Workspace	Oui	Oui

Message de l'événement	Type d'événement	Type de cible	ID de l'acteur	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Échec de la mise à jour de la stratégie d'options de modification du mot de passe de l'espace de travail	wxp/changepasswordoptions/updatepolicyfailed	workspaceconfiguration	Administrateur qui a tenté de mettre à jour la stratégie de modification du mot de passe dans Citrix Workspace	Oui	Oui
Options de modification du mot de passe de l'espace de travail activées	wxp/changepasswordoptions/enable	workspaceconfiguration	Administrateur qui a activé le paramètre de modification du mot de passe dans Citrix Workspace	Non	Oui
Échec de l'activation des options de modification du mot de passe de l'espace de travail	wxp/changepasswordoptions/enablefailed	workspaceconfiguration	Administrateur qui a essayé d'activer le paramètre de modification du mot de passe dans Citrix Workspace	Non	Oui

Message de l'événement	Type d'événement	Type de cible	ID de l'acteur	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Options de modification du mot de passe de l'espace de travail désactivées	wxp/changepasswordoptions/disable	subscription	Administrateur qui a désactivé le paramètre de modification du mot de passe dans Citrix Workspace	Non	Oui
Échec de la désactivation des options de modification du mot de passe de l'espace de travail	wxp/changepasswordoptions/disablefailed	subscription	Administrateur qui a tenté de désactiver le paramètre de modification du mot de passe dans Citrix Workspace	Non	Oui

Jetons de longue durée

Message de l'événement	Type d'événement	Type de cible	ID de l'acteur	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Configuration du jeton longue durée de l'espace de travail mise à jour	wxp/longlivedtoken/update	subscription	Administrateur qui a mis à jour la configuration du jeton	Oui	Oui
Échec de la mise à jour de la configuration du jeton de longue durée de l'espace de travail	wxp/longlivedtoken/updatefailed	subscription	Administrateur qui a tenté de mettre à jour la configuration du jeton	Oui	Oui

Délai d'inactivité du Web

Message de l'événement	Type d'événement	Type de cible	ID de l'acteur	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Configuration des sessions de l'espace de travail mise à jour	wxp/sessions/updatesubscriber		Administrateur qui a mis à jour le temps d'inactivité pour le paramètre Délai d'inactivité pour le Web	Oui	Oui
Échec de la mise à jour de la configuration des sessions de l'espace de travail	wxp/sessions/updatefailed	subscriber	Administrateur qui a essayé de mettre à jour le temps d'inactivité pour le paramètre Délai d'inactivité pour le Web	Oui	Oui

Déploiement des fonctionnalités

Message de l'événement	Type d'événement	Type de cible	ID de l'acteur	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Utilisateurs et groupes attribués mis à jour pour l'expérience d'espace de travail intelligent	wxp/iws/features/subscribers/usersgroups/updated		Administrateur qui a mis à jour les utilisateurs et les groupes affectés pour accéder aux notifications de flux d'activité dans Citrix Workspace	Non	Non
Échec de l'attribution d'utilisateurs et de groupes mis à jour pour l'expérience d'espace de travail intelligent	wxp/iws/features/subscribers/usersgroups/failed		Administrateur qui a tenté de mettre à jour les utilisateurs et les groupes affectés pour accéder aux notifications de flux d'activité dans Citrix Workspace	Non	Non
Expérience d'espace de travail intelligent activée	wxp/iws/features/enable		Administrateur qui a activé les notifications de flux d'activité dans Citrix Workspace	Non	Non

Message de l'événement	Type d'événement	Type de cible	ID de l'acteur	Champs d'objet actuels enregistrés avant l'événement	Champs d'objet mis à jour enregistrés après l'événement
Échec de l'activation de l'expérience de l'espace de travail intelligent	wxp/iws/features/enable/failed		Administrateur qui a tenté d'activer les notifications de flux d'activité dans Citrix Workspace	Non	Non
Expérience d'espace de travail intelligent désactivée	wxp/iws/features/disable		Administrateur qui a désactivé les notifications de flux d'activité dans Citrix Workspace	Non	Non
Échec de la désactivation de l'expérience de l'espace de travail intelligent	wxp/iws/features/disable/failed		Administrateur qui a tenté de désactiver les notifications de flux d'activité dans Citrix Workspace	Non	Non

SDK et API

July 2, 2024

Citrix Cloud fournit plusieurs API que vous pouvez utiliser pour récupérer des informations et automatiser des tâches complexes et répétitives, notamment :

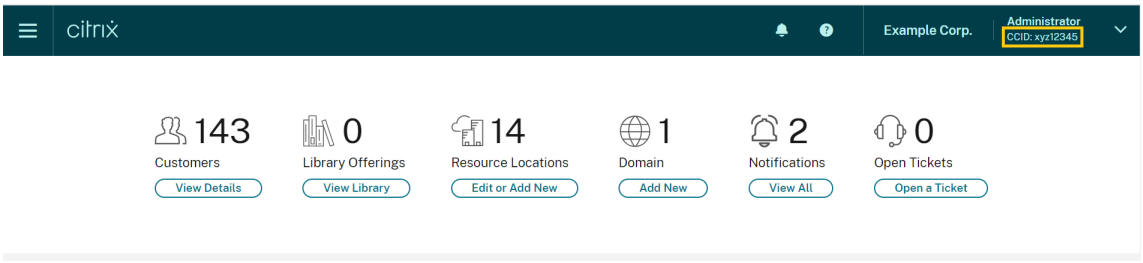
- Installer Citrix Cloud Connector de manière silencieuse
- Créer et utiliser des rapports pour la gestion des licences cloud
- Déterminer les droits d'utilisation d'un client
- Envoyer des notifications aux administrateurs Citrix Cloud
- Récupérer les événements du journal système
- Récupérer des informations sur vos emplacements de ressources à utiliser avec d'autres API

Plusieurs services Citrix Cloud fournissent également des kits SDK et des API qui vous permettent de récupérer des informations, d'interroger des données et d'effectuer des tâches administratives.

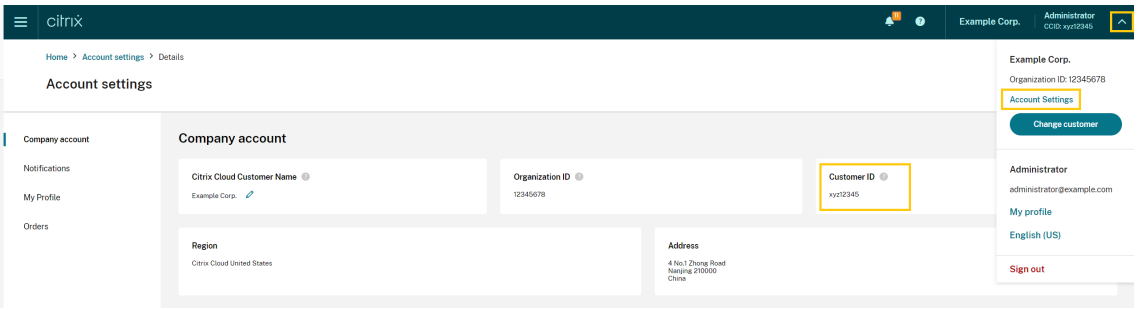
Clients sécurisés

Pour utiliser les API Citrix Cloud, vous devez créer un client sécurisé qui accède à Citrix Cloud en votre nom. Pour créer un client sécurisé, vous devez fournir l'ID client de votre compte Citrix Cloud. Votre numéro client se trouve aux emplacements suivants dans la console de gestion :

- Dans le coin supérieur droit de la console, sous votre nom d'utilisateur



- Sur votre page **Paramètres du compte**



- Sur la page **Accès aux API**

Autorisations héritées

Les clients sécurisés sont liés à un seul administrateur et à un seul ID client dans Citrix Cloud. Cela signifie que vos clients sécurisés héritent du même niveau d'autorisations que celui dont vous disposez sous un ID client spécifique. Ainsi, si vous disposez d'autorisations d'accès complet, vos clients

sécurisés disposent également d'autorisations d'accès complet. Si votre niveau d'autorisation est réduit ultérieurement, les clients sécurisés que vous avez déjà créés héritent automatiquement de vos autorisations réduites.

Pour obtenir des instructions sur la création de clients sécurisés, consultez la section Get started with Citrix Cloud APIs dans la documentation Citrix Developer.

API Cloud Licensing

Les entreprises clientes peuvent utiliser les API Cloud Licensing pour effectuer des tâches de gestion telles que l'exportation des données d'utilisation et la libération des licences. Les partenaires Citrix peuvent utiliser ces API pour récupérer des données de synthèse et historiques pour les instances Citrix Virtual Apps and Desktops et Citrix DaaS locales.

Pour plus d'informations, consultez la section APIs to manage Citrix cloud licensing dans la documentation Citrix Developer.

API SystemLog

L'API SystemLog vous permet de récupérer les événements qui se sont produits sur votre compte Citrix Cloud pendant des périodes que vous spécifiez. Pour plus d'informations sur l'utilisation de cette API, consultez Citrix Cloud - SystemLog dans la documentation Citrix Developer.

API Resource Locations

L'API Resource Locations vous permet de récupérer des informations sur vos emplacements de ressources pour les utiliser avec d'autres applications et scripts. Par exemple, supposons que vous souhaitiez installer Citrix Cloud Connector de manière silencieuse dans l'un des emplacements de ressources de votre compte Citrix Cloud. Vous pouvez utiliser cette API pour récupérer l'ID d'emplacement de ressources et le transmettre à votre script d'installation.

Pour plus d'informations sur l'utilisation de cette API, consultez Citrix Cloud - Resource Location dans la documentation Citrix Developer.

API Service Entitlement

L'API Service Entitlement récupère les informations liées aux services qu'un client est autorisé à utiliser, les jours restants pour chaque droit de licences et la quantité de droits de licences que le client a achetés. Pour plus d'informations sur l'utilisation de cette API, consultez Citrix Cloud - Service Entitlement dans la documentation Citrix Developer.

API Notifications

L'API Notifications vous permet d'envoyer des messages à d'autres administrateurs Citrix Cloud. Les destinataires reçoivent vos messages via la page Notifications de la console de gestion.

SDK et API pour d'autres services

Pour plus d'informations sur les kits SDK et les API disponibles pour les autres services Citrix Cloud, consultez les articles suivants :

- Espaces de travail numériques : inclut des kits SDK et des API pour les services d'espace de travail, tels que Citrix DaaS et Citrix Workspace.
- App Delivery and Security : inclut des kits SDK et des API pour les services de mise en réseau et de mise à disposition d'applications, tels que NetScaler Console, Intelligent Traffic Management et SD-WAN Orchestrator.

Informations supplémentaires

Pour en savoir plus sur la façon dont les API Citrix Cloud et les clients sécurisés peuvent vous aider à effectuer des opérations complexes, telles que la migration vers le cloud et la configuration de l'authentification avec des jetons push, consultez les articles Tech Zone suivants :

- PoC Guide: nFactor for Citrix Gateway Authentication with Push Token
- Deployment Guide: Migrating Citrix Virtual Apps and Desktops from VMware vSphere to Citrix Virtual Apps and Desktops service on Microsoft Azure
- PoC Guide: Automated Configuration Tool

Citrix Cloud pour les partenaires

April 5, 2024

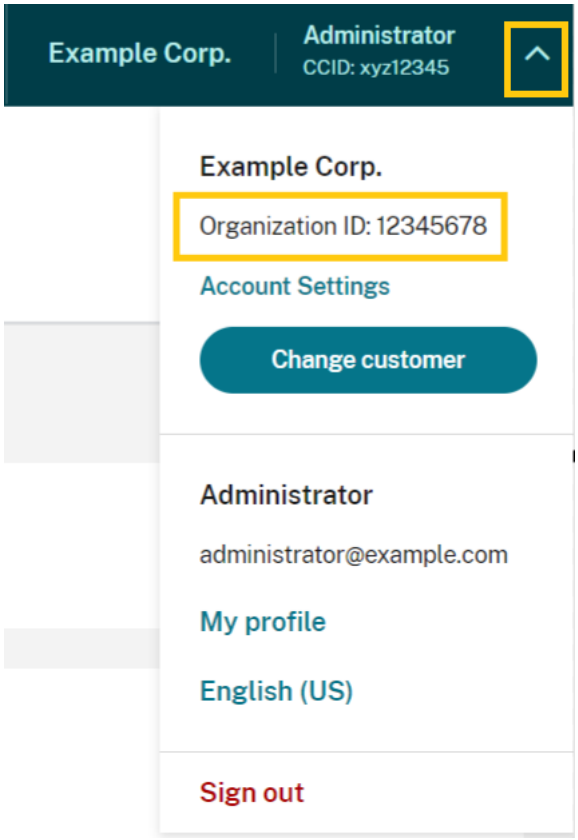
Citrix Cloud propose des services, des fonctionnalités et des expériences conçus pour les clients et les partenaires. Cette section présente les fonctionnalités à disposition des partenaires Citrix qui les aideront à collaborer avec leurs clients sur les services et les solutions Citrix Cloud.

Identification des partenaires

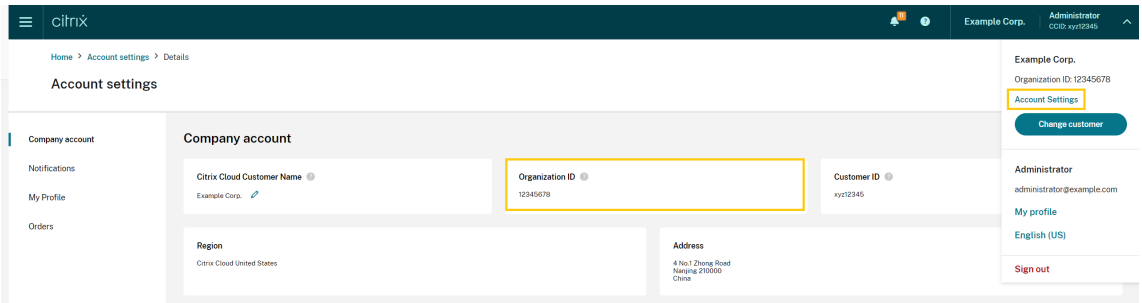
Les partenaires sont identifiés dans Citrix Cloud en fonction de leur ID d'organisation Citrix. Les partenaires peuvent afficher l'ID d'organisation (ou ORGID) associé à leur compte Citrix Cloud aux emplace-

ments suivants de la console de gestion Citrix Cloud :

- Dans le menu client. Cliquez sur le nom de votre client dans le coin supérieur droit de la console. Votre ORGID apparaît sous le nom de votre société dans le menu.



- Sur la page **Paramètres du compte**. Dans le menu client situé dans le coin supérieur droit, sélectionnez **Paramètres de compte**.



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.

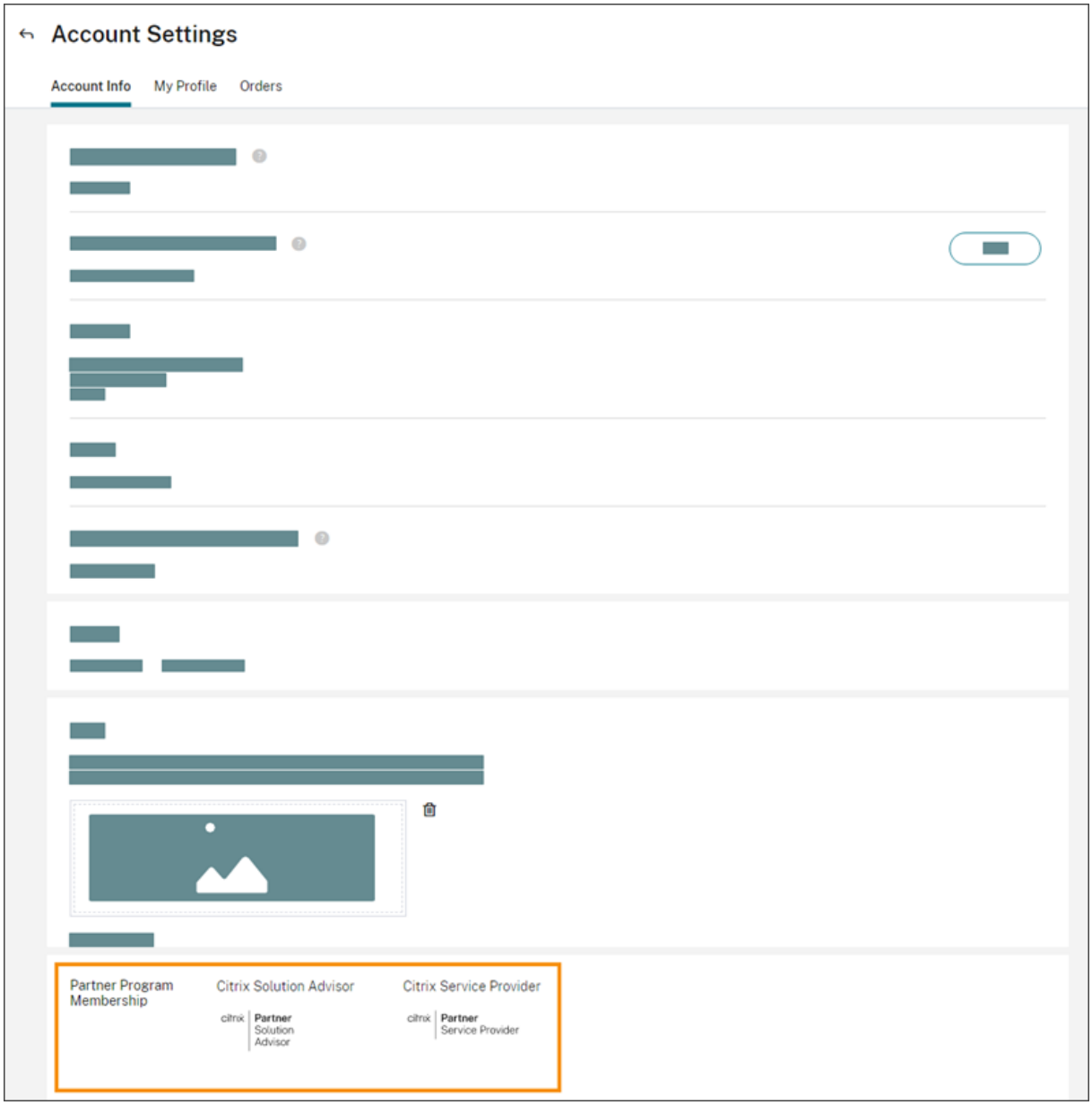
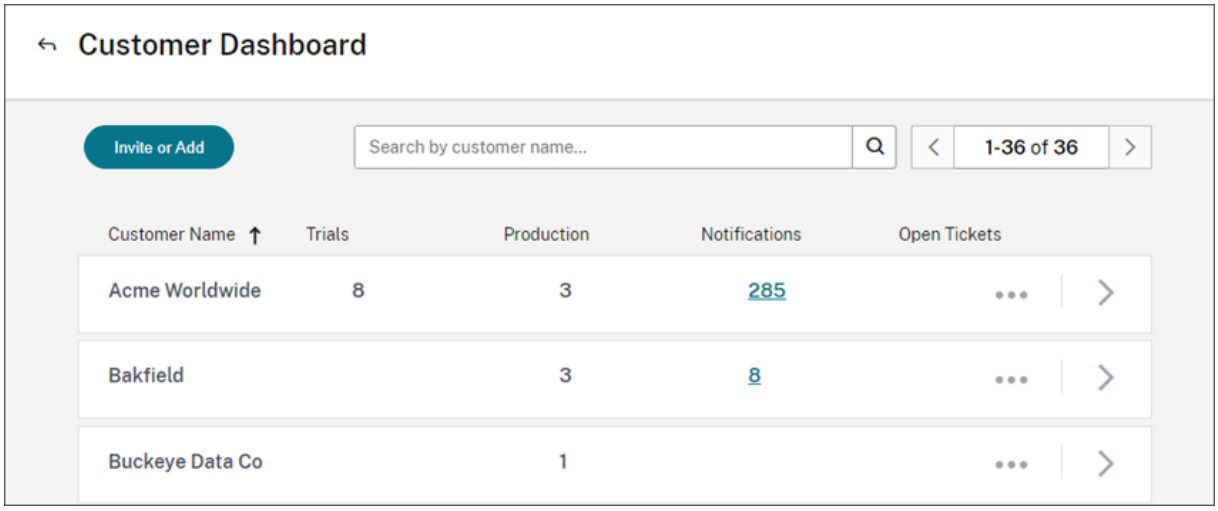
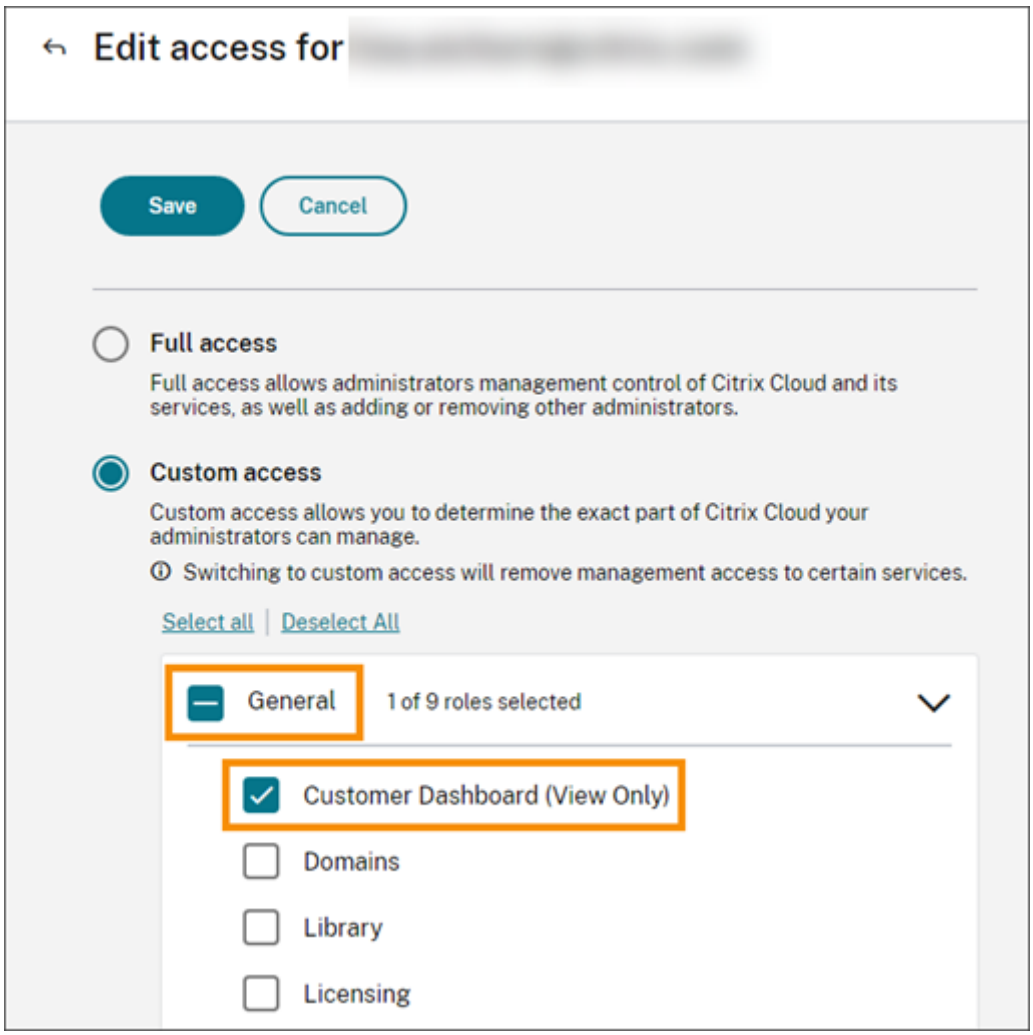


Tableau de bord client

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.



Par défaut, les administrateurs disposant d'un accès complet peuvent consulter le tableau de bord client. Les administrateurs disposant d'un accès personnalisé peuvent afficher le tableau de bord si l'autorisation **Tableau de bord client (lecture seule)** est sélectionnée. Pour plus d'informations sur les autorisations d'administrateur dans Citrix Cloud, consultez la section Modifier les autorisations d'administrateur.



Connexions partenaires 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 se connectant 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

Une fois qu'un partenaire et un client sont connectés, les administrateurs du 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.

Les connexions des partenaires avec les clients n'expirent pas

Connexions avec plusieurs partenaires ou clients

Les partenaires peuvent établir des connexions avec plusieurs clients. Les partenaires peuvent être associés à un maximum de 100 comptes clients. Si un partenaire doit gérer plus de 100 comptes clients, il doit créer un compte partenaire distinct avec une adresse e-mail différente pour gérer les clients supplémentaires. Le partenaire peut également envisager de supprimer les comptes clients qu'il n'a plus besoin de gérer.

Les clients peuvent établir des connexions avec plusieurs partenaires. Il n'y a pas de limite au nombre de connexions client-partenaire.

Notifications de connexion

Citrix Cloud envoie des notifications aux partenaires lorsque :

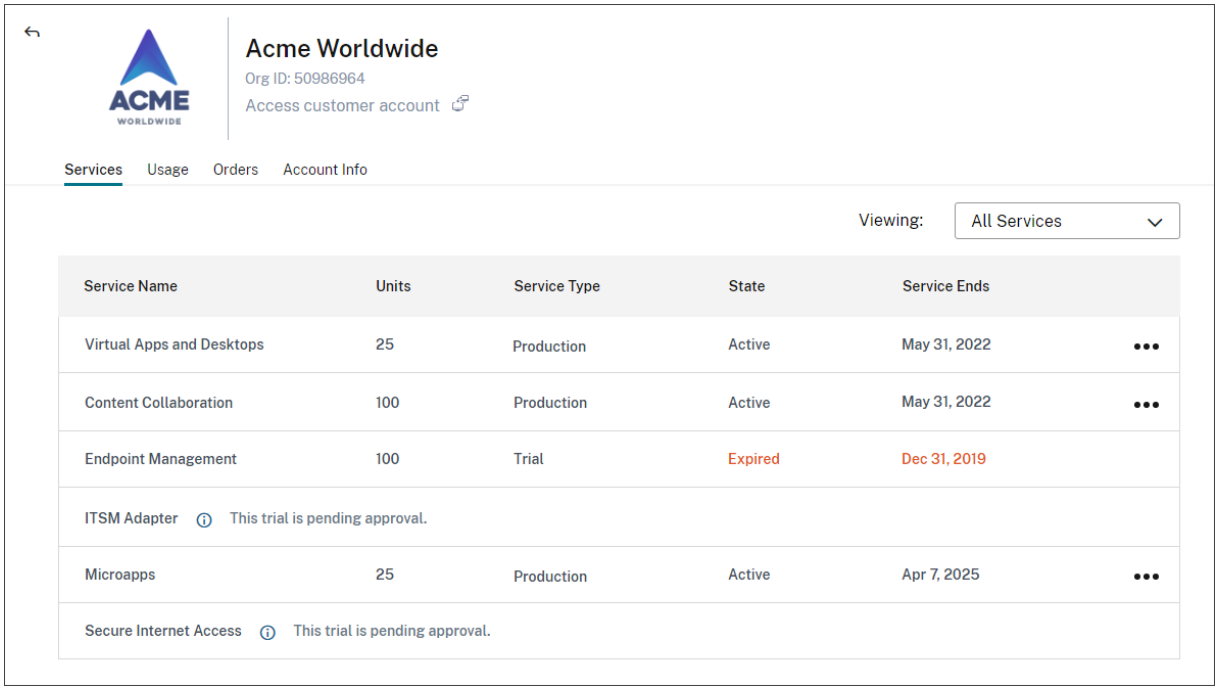
- Le partenaire crée une connexion avec un client
- Un client met fin à sa connexion avec le partenaire

Citrix Cloud envoie des notifications aux clients lorsque le partenaire met fin à sa connexion avec le client.

Les partenaires voient les droits d'utilisation des services

Lorsqu'il est connecté à un client, le partenaire peut consulter les droits d'utilisation de ce client. Ces informations incluent l'état des droits d'utilisation des versions d'évaluation et standard. Les partenaires peuvent également consulter les informations suivantes :

- 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



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.

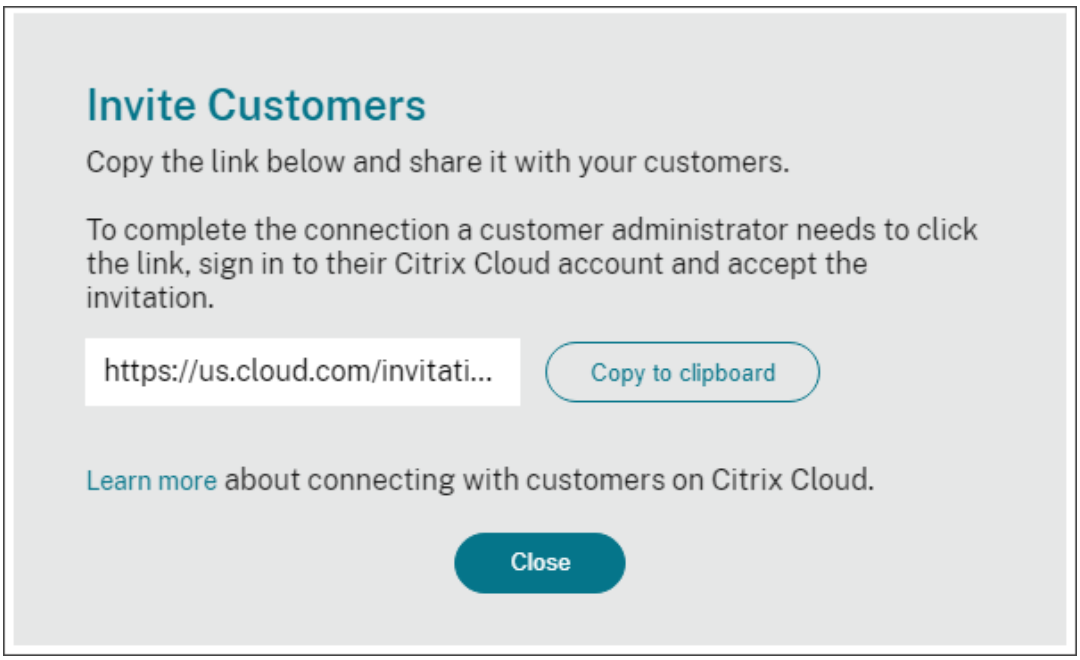
Créer des connexions avec des clients

Les partenaires créent des connexions avec les clients à l'aide d'un lien d'invitation unique. Ce lien est fixe et ne peut être ni modifié ni personnalisé.

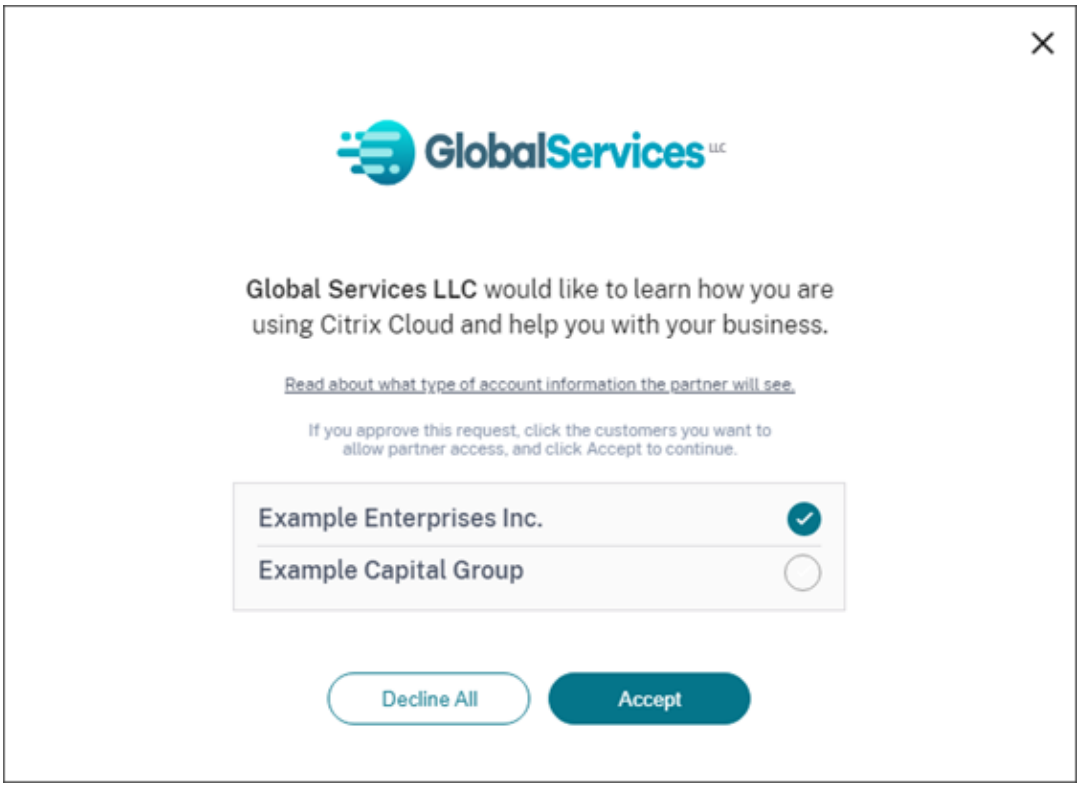
Les partenaires peuvent utiliser leur lien d'invitation un nombre illimité de fois pour créer ou recréer des connexions. Les liens d'invitation n'expirent pas.

Pour créer une connexion :

1. Dans le menu Citrix Cloud, sélectionnez **Mes clients**.
2. Dans le tableau de bord client, sélectionnez **Inviter ou Ajouter**.
3. Pour vous connecter à un client Citrix Cloud existant :
    a) Sélectionnez **Inviter un client Citrix Cloud**, puis sélectionnez **Continuer**.
    b) Copiez le lien d'invitation et envoyez-le au client.



Pour finaliser la connexion, le client clique sur le lien d'invitation, se connecte à Citrix Cloud et accepte l'invitation.



4. Pour créer une connexion avec un nouveau client qui ne possède pas encore de compte Citrix Cloud, procédez comme suit :

    a) Sélectionnez **Ajouter un client**, puis sélectionnez **Continuer**.

b) Entrez les coordonnées professionnelles du client, puis sélectionnez **Terminer**. Citrix Cloud crée un nouveau compte pour le client.

Le client reçoit ensuite une notification indiquant que le partenaire a été ajouté en tant qu'administrateur au nouveau compte. Le client peut définir un mot de passe pour le nouveau compte en utilisant le lien **Mot de passe oublié ?** sur la page de connexion à Citrix Cloud. Après avoir défini son mot de passe, le client peut se connecter à son compte à l'aide de son adresse e-mail professionnelle et terminer le processus d'intégration comme décrit dans la section Ouvrir un compte sur Citrix Cloud.

Supprimer les connexions avec des partenaires ou des clients

Le partenaire ou le client peut mettre fin à une connexion à tout moment.

Supprimer une connexion avec un client

Pour mettre fin à une connexion avec un client, le partenaire effectue les étapes suivantes :

1. Dans le menu Citrix Cloud situé dans le coin supérieur droit de la console, sélectionnez **Mes clients**.
2. Dans le tableau de bord client, localisez le client que vous souhaitez gérer.
3. Cliquez sur le menu représentant des points de suspension pour le client, puis sélectionnez **Supprimer connexion au client**.
4. Lorsque vous êtes invité à confirmer la suppression, sélectionnez **Supprimer**.

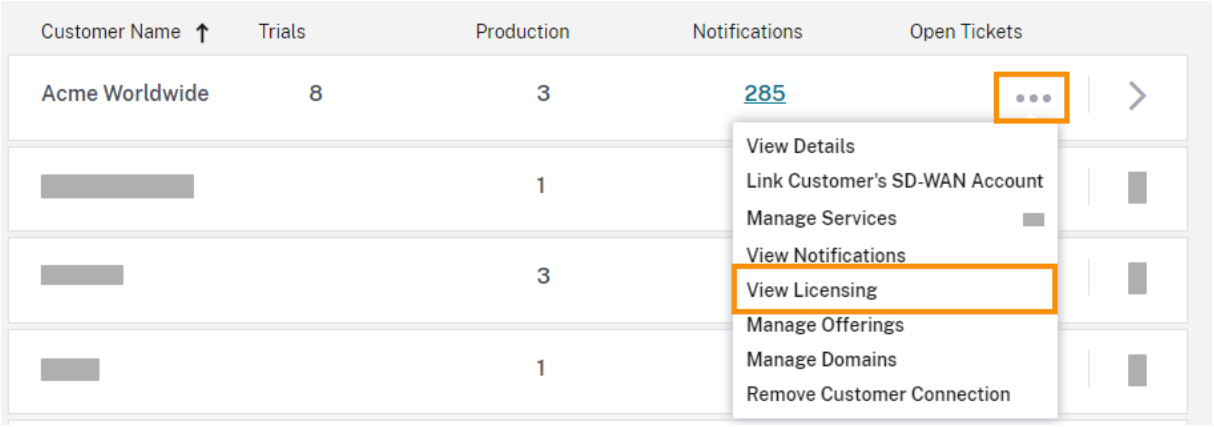
Supprimer une connexion avec un partenaire

Pour mettre fin à une connexion avec un partenaire, le client effectue les étapes suivantes :

1. Dans le menu utilisateur situé dans le coin supérieur gauche, sélectionnez **Paramètres de compte**.
2. Sur la page **Compte d'entreprise**, recherchez la section **Connexions à des partenaires**.
3. Localisez le partenaire que vous souhaitez gérer, puis sélectionnez **Supprimer**.
4. Lorsque vous êtes invité à confirmer la suppression, sélectionnez **Confirmer**.

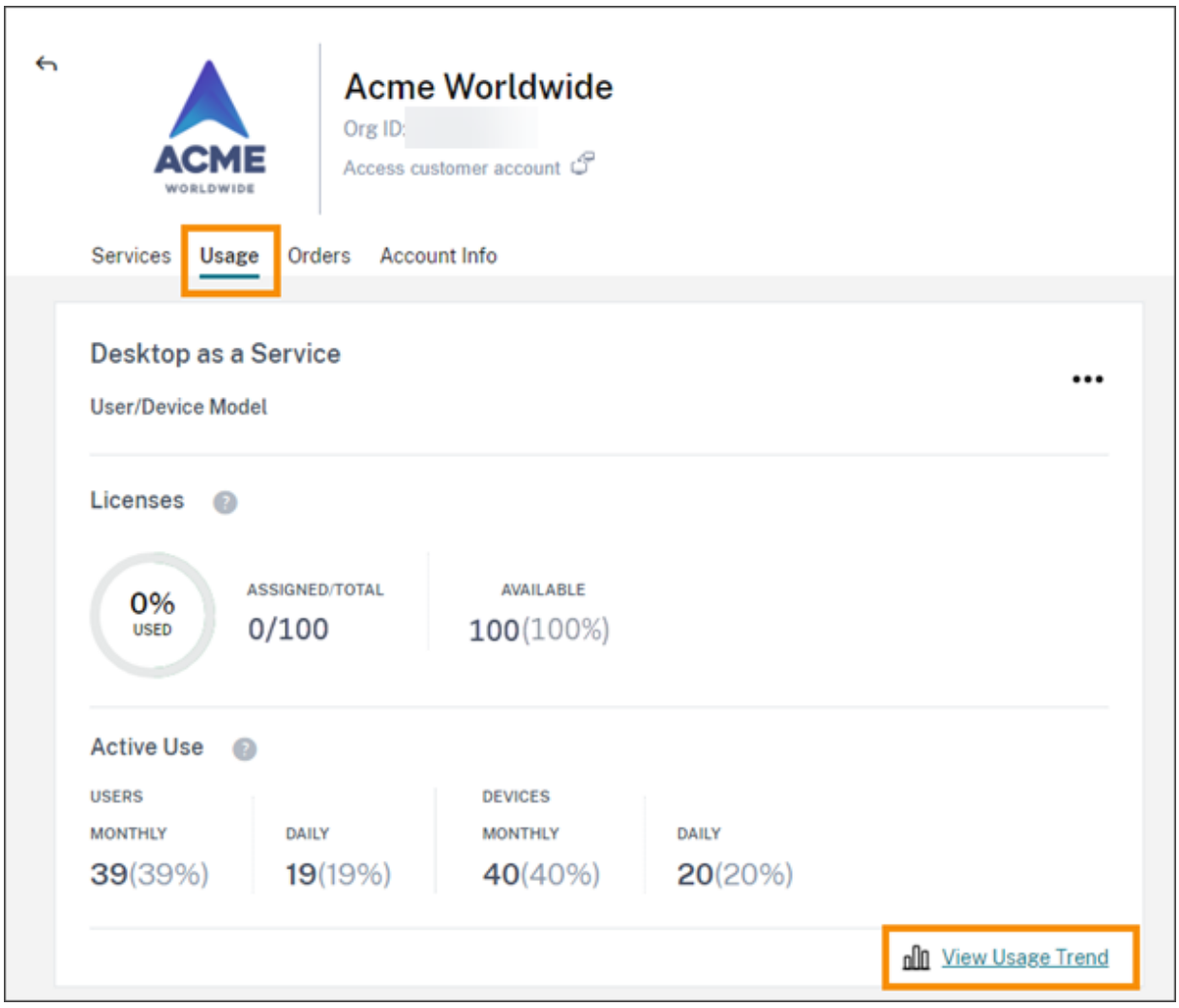
Tendances du système de licences

Les partenaires peuvent consulter les informations de licence d'un client en sélectionnant **Afficher les licences** dans le menu des points de suspension du tableau de bord client.



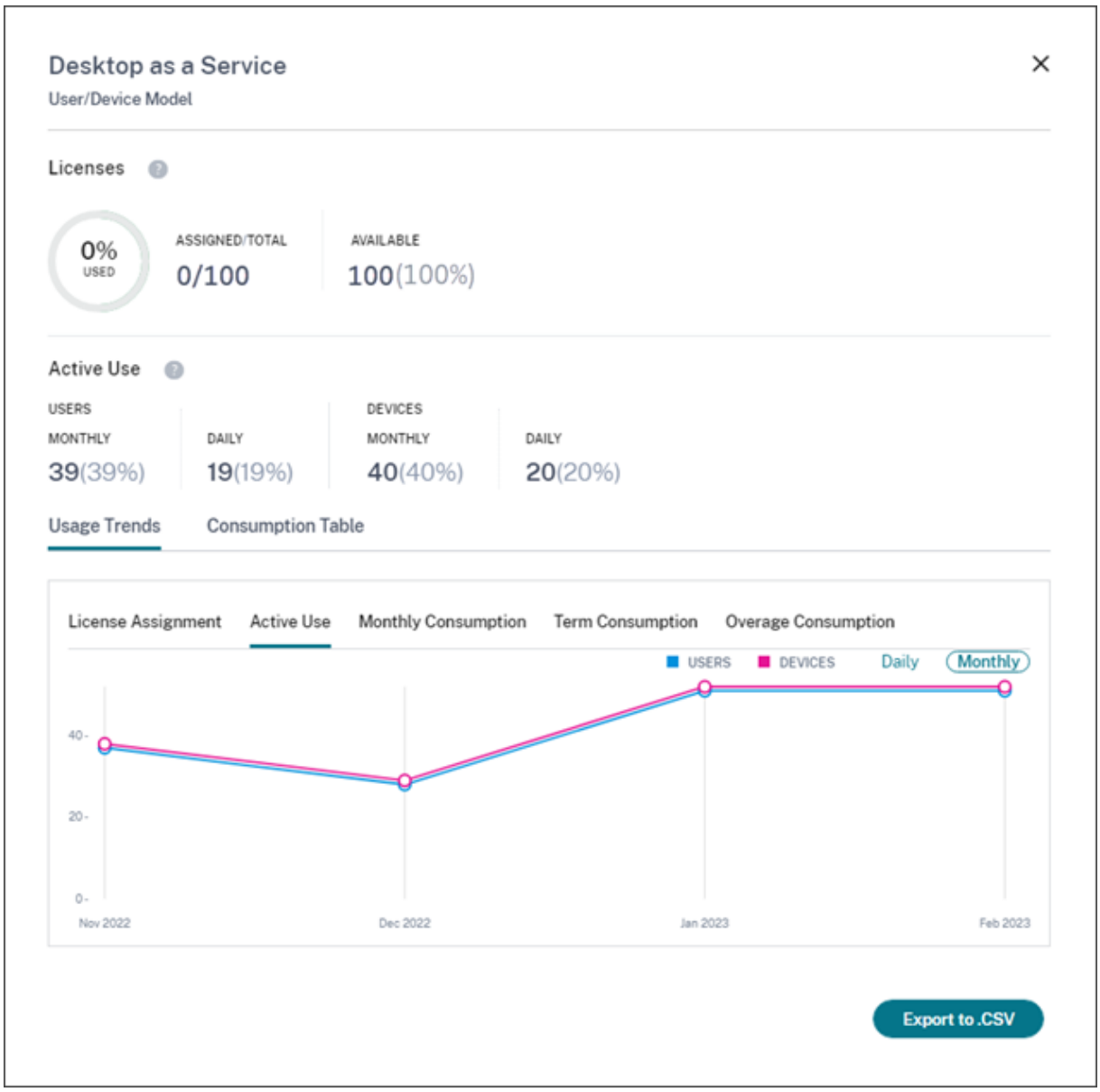
> **Remarque :**
>
> Les partenaires Citrix ne peuvent afficher que la vue de résumé de l'option Système de licences et les tendances historiques de l'utilisation active. Ils ne peuvent pas afficher les utilisateurs individuels qui consomment des licences pour un service donné.

Pour consulter le résumé des licences du client pour chaque service, sélectionnez l'onglet **Utilisation**. Pour plus d'informations sur l'utilisation, sélectionnez **Afficher tendance d'utilisation** pour le droit au service que vous souhaitez consulter.



En fonction du service, les tendances d'utilisation incluent les informations suivantes :

- Le ratio de licences attribuées par rapport au nombre total de licences achetées
- Utilisateurs actifs mensuels et quotidiens
- Répartition visuelle des attributions de licences, de l'utilisation active, de la consommation par droit et de l'excédent.



Si nécessaire, les partenaires peuvent exporter ces informations sous forme de fichier .csv.

Utilisation de la bande passante

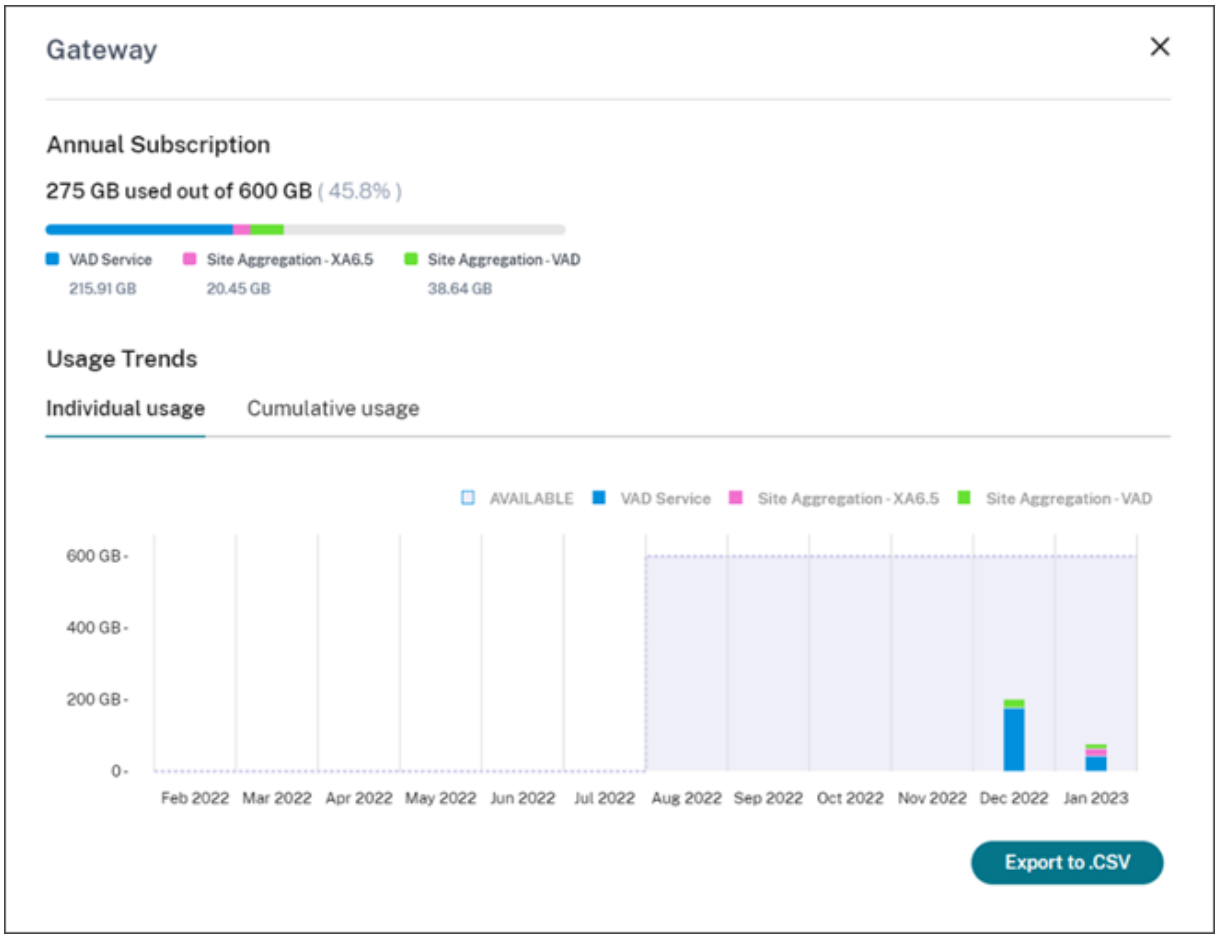
Pour Citrix Gateway Service, le résumé des licences comprend les informations suivantes :

- Utilisation totale de la bande passante sur l'ensemble des droits du client.
- Utilisation totale de la bande passante répartie selon les droits mensuels, annuels et à durée déterminée du client.
- Excédent total pour le mois en cours. Pour plus d'informations sur la façon dont l'excédent est calculé, consultez Dépassement.

Sélectionnez **Afficher tendance d'utilisation** à droite de la page pour consulter le résumé de l'utilisation. Sélectionnez **Afficher tableau des excédents** pour voir les excédents des 12 derniers mois.

En fonction des droits, les tendances d'utilisation incluent les informations suivantes :

- Quantité de bande passante consommée par les déploiements de Citrix DaaS (**VAD Service**) et de Virtual Apps and Desktops locaux avec agrégation de sites.
- Répartition visuelle de l'utilisation de la bande passante pour chaque mois au cours duquel elle a été utilisée. (Droits mensuels)
- Répartition visuelle de l'**utilisation individuelle** de la bande passante au cours de chaque mois de la période de facturation. (Droits annuels et trimestriels)
- Répartition visuelle de l'**utilisation cumulée** de la bande passante cumulée chaque mois au cours de la période de facturation. (Droits annuels et trimestriels)



Si nécessaire, les partenaires peuvent exporter ces informations sous forme de fichier .csv.

Utilisation et système de licences client pour les partenaires Citrix Service Provider

La fonctionnalité Système de licences de Citrix Cloud permet aux clients des partenaires Citrix Service Provider (CSP) de surveiller leurs licences et leur utilisation pour les produits Citrix DaaS (anciennement Citrix Virtual Apps and Desktops) pris en charge. Les partenaires Citrix Service Provider peuvent également se connecter au compte Citrix Cloud de leur client pour afficher et exporter ces informations. Pour plus d'informations, consultez les articles suivants :

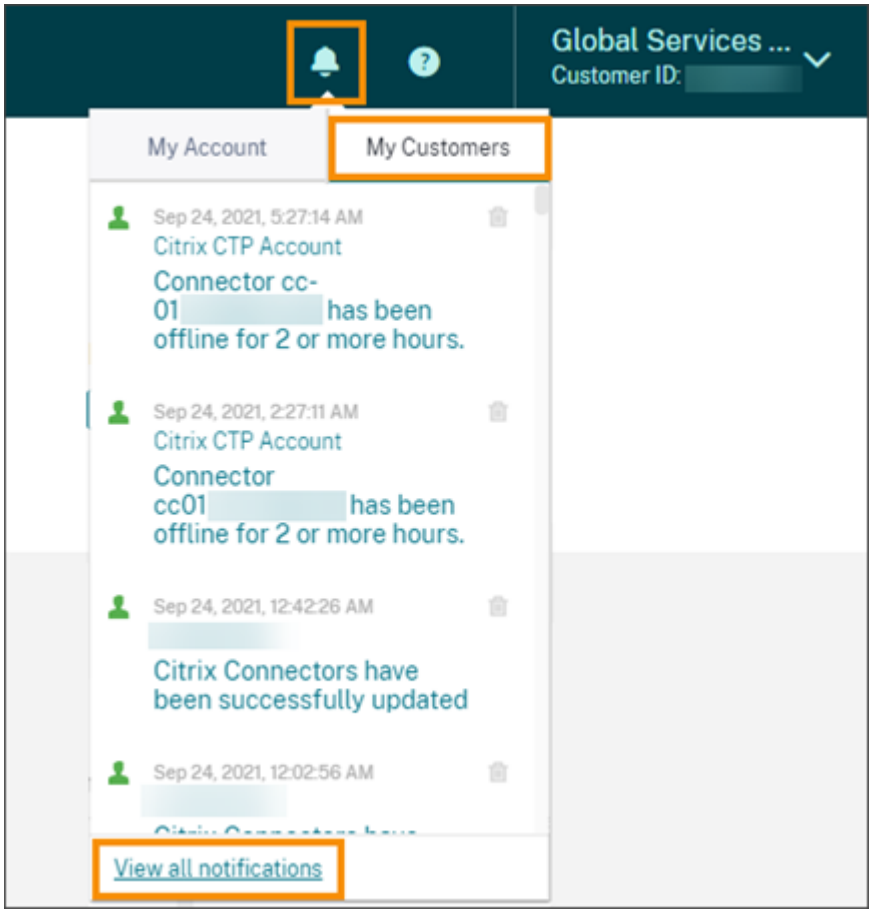
- Surveillance des licences client et de l'utilisation pour Citrix DaaS
- Surveillance des licences client et de l'utilisation pour Citrix DaaS Standard pour Azure

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

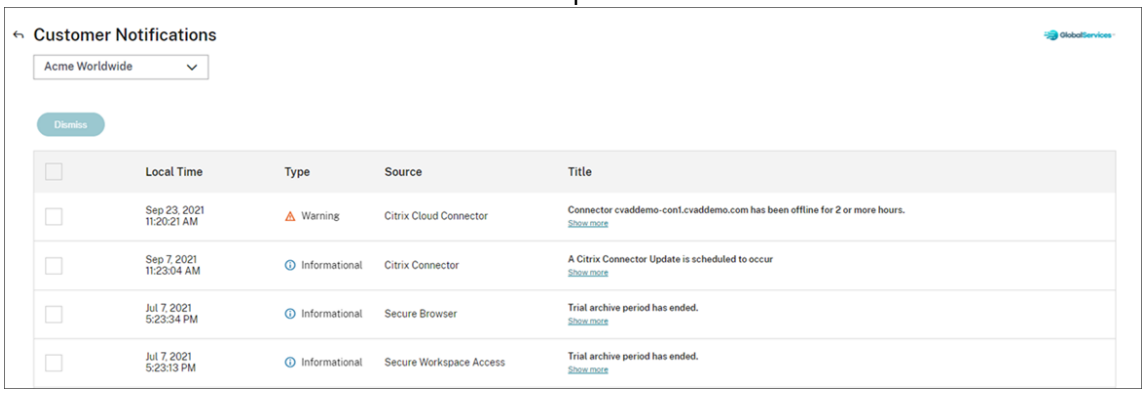
Les partenaires peuvent consulter les notifications de leurs clients connectés. Les partenaires peuvent également filtrer les notifications spécifiques au client et prendre des mesures comme ignorer une notification. Les notifications ignorées ne s'affichent pas pour le partenaire. Toutefois, les clients peuvent toujours voir la notification dans leur compte une fois qu'ils se sont connectés à Citrix Cloud.

Pour afficher les notifications des clients :

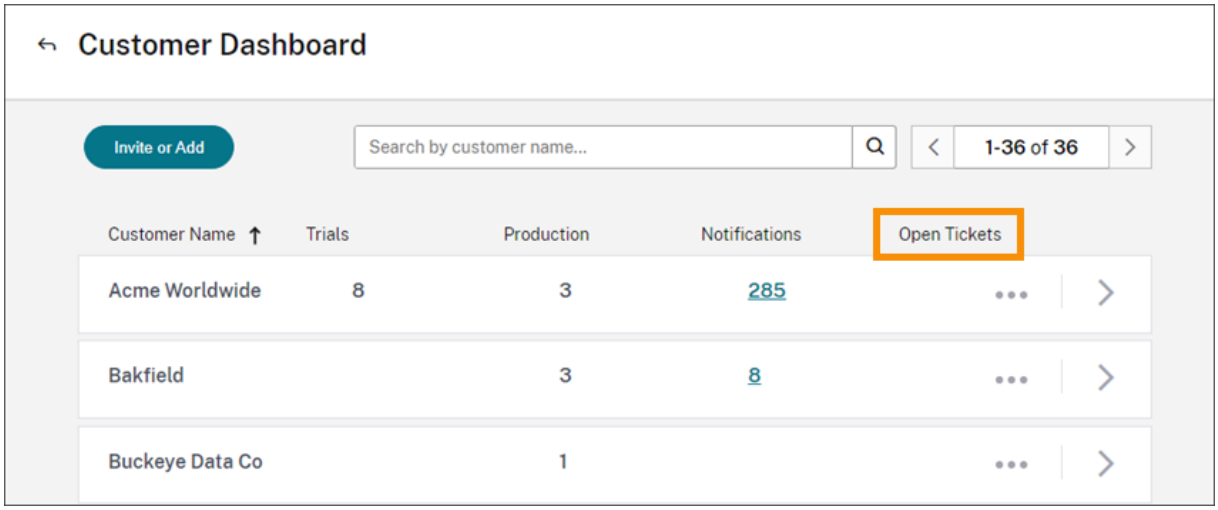
1. Cliquez sur l'icône en forme de cloche située en haut de la console de gestion, sélectionnez **Mes clients**, puis **Afficher toutes les notifications**.



2. Sélectionnez un client dans le menu déroulant pour afficher les notifications de ce client.



Les partenaires peuvent consulter le nombre de tickets de support de leurs clients via le tableau de bord client.



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 Citrix DaaS.

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 fournir des applications et des bureaux, consultez Citrix DaaS pour Citrix Service Providers.

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, consultez 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.

Service de cloud

July 2, 2024

Cet article répertorie les services de cloud proposés via Citrix Cloud et des liens vers la documentation produit de chaque service. Pour obtenir des descriptions de ces services et les offres dans lesquelles ils sont inclus, consultez Service Descriptions for Citrix Services.

Services Citrix

Analytics

- Analytics for Security
- Analytics for Performance
- Analytics - Utilisation

Citrix DaaS

Citrix DaaS Standard pour Azure

Endpoint Management

Gateway

Adaptateur ITSM pour ServiceNow

Remote Browser Isolation

Secure Private Access

Service d'enregistrement de session

Virtual Apps Essentials

Virtual Desktops Essentials

Workspace Environment Management

Services NetScaler

Console

Sécurité et mise à disposition d'applications

SD-WAN Orchestrator

Secure Internet Access

Web App Firewall