Citrix Analytics

Machine translated content

Disclaimer

La version officielle de ce document est en anglais. Certains contenus de la documentation Cloud Software Group ont été traduits de façon automatique à des fins pratiques uniquement. Cloud Software Group n'exerce aucun contrôle sur le contenu traduit de façon automatique, qui peut contenir des erreurs, des imprécisions ou un langage inapproprié. Aucune garantie, explicite ou implicite, n'est fournie quant à l'exactitude, la fiabilité, la pertinence ou la justesse de toute traduction effectuée depuis l'anglais d'origine vers une autre langue, ou quant à la conformité de votre produit ou service Cloud Software Group à tout contenu traduit de façon automatique, et toute garantie fournie en vertu du contrat de licence de l'utilisateur final ou des conditions d'utilisation des services applicables, ou de tout autre accord avec Cloud Software Group, quant à la conformité du produit ou service à toute documentation ne s'applique pas dans la mesure où cette documentation a été traduite de façon automatique. Cloud Software Group ne pourra être tenu responsable de tout dommage ou problème dû à l'utilisation de contenu traduit de façon automatique.

Contents

Nouveautés

September 21, 2023

Citrix a pour objectif de fournir de nouvelles fonctionnalités et mises à jour de produits aux clients Citrix Analytics lorsqu'elles sont disponibles. Les nouvelles versions étant plus avantageuses, il est important que vous en profitiez le plus rapidement possible.

Pour vous, en tant que client, ce processus est transparent. Les mises à jour initiales sont uniquement appliquées aux sites Citrix internes pour être ensuite graduellement appliquées aux environnements des clients. La mise à jour progressive par vagues permet d'assurer la qualité des produits et de maximiser la disponibilité.

Citrix Analytics propose les produits ou offres suivants. Consultez les articles Nouveautés spécifiques à chaque offre pour en savoir plus sur les nouvelles fonctionnalités et les mises à jour des produits.

- Citrix Analytics for Security
- Citrix Analytics for Performance

Ces notes de mise à jour mettent en évidence les nouvelles fonctionnalités et mises à jour de produits spécifiques à la plateforme Citrix Analytics.

21 septembre 2023

Simplifiez l'intégration de StoreFront à l'aide du script PowerShell

Un nouveau script **PowerShell** a été introduit pour automatiser le processus de vérification des prérequis, d'installation et de configuration de StoreFront. Le client doit exécuter ce script en mode administrateur sur StoreFront pour intégrer, déconnecter, effectuer des autovérifications, résoudre les problèmes et vérifier si l'intégration à l'interface graphique du service Citrix Analytics est réussie.

Pour plus d'informations, consultez Se connecter à un déploiement StoreFront.

28 août 2023

Service de micro-apps (fin de vie)

Le service Citrix Microapps a atteint sa fin de vie et n'est plus disponible pour les utilisateurs.

01 août 2023

Citrix Analytics - Utilisation (fin de vie)

Citrix Usage Analytics a atteint sa fin de vie et n'est plus disponible pour les utilisateurs.

23 février 2023

Problèmes résolus

Avant la sortie de Citrix Virtual Apps and Desktops 2112, Citrix Analytics ne parvenait pas à découvrir les sites locaux connectés à partir de Citrix Director et récemment enregistrés sur Citrix Cloud. Par conséquent, vous ne voyez pas ces sites connectés sur votre carte de site **Virtual Apps and Desktops - Surveillance** . Ce problème est désormais résolu. [CAS-63132]

28 septembre 2022

Webhooks pour les notifications d'alerte

Vous pouvez utiliser des webhooks pour envoyer des notifications d'alerte Citrix Analytics à toutes les applications tierces dont les URL de webhook entrantes sont configurées. Les webhooks sont des callbacks HTTP qui permettent la messagerie en temps réel entre les applications du fournisseur de services et les applications grand public. Comme les notifications d'alerte sont envoyées en temps réel, vous êtes averti lorsque les événements se produisent. Pour plus d'informations, voir Webhooks pour les notifications d'alerte.

September 08, 2022

Augmentation de la limite d'exportation dans l'exportation CSV

La limite du nombre de lignes que vous pouvez exporter **à l'aide de la fonctionnalité Exporter au format CSV** est désormais augmentée de 10 000 lignes à 100 000 lignes. Pour plus d'informations, voir Exporter les événements vers un fichier CSV.

18 août 2022

Problème résolu

- Dans la recherche en libre-service pour Apps and Desktops, la valeur de version de l'application Workspace a été renseignée en tant que **NA** (non disponible) dans le fichier CSV téléchargé, alors

qu'elle était disponible dans la vue de page. Ce problème est désormais résolu. [CAS-70361]

10 août 2022

Intégration de StoreFront sans agrégation de sites

La dépendance d'agrégation de sites pour StoreFront a été supprimée de la carte de site **Apps and Desktops- Workspace app** . Vous pouvez voir l'option **Connect Storefront Deployment** sur votre application Workspace, même si aucun site n'a été ajouté à l'agrégation de sites. Pour plus de détails, consultez la source de données Citrix Virtual Apps and Desktops.

5 avril 2022

Secure Workspace Access est renommé Secure Private Access

Dans les tableaux de bord et les rapports Analytics, toutes les étiquettes **Secure Workspace Access** de travail sont désormais mises à jour en tant qu'**accès privé sécurisé** pour s'aligner sur le nom du produit renommé.

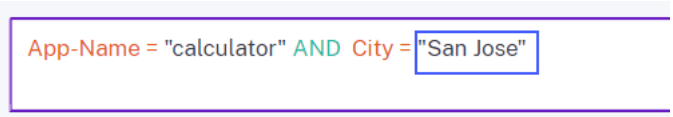
Par exemple, sur la page **Sources de données** et la page de **recherche en libre-service**, les étiquettes **Secure Workspace Access** de travail sont renommées **Accès privé sécurisé**.

21 mars 2022

Problème résolu

- Dans la page **Rechercher**, les suggestions automatiques de dimensions et d'opérateurs ne fonctionnent pas si la condition précédente de votre requête de recherche contient une valeur de dimension séparée par un espace.

  Par exemple, dans la requête suivante, les suggestions automatiques cessent de fonctionner une fois que vous avez sélectionné la ville en tant que `San Jose`. Ce problème est désormais résolu. [CAS-64126]

10 février 2022

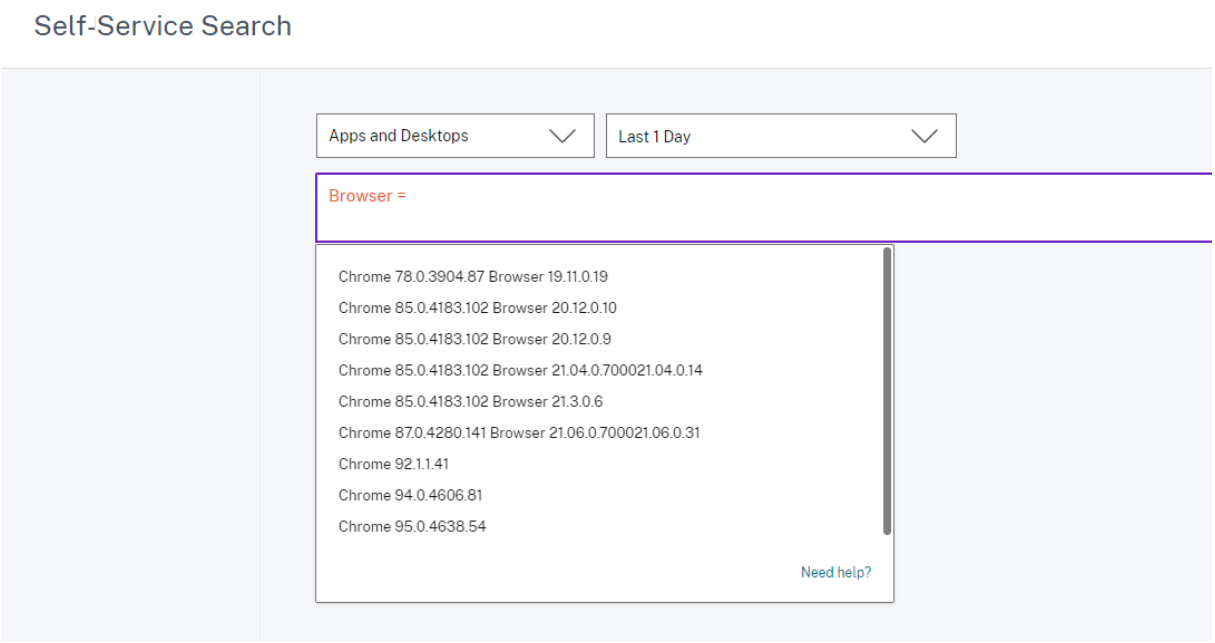
Nouveautés

Valeurs suggérées automatiquement pour les dimensions dans la zone de recherche en libre-service Dans la page de recherche en libre-service, lorsque vous sélectionnez une dimension et un opérateur valide dans la zone de recherche, les valeurs de la dimension s'affichent automatiquement. Sélectionnez une valeur dans la liste des suggestions automatiques ou saisissez manuellement une valeur en fonction de vos cas d'utilisation. Lorsque vous saisissez une valeur, les valeurs correspondantes disponibles dans les enregistrements sont suggérées automatiquement.

La liste des valeurs suggérées pour une dimension est soit prédéfinie (valeurs connues) dans la base de données, soit basée sur des événements historiques.

Par exemple, lorsque vous sélectionnez la dimension `Browser` et l'opérateur d'affectation, les valeurs connues sont suggérées automatiquement. Vous pouvez sélectionner une valeur en fonction de vos besoins.

Pour plus d'informations, consultez la rubrique Recherche en libre-service.



20 décembre 2021

Nouveautés

Access Control est renommé Secure Workspace Access Dans les tableaux de bord et les rapports Analytics, toutes les étiquettes de **contrôle d'accès** sont désormais mises à jour en tant qu'**Secure**

Workspace Access de travail pour s'aligner sur le nom du produit renommé.

Par exemple, sur la page **Sources de données** et la page de **recherche en libre-service**, les étiquettes de **contrôle d'accès** sont renommées **Secure Workspace Access**.

06 décembre 2021

Nouveautés

Citrix Analytics est désormais pris en charge dans la région Sud de l'Asie-Pacifique

- Vous pouvez désormais choisir Asie-Pacifique Sud comme région d'origine lors de l'intégration de votre organisation à Citrix Cloud et de l'utilisation du service Citrix Analytics. Pour plus d'informations, voir Considérations géographiques.
- Citrix Analytics stocke désormais les événements utilisateur et les métadonnées de votre organisation dans la région Asie-Pacifique Sud lorsque vous la choisissez comme région d'origine. Pour plus d'informations, voir Gouvernance des données.
- Pour plus d'informations sur la configuration réseau requise pour la région Sud de l'Asie-Pacifique, voir Vue d'ensemble de la sécurité technique.
- Pour plus d'informations sur les sources de données prises en charge dans la région Sud de l'Asie-Pacifique, voir Sources de données.

19 août 2021

Nouveautés

Prise en charge de l'opérateur IS EMPTY Dans la recherche en libre-service, vous pouvez désormais utiliser l'opérateur **IS EMPTY** dans votre condition pour rechercher une dimension nulle ou vide.

> **Remarque**
>
> L'opérateur fonctionne uniquement pour les dimensions de type chaîne telles que App-Name, Browser et Country.

Pour plus d'informations, consultez la rubrique Recherche en libre-service.

14 juillet 2021

Nouveautés

Prise en charge de l'opérateur IS NOT EMPTY Dans la recherche en libre-service, vous pouvez désormais utiliser l'opérateur **IS NOT EMPTY** dans votre requête pour vérifier si la dimension n'est pas vide (pas vide).

> **Remarque**
>
> L'opérateur fonctionne uniquement pour les dimensions de type chaîne telles que App-Name, Browser et Country.

Pour plus d'informations, consultez la rubrique Recherche en libre-service.

07 juin 2021

Fonctionnalité obsolète

Environnement de démonstration Citrix Analytics supprimé Les liens **Essayer la démonstration** pour Security Analytics et Performance Analytics sont désormais supprimés de la page de présentation Analytics. Vous ne pouvez plus accéder à l'environnement de démonstration de chaque offre. Pour plus d'informations sur la façon d'accéder aux offres Citrix Analytics, consultez Mise en route.

18 mai 2021

Nouveautés

Prise en charge de l'opérateur* avec ! = opérateur Dans votre requête de recherche, vous pouvez désormais utiliser l'opérateur* avec l'opérateur ! = pour trouver les événements utilisateur. Par exemple :

- Pour trouver tous les événements utilisateur qui ne commencent pas par le nom « John », utilisez la requête : Nom d'utilisateur ! = John*
- Pour trouver tous les événements utilisateur qui ne se terminent pas par le nom « Smith », utilisez la requête : Nom d'utilisateur ! = *Smith

> **Remarque**
>
> Les résultats de la recherche respectent la casse.

Pour plus d'informations, consultez la rubrique Recherche en libre-service.

Barre de recherche améliorée dans la page de recherche en libre-service

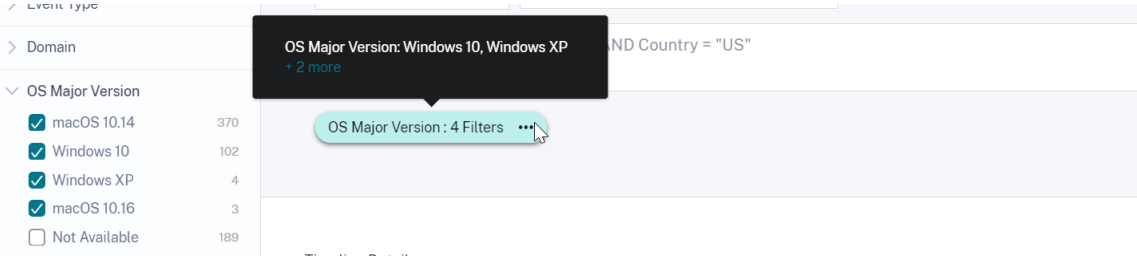
- La barre de recherche offre désormais une meilleure vue de vos requêtes lorsqu'elle s'étend sur plusieurs lignes. Utilisez la barre de défilement pour faire défiler vos requêtes multilignes. Auparavant, il était difficile d'afficher les requêtes multilignes.

- Le problème de saut de curseur observé dans le navigateur Safari est désormais résolu.

Pour plus d'informations, consultez la rubrique Recherche en libre-service.

Vue des puces repensée dans la recherche en libre-service

- Les puces redessinées vous offrent désormais une meilleure vue des multiples facettes que vous avez sélectionnées.



- Cliquez sur une puce pour sélectionner ou désélectionner les facettes en fonction de vos besoins.

Problème résolu

- Sur Citrix Director, le lien **Accéder à Analytics** ne fonctionne pas. Ce problème est observé pour un utilisateur qui a intégré son organisation dans la région de l'Union européenne de Citrix Cloud. [CAS-50224]

31 mars 2021

Prise en charge des opérateurs IN et NOT IN pour les requêtes de recherche d'applications et de bureaux

Avec les dimensions Apps and Desktops- `Device ID`, `Domain`, `Event-Type`, et `User-Name`, vous pouvez désormais utiliser les opérateurs suivants :

- **IN** : Attribuez plusieurs valeurs à une dimension pour obtenir les événements liés à une ou plusieurs valeurs.
- **NOT IN** : affectez plusieurs valeurs à une dimension et recherchez les événements qui ne contiennent pas les valeurs spécifiées.

> **Remarque**
>
> Ces opérateurs ne s'appliquent qu'aux valeurs de chaîne.

Pour plus d'informations sur les opérateurs, consultez la rubrique Recherche en libre-service.

18 mars 2021

Nouveautés

Prise en charge du programme NOT LIKE (! ~) opérateur Pour la requête de recherche en libre-service, vous pouvez maintenant utiliser le paramètre NOT LIKE (! ~). L'opérateur recherche les événements utilisateur correspondant au modèle de correspondance que vous avez spécifié. Elle renvoie les événements qui ne contiennent pas le modèle spécifié dans la chaîne d'événements.

Par exemple, la requête `User-Name !~ "John"` affiche des événements pour les utilisateurs, à l'exception de John, John Smith ou de tout autre utilisateur qui contient le nom correspondant « John ».

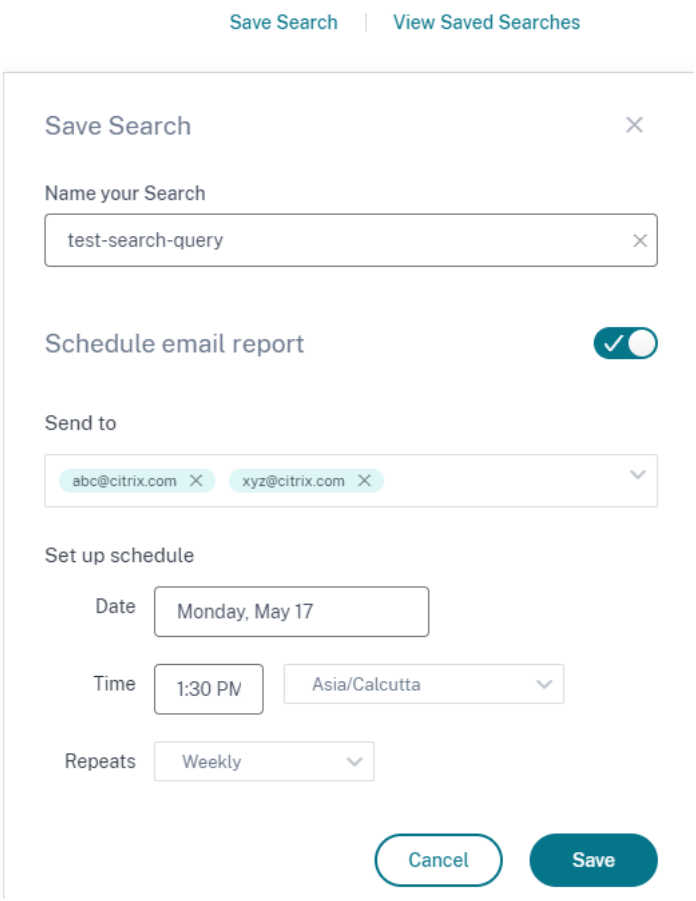
Pour plus d'informations, consultez la rubrique Recherche en libre-service.

23 février 2021

Nouveautés

Planifier la livraison d'un e-mail pour une requête de recherche Sur la page de recherche en libre-service, lors de l'enregistrement d'une requête de recherche, vous pouvez également planifier la diffusion d'un e-mail afin d'envoyer une copie de la requête de recherche enregistrée et du rapport de synthèse visuel correspondant à vous-même et aux autres utilisateurs. Définissez la date, l'heure et la fréquence (quotidienne, hebdomadaire ou mensuelle) pour commencer à envoyer un e-mail. Vous pouvez également planifier l'envoi par e-mail des requêtes de recherche que vous avez précédemment enregistrées.

Pour plus d'informations, consultez la rubrique Recherche en libre-service.

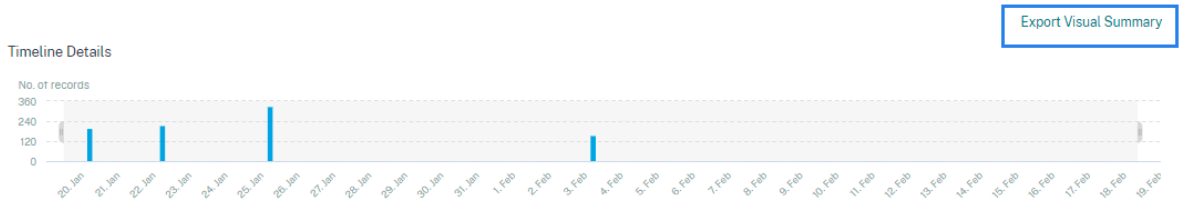


Télécharger le résumé visuel d'une requête de recherche Sur la page en libre-service, vous pouvez désormais télécharger le rapport récapitulatif visuel de votre requête de recherche pour une période sélectionnée et en partager une copie avec d'autres utilisateurs. Cliquez sur **Exporter le résumé visuel** pour télécharger le rapport de synthèse visuel au format PDF.

Le rapport contient les informations suivantes :

- La requête de recherche que vous avez spécifiée pour les événements.
- Les facettes (filtres) que vous avez appliquées aux événements.
- Le résumé visuel, tel que les graphiques chronologiques, les graphiques à barres ou les graphiques des événements de recherche.

Pour plus d'informations, consultez la rubrique Recherche en libre-service.

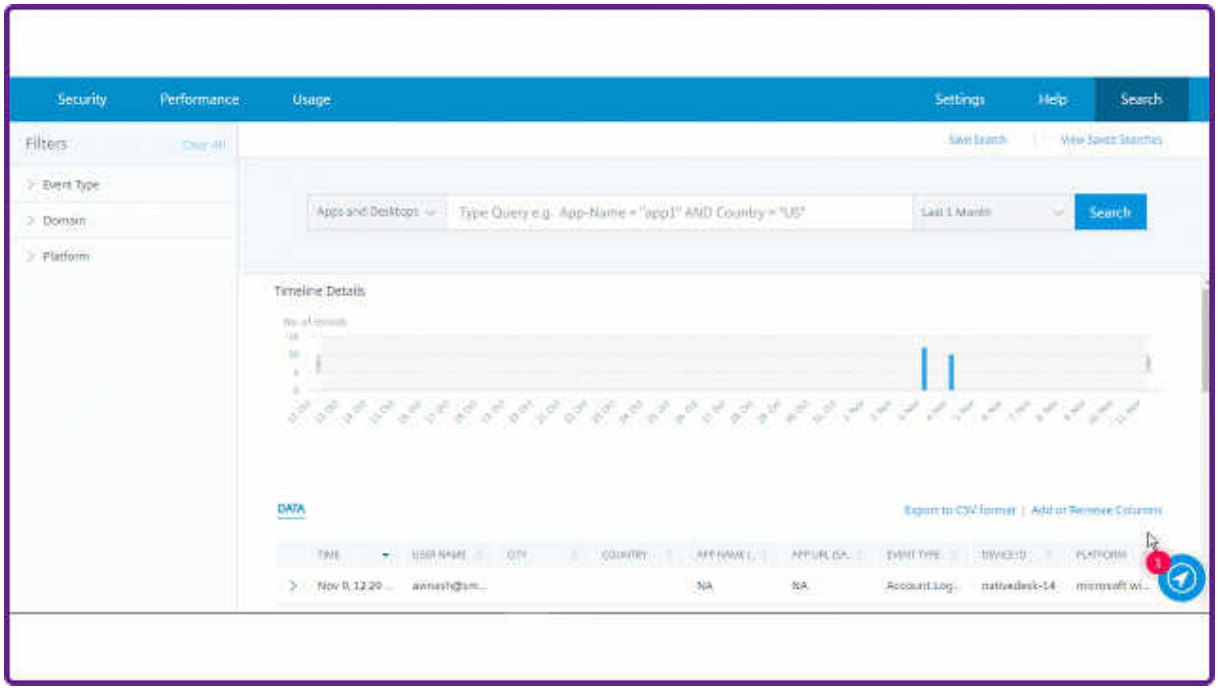


November 12, 2020

Nouvelle fonctionnalité

Enregistrer une requête en libre-service Après avoir créé une requête en libre-service, vous pouvez l'enregistrer pour une utilisation ultérieure. Les options suivantes sont enregistrées avec la requête :

- Filtres de recherche appliqués
- Source de données et durée sélectionnées



Pour plus d'informations, consultez la rubrique Comment enregistrer la recherche en libre-service.

20 octobre 2020

Nouvelles fonctionnalités

Prise en charge de NetScaler Gateway dans la région de l'Union européenne Citrix Analytics prend désormais en charge NetScaler Gateway dans la région de l'UE. Pour plus d'informations, consultez la section Source de données NetScaler Gateway.

09 juillet 2020

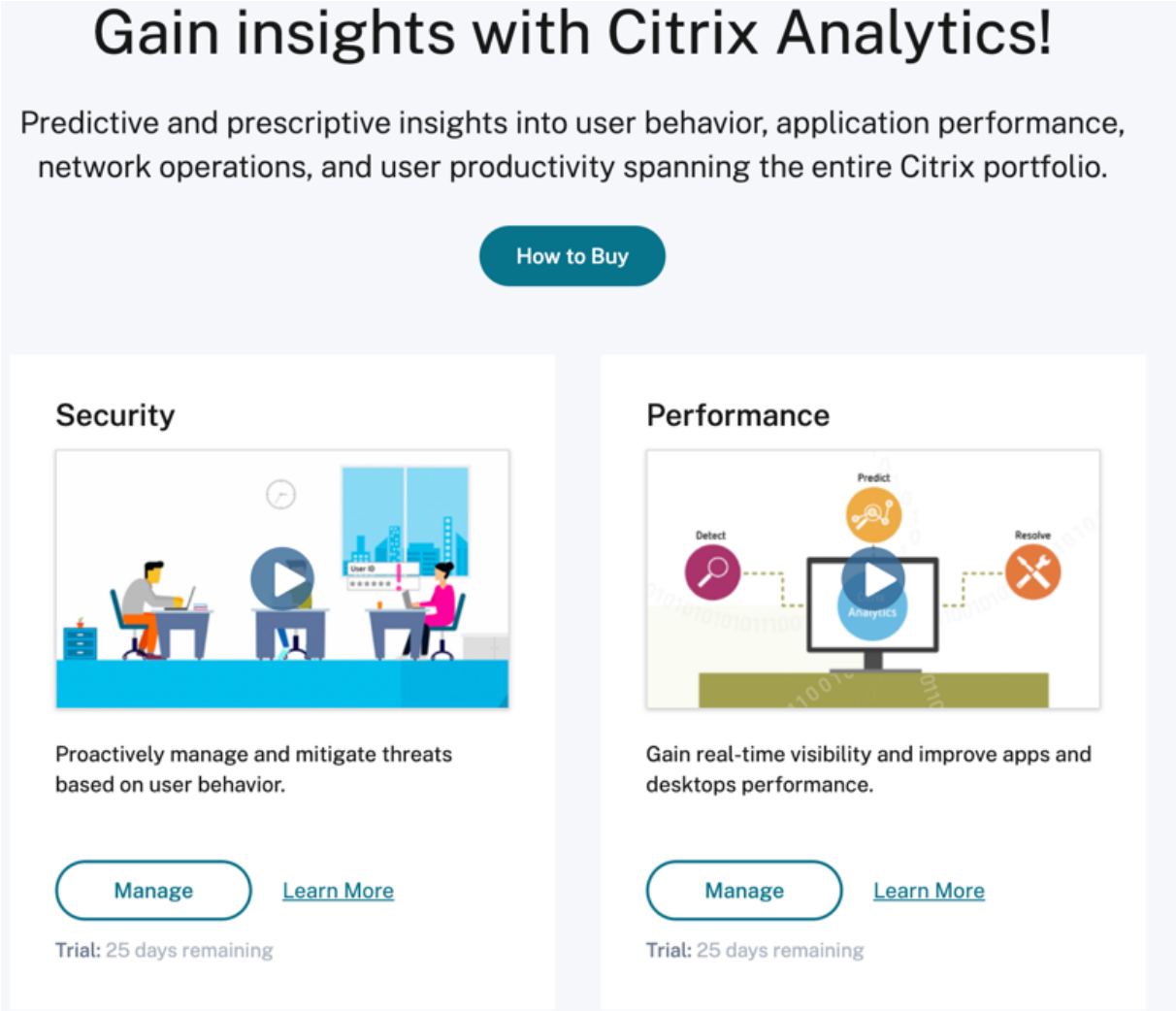
Prise en charge dépréciée

Microsoft Internet Explorer 11 est désormais supprimé de la liste des navigateurs pris en charge. Cette dépréciation est due à la vulnérabilité de sécurité observée dans le navigateur. Pour obtenir la liste des navigateurs pris en charge, consultez la section Configuration système requise.

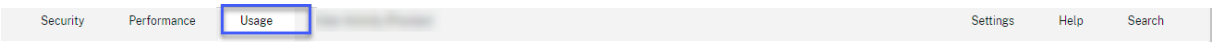
02 juin 2020

Nouvelles fonctionnalités

La page de présentation et la barre supérieure ont été repensées dans Analytics La page de présentation d'Analytics affiche la vignette **Utilisation** qui remplace la vignette **Opérations** qui existait précédemment. La vignette **Productivité** est également supprimée de cette page. Pour afficher la page de présentation, sélectionnez **Aide** > **Vue d'ensemble**.



De même, dans la barre supérieure, l'onglet **Usage** remplace l'onglet **Opérations** .



20 février 2020

Nouvelles fonctionnalités

Offres d'abonnement Citrix Analytics Offrant des options d'achat flexibles aux utilisateurs, Citrix propose désormais trois produits Citrix Analytics individuels basés sur un abonnement. Citrix Analytics fournit des informations uniques sur la sécurité ou les performances (ou les deux) en fonction de l'offre à laquelle vous êtes abonné.

Vous pouvez acheter les offres d'abonnement Citrix Analytics suivantes :

- Citrix Analytics for Security

- Citrix Analytics for Performance
- Citrix Analytics pour la sécurité et les performances (offre groupée)

Mises à jour des journaux de gouvernance Ajout de nouveaux journaux pour les sources de données suivantes :

- Fournisseur d'identité Citrix
- Citrix Gateway
- Secure Browser
- Microsoft Graph Security
- Microsoft Active Directory

Pour plus d'informations, voir Gouvernance des données.

Problèmes résolus

- La recherche en libre-service ne fonctionne pas correctement sur Internet Explorer 11. Par conséquent, vous ne pouvez pas saisir votre requête de recherche et effectuer une opération de recherche. [CAS-18657]

09 janvier 2020

Problèmes résolus

- La fonctionnalité de présentation de Citrix Analytics ne fonctionne pas pour les utilisateurs de la région d'origine de l'Union européenne. [CAS-26297]

18 décembre 2019

Problèmes résolus

La vignette **Analytics** de la page **Citrix Cloud** affichait le bouton **Afficher le service** . Ce bouton est désormais remplacé par **Gérer** pour une meilleure expérience utilisateur. [CAS-27922]

12 décembre 2019

Nouvelles fonctionnalités

Prise en charge des événements de service de micro-apps en Asie-Pacifique Sud La plateforme Citrix Analytics traite désormais les notifications du service de micro-apps dans la région

Asie-Pacifique Sud. Toutefois, les enregistrements qui mesurent les performances, la stabilité, l'utilisation, la sécurité et le support sont agrégés et stockés aux États-Unis. Pour plus d'informations, voir Gouvernance des données.

> **Remarque :**
>
> Le service de micro-apps est proposé dans le cadre de Citrix Workspace. Pour plus d'informations, consultez la documentation des micro-apps .

04 décembre 2019

Problèmes résolus

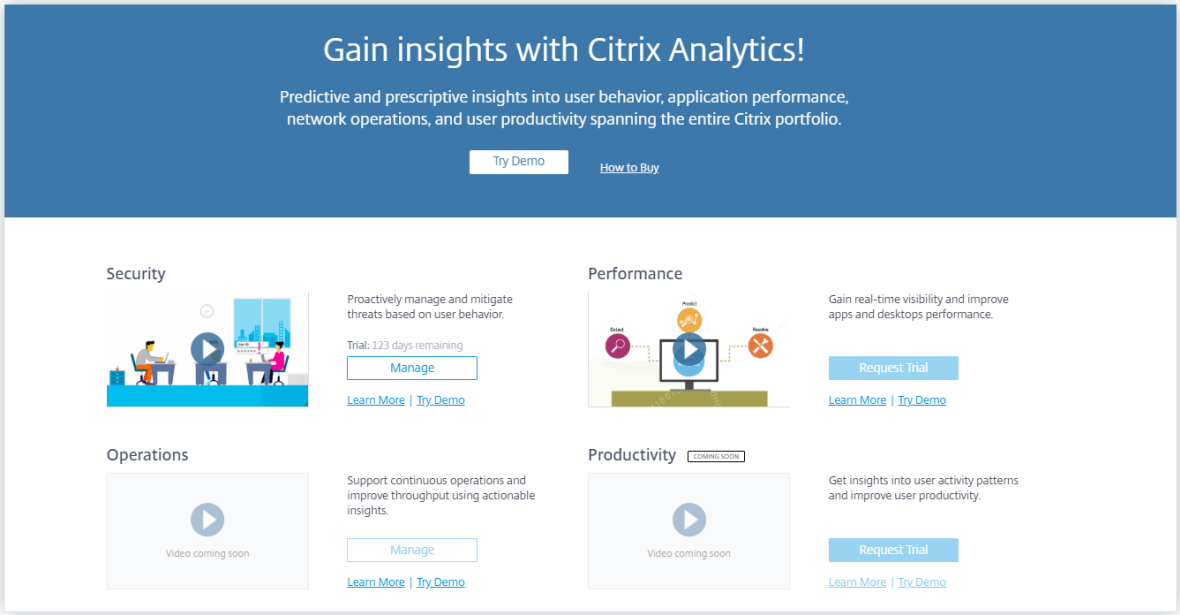
Certains utilisateurs de la région Asie-Pacifique-Sud ne peuvent pas se connecter à Citrix Analytics bien qu'ils aient intégré Citrix Cloud en sélectionnant **États-Unis** comme région d'origine. [CAS-27368]

22 novembre 2019

Nouvelles fonctionnalités

Page de présentation repensée pour Analytics La page de présentation d'Analytics a été repensée pour permettre l'accès à toutes les offres Analytics de cette page. Vous pouvez demander un essai, essayer la démo ou gérer votre offre Analytics. Actuellement, seuls Security Analytics et Operations Analytics sont globalement disponibles et, par conséquent, actifs sur cette page.

Pour afficher la page de présentation, sélectionnez **Aide** > **Vue d'ensemble**.



21 octobre 2019

Nouvelles fonctionnalités

Vue d'ensemble de la sécurité technique La présentation technique de la sécurité vous permet de comprendre les meilleures pratiques de sécurité liées à Citrix Analytics. Ce document décrit le flux de données, la protection des données, les exigences réseau et les responsabilités de sécurité à prendre en compte lors de l'utilisation de Citrix Analytics.

11 septembre 2019

Problèmes résolus

- Citrix Cloud n'est pas en mesure de rediriger les utilisateurs vers la page Citrix Analytics spécifique à la région. [CAS-20559]

20 août 2019

Problèmes résolus

- La fonctionnalité de procédure pas à pas de Citrix Analytics ne se charge pas correctement sur les navigateurs Microsoft Edge et Safari. [CAS-20906]

31 juillet 2019

Nouvelles fonctionnalités

Soutien à la région de l'Union européenne Citrix Analytics prend désormais en charge la région de l'Union européenne. Vous pouvez choisir **l'Union européenne** comme région d'origine lors de l'intégration de votre organisation à Citrix Cloud et de l'utilisation du service Citrix Analytics. Citrix Analytics stocke les événements utilisateur et les métadonnées de votre organisation dans la région de l'Union européenne. Pour plus d'informations sur les régions Citrix Cloud, consultez la section Considérations géographiques.

26 juin 2019

Problèmes résolus

- Citrix Analytics ne se charge pas correctement sur Internet Explorer 11. [CAS-19867]

19 juin 2019

Problèmes résolus

- Citrix Analytics ne se charge pas correctement sur Microsoft Edge. [CAS-19930]

16 novembre 2018

Problèmes résolus

- Si vous accédez à Citrix Analytics à l'aide d'Internet Explorer version 11.0, la barre de navigation de **Citrix Cloud** ne se charge pas et vous empêche d'accéder au menu hamburger.

10 octobre 2018

Améliorations de l'architecture et de la plateforme

De nombreuses améliorations de l'architecture et de la plate-forme ont été apportées dans cette version pour améliorer les performances, l'évolutivité, la surveillance, la prise en charge, la sécurité et l'expérience utilisateur.

23 août 2018

Citrix Analytics est un service cloud fourni via Citrix Cloud. Il collecte des données sur les produits du portefeuille Citrix et fournit des informations exploitables, permettant aux administrateurs de gérer de manière proactive les menaces de sécurité, d'améliorer les performances des applications et de prendre en charge les opérations continues. Actuellement, Citrix Analytics propose les offres d'analyse suivantes :

- **Security Analytics** : rassemble et fournit une visibilité sur le comportement des utilisateurs et des entités. Pour plus d'informations, consultez la section Analyses de sécurité.
- **Operations Analytics** : rassemble et présente des informations sur les activités des utilisateurs, telles que les sites Web visités et la bande passante utilisée. Pour plus d'informations, consultez Operations Analytics.

Nouveaux noms de produits

Les produits Citrix pris en charge par Citrix Analytics sont désormais renommés dans le portefeuille de produits unifiés Citrix.

Vous remarquerez peut-être de nouveaux noms dans nos produits et dans la documentation produit. Ce changement de marque est le résultat de l'expansion du portefeuille Citrix et de la stratégie cloud. Pour plus d'informations sur le portefeuille unifié Citrix, consultez le guide produit Citrix. L'implémentation de cette transition dans nos produits et leur documentation est en cours.

- Le contenu intégré au produit et à la documentation peut encore contenir les anciens noms. Par exemple, vous pouvez voir des instances des anciens noms dans le texte de la console, les messages, les noms de répertoire/fichier, les captures d'écran et les diagrammes.
- Il est possible que certains éléments (tels que les commandes) conservent leur ancien nom pour éviter de casser les scripts client existants.
- La documentation produit associée et les autres ressources (telles que les vidéos et les billets de blog) auxquelles la documentation de ce produit renvoie peuvent toujours contenir des noms anciens.

Problèmes connus

September 21, 2023

Cet article met en évidence les problèmes connus applicables à l'ensemble des offres Citrix Analytics (performances et sécurité).

Pour les problèmes spécifiques à chaque offre, consultez les articles correspondants sur les problèmes connus : Sécurité et performances.

- L'**indicateur Gateway First time access from new IP** est déclenché pour les utilisateurs qui accèdent à des services ou à des applications via Gateway lors de leur première connexion. [CAS-57963]

Sources de données

September 21, 2023

Les sources de données sont les services cloud et les produits locaux qui envoient des données à Citrix Analytics.

Citrix Analytics collecte des données à partir des sources de données suivantes :

- **Sources de données Citrix**. Services Citrix Cloud et produits sur site qui envoient des données à Citrix Analytics. Citrix Analytics découvre automatiquement les services Citrix Cloud tels que Content Collaboration et Endpoint Management associés à votre compte Citrix Cloud.

  Pour les produits locaux tels que Citrix Gateway et Citrix Virtual Apps and Desktops, vous devez effectuer une série de configurations pour vous connecter à Citrix Analytics. Par exemple, les instances de passerelle locales doivent être ajoutées à la gestion de la mise à disposition des applications. De plus, les sites Virtual Apps and Desktops locaux doivent être ajoutés à Workspace ou les serveurs StoreFront doivent être configurés.
- **Sources de données externes**. Des applications tierces telles que Microsoft Graph Security, Microsoft Active Directory qui peuvent être intégrées à Citrix Analytics. Citrix Analytics collecte des données à partir de ces sources de données externes après une intégration réussie.

sources de données prises en charge

Selon l'offre Citrix Analytics que vous utilisez, les sources de données varient. Consultez les articles suivants pour consulter les sources de données prises en charge par chaque offre :

- Sources de données prises en charge par Citrix Analytics for Security
- Sources de données prises en charge par Citrix Analytics for Performance

Les sources de données Citrix Gateway, Citrix DaaS (anciennement Citrix Virtual Apps and Desktops service) et Citrix Virtual Apps and Desktops sont prises en charge par les deux offres : Citrix Analytics for Security et Citrix Analytics for Performance. Pour plus d'informations sur les étapes d'intégration applicables aux deux offres, consultez les articles suivants :

- Source de données de Citrix Gateway
- Source de données Citrix Virtual Apps and Desktops

Source de données de Citrix Gateway

April 12, 2024

La source de données **Gateway** représente les instances NetScaler Gateway locales de votre environnement. Citrix Analytics découvre automatiquement les agents NetScaler Application Delivery Management (ADM) et les instances Gateway ajoutées au service NetScaler ADM.

Lorsque les utilisateurs accèdent à des services ou des applications via Gateway, Citrix Analytics reçoit les événements d'accès utilisateur en temps réel. Les événements utilisateur sont traités pour détecter les éventuelles menaces à la sécurité.

Cet article décrit les étapes pour ajouter NetScaler Gateway à Citrix Analytics. Ces étapes s'appliquent aux deux offres : Citrix Analytics pour les performances et Citrix Analytics pour la sécurité.

Conditions préalables

- Abonnez-vous à NetScaler ADM proposé sur Citrix Cloud. Pour savoir comment démarrer avec NetScaler ADM, consultez la section Mise en route.
- Licence Citrix ADM vérifiée. Pour en savoir plus sur les licences Citrix ADM, consultez la section Licences.
- Passez en revue la configuration système requise et assurez-vous qu'elle est respectée.

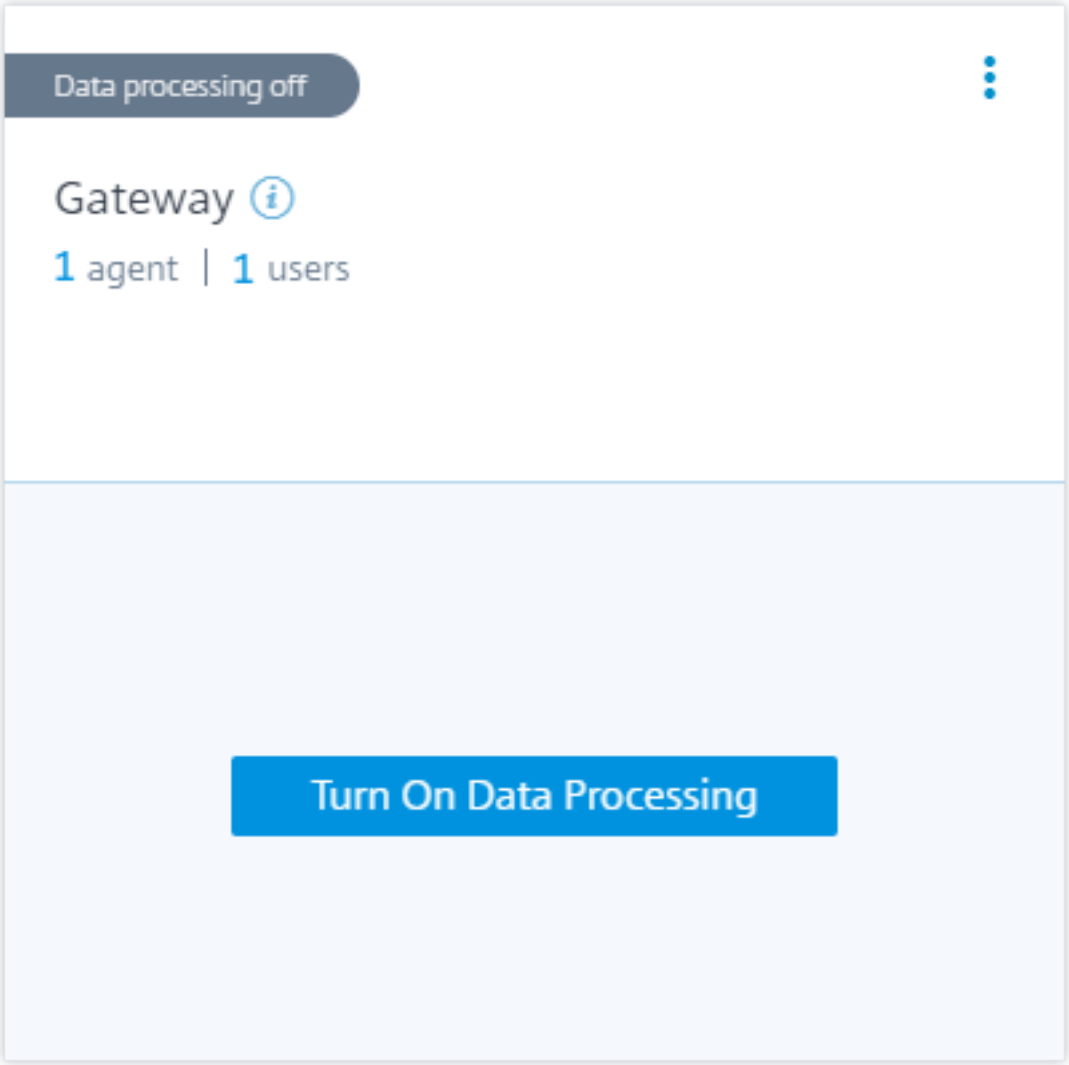
Sources de données Gateway ajoutées à NetScaler ADM

Citrix Analytics découvre automatiquement les agents NetScaler ADM et les instances NetScaler Gateway déjà ajoutées au service NetScaler ADM.

Pour afficher la source de données :

Dans la barre supérieure, cliquez sur **Paramètres** > **Sources de données**. Selon votre offre, sélectionnez **Sécurité** ou **Performance** pour afficher la carte de site Gateway.

Les agents découverts et les utilisateurs s'affichent sur la carte de site Gateway. Cliquez **sur Activer le traitement des données** pour permettre à Citrix Analytics de commencer à traiter les données de cette source de données.

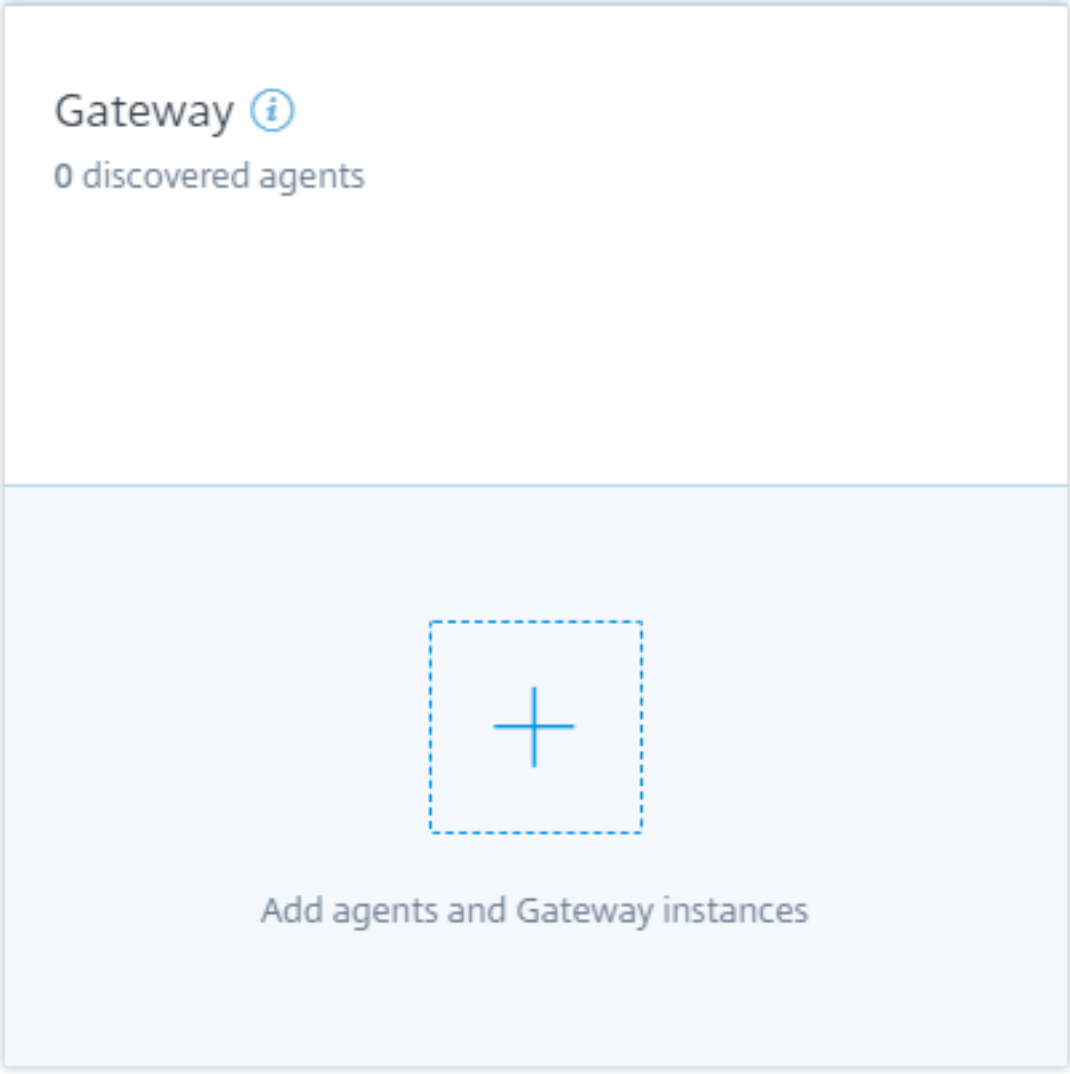


Vous pouvez consulter les événements reçus.

Reportez-vous à Un processus unifié pour activer les analyses sur les serveurs virtuels afin d'activer Citrix Analytics s'il n'est pas déjà activé sur le service Citrix ADM.

Sources de données de passerelle non ajoutées à NetScaler ADM

La carte de site Gateway affiche **0 agent découvert** lorsque les agents NetScaler ADM et les instances NetScaler Gateway ne sont pas ajoutés au service NetScaler ADM.



Pour découvrir les agents et les instances de passerelle, procédez comme suit :

1. Si vous avez déjà un abonnement au service NetScaler ADM, cliquez **sur+sur** la carte de site pour ajouter les agents et les instances Gateway.
2. Si vous n'avez pas d'abonnement au service NetScaler ADM, vous devez vous y abonner. Accédez à votre compte Citrix Cloud et procédez comme suit :

    a) Sous **Services disponibles**, cliquez sur **Gérer** dans la vignette **Gestion de la mise à disposition des applications** .

    b) Suivez les instructions à l'écran pour créer un compte Express pour NetScaler ADM. Pour plus d'informations, consultez la section Mise en route de la documentation NetScaler ADM.

    c) Après avoir créé le compte Express, reconnectez-vous à Analytics et cliquez sur **Paramètres > Sources de données > Sécurité**.

d) Sur la carte de site Gateway, cliquez **sur+pour** ajouter les agents et les instances Gateway.

3. Sur la page suivante, cliquez sur **Commencer**.

4. Exécutez les tâches suivantes :

   - Installation d'un agent NetScaler ADM
   - Ajoutez vos instances Gateway
   - Activer Analytics sur les serveurs virtuels

Conditions préalables

- **Exigence d'installation de l'agent NetScaler ADM** : Dans votre centre de données, vous pouvez installer un agent sur Citrix Hypervisor, VMware ESXi, Microsoft Hyper-V et Linux KVM Server.

  Le tableau suivant répertorie les ressources informatiques virtuelles que l'hyperviseur doit fournir à l'agent.

Composant	Exigences
RAM	8 Go (32 Go recommandés pour de meilleures performances.)
CPU virtuel	4 (8 processeurs virtuels recommandés pour de meilleures performances)
Espace de stockage	120 GB
Interfaces réseau virtuelles	1

Composant	Exigences
Débit	1 Gbit/s

- **Exigences en matière de port** : assurez-vous que les ports suivants sont ouverts pour que l'agent NetScaler ADM puisse communiquer avec les instances de NetScaler Gateway.

Type	Port	Description
TCP	80/443	Pour la communication NITRO entre l'agent et les instances NetScaler Gateway
TCP	22	Pour la communication SSH entre l'agent et l'instance NetScaler Gateway.
UDP	4739	Pour la communication AppFlow entre NetScaler Gateway et l'agent
ICMP	Aucun port réservé	Pour détecter l'accessibilité réseau entre l'agent et les instances NetScaler Gateway.
SNMP	161, 162	Pour recevoir des événements SNMP de l'instance NetScaler Gateway vers l'agent.
Syslog	514	Pour recevoir des messages Syslog dans l'agent à partir d'une instance NetScaler Gateway.
TCP	5557	Pour la communication de flux de journaux entre les instances NetScaler Gateway et l'agent.

Pour la communication entre l'agent NetScaler ADM et Citrix Analytics, assurez-vous que le port suivant est ouvert :

Type	Port	Description
TCP	443	Pour la communication NITRO entre l'agent et le service NetScaler Application Delivery Management.

Pour la communication entre l'agent NetScaler ADM et Citrix Analytics, assurez-vous que le point de terminaison suivant est sur liste blanche :

Point de terminaison	Région des États-Unis	UE
Hub d'événements	`https://cas-eh-ns-alias.servicebus.windows.net/`	`https://cas-eh-ns-eu-alias.servicebus.windows.net/`

Installer et configurer un agent

Installez et configurez l'agent de service NetScaler ADM dans votre environnement réseau pour permettre la communication entre Analytics et les instances Gateway de votre centre de données.

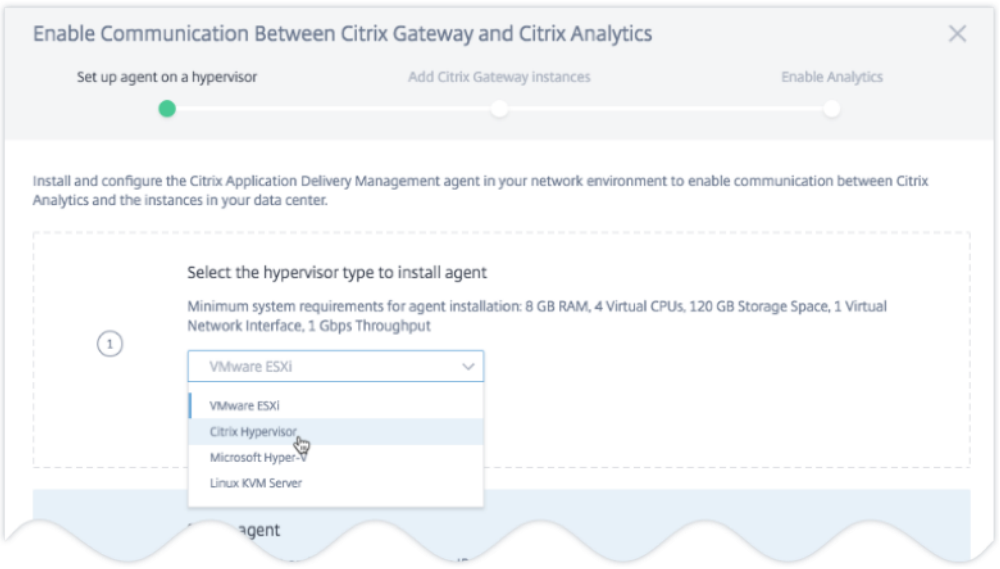
Vous pouvez installer un agent sur les hyperviseurs suivants dans votre centre de données d'entreprise :

- Citrix Hypervisor
- VMware ESXi
- Microsoft Hyper-V
- Serveur KVM Linux

Pour installer et configurer un agent, procédez comme suit :

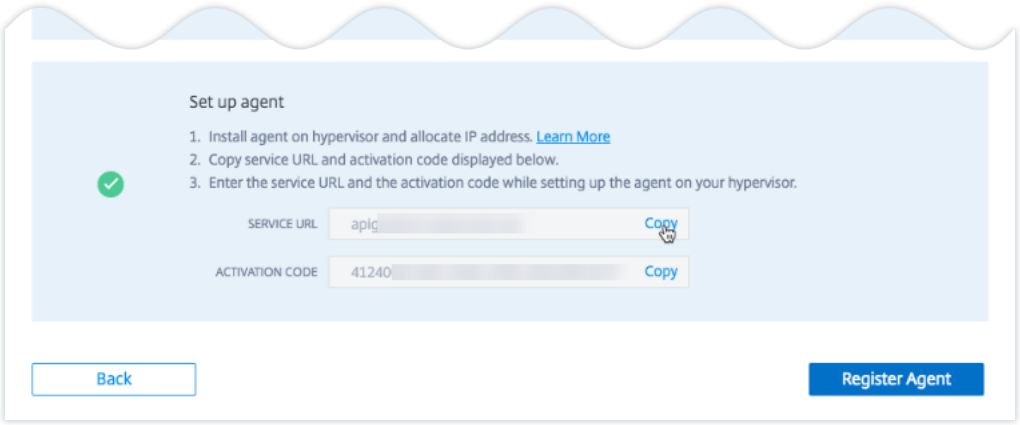
1. Téléchargez l'image de l'agent.

   Sur la page **Configurer l'agent sur un hyperviseur**, sélectionnez l'hyperviseur, puis cliquez sur **Télécharger l'image** pour télécharger l'image de l'agent sur votre système local.



2. Copiez l'URL du service et le code d'activation

   Une URL de service et un code d'activation sont générés et affichés sur l'interface utilisateur, comme illustré dans l'image suivante. (Ce processus peut prendre quelques secondes.) L'agent utilise l'URL du service pour localiser le service et le code d'activation pour s'inscrire auprès du service. Entrez l'URL du service et le code d'activation lors de l'installation de l'agent sur votre hyperviseur.

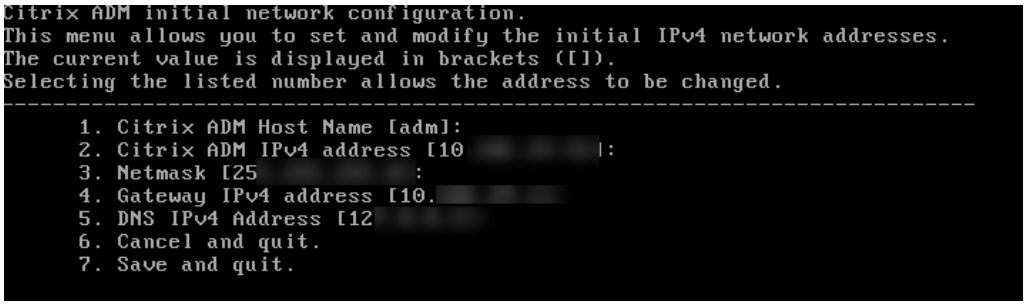


3. Installez l'agent sur un hyperviseur.

> **Remarque**
>
> Avant de commencer l'installation de l'agent, assurez-vous que :
>
> - Vous disposez des ressources informatiques virtuelles requises que l'hyperviseur doit fournir pour chaque agent : RAM : 8 Go, processeur virtuel : 4, espace de stockage : 120 Go, interface réseau virtuelle : 1 et débit : 1 Gbps
> - Vous configurez votre DNS pour autoriser l'accès Internet à votre agent.

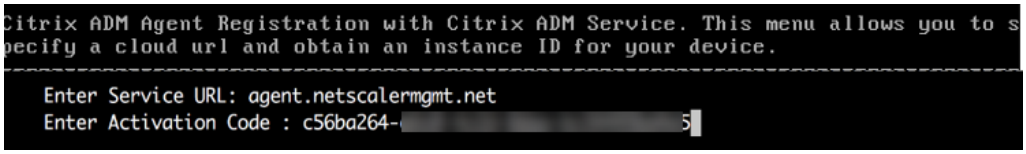
- Sur un Citrix Hypervisor, effectuez les opérations suivantes :

  a) Importez le fichier image de l'agent sur votre hyperviseur. Dans l'onglet **Console**, configurez les options de configuration réseau initiales, comme illustré dans l'exemple suivant.



  Si vous avez saisi des valeurs incorrectes ou si vous souhaitez modifier une valeur, connectez-vous à l'invite de l'interpréteur de commandes en utilisant les informations d'identification par défaut `nsrecover`/`nsroot`. Exécutez ensuite la commande `networkconfig`.

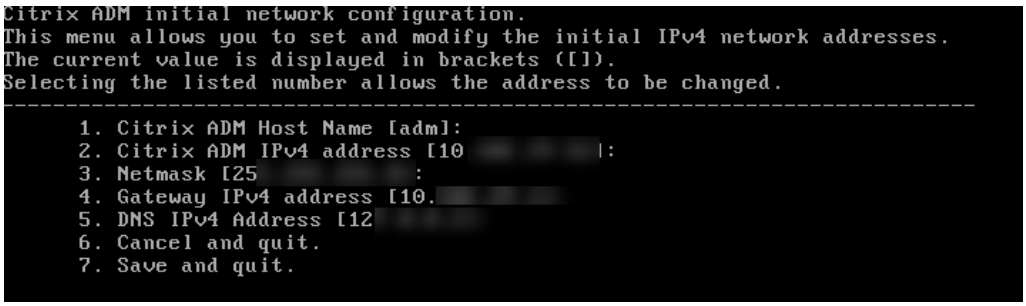
  b) Entrez l'**URL du service** et le **code d'activation** que vous avez enregistrés lors du téléchargement de l'image de l'agent.



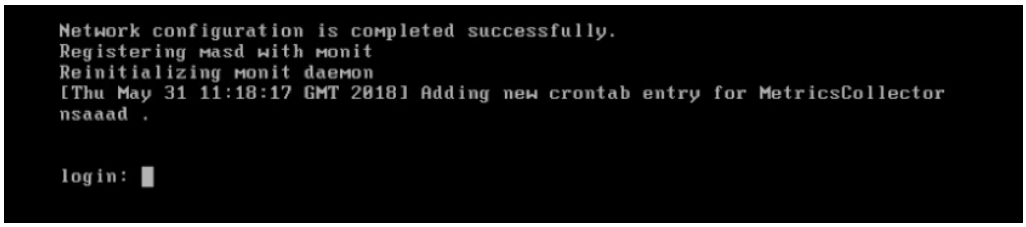
  Si vous avez saisi l'URL du service ou le code d'activation incorrectement, connectez-vous à l'invite de l'interpréteur de commandes de l'agent, puis exécutez le script : `deployment_type.py`. Ce script vous permet de saisir à nouveau l'URL du service et le code d'activation.

- Sur un hyperviseur VMware ESXi, effectuez les opérations suivantes :

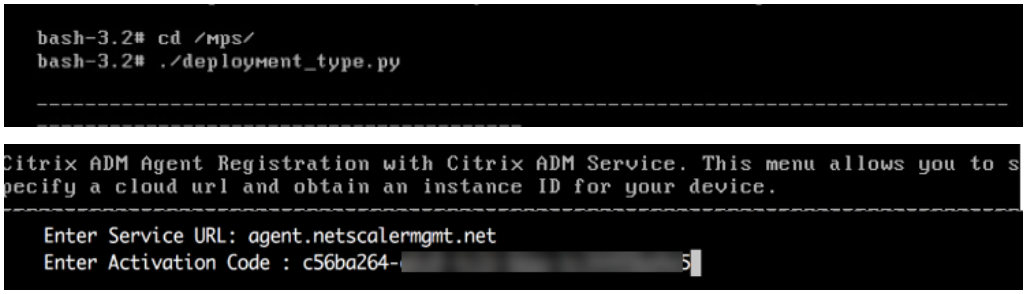
  a) Importez le fichier image de l'agent sur votre hyperviseur. Dans l'onglet **Console**, configurez les options de configuration réseau initiales, comme illustré dans l'exemple suivant.



b) Après avoir configuré le réseau, lorsque vous y êtes invité, connectez-vous à l'invite de l'interpréteur de commandes de l'agent à l'aide des informations d'identification par défaut `nsrecover`/`nsroot`.



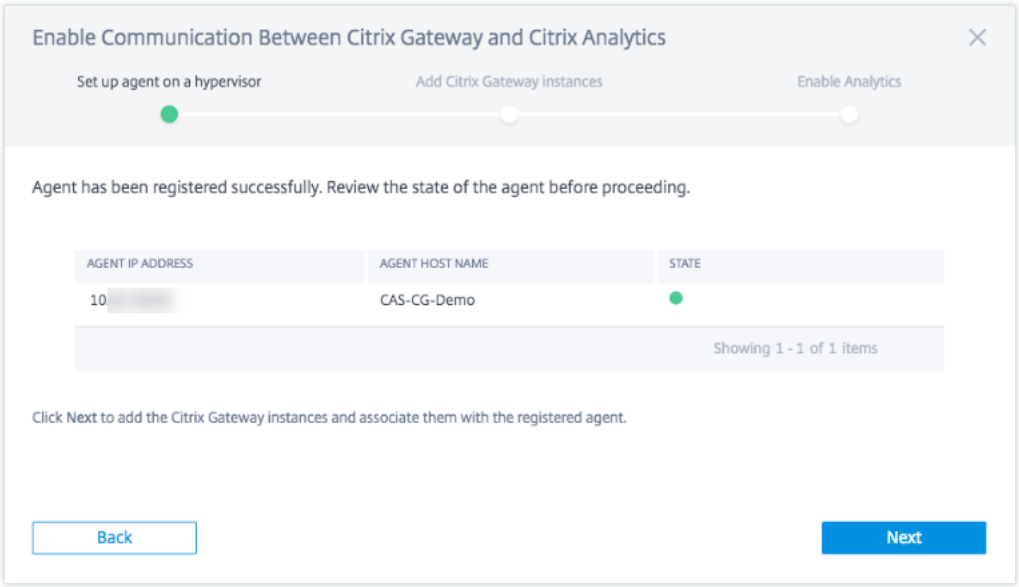
c) Accédez au répertoire **/mps**, exécutez le script et saisissez l'**URL du service** et le **code d'activation** que vous avez enregistrés lors du téléchargement de l'image de l'agent.



> **Remarque**
>
> Vous pouvez utiliser le même fichier image pour installer plusieurs agents. Toutefois, vous ne pouvez pas utiliser le même code d'activation sur plusieurs agents. Pour générer un nouveau code d'activation, accéder à Citrix Analytics, et sur l'agent d'installation sur une étape d'hyperviseur, cliquez à nouveau sur **Télécharger l'image** . Un nouveau code d'activation est généré.

4. Enregistrer l'agent.

   Une fois l'enregistrement de l'agent réussi, l'agent redémarre pour terminer le processus d'installation. Une fois l'agent redémarré, accédez à Citrix Analytics et cliquez sur **Enregistrer l'agent**, puis vérifiez l'état de l'agent.

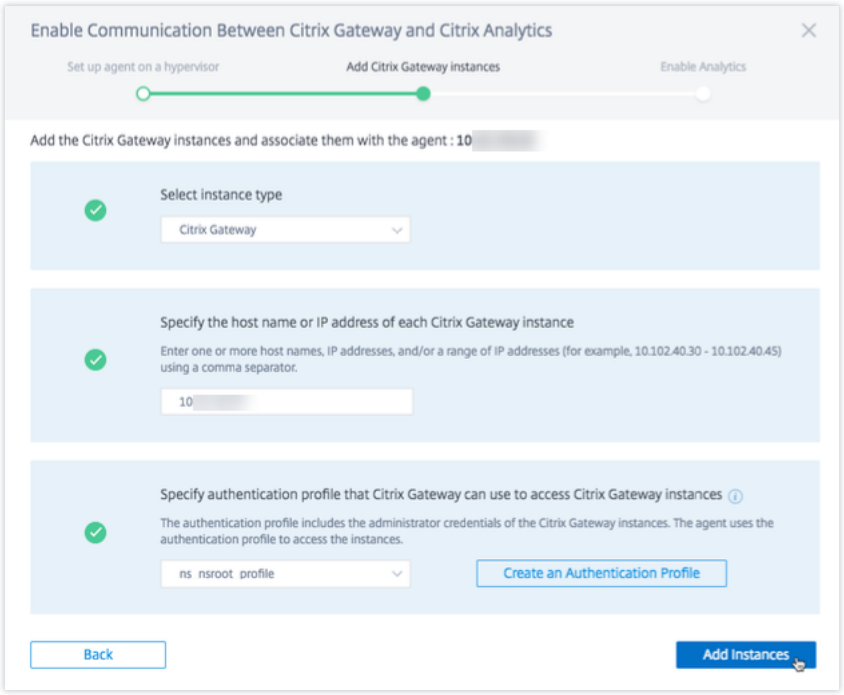


Lorsque l'état de l'agent est à l'état UP, désigné par un point vert à côté de celui-ci, cliquez sur **Suivant** pour commencer à ajouter des instances au service.

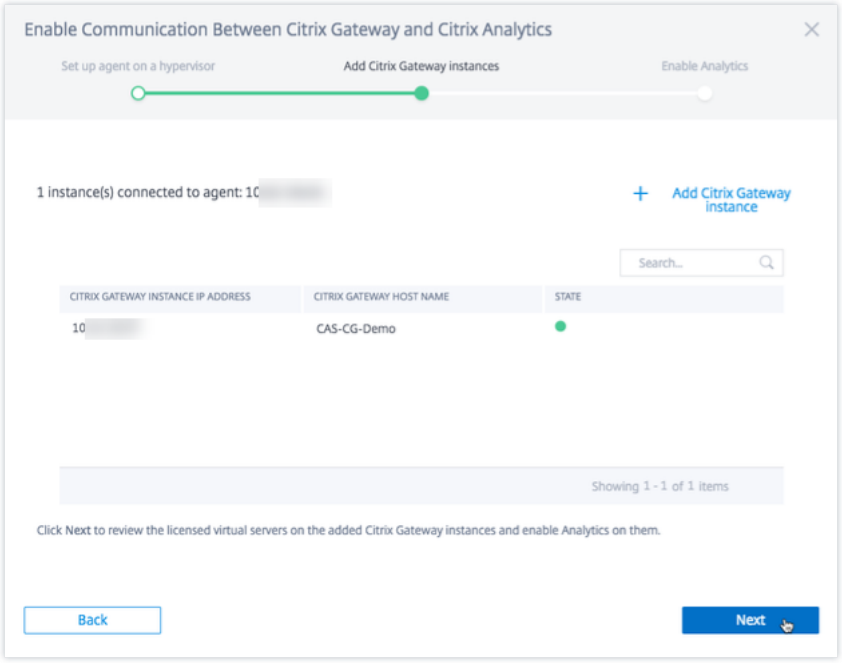
Ajouter des instances NetScaler Gateway

Les instances sont des appliances NetScaler Gateway ou des dispositifs virtuels qui sont les sources de données de Citrix Analytics.

1. Sur la page **Ajouter des instances NetScaler Gateway**, sélectionnez le type d'instance et spécifiez les noms d'hôte ou les adresses IP ou la plage d'adresses IP des instances de passerelle à découvrir.
2. Créez un profil d'authentification que l'agent peut utiliser pour accéder aux instances de Gateway. Ce profil correspond aux informations d'identification d'administrateur d'une instance Gateway. Cliquez ensuite sur **Ajouter des instances**.



Une fois les instances ajoutées, vous pouvez afficher le nombre d'instances qui ont été découvertes avec succès. Pour ajouter d'autres instances, cliquez sur **Ajouter une instance NetScaler Gateway**.



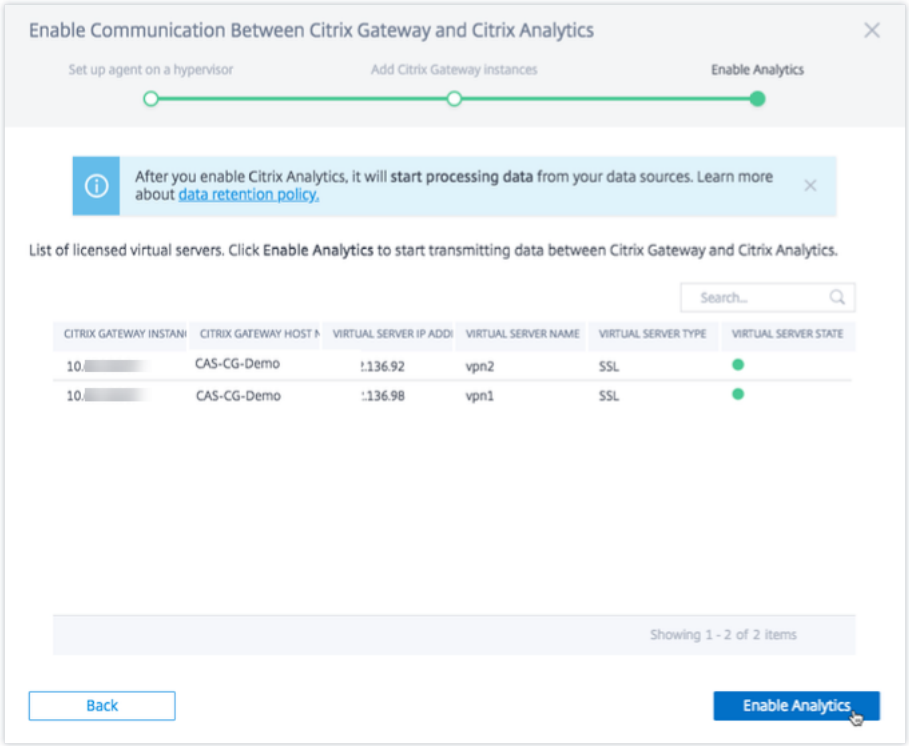
Cliquez sur **Suivant** pour activer les analyses.

Activer l'analyse

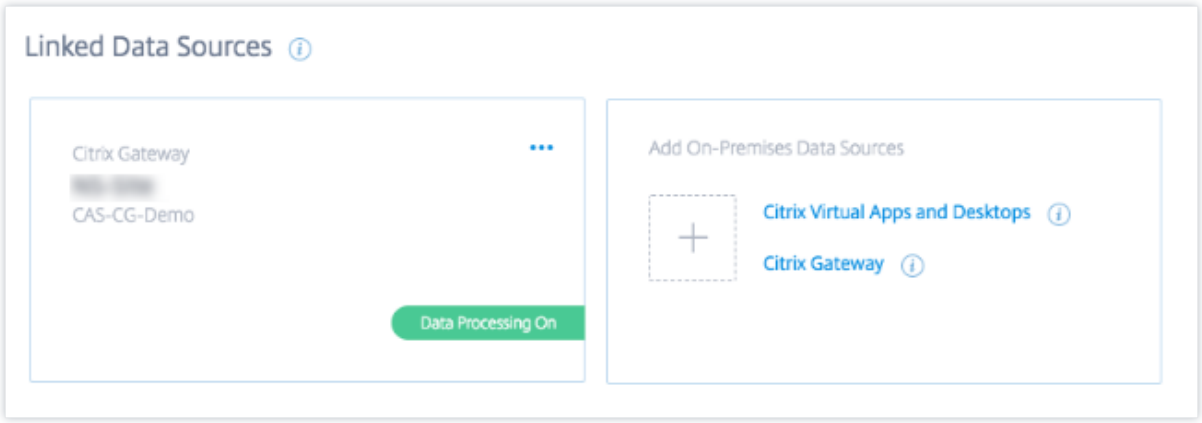
Citrix Analytics découvre automatiquement les serveurs virtuels sous licence sur les instances NetScaler Gateway ajoutées. Activez les analyses sur tous les serveurs virtuels découverts.

Sur la page **Activer Analytics**, par défaut, tous les serveurs virtuels sous licence à partir des instances de Gateway apparaissent. Consultez la liste des serveurs virtuels sous licence et cliquez sur **Activer Analytics** pour activer les analyses sur les serveurs virtuels.

> **Remarque**
>
> Les serveurs virtuels peuvent prendre un certain temps, environ 10 minutes, pour apparaître sur la page.



L'état de la fiche de site passe à **Traitement des données activé**. Vous pouvez consulter les événements reçus.



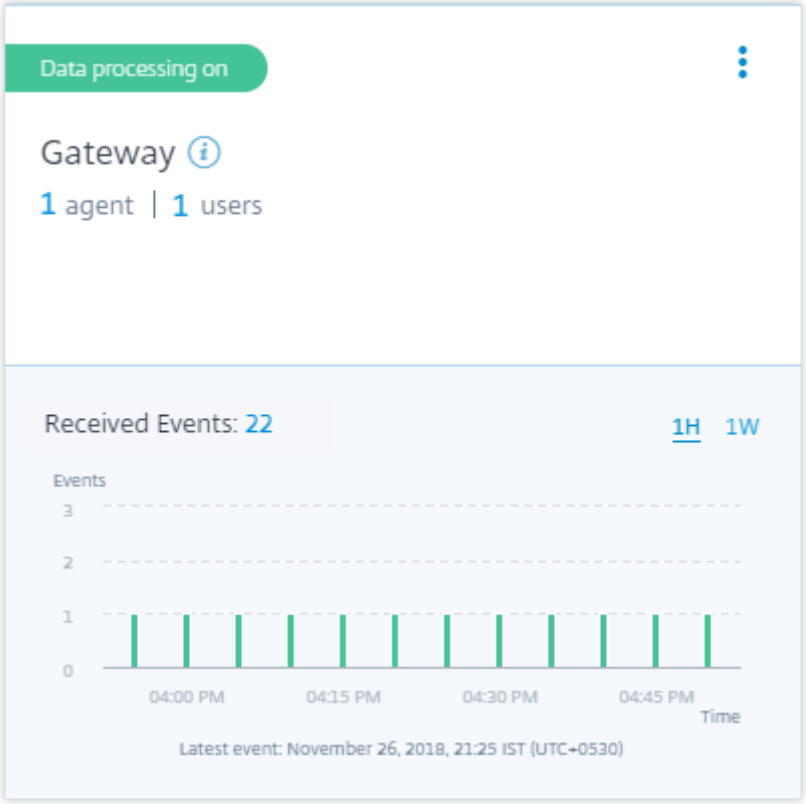
Regardez la vidéo d'intégration

La vidéo suivante montre les étapes à suivre pour intégrer une instance Gateway :

Il s'agit d'une vidéo intégrée. Cliquez sur le lien pour visionner la vidéo

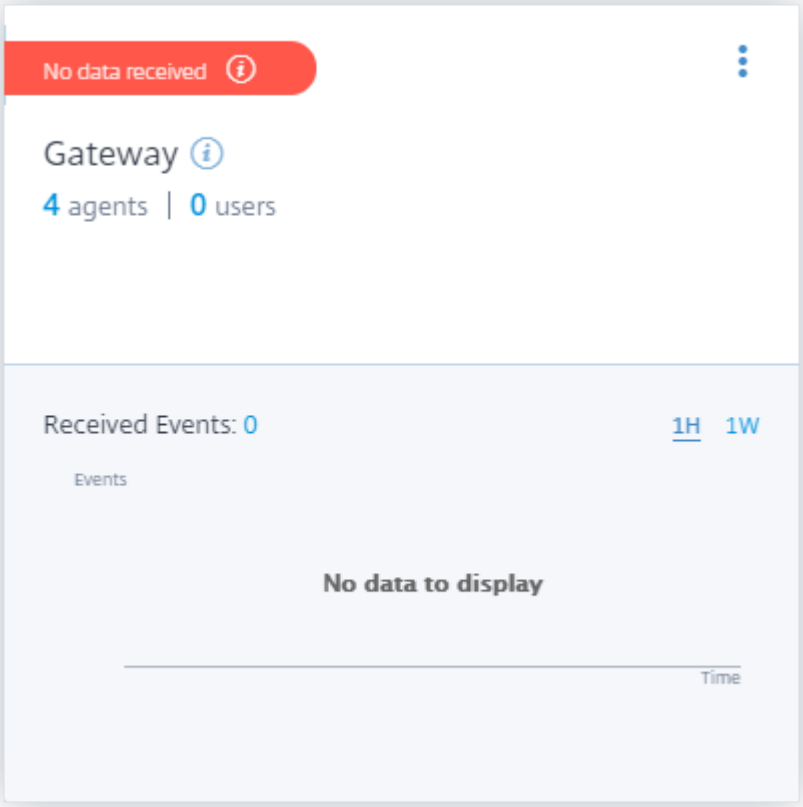
Afficher les événements, les utilisateurs et les agents reçus

La fiche de site affiche le nombre d'utilisateurs Gateway, d'agents NetScaler ADM et les événements reçus de la source de données au cours de la dernière heure, qui est la sélection de l'heure par défaut. Vous pouvez également sélectionner 1 semaine (**1 W**) et afficher les données. Cliquez sur le nombre d'utilisateurs à afficher sur la page **Utilisateurs** . Cliquez sur le nombre d'agents pour afficher les instances NetScaler Gateway et les agents.



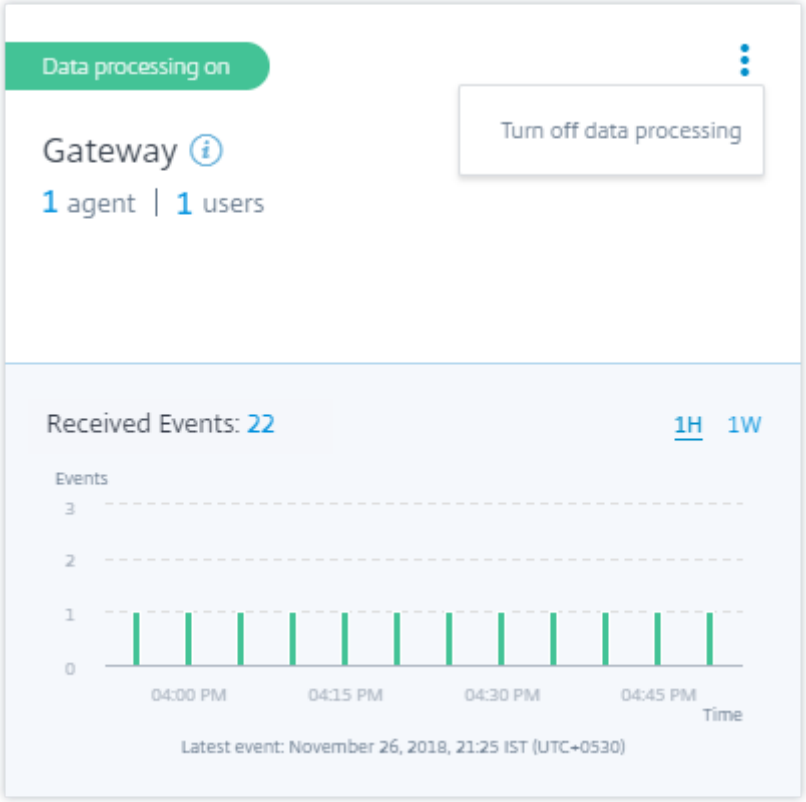
Une fois que vous avez activé le traitement des données, la carte de site peut afficher l'état **No data received** (Aucune donnée reçue). Cet état apparaît pour deux raisons :

1. Si vous avez activé le traitement des données pour la première fois, les événements mettent un certain temps à atteindre le hub d'événements dans Citrix Analytics. Lorsque Citrix Analytics reçoit les événements, l'état passe à **Data processing on** (Traitement des données activé). Si l'état ne change pas après un certain temps, actualisez la page **Sources de données** .
2. Analytics n'a reçu aucun événement de la source de données au cours de la dernière heure.

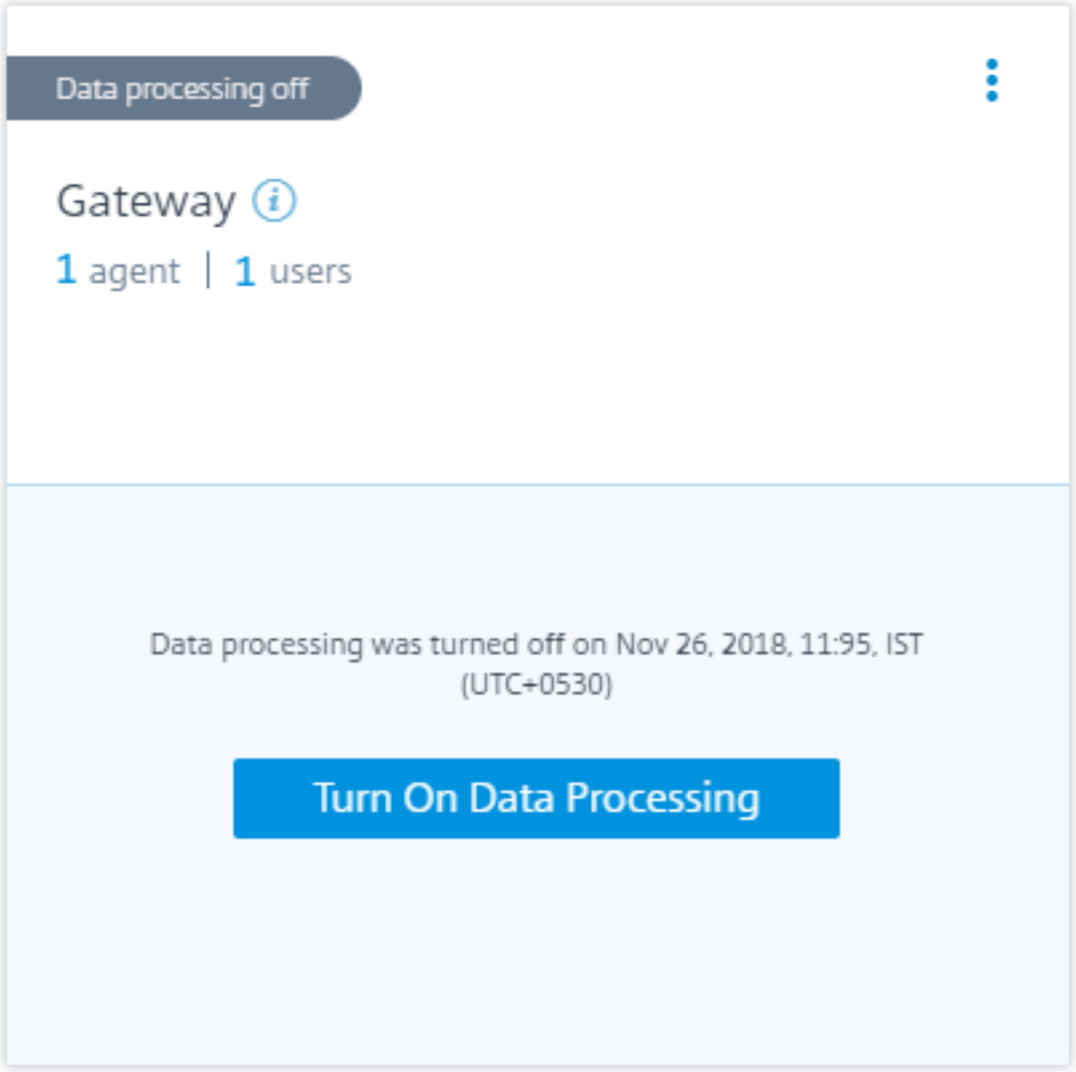


Activer ou désactiver le traitement des données

Pour arrêter le traitement des données, cliquez sur les points de suspension verticaux () sur la fiche de site, puis sur **Désactiver le traitement des données**. Citrix Analytics cesse de traiter les données de cette source de données.

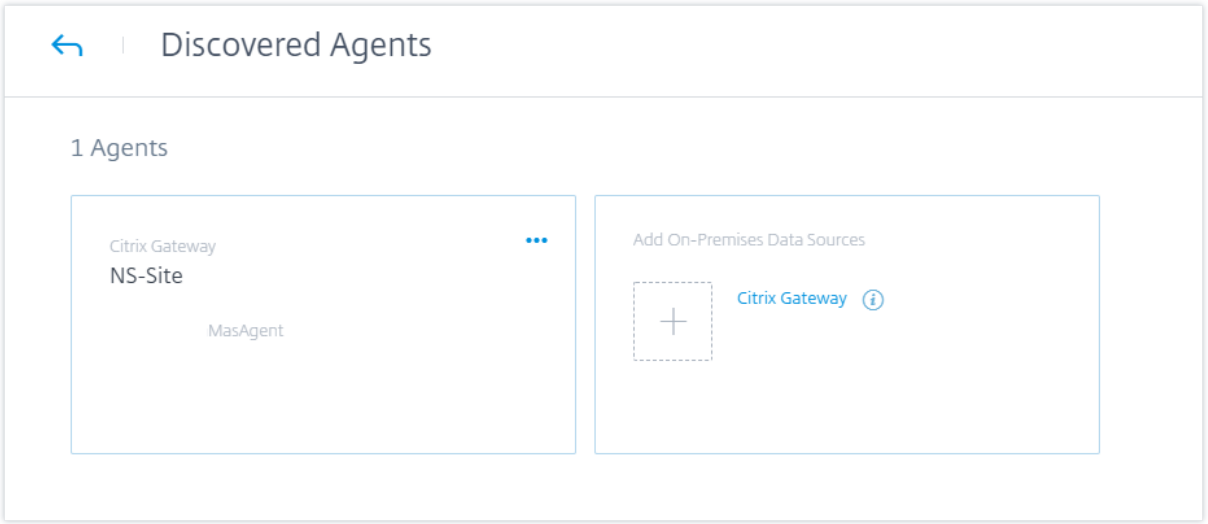


Pour réactiver le traitement des données, cliquez **sur Activer le traitement des données**.



Ajouter d'autres instances Gateway

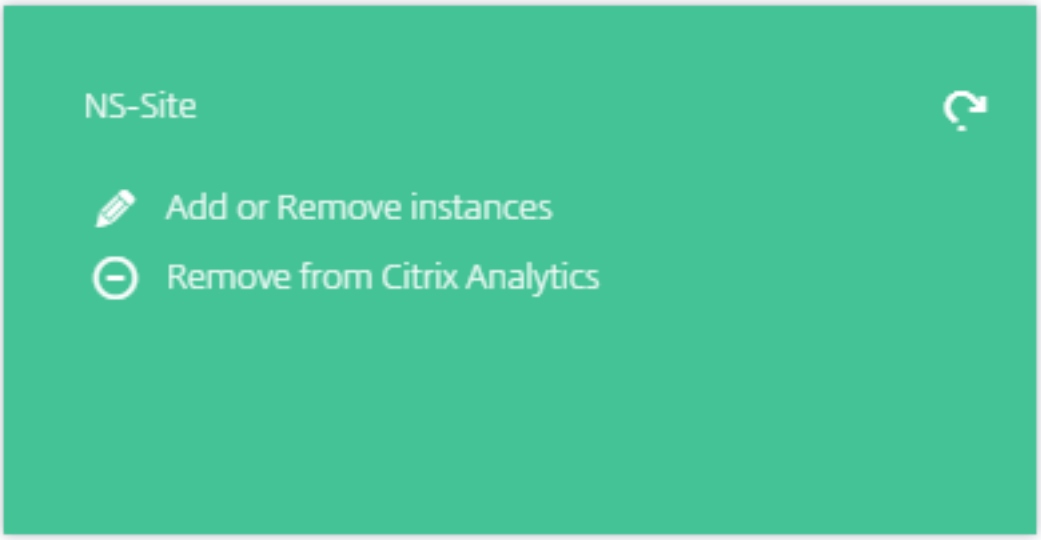
Si vous souhaitez ajouter d'autres instances Gateway, cliquez sur le nombre d'agents sur la carte de site Gateway pour afficher la page **Agents découverts** . Dans la vignette **Ajouter des sources de données locales**, cliquez sur **NetScaler Gateway**.



Gérer la source de données

Vous pouvez également ajouter d'autres instances à un agent ou supprimer des instances associées à un agent. Vous pouvez également supprimer l'agent et ses instances associées de Citrix Analytics.

Retournez la carte de site d'un agent et effectuez l'une des opérations suivantes :



- **Ajoutez ou supprimez des instances**. Vous pouvez ajouter d'autres instances Gateway à un agent et activer Analytics sur les serveurs virtuels configurés sur ces instances. Vous pouvez également supprimer des instances ajoutées à un agent. Lorsque vous dissociez une instance d'un agent, Citrix Analytics ne peut pas communiquer avec cette instance.
- **Supprimer de Citrix Analytics**. Une fois que vous avez supprimé un site d'agent, Citrix Analytics arrête de collecter des données à partir des instances associées à cet agent. Mais toutes les

données précédemment traitées sont disponibles pendant la période de conservation.

Source de données Citrix Virtual Apps and Desktops

April 12, 2024

Cet article décrit les étapes à suivre pour connecter vos sites Citrix Virtual Apps and Desktops locaux à Citrix Analytics à l'aide de StoreFront. Les étapes d'intégration mentionnées dans cet article s'appliquent aux deux offres : Citrix Analytics for Performance (Performance Analytics) et Citrix Analytics for Security (Security Analytics).

Pour connaître les étapes d'intégration spécifiques à chaque offre, consultez les articles suivants :

- Configuration de sites Citrix Virtual Apps and Desktops locaux avec Citrix Analytics for Performance
- Configuration de Citrix Virtual Apps and Desktops et de la source de données Citrix DaaS pour Citrix Analytics for Security

Sites locaux Citrix Virtual Apps and Desktops intégrés à l'aide de StoreFront

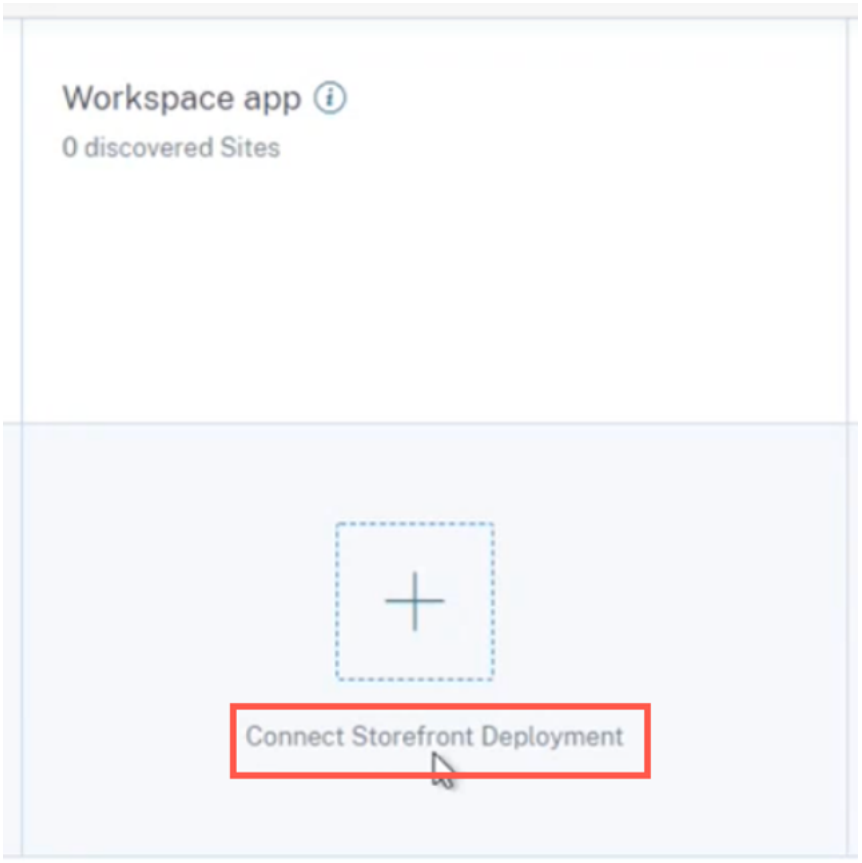
Si votre organisation utilise un déploiement StoreFront local, vous devez configurer vos serveurs StoreFront pour permettre à l'application Citrix Workspace d'envoyer des événements à Citrix Analytics. Citrix Analytics traite les événements pour fournir des informations exploitables sur les performances de votre infrastructure informatique Citrix et le comportement des utilisateurs.

Pour plus d'informations sur la façon de configurer un déploiement StoreFront pour Citrix Analytics, consultez l'article sur le service Citrix Analytics dans la documentation StoreFront.

Auparavant, les clients utilisant les sites locaux Citrix Apps and Desktops étaient obligés d'utiliser l'agrégation de sites pour intégrer les sites locaux à Citrix Analytics for Security and Performance.

Vous pouvez désormais intégrer des sites locaux Citrix Apps and Desktops sans dépendre de l'agrégation de sites.

Vous pouvez voir l'option **Connect Storefront Deployment** sur votre application Workspace, même si aucun site n'a été ajouté à l'agrégation de sites.



Pré-requis

Avant de commencer, vérifiez les points suivants :

- Votre version StoreFront doit être 1906 ou ultérieure.
- Le déploiement StoreFront doit pouvoir se connecter aux adresses suivantes :
  - https://*.cloud.com
  - https://api.analytics.cloud.com
- Le déploiement de StoreFront doit avoir le port 443 ouvert pour les connexions Internet sortantes. Tous les serveurs proxy du réseau doivent autoriser cette communication avec Citrix Analytics.
- Si le déploiement de StoreFront est hébergé sur un serveur Web qui utilise un proxy Web pour se connecter à Internet, le proxy de chaque magasin doit être configuré manuellement pour autoriser le trafic sortant. StoreFront n'utilise pas automatiquement le paramètre proxy du serveur Web hôte. Pour plus d'informations, consultez la rubrique Configurer un déploiement StoreFront hébergé sur un serveur Web qui utilise un proxy HTTP.

- Le déploiement StoreFront doit être accessible à l'aide de l'un des clients suivants :
  - Citrix Receiver pour sites Web dans des navigateurs compatibles HTML5.

    > **Remarque**
    >
    > Si vous êtes un utilisateur HTML5, Citrix Virtual Apps and Desktops peut lancer des événements lorsque certaines configurations sont activées sur StoreFront. Pour plus d'informations sur les étapes de configuration, consultez l'article Installer dans la documentation de l'application Citrix Workspace pour HTML5. Pour les événements liés à l'impression, des stratégies supplémentaires doivent être configurées sur StoreFront. Pour plus d'informations, consultez l'article Impression PDF dans la documentation de l'application Citrix Workspace pour HTML5.

  - Application Citrix Workspace 1907 pour Windows ou version ultérieure.
  - Application Citrix Workspace 2006 pour Linux ou version ultérieure.
  - Application Citrix Workspace 2006 pour Mac ou version ultérieure
- Si vous utilisez Citrix Virtual Apps and Desktops 7 1912 LTSR, la version StoreFront prise en charge est 1912.

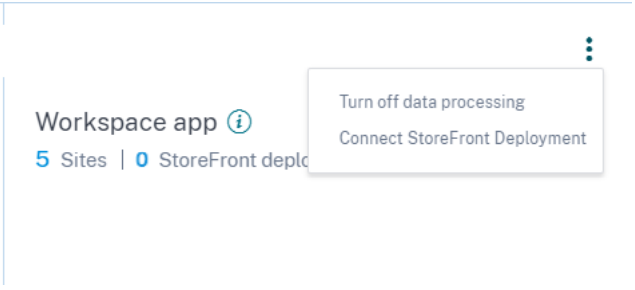
Connexion à un déploiement StoreFront

Vous pouvez vous connecter à un déploiement StoreFront des manières suivantes :

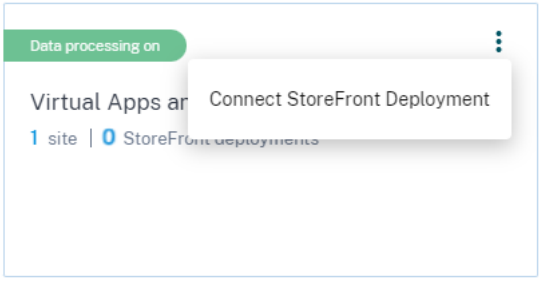
- À l'aide de la carte de site **Apps and Desktops —application Workspace** et de la carte de site **Apps and Desktops —Monitoring**
- À l'aide du panneau **Recommandations**

Connectez-vous à l'aide de la carte de site Apps and Desktops —application Workspace et de la carte de site Apps and Desktops —Monitoring

1. Accédez à **Paramètres > Sources de données > Sécurité**. Sur la fiche de site **Apps and Desktops- Workspace app**, cliquez sur les points de suspension verticaux (⋮), puis sélectionnez **Déploiement Connect StoreFront**.

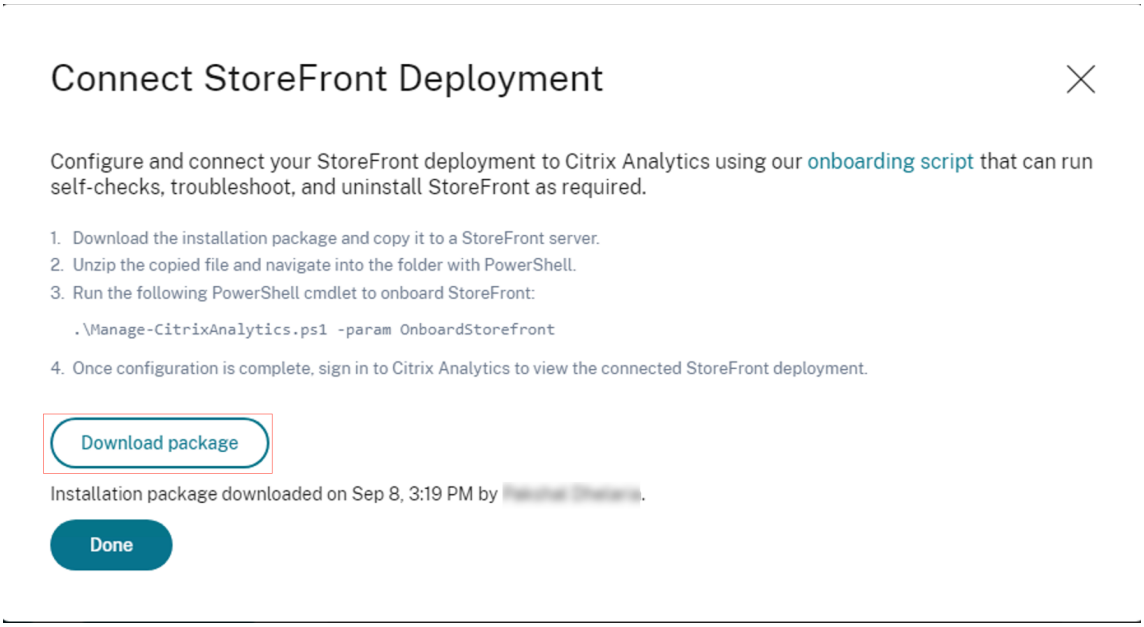


2. Accédez à **Paramètres > Sources de données > Performances**. Sur la carte de site **Apps and Desktops- Monitoring**, cliquez sur les points de suspension verticaux (⋮), puis sélectionnez **Déploiement Connect StoreFront**.



L'assistant d'intégration de StoreFront ou la fenêtre contextuelle **Connect StoreFront Deployment** s'affiche.

3. Cliquez sur **Télécharger le package**.



> **Remarque**
>
> Le fichier contient des informations sensibles. Conservez le fichier dans un endroit sûr et sécurisé.

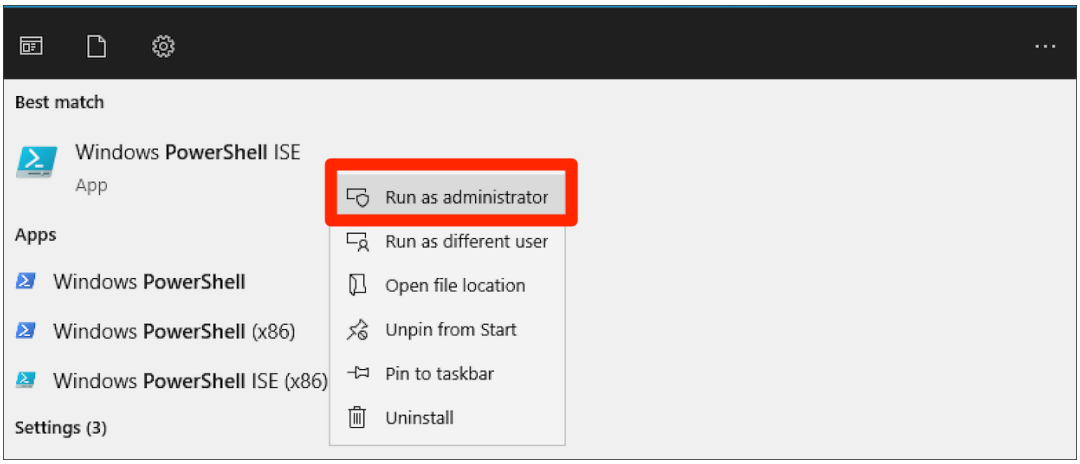
4. Pour configurer le déploiement de StoreFront,

   a) Copiez le package d'installation sur le serveur StoreFront.

   b) Décompressez le fichier copié et accédez au dossier dans PowerShell.

   c) Vous devez exécuter la commande suivante en tant qu'administrateur pour intégrer StoreFront :

.\Manage-CitrixAnalytics.ps1 –param OnboardStorefront



Pour plus d'options ou de paramètres, reportez-vous à la section PowerShell Script .

d) Ouvrez le serveur StoreFront et exécutez le script PowerShell.

e) Si le site StoreFront n'apparaît pas dans l'interface graphique de Citrix Analytics Service même après avoir exécuté OnboardStoreFront, exécutez la commande iisreset.

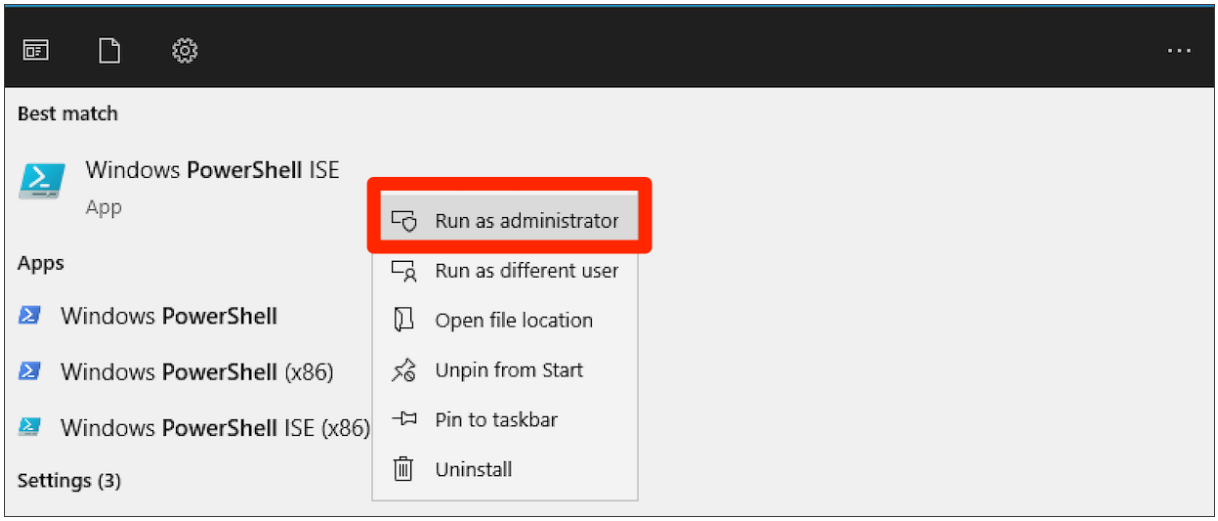
f) Connectez-vous à l'interface graphique du service Citrix Analytics et vérifiez si l'ID du cluster correspond à celui connecté à la console par le script.

g) Une fois la configuration terminée, connectez-vous à Citrix Analytics pour consulter le déploiement StoreFront connecté.

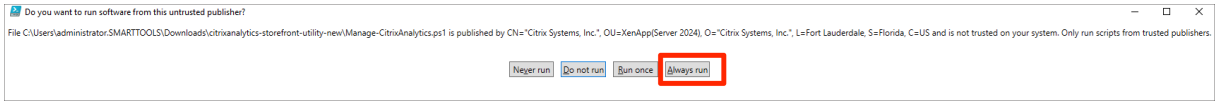
5. Une fois la configuration terminée, cliquez sur **Terminé**.
6. Cliquez **sur Activer le traitement des données** pour permettre à Citrix Analytics de traiter les données.

Script PowerShell

Un nouveau script PowerShell a été introduit pour simplifier le processus d'intégration de StoreFront à Citrix Analytics Service. Ce script PowerShell automatise le processus de vérification des prérequis, d'installation et de configuration de StoreFront. Le script PowerShell doit être exécuté en mode administrateur.



Les clients peuvent exécuter ce script PowerShell sur StoreFront pour intégrer, déconnecter, effectuer des autovérifications, résoudre des problèmes et vérifier si l'intégration à l'interface graphique du service Citrix Analytics est réussie. Lorsqu'un client exécute le script pour la première fois, un message d'avertissement de sécurité apparaît pour confirmer auprès de l'éditeur. Sélectionnez l'option Toujours exécuter si l'éditeur est fiable.



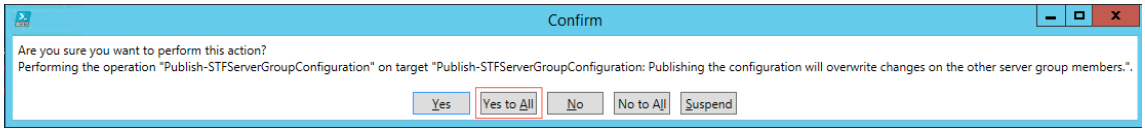
Le script PowerShell est disponible sur la page de **déploiement de Connect StoreFront** dans un fichier .zip avec le fichier StoreFrontConfiguration.json, quelques fichiers CCAuth et .dll. Les journaux de script PowerShell sont enregistrés dans le fichier cas-logs du dossier **Téléchargements**.

Le script PowerShell prend en charge les paramètres suivants :

- **SelfCheck** : le paramètre **SelfCheck** est utilisé pour vérifier que les conditions préalables à l'intégration de StoreFront sont remplies. Il vérifie l'installation de StoreFront, la version requise, la connexion sortante, la connectivité réseau du serveur cURL Analytics, la connectivité Internet, la configuration du groupe de serveurs et toute configuration existante du service Citrix Analytics. Utilisez la commande suivante pour exécuter l'**autocontrôle** :

  ```
  .\Manage-CitrixAnalytics.ps1 –param SelfCheck
  ```

- **OnboardStorefront** : le paramètre **OnboardStorefront** effectue rapidement une autovérification pour vérifier si l'installation est prête pour la configuration de Citrix Analytics Service. Si l'installation est prête, elle importe la configuration du service Citrix Analytics et publie les modifications sur les autres serveurs du groupe de serveurs. Pour un groupe de serveurs, la commande PublishConfiguration s'exécute automatiquement à partir du script afin de publier la configuration StoreFront sur tous les serveurs de ce StoreFront. Vous pouvez voir une fenêtre contextuelle vous demandant de confirmer `PublishConfiguration` l'action. Sélectionnez le bouton **Oui pour tout**.



Une fois la publication de la configuration terminée, le script appelle l'API du service Citrix Analytics pour vérifier si le StoreFront est intégré à l'interface graphique du service Citrix Analytics. Pour appeler cette API, une clé privée est requise pour l'authentification. Pour générer cette clé privée, vous avez besoin des fichiers CCAuth et dll, ainsi que des informations d'identification disponibles dans le fichier JSON téléchargé.

> **Remarque**
>
> Une fois le processus d'intégration de StoreFront terminé, l'affichage de StoreFront dans l'interface graphique de Citrix Analytics Service peut prendre de deux à cinq minutes. Si le site StoreFront n'apparaît pas dans l'interface graphique de Citrix Analytics Service, vous devez exécuter un IISRESET pour réinitialiser les services d'information Internet.

Utilisez la commande suivante pour exécuter **OnBoardStoreFront** :

```
.\Manage-CitrixAnalytics.ps1 –param OnboardStorefront
```

- **IsonBoarded** : le paramètre **IsonBoarded** est utilisé pour vérifier si le StoreFront est intégré à l'interface graphique de Citrix Analytics Service. Le script attend une minute avant de se fermer, mais StoreFront peut mettre jusqu'à cinq minutes pour apparaître dans l'interface graphique une fois l'intégration réussie. Vous devez exécuter cette commande pour le vérifier. Cette commande est également dépendante des fichiers CCAuth et dll. Utilisez la commande suivante pour exécuter **IsOnboarded** :

  ```
  .\Manage-CitrixAnalytics.ps1 –param IsOnboarded
  ```

- **Résolution**des problèmes : après cinq minutes d'attente, si le site StoreFront n'apparaît pas dans l'interface graphique du service Citrix Analytics, vous devez exécuter un IISRESET pour réinitialiser les services d'information Internet. Si le site StoreFront n'apparaît toujours pas dans l'interface graphique, utilisez le paramètre **Troubleshoot** . Il vous aide à résoudre les problèmes de connectivité et à collecter des journaux. Utilisez la commande suivante pour exécuter le **dépannage** :

  ```
  .\Manage-CitrixAnalytics.ps1 –param TroubleShoot
  ```

  Le paramètre de dépannage est utile dans les deux cas d'utilisation suivants :

  - **Cas d'utilisation 1** : dans le cadre de l'autovérification, si CurlAnalytics échoue, une règle de pare-feu est créée. Cette règle de pare-feu ouvre un port 443 et vérifie sa connectivité à Analytics. Si ce n'est pas le cas, cela signifie que le serveur Analytics n'est pas accessible et que le script sort d'ici. Réexécutez le script une fois que la connectivité à Citrix Analytics Service est rétablie.

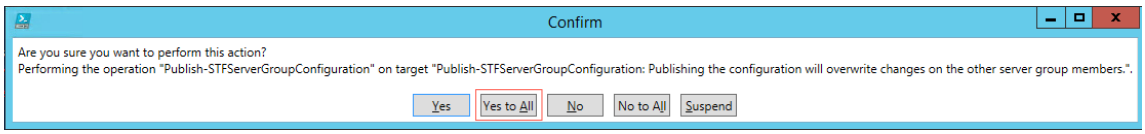
- **Cas d'utilisation 2** : si le cURL fonctionne correctement et que le site StoreFront ne s'affiche pas dans l'interface graphique, l'administrateur doit télécharger le fichier .zip de l'outil DebugView depuis Download DebugView, le décompresser et le placer dans le dossier **Téléchargements**. Le script PowerShell désinstalle d'abord Citrix Analytics Service s'il est déjà configuré. Il active la journalisation Verbose. Ensuite, il démarre l'outil DebugView et réinstalle Citrix Analytics Service. Enfin, il arrête DebugView et désactive la journalisation Verbose.

Les journaux des vues de débogage peuvent être capturés et partagés avec le support Citrix. L'administrateur Citrix poursuit le débogue et essaie de découvrir le problème et de le résoudre. Les journaux sont générés et enregistrés sous forme de fichier journal dans le dossier DebugView.

Vous devez partager les trois fichiers journaux suivants avec l'administrateur Citrix :

- Le fichier journal DebugView (Downloads \ DebugView \ log)
- Fichier journal StoreFront (C:\Program Files\Citrix\Receiver StoreFront\Admin\trace)
- Le fichier journal CAS. Ces journaux sont générés dans le cadre de l'exécution du script et sont enregistrés dans le dossier **Téléchargements > cas-logs** .

Pour un groupe de serveurs, la `PublishConfiguration` commande s'exécute automatiquement lorsque le script tente de déconnecter ou d'intégrer StoreFront. La commande PublishConfiguration permet de publier la configuration de StoreFront sur tous les serveurs de ce StoreFront. Vous pouvez voir une fenêtre contextuelle pour confirmer cette action. Sélectionnez le bouton **Oui pour tout**.



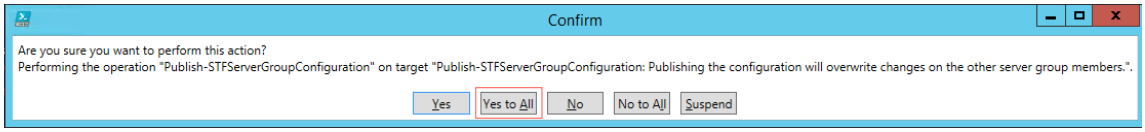
- **DeboardStoreFront** : le paramètre DeboardStorefront est utilisé pour déconnecter le serveur StoreFront de Citrix Analytics Service. Utilisez la commande suivante pour exécuter DeBoardStoreFront :

```
.\Manage-CitrixAnalytics.ps1 –param DeboardStoreFront
```

Le script PowerShell supprime d'abord toutes les configurations du service Citrix Analytics de StoreFront et vérifie que la suppression est réussie. Ensuite, il vérifie si le ServerGroup est présent, puis publie la configuration afin que les configurations supprimées soient publiées sur l'ensemble du StoreFront. Enfin, il invoque DeleteSiteOnboarded. Si le site n'est pas supprimé de l'interface utilisateur du service Citrix Analytics, vous devez supprimer manuellement le site StoreFront avec le déploiement de StoreFront et depuis la carte de site de l'application Workspace dans le cadre du déploiement de StoreFront.

Pour un groupe de serveurs, la commande PublishConfiguration s'exécute automatiquement à

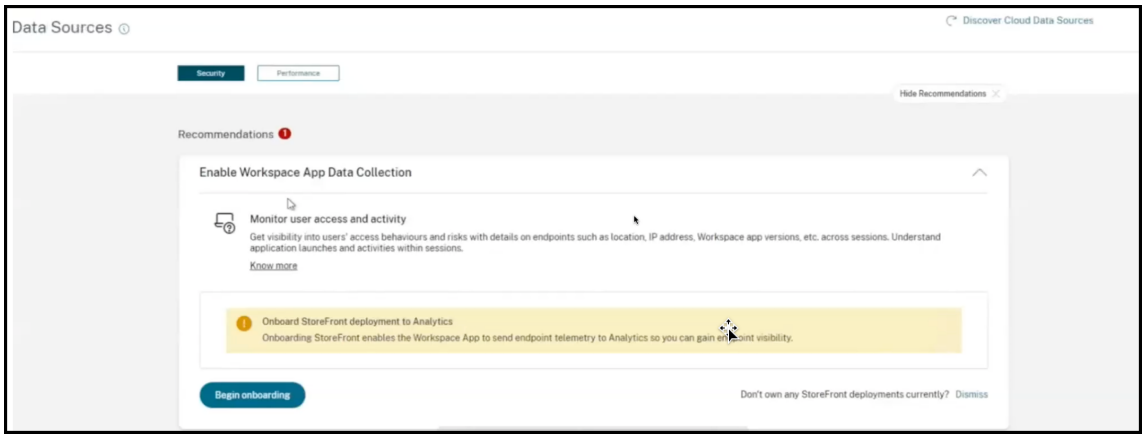
partir du script afin de publier la configuration StoreFront sur tous les serveurs de ce StoreFront. Vous pouvez voir une fenêtre contextuelle pour confirmer cette action. Sélectionnez le bouton **Oui pour tout**.



Connexion à l'aide du panneau de recommandations

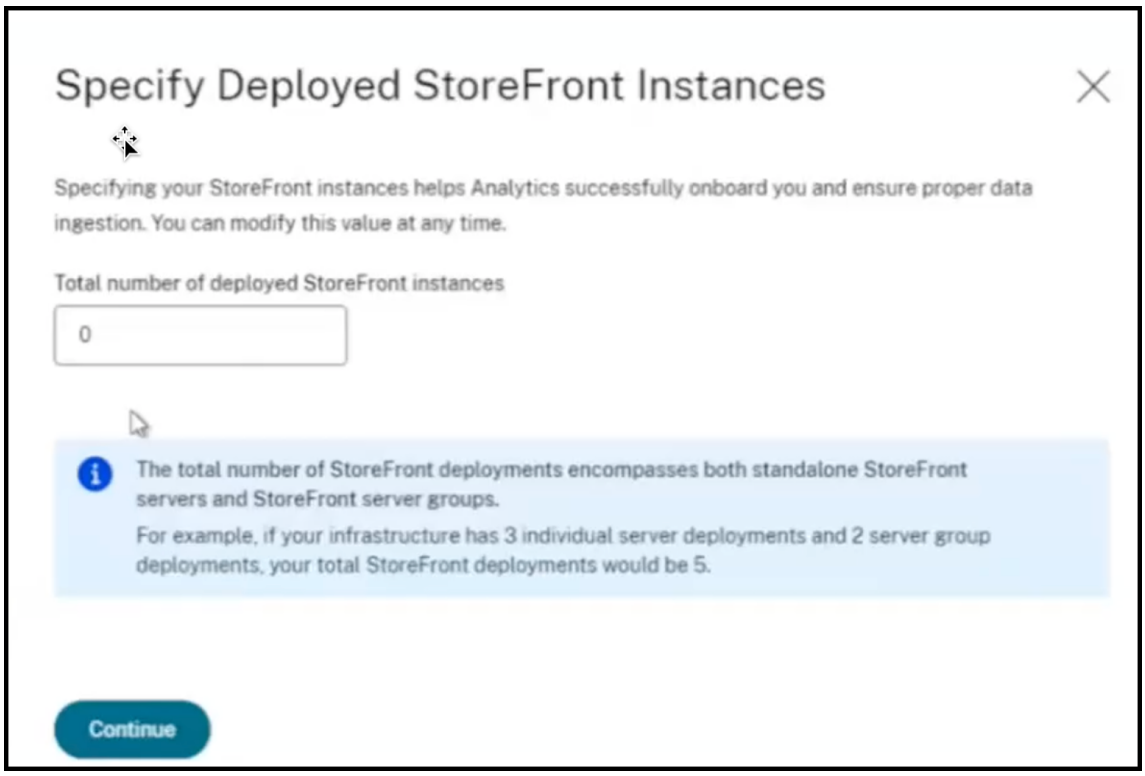
Le panneau **Recommandations** de la page **Sources de données** informe l'utilisateur sur l'importance de l'intégration des sources de données. Il permet à l'utilisateur d'intégrer facilement les sources de données et offre également à l'utilisateur la possibilité de vérifier et de s'assurer qu'il a intégré toutes les sources de données disponibles.

1. Si vous utilisez l'offre Security Analytics, sélectionnez **Paramètres > Sources de données > Sécurité**.
2. Si vous utilisez l'offre Performance Analytics, accédez à **Paramètres > Sources de données > Performances**.
3. Sur la page **Sources de données**, consultez les informations et les recommandations du panneau **Recommandations** pour intégrer le déploiement de Storefront.



> **Remarque**
>
> L'intégration d'une source de données StoreFront permet à l'application Workspace d'envoyer des données de télémétrie sur la visibilité des terminaux à Analytics.

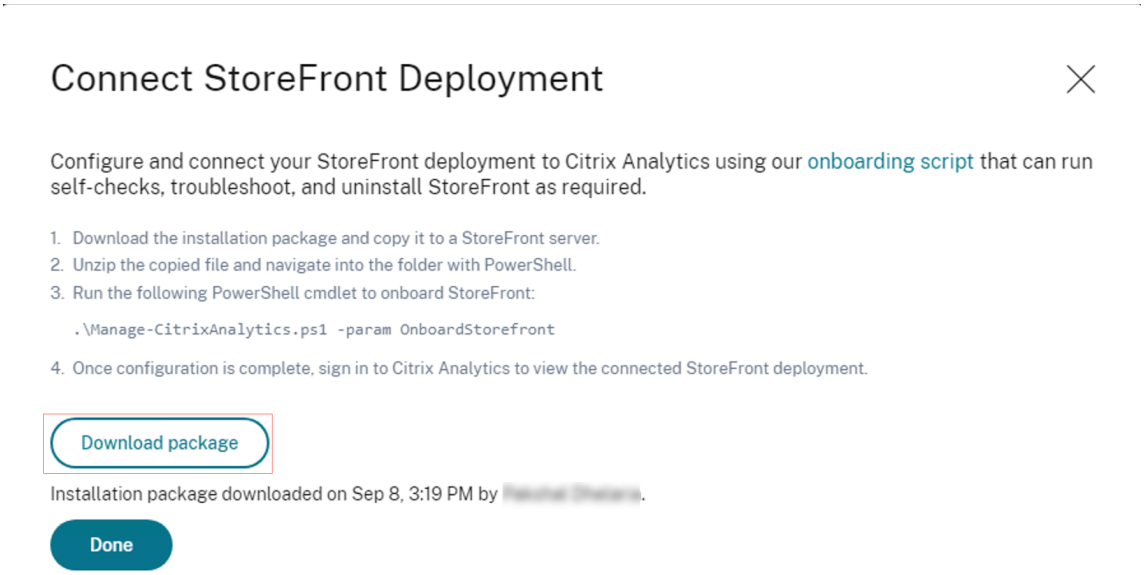
4. Cliquez sur **Commencer l'intégration**. La page **Spécifier les instances Storefront déployées** s'affiche.



5. Pour vous assurer qu'Analytics intègre correctement la source de données, spécifiez le **nombre total d'instances StoreFront déployées**.

   > **Remarque :**
   >
   > Le **nombre total d'instances StoreFront déployées** est le nombre total de groupes StoreFront et non le nombre de serveurs StoreFront individuels.

6. Cliquez sur **Continuer**. L'assistant d'intégration de StoreFront ou la fenêtre contextuelle **Connect StoreFront Deployment** s'affiche.
7. Sur la page de **déploiement de Connect StoreFront**, cliquez sur Télécharger le package pour télécharger le package d'installation.



> **Remarques**
>
> Le fichier contient des informations sensibles. Conservez le fichier dans un endroit sûr et sécurisé.
>
> Vous pouvez télécharger un package et l'utiliser pour intégrer un seul groupe StoreFront. Si vous possédez plusieurs groupes StoreFront, vous devez télécharger le package séparément pour chaque groupe StoreFront. Une fois l'intégration d'un groupe StoreFront terminée à l'aide d'un package, téléchargez à nouveau le package et poursuivez l'intégration du groupe StoreFront suivant.
>
> Si l'intégration de StoreFront n'est pas terminée correctement dans les deux jours avec un package en raison d'un problème, vous devez télécharger à nouveau un nouveau package au bout de deux jours. Parce que la clé contenue dans le package expirera si elle n'est pas intégrée correctement dans les deux jours.

8. Pour configurer le déploiement de StoreFront,
   a) Copiez le package d'installation sur le serveur StoreFront.
   b) Décompressez le fichier copié et accédez au dossier dans PowerShell.
   c) Exécutez la commande suivante pour intégrer StoreFront :

      ```
      .\Manage-CitrixAnalytics.ps1 –param OnboardStorefront
      ```

   d) Ouvrez le serveur StoreFront et exécutez le script PowerShell.
   e) Si le site StoreFront n'apparaît pas dans l'interface graphique de Citrix Analytics Service, exécutez la commande suivante :

      ```
      Execute iisreset
      ```


f) Enregistrez et vérifiez l'ID de cluster disponible dans le script PowerShell.

g) Une fois la configuration terminée, connectez-vous à Citrix Analytics pour consulter le déploiement StoreFront connecté.

9. Une fois la configuration terminée, cliquez sur **Terminé**.

Si vous procédez à l'intégration via le panneau **Recommandations**, le système extrait le nombre de déploiements StoreFront que vous avez intégrés au service Citrix Analytics. Le panneau **Recommandations** apparaît et vous pouvez consulter les déploiements StoreFront intégrés. Vous pouvez consulter le message dans le panneau **Recommandations** et cliquer sur **Marquer comme terminé**.

> **Remarque**
>
> Le panneau **Recommandations** et les messages ne disparaissent que lorsque tous les déploiements Storefront déclarés sont intégrés.

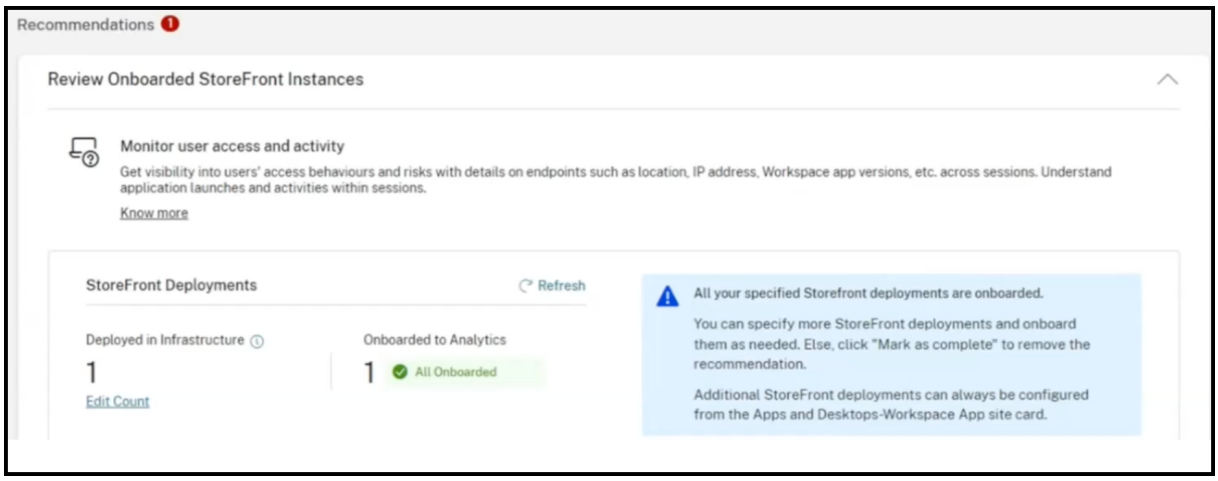
1. Cliquez **sur Activer le traitement des données** pour permettre à Citrix Analytics de traiter les données.

Consulter le panneau des recommandations

Vous pouvez comparer le nombre de déploiements StoreFront déclarés au nombre de déploiements StoreFront intégrés dans le panneau **Recommandations** .

Si le nombre de déploiements StoreFront déclarés est identique au nombre de déploiements StoreFront intégrés, un message All Onboarding apparaît indiquant que **tous les déploiements StoreFront sont** intégrés. Vous pouvez consulter le message dans le panneau **Recommandations** et cliquer sur **Marquer comme terminé**.

> **Remarque**
>
> Si vous souhaitez intégrer d'autres déploiements StoreFront, cliquez sur **Afficher les étapes d'intégration**. L'assistant d'intégration de StoreFront ou la fenêtre contextuelle **Connect StoreFront Deployment** réapparaissent.



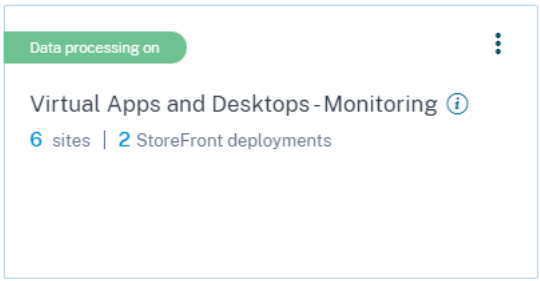
Si le nombre de déploiements StoreFront déclarés est inférieur au nombre de déploiements StoreFront intégrés, cliquez sur **Modifier le nombre**et la page **Spécifier les instances Storefront déployées** s'affiche. Vous pouvez ensuite saisir le **nombre total d'instances StoreFront déployées**, puis cliquer sur **Continuer**. L'assistant d'intégration de StoreFront ou la fenêtre contextuelle **Connect StoreFront Deployment** s'affiche à nouveau. Suivez les étapes pour intégrer d'autres déploiements StoreFront.

> **Remarque :**
>
> Le **nombre total d'instances StoreFront déployées** est le nombre total de groupes StoreFront et non le nombre de serveurs StoreFront individuels.

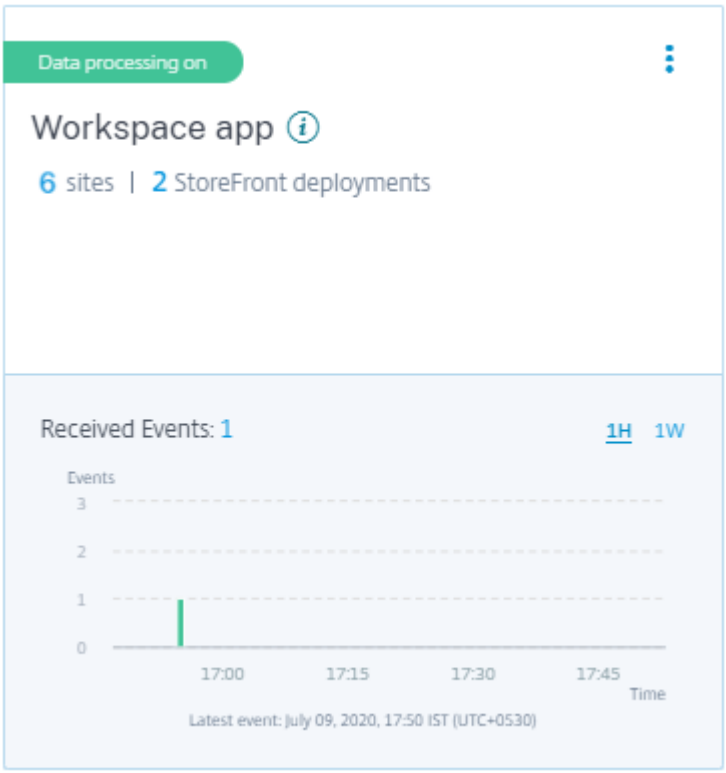
Afficher les déploiements StoreFront connectés

Les déploiements StoreFront apparaissent sur la carte de site uniquement si la configuration est réussie. La fiche de site indique le nombre de déploiements StoreFront qui ont établi des connexions avec Citrix Analytics.

- Si vous utilisez l'offre Performance Analytics, les informations suivantes s'affichent sur la carte de site **Surveillance des applications et des postes** de travail :

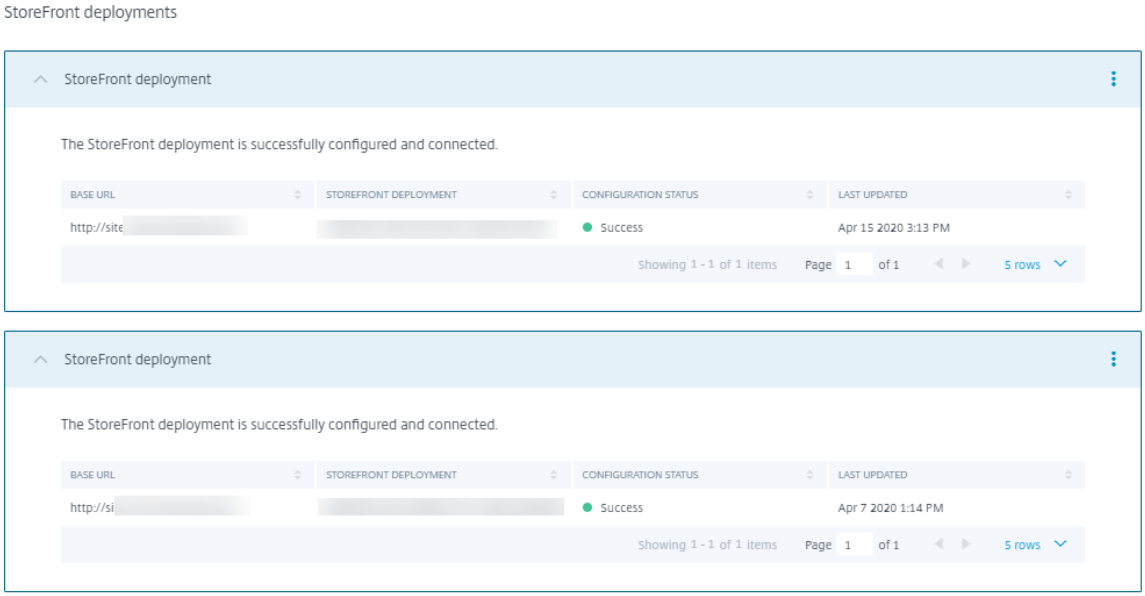


- Si vous utilisez l'offre Security Analytics, les informations suivantes s'affichent sur la fiche de site de **l'application Workspace** :



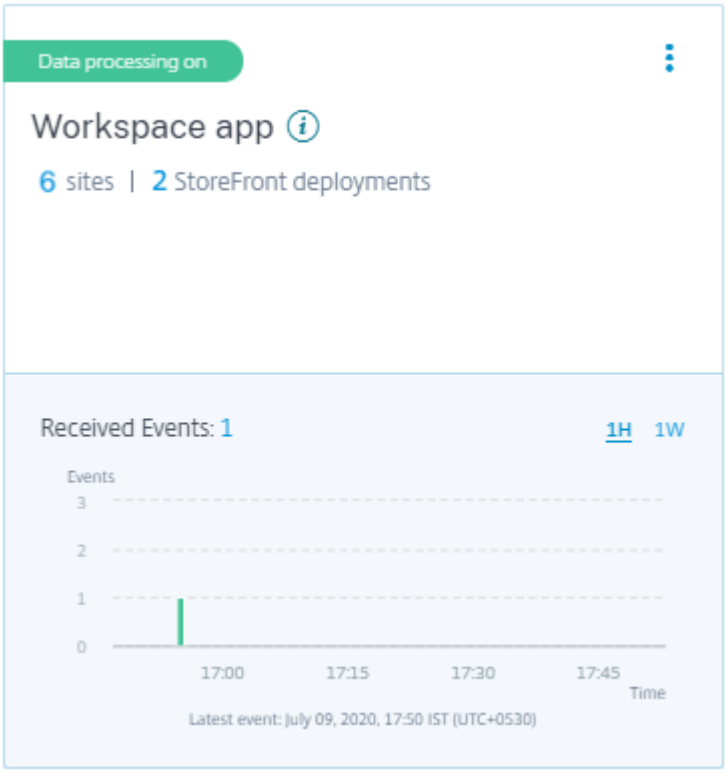
Cliquez sur le nombre de déploiements StoreFront sur la fiche de site pour afficher les groupes de serveurs.

Chaque déploiement StoreFront est représenté par une URL de base et un ID ServerGroupID.



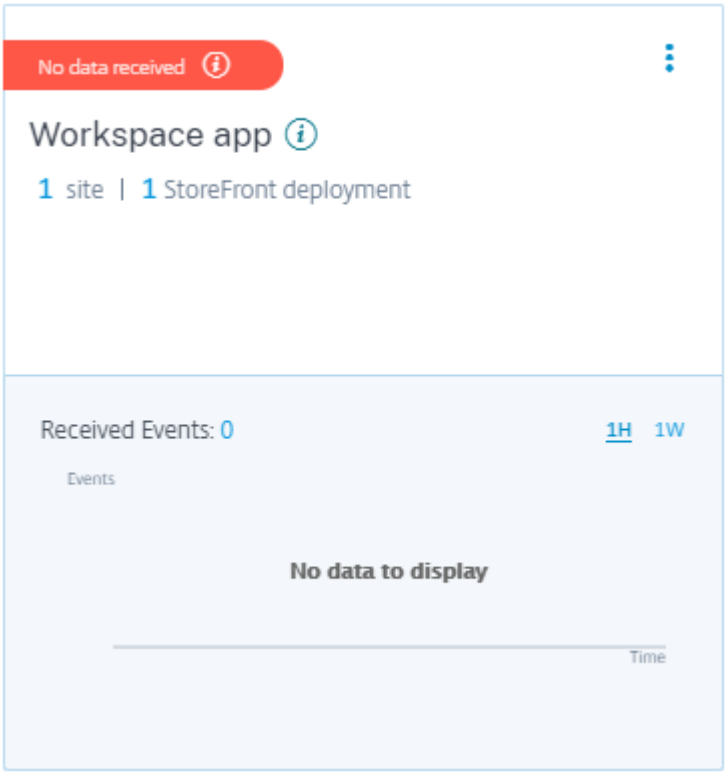
Si vous utilisez l'offre Security Analytics, la fiche de site affiche également les informations suivantes concernant les événements reçus :

- Les événements reçus des déploiements StoreFront au cours de la dernière heure, qui est la sélection de l'heure par défaut. Vous pouvez également sélectionner 1 semaine (1 W) et afficher les données. Cliquez sur le nombre d'événements reçus pour afficher les événements sur la page de recherche en libre-service .



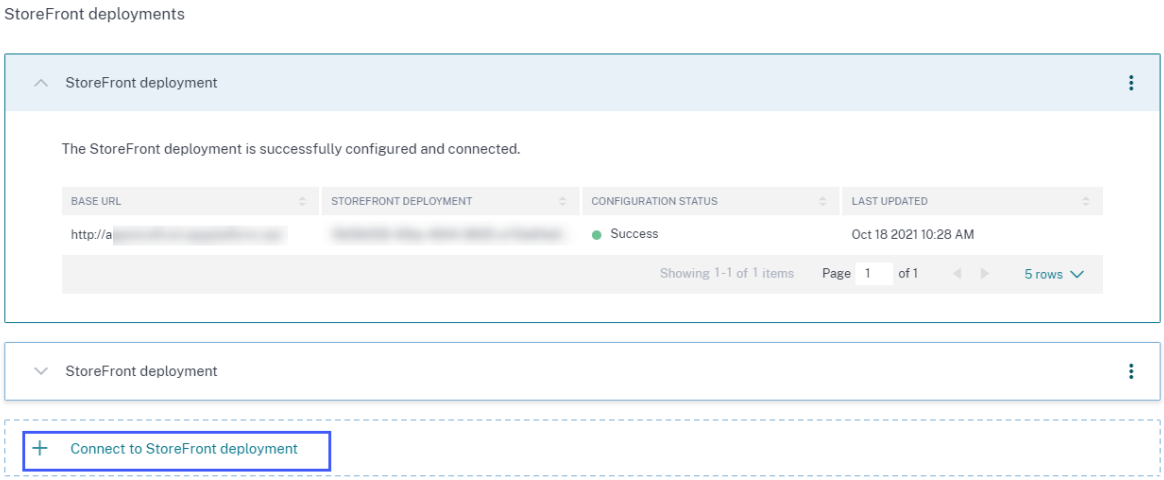
- Une fois que vous avez activé le traitement des données, la carte de site peut afficher l'état **No data received** (Aucune donnée reçue). Cet état apparaît pour deux raisons :

  1. Si vous avez activé le traitement des données pour la première fois, les événements mettent un certain temps à atteindre le hub d'événements dans Citrix Analytics. Lorsque Citrix Analytics reçoit les événements, l'état passe à **Data processing on** (Traitement des données activé). Si l'état ne change pas après un certain temps, actualisez la page **Sources de données** .
  2. Citrix Analytics n'a reçu aucun événement de la source de données au cours de la dernière heure.



Ajouter ou supprimer des déploiements StoreFront

Pour ajouter un déploiement StoreFront, cliquez sur **Se connecter aux déploiements StoreFront** dans la section **Déploiements StoreFront** . Téléchargez le fichier de configuration et suivez les étapes pour configurer un déploiement StoreFront.



Pour arrêter la transmission d'événements à partir d'un déploiement StoreFront configuré et le supprimer de Citrix Analytics, procédez comme suit :

1. Accédez au déploiement StoreFront que vous souhaitez supprimer de Citrix Analytics. Exécutez la commande suivante pour supprimer les paramètres de configuration de votre serveur StoreFront :

```
Remove-STFCasConfiguration
```

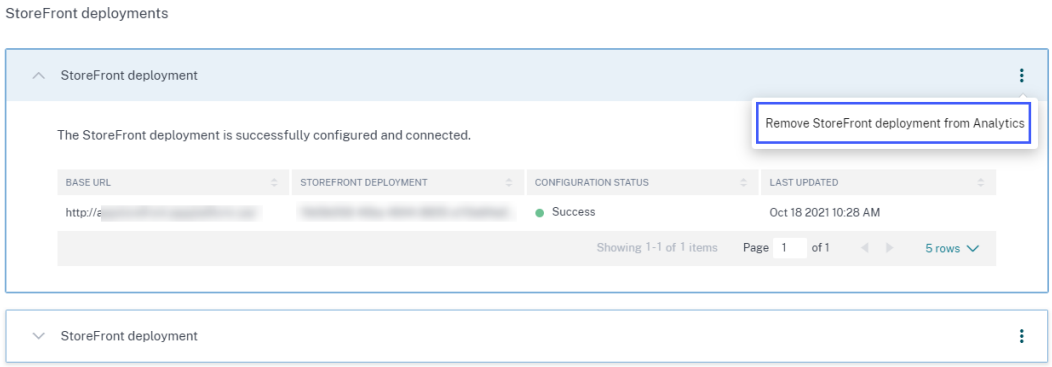
2. Si vous utilisez le déploiement multiserveur, exécutez la commande suivante pour propager les modifications et supprimer les paramètres de configuration de tous les serveurs du groupe de serveurs StoreFront :

```
Publish-STFServerGroupConfiguration
```

3. Exécutez la commande suivante pour vérifier que les paramètres de configuration ont bien été supprimés. La commande ne renvoie rien si les paramètres ont été supprimés avec succès.

```
Get-STFCasConfiguration
```

4. Reconnectez-vous à Citrix Analytics et choisissez le déploiement StoreFront dans la section **Déploiements StoreFront** . Cliquez sur les points de suspension verticaux () et sélectionnez **Supprimer les déploiements StoreFront d'Analytics**.



> **Remarque**
>
> Exécutez les commandes spécifiées sur le déploiement StoreFront avant de le supprimer de Citrix Analytics. Si vous ne parvenez pas à exécuter les commandes, Citrix Analytics continue de recevoir les événements et le déploiement StoreFront est ajouté à nouveau lors du prochain cycle de regroupement d'événements.

Configurer un déploiement StoreFront hébergé sur un serveur Web qui utilise un proxy HTTP

Si un StoreFront est hébergé sur un serveur Web qui utilise un proxy Web pour se connecter à Internet, le magasin doit être configuré manuellement pour s'enregistrer auprès de Citrix Analytics. Cette configuration nécessite l'ajout d'une section <system.net> au fichier web.config du magasin. Vous

devez configurer chaque magasin du déploiement StoreFront qui envoie des événements à Citrix Analytics.

Il existe deux méthodes pour ajouter la section <system.net> au fichier web.config du magasin :

- Définissez la configuration du proxy de magasin via PowerShell pour un ou plusieurs magasins (méthode recommandée).
- Ajoutez manuellement une section <system.net> au fichier web.config du magasin.

Pour plus d'informations sur ces méthodes, consultez l'article Configurer StoreFront pour utiliser un proxy Web pour contacter Citrix Cloud et s'inscrire auprès de Citrix Analytics dans la documentation StoreFront.

Gouvernance des données

December 7, 2023

Cette section fournit des informations concernant la collecte, le stockage et la conservation des journaux par le service Citrix Analytics. Tous les termes en majuscules qui ne sont pas définis dans la section Définitions ont la signification spécifiée dans le contrat Citrix End User Services Agreement.

Citrix Analytics est conçu pour fournir aux clients un aperçu des activités de leur environnement informatique Citrix. Citrix Analytics permet aux administrateurs de sécurité de choisir les journaux qu'ils souhaitent surveiller et de prendre des mesures dirigées en fonction de l'activité consignée. Ces informations aident les administrateurs de sécurité à gérer l'accès à leurs environnements informatiques et à protéger le contenu client dans l'environnement informatique du client.

Résidence de données

Les journaux Citrix Analytics sont conservés séparément des sources de données et sont agrégés dans plusieurs environnements Microsoft Azure Cloud, situés aux États-Unis, dans l'Union européenne et dans les régions sud de l'Asie-Pacifique. Le stockage des journaux dépend de la région d'accueil sélectionnée par les administrateurs Citrix Cloud lors de l'intégration de leurs organisations à Citrix Cloud. Par exemple, si vous choisissez la **région européenne** lors de l'intégration de votre organisation à Citrix Cloud, les journaux Citrix Analytics sont stockés dans des environnements Microsoft Azure au sein de l'Union européenne.

Pour plus d'informations, consultez Citrix Cloud Services Customer Content and Log Handling andGeographical Considerations.

Collecte des données

Les services Citrix Cloud sont instrumentés pour transmettre des journaux à Citrix Analytics. Les journaux sont collectés à partir des sources de données suivantes :

- Citrix ADC (local) avec abonnement à NetScaler Application Delivery Management
- Citrix Endpoint Management
- Citrix Gateway (local)
- Fournisseur d'identité Citrix
- Citrix Secure Browser
- Citrix Secure Private Access
- de Citrix Virtual Apps and Desktops
- Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service)
- Microsoft Active Directory
- Microsoft Graph Security

Transmission de données

Les journaux Citrix Cloud sont transmis en toute sécurité à Citrix Analytics. Lorsque l'administrateur de l'environnement client active explicitement Citrix Analytics, ces journaux sont analysés et stockés dans une base de données client. Il en va de même pour les sources de données de de Citrix Virtual Apps and Desktops
sur lesquelles Citrix Workspace est configuré.

Pour les sources de données Citrix ADC, la transmission du journal est lancée uniquement lorsque l'administrateur active explicitement Citrix Analytics pour la source de données spécifique.

Contrôle des données

Les journaux envoyés à Citrix Analytics peuvent être activés ou désactivés à tout moment par l'administrateur.

Lorsque cette option est désactivée pour les sources de données locales Citrix ADC, la communication entre la source de données ADC particulière et Citrix Analytics s'arrête.

Lorsque cette option est désactivée pour les autres sources de données, les journaux de la source de données particulière ne sont plus analysés et stockés dans Citrix Analytics.

Rétention des données

Les journaux Citrix Analytics sont conservés sous une forme identifiable pendant 13 mois ou 396 jours maximum. Tous les journaux et les données analytiques associées, telles que les profils de risque utilisateur, les détails du score de risque utilisateur, les détails des événements de risque utilisateur, la liste de surveillance des utilisateurs, les actions utilisateur et le profil utilisateur, sont conservés pendant cette période.

Par exemple, si vous avez activé Analytics sur une source de données le 1er janvier 2021, les données collectées le 1er janvier 2021 seront conservées par défaut dans Citrix Analytics jusqu'au 31 janvier 2022. De même, les données collectées le 15 janvier 2021 seront conservées jusqu'au 15 février 2022, et ainsi de suite.

Ces données sont stockées pour la période de rétention des données par défaut, même après avoir désactivé le traitement des données pour la source de données ou après avoir supprimé la source de données de Citrix Analytics.

Citrix Analytics supprime tout le contenu client 90 jours après l'expiration de l'abonnement ou la période d'essai.

Exportation de données

Cette section explique les données exportées depuis Citrix Analytics for Security et Citrix Analytics for Performance.

Citrix Analytics for Performance collecte et analyse les mesures de performance des sources de données.

Vous pouvez télécharger les données depuis la page de recherche en libre-service sous forme de fichier CSV.

Citrix Analytics for Security collecte les événements utilisateur provenant de différents produits (sources de données). Ces événements sont traités pour fournir une visibilité sur le comportement risqué et inhabituel des utilisateurs. Vous pouvez exporter ces données traitées relatives aux informations sur les risques des utilisateurs et aux événements des utilisateurs vers votre service de gestion des informations et des événements système (SIEM).

Actuellement, les données peuvent être exportées de deux manières à partir de Citrix Analytics for Security :

- Intégration de Citrix Analytics for Security à votre service SIEM
- Téléchargement des données de la page de recherche en libre-service sous forme de fichier CSV.

Lorsque vous intégrez Citrix Analytics for Security à votre service SIEM, les données sont envoyées à votre service SIEM à l'aide de la rubrique Kafka vers le nord ou d'un connecteur de données basé sur Logstash.

Actuellement, vous pouvez intégrer les services SIEM suivants :

- Splunk (en vous connectant via le module complémentaire Citrix Analytics)
- Tout service SIEM prenant en charge les connecteurs de données basés sur Kafka Topic ou Logstash tels qu'Elasticsearch et Microsoft Azure Sentinel

Vous pouvez également exporter les données vers votre service SIEM à l'aide d'un fichier CSV. Dans la page de recherche en libre-service, vous pouvez afficher les données (événements utilisateur) d'une source de données et télécharger ces données sous forme de fichier CSV. Pour plus d'informations sur le fichier CSV, consultez la section Recherche en libre-service.

> **Important**
>
> Une fois les données exportées vers votre service SIEM, Citrix n'est pas responsable de la sécurité, du stockage, de la gestion et de l'utilisation des données exportées dans votre environnement SIEM.

Vous pouvez activer ou désactiver la transmission de données de Citrix Analytics for Security vers votre service SIEM.

Pour plus d'informations sur les données traitées et l'intégration SIEM, consultez Intégration de la gestion des informations et des événements de sécurité (SIEM) et Format de données Citrix Analytics pour SIEM.

Annexe sur la sécurité des Services Citrix

Des informations détaillées concernant les contrôles de sécurité appliqués à Citrix Analytics, y compris l'accès et l'authentification, la gestion des programmes de sécurité, la continuité des activités et la gestion des incidents, sont incluses dans l'exposition Citrix Services Security Exhibit.

Définitions

Le contenu client désigne toutes les données téléchargées sur un compte client à des fins de stockage ou les données dans un environnement client auquel Citrix a accès pour fournir des services.

Journal désigne un enregistrement des événements liés aux services, y compris les enregistrements qui mesurent les performances, la stabilité, l'utilisation, la sécurité et l'assistance.

Services désigne les services Citrix Cloud décrits ci-dessus aux fins de Citrix Analytics.

Accord de collecte de données

En téléchargeant vos données vers Citrix Analytics et en utilisant les fonctionnalités de Citrix Analytics, vous acceptez et consentez à ce que Citrix puisse collecter, stocker, transmettre, maintenir, traiter et utiliser des informations techniques, utilisateur ou connexes concernant vos produits et services Citrix.

Citrix traite toujours les informations reçues conformément à la stratégie de confidentialité de Citrix.

Annexe : journaux collectés

- Journaux Citrix Analytics for Security
- Journaux Citrix Analytics for Performance

Journaux Citrix Analytics for Security

Journaux généraux

En général, les journaux Citrix Analytics contiennent les points de données d'identification d'en-tête suivants :

- Header Keys
- Device Identification
- Identification
- Adresse IP
- Organization
- Produit
- Product Version
- System Time
- Tenant Identification
- Type
- User: Email, Id, SAM Account Name, Domain, UPN
- Version

Journaux de Citrix Endpoint Management Service

Les journaux de Citrix Endpoint Management Service contiennent les points de données suivants :

- Conformité
- Corporate Owned
- Device Id
- Device Model
- Type d'appareil
- Geo Latitude
- Geo Longitude
- Nom d'hôte
- IMEI
- Adresse IP
- Jailbroken
- Last Activity
- Management Mode
- Système d'exploitation
- Operating System Version
- Platform Information
- Raison
- Serial Number
- Supervisé

Journaux Citrix Secure Private Access

- AAA User Name
- Auth Policy Action Name
- Authentication Session ID
- Request URL
- URL Category Policy Name
- VPN Session ID

- Vserver IP
- AAA User Email ID
- Actual Template Code
- App FQDN
- Nom de l'application
- App Name Vserver LS
- Application Flags
- Authentication Type
- Authentication Stage
- Authentication Status Code
- Adresse IPv4 Dst du serveur dorsal
- Adresse IPv4 du serveur principal
- Adresse IPv6 du serveur principal
- Category Domain Name
- Category Domain Source
- IP du client
- Client MSS
- Client Fast Retx Count
- Client TCP Jitter
- Client TCP Packets Retransmited
- Client TCP RTO Count
- Client TCP Zero Window Count
- Clt Flow Flags Rx
- Clt Flow Flags Tx
- Clt TCP Flags Rx
- Clt TCP Flags Tx
- Connection Chain Hop Count
- Connection Chain ID
- Egress Interface

- Exporting Process ID
- Flow Flags Rx
- Flow Flags Tx
- HTTP Content Type
- HTTP Domain Name
- HTTP Req Authorization
- HTTP Req Cookie
- HTTP Req Forw FB
- HTTP Req Forw LB
- HTTP Req Host
- HTTP Req Method
- HTTP Req Rcv FB
- HTTP Req Rcv LB
- HTTP Req Referer
- HTTP Req URL
- HTTP Req XForwarded For
- HTTP Res Forw FB
- HTTP Res Forw LB
- HTTP Res Location
- HTTP Res Rcv FB
- HTTP Res Rcv LB
- HTTP Res Set Cookie
- HTTP Rsp Len
- HTTP Rsp Status
- HTTP Transaction End Time
- HTTP Transaction ID
- IC Cont Grp Name
- IC Flags
- IC No Store Flags

- IC Policy Name
- Ingress Interface Client
- NetScaler Gateway Service App ID
- NetScaler Gateway Service App Name
- NetScaler Gateway Service App Type
- NetScaler Partition ID
- Observation Domain ID
- Observation Point ID
- Origin Res Status
- Origin Rsp Len
- Protocol Identifier
- Rate Limit Identifier Name
- Record Type
- Responder Action Type
- Response Media Type
- Srv Flow Flags Rx
- Srv Flow Flags Tx
- Srvr Fast Retx Count
- Srvr TCP Jitter
- Srvr TCP Packets Retransmitted
- Srvr TCP Rto Count
- Srvr TCP Zero Window Count
- SSL Cipher Value BE
- SSL Cipher Value FE
- SSL Client Cert Size BE
- SSL Client Cert Size FE
- SSL Clnt Cert Sig Hash BE
- SSL Clnt Cert Sig Hash FE
- SSL Err App Name

- SSL Err Flag
- SSL FLags BE
- SSL FLags FE
- SSL Handshake Error Msg
- SSL Server Cert Size BE
- SSL Server Cert Size FE
- SSL Session ID BE
- SSL Session ID FE
- SSL Sig Hash Alg BE
- SSL Sig Hash Alg FE
- SSL Srvr Cert Sig Hash BE
- SSL Srvr Cert Sig Hash FE
- SSL iDomain Category
- SSL iDomain Category Group
- SSL iDomain Name
- SSL iDomain Reputation
- SSL iExecuted Action
- SSL iPolicy Action
- SSL iReason For Action
- SSL iURL Set Matched
- SSL iURL Set Private
- Subscriber Identifier
- Svr Tcp Flags Rx
- Svr Tcp Flags Tx
- Tenant Name
- Tracing Req Parent Span ID
- Tracing Req Span ID
- Tracing Trace ID
- Trans Clt Dst IPv4 Address

- Trans Clt Dst IPv6 Address
- Trans Clt Dst Port
- Trans Clt Flow End Usec Rx
- Trans Clt Flow Fin Usec Tx
- Trans Clt Flow Start Usec Rx
- Trans Clt Flow Start Usec Tx
- Trans Clt IPv4 Address
- Trans Clt IPv6 Address
- Trans Clt Packet Tot Cnt Rx
- Trans Clt Packet Tot Cnt Tx
- Trans Clt RTT
- Trans Clt Src Port
- Trans Clt Tot Rx Oct Cnc
- Trans Clt Tot Tx Oct Cnc
- Trans Info
- Trans Srv Dst Port
- Trans Srv Packet Tot Cnt Rx
- Trans Srv Packet Tot Cnt Tx
- Trans Srv Src Port
- Trans Svr Flow End Usec Rx
- Trans Svr Flow End Usec Tx
- Trans Svr Flow Start Usec Rx
- Trans Svr Flow Start Usec Tx
- Trans Svr RTT
- Trans Svr Tot Rx Oct Cnc
- Trans Svr Tot Tx Oct Cnc
- Transaction ID
- URL Category
- URL Category Group

- URL Category Reputation
- URL Category Action Reason
- URL Set Matched
- URL set Private
- URL Object ID
- VLAN Number

Journaux Citrix Virtual Apps and Desktops et Citrix DaaS

Les journaux Citrix Virtual Apps and Desktops et Citrix DaaS contiennent les points de données suivants :

- Nom de l'application
- Navigateur
- ID client
- Détails : taille du format, type de format, initiateur, résultat
- ID de l'appareil
- Type d'appareil
- Commentaires
- Identifiant du commentaire
- Nom du fichier
- Chemin du fichier
- Taille du fichier
- Équivaut à
- Jailbroken
- Détails de la tâche : nom du fichier, format, taille
- Emplacement : estimé, latitude, longitude

  > **Remarque**
  >
  > Les informations de localisation sont fournies au niveau de la ville et du pays et ne représentent pas une géolocalisation précise.

- Long CMD Line

- Module File Path
- Operation
- Système d'exploitation
- Platform Extra Information
- Printer Name
- Question
- ID de question
- SaaS App Name
- Session Domain
- Session Server Name
- Session User Name
- Session GUID
- Timestamp
- Time Zone: Bias, DST, Name
- Nombre total d'exemplaires imprimés
- Nombre total de pages imprimées
- Type
- URL
- User Agent

Journaux de Citrix ADC

Les journaux Citrix ADC contiennent les points de données suivants :

- Container
- Fichiers
- Format
- Type

Journaux Citrix DaaS Standard pour Azure

Les journaux Citrix DaaS Standard pour Azure contiennent les points de données suivants :

- Nom de l'application
- Navigateur
- Détails : taille du format, type de format, initiateur, résultat
- Device Id
- Type d'appareil
- Nom du fichier
- Chemin du fichier
- Taille du fichier
- Jailbroken
- Détails de la tâche : nom du fichier, format, taille
- Emplacement : estimé, latitude, longitude

  > **Remarque**
  >
  > Les informations de localisation sont fournies au niveau de la ville et du pays et ne représentent pas une géolocalisation précise.

- Long CMD Line
- Module File Path
- Operation
- Système d'exploitation
- Platform Extra Information
- Printer Name
- SaaS App Name
- Session Domain
- Session Server Name
- Session User Name
- Session GUID
- Timestamp
- Time Zone: Bias, DST, Name

- Type
- URL
- User Agent

Journaux du fournisseur d'identités Citrix

- User Login:
  - Authentication Domains: Name, Product, IdP Type, IdP Display Name
    - IdP Properties: App, Auth Type, Customer Id, Client Id, Directory, Issuer, Logo, Resources, TID
    - Extensions:
      - Workspace: Background Color, Header Logo, Logon Logo, Link Color, Text Color, StoreFront Domains
      - ShareFile: Customer Id, Customer Geo
      - Long Lived Token: Enabled, Expiry Type, Absolute Expiry Seconds, Sliding Expiry Seconds
  - Authentication Result: User Name, Error Message
  - Sign-in Message: Client Id, Client Name
  - User Claim: AMR, Access Token Hash, Aud, Auth Time, CIP Cred, Auth Alias, Auth Domains, Groups, Product, System Aliases, Email, Email Verified, Exp, Family Name, Given Name, IAT, IdP, ISS, Locale, Name, NBF, SID, Sub
    - Auth Alias Claims: Name, Value
    - Directory Context: Domain, Forrest, Identity Provider, Tenant Id
    - User: Customers, Email, OID, SID, UPN
    - IdP Extra Fields: Azure AD OID, Azure AD TID
- User Logoff: Client Id, Client Name, Nonce, Sub
- Client Update: Action, Client Id, Client Name

Journaux de Citrix Gateway

- Événements de transaction :

- ICA App: Record Type, Actual Template Code, Observation Domain Id, Observation Point Id, Exporting Process Id, ICA Session Guid, MSI Client Cookie, Flow Id Rx, ICA Flags, Connection Id, Padding Octets Two, ICA Device Serial Number, IP Version 4, Protocol Identifier, Source IPv4 Address Rx, Destination IPv4 Address Rx, Source Transport Port Rx, Destination Transport Port Rx, ICA Application Start up Duration, ICA Launch Mechanism, ICA Application Start up Time, ICA Process ID Launch, ICA Application Name, ICA App Module Path, ICA Application Termination Type, ICA Application Termination Time, Application Name App Id, ICA App Process ID Terminate, ICA App
- ICA Event: Record Type, Actual Template Code, Source IPv4 Address Rx, Destination IPv4 Address Rx, ICA Session Guid, MSI Client Cookie, Connection Chain ID, ICA Client Version, ICA Client Host Name, ICA User Name, ICA Domain Name, Logon Ticket Setup, Server Name, Server Version, Flow Id Rx, ICA Flags, Observation Point Id, Exporting Process Id, Observation Domain Id, Connection Id, ICA Device Serial Number, ICA Session Setup Time, ICA Client IP, NS ICA Session Status Setup, Source Transport Port Rx, Destination Transport Port Rx, ICA Client Launcher, ICA Client Type, ICA Connection Priority Setup, NS ICA Session Server Port, NS ICA Session Server IP Address, IPv4, Protocol Identifier,Connection Chain Hop Count, Access Type
- ICA Update: Record Type, Actual Template Code, Observation Domain Id, Observation Point Id, Exporting Process Id, ICA Session Guid, MSI Client Cookie, Flow Id Rx,ICA Flags, Connection Id, ICA Device Serial Number, IPv4, Protocol Identifier, Padding Octets Two, ICA RTT, Client Side RX Bytes, Client Side Packets Retransmit, Server Side Packets Retransmit, Client Side RTT, Client Side Jitter, Server Side Jitter, ICA Network Update Start Time, ICA Network Update End Time, Client Side SRTT, Server Side SRTT,Client Side Delay, Server Side Delay, Host Delay, Client Side Zero Window Count, Server Side Zero Window Count, Client Side RTO Count, Server Side RTO Count, L7 Client Latency, L7 Server Latency, App Name App Id, Tenant Name, ICA Session Update Begin Sec, ICA Session Update End Sec, ICA Channel Id 1, ICA Channel Id 2, ICA Channel Id 2 Bytes, ICA Channel Id 3, ICA Channel Id 3 Bytes, ICA Channel Id 4, ICA Channel Id 4 Bytes, ICA Channel Id 5, ICA Channel Id 5 Bytes
- AppFlow Config: Record Type, Actual Template Code, Observation Domain Id, Observation Point Id, Exporting Process Id, System Rule Flag 1, System Safety Index, AppFlow Profile Relaxed Flags, AppFlow Profile Block Flags, AppFlow Profile Log Flags, AppFlow Profile Learn Flags, AppFlow Profile Stats Flags, AppFlow Profile None Flags, AppFlow App Name Id, AppFlow Profile Sign Disabled, AppFlow Profile Sign Block Count, AppFlow Profile Sign Log Count, AppFlow Profile Sign Stat Count, AppFlow Incarnation Number,AppFlow Sequence Number, AppFlow Profile Sign Auto Update, AppFlow Safety Index, AppFlow App Safety Index, AppFlow Profile Sec Checks Safety Index, AppFlow Profile Type, Iprep App Safety Index, AppFlow Profile Name, AppFlow Sig Name, AppFlow App Name Ls, AppFlow Sig Rule ID1, AppFlow Sig Rule ID2, AppFlow Sig Rule ID3, AppFlow Sig Rule ID4, AppFlow

Sig Rule ID5, AppFlow Sig Rule Enabled Flags, AppFlow Sig Rule Block Flags, AppFlow Sig Rule Log Flags, AppFlow Sig Rule File Name, AppFlow Sig Rule Category1, AppFlow Sig Rule Logstring1, AppFlow Sig Rule Category2, AppFlow Sig Rule Logstring2, AppFlow Sig Rule Category3, AppFlow Sig Rule Category4, AppFlow Sig Rule Logstring4, AppFlow Sig Rule Category5, AppFlow Sig Rule LogString5

- AppFlow: Actual Template Code, Observation Domain Id, Observation Point Id, Exporting Process Id, Transaction Id, Appfw Violation Occurred Time, App Name App Id, Appfw Violation Severity, Appfw Violation Type, Appfw Violation Location, Appfw Violation Threat Index, Appfw NS Longitude, Appfw NS Latitude, Source IPv4 Address Rx, Appfw Http Method, Appfw App Threat Index, Appfw Block Flags, Appfw Transform Flags, Appfw Violation Profile Name, Appfw Session Id, Appfw Req Url, Appfw Geo Location, Appfw Violation Type Name 1, Appfw Violation Name Value 1, Appfw Sig Category 1, Appfw Violation Type Name 2, Appfw Violation Name Value 2, Appfw Sig Category 2, Appfw Violation Type Name 3, Appfw Violation Name Value 3, Appfw Sig Category3, Appfw Req X Forwarded For, Appfw App Name Ls,App Name Ls, Iprep Category, Iprep Attack Time, Iprep Reputation Score, Iprep NS Longitude, Iprep NS Latitude, Iprep Severity, Iprep HTTP Method, Iprep App Threat Index, Iprep Geo Location, Tcp Syn Attack Cntr, Tcp Slow Ris Cntr, Tcp Zero Window Cntr, Appfw Log Expr Name, Appfw Log Expr Value, Appfw Log Expr Comment
- VPN: Actual Template Code, Observation Domain Id, Access Insight Flags, Observation Point Id, Exporting Process Id, Access Insight Status Code, Access Insight Timestamp, Authentication Duration, Device Type, Device ID, Device Location, App Name App Id, App Name App Id1, Source Transport Port Rx, Destination Transport Port Rx, Authentication Stage, Authentication Type, VPN Session ID, EPA Id, AAA User Name, Policy Name, Auth Agent Name, Group Name, Virtual Server FQDN, cSec Expression, Source IPv4 Address Rx, Destination IPv4 Address Rx, Cur Factor Policy Label, Next Factor Policy Label, App Name Ls, App Name 1 Ls,AAA User Email Id, Gateway IP, Gateway Port, Application Byte Count, VPN Session State, VPN Session Mode, SSO Auth Method, IIP Address, VPN Request URL, SSO Request URL, Backend Server Name, VPN Session Logout Mode, Logon Ticket File Info, STA Ticket, Session Sharing Key, Resource Name, SNIP Address, Temp VPN Session ID
- HTTP: Actual Template Code, Http Req Method, Http Req Url, Http Req User Agent, Http Content Type, Http Req Host, Http Req Authorization, Http Req Cookie, Http Req Referer, Http Res Set Cookie, Ic Cont Grp Name, Ic Flags, Ic Nostore Flags, Ic Policy Name, Response Media Type, Ingress Interface Client, Origin Res Status, Origin Rsp Len, Srv Flow Flags Rx, Srv Flow Flags Tx, Flow Flags Rx, Flow Flags Tx, App Name, Observation Point Id, Exporting Process Id, Observation Domain Id, Http Trans End Time, Transaction Id, Http Rsp Status, Trans Clt Ipv4 Address, Trans Clt Dst Ipv4 Address, Backend Svr Dst Ipv4 Address, Backend Svr Ipv4 Address, Http Rsp Len, Trans Svr RTT, Trans Clt RTT, Http Req Rcv FB, Http Req Rcv LB, Http Res Rcv FB, Http Res Rcv LB, Http Req Forw FB, Http Req Forw LB, Http Res Forw

FB, Http Res Forw LB, Http Req X Forwarded For, Http Domain Name, Http Res Location, Protocol Identifier, Egress Interface, Backend Svr Ipv6 Address, SSL Flags BE, SSL Flags FE, SSL Session IDFE, SSL Session IDBE, SSL Cipher Value FE, SSL Cipher Value BE, SSL Sig Hash Alg BE, SSL Sig Hash Alg FE, SSL Srvr Cert Sig Hash BE, SSL Srvr Cert Sig Hash FE, SSL Clnt Cert Sig Hash FE, SSL Clnt Cert Sig Hash BE, SSL Server Cert Size FE, SSL Server Cert Size BE, SSL Client Cert Size FE, SSL Client Cert Size BE, SSL Err App Name, SSL Err Flag, SSL Handshake Error Msg, Client IP, Virtual Server IP, Connection Chain Id, Connection Chain Hop Count, Trans Clt Tot Rx Oct Cnt, Trans Clt TotTx Oct Cnt, Trans Clt Src Port, Trans Clt Dst Port, Trans Srv Src Port, Trans Srv Dst Port, VLAN Number, Client Mss, Trans Info, Trans Clt Flow End Usec Rx, Trans Clt Flow End Usec Tx, Trans Clt Flow Start Usec Rx, Trans Clt Flow Start Usec Tx, Trans Svr Flow End Usec Rx, Trans Svr Flow End Usec Tx, Trans Svr Flow Start Usec Rx, Trans Svr Flow Start Usec Tx, Trans Svr Tot Rx Oct Cnt, Trans Svr Tot Tx Oct Cnt, Clt Flow Flags Tx, Clt Flow Flags Rx, Trans Clt Ipv6 Address, Trans Clt Dst Ipv6 Address, Subscriber Identifier, SSLi Domain Name, SSLi Domain Category, SSLi Domain Category Group, SSLi Domain Reputation, SSLi Policy Action, SSLi Executed Action, SSLi Reason For Action, SSLi URL Set Matched, SSLi URL Set Private, URL Category, URL Category Group, URL Category Reputation, Responder Action Type, URL Set Matched, URL Set Private, Category Domain Name, Category Domain Source, AAA User Name, VPN Session ID, Tenant Name

- Metric events:
  - VServer LB: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Representation, Schema Type, Time, CPU, GSLB Server, GSLB VServer, Interface, Memory Pool, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, VServer LB: RATE Si Tot Request Bytes, RATE Si Tot Requests, RATE Si Tot Response Bytes, RATE Si Tot Responses, RATE Si Tot Clt Ttlb Transactions, RATE Si Tot Clt Ttlb Pkt Rcvd, RATE Si Tot Clt Ttlb Pkt Sent, RATE Vsvr Tot Hits, Si Cur Clients, Si Cur Conn Established, Si Cur Servers, Si Cur State, Si Tot Request Bytes, Si Tot Responses, Si Tot Clt Ttlb, Si Tot Clt Ttlb Transactions, Si Tot Pkt Rcvd, Si Tot Pkt Sent, Si Tot Ttlb Frustrating Transactions, Si Tot Ttlb Tolerating Transactions, Vsvr Active Svcs, Vsvr Tot Hits, Vsvr tot Req Resp Invalid, Vsvr Tot Req Resp Invalid Dropped
  - CPU: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Representation, Schema Type, Time, Cc CPU Use GSLB Server, GSLB Vserver, Interface, Memory Pool, NetScaler, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, VServer Lb, VServer SSL, VServer User
  - Server Service Group: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Representation, Schema Type, Time, Cc CPU Use, GSLB Server, GSLB Vserver, Interface, Memory Pool, NetScaler, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, VServer Lb, VServer SSL, VServer User, Server Service Group: RATE Si Tot Request Bytes, RATE Si Tot

Requests, RATE Si Tot_Response Bytes, RATE Si Tot Responses, RATE Si Tot Clt Ttlb, RATE Si Tot Clt Ttlb Transactions, RATE Si Tot Svr Ttfb, RATE Si Tot Svr Ttfb Transactions, RATE Si Tot Svr Ttlb, RATE Si Tot Svr Ttlb Transactions, RATE Si Tot Ttlb Frustrating Transactions, RATE Si Tot Ttlb Tolerating Transactions, Si Cur State, Si Tot Request Bytes, Si Tot Requests, Si Tot Response Bytes, Si Tot Responses, Si Tot Clt Ttlb, Si Tot Clt Ttlb Transactions, Si Tot Svr Ttfb, Si Tot Svr Ttfb Transactions,Si Tot Svr Tlb, Si Tot Svr Ttlb Transactions, Si Tot Ttlb Frustrating Transactions, Si Tot Ttlb Tolerating Transactions

- Server SVC CFG: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Representation, Schema Type, Time, CPU Use, GSLB Server, GSLB Vserver, Interface, Memory Pool, NetScaler, VServer Authn, VServer Cr, VServer Cs, VServer Lb, VServer SSL, VServer User, Server Svc Cfg: RATE Si Tot Request Bytes, RATE Si Tot Requests, RATE Si Tot Response Bytes, RATE Si Tot Responses, Si Tot Clt Ttlb, RATE Si Tot Clt Ttlb Transactions, RATE Si Tot Pkt Rcvd, RATE Si Tot Pkt Sent, RATE Si Tot Svr Busy Err, RATE Si Tot Svr Ttfb, RATE Si Tot Svr Ttfb Transactions, RATE Si Tot Svr Ttlb, RATE Si Tot Svr Ttlb Transactions, RATE Si Tot Ttlb Frustrating Transactions, RATE Si Tot Ttlb Tolerating Transactions, Si Cur State, Si Cur Transport, Si Tot Request Bytes, Si Tot Requests, Si Tot Response Bytes, Si Tot Responses, Si Tot Clt Ttlb, Si Tot Clt Ttlb Transactions, Si Tot Pkt Rcvd, Si Tot Pkt Sent, Si Tot Svr Busy Err, Si Tot Svr Ttfb, Si Tot Svr Ttfb Transactions, Si Tot Svr Ttlb, Si Tot Svr Ttlb Transactions, Si Tot Ttlb Frustrating Transactions, Si Tot Ttlb Tolerating Transactions
- NetScaler: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Representation, Schema Type, Time, GSLB Server, GSLB VServer, Interface, Memory Pool, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, VServer Lb, VServer SSL, VServer User, NetScaler: RATE All Nic Tot Rx Mbits, RATE All Nic Tot Rx Mbits, RATE Dns Tot Queries, RATE Dns Tot Neg Nxdmn Entries,RATE Http Tot Gets, RATE Http Tot Others, RATE Http Tot Posts, RATE Http Tot Requests, RATE Http Tot Requests 1.0, RATE Http Tot Requests 1.1, RATE Http Tot Responses, RATE Http Tot Rx Request Bytes, RATE Http Tot Rx Response Bytes, RATE Ip Tot Rx Mbits, RATE Ip Tot Rx Bytes, RATE Ip Tot Rx Pkts, RATE Ip Tot Tx Mbits, RATE Ip Tot Tx Bytes, RATE Ip Tot Tx Pkts, RATE SSL Tot Dec Bytes, RATE SSL Tot Enc Bytes,RATE SSL Tot SSL Info Session Hits, RATE SSL Tot SSL Info Total Tx Count, RATE Tcp Err Rst, RATE Tcp Tot Client Open, RATE Tcp Tot Server Open, RATE Tcp Tot Rx Bytes, RATE Tcp Tot Rx Pkts, RATE Tcp Tot Syn, RATE Tcp Tot Tx Bytes, RATE Tcp Tot Tx Pkts, RATE Udp Tot Rx Bytes, RATE Udp Tot Rx Pkts, RATE Udp Tot Tx Bytes, RATE Udp Tot Tx Pkts, All Nic Tot Rx Mbits, All Nic Tot Tx Mbits, Cpu Use, Dns Tot Queries, Dns Tot Neg Nxdmn Entries, Http Tot Gets, Http Tot Others, Http Tot Posts, Http Tot Requests, Http Tot Requests1.0, Http Tot Requests1.1, Http Tot Responses, Http Tot Rx Request Bytes, Http Tot Rx Response Bytes, Ip Tot Rx Mbits, Ip Tot Rx Bytes, Ip Tot Rx Pkts, Ip Tot Tx Mbits, Ip Tot Tx Bytes, Ip Tot Tx Pkts, Mem Cur Free size, Mem Cur Free size Actual, Mem Cur Used size, Mem Tot Available, Mgmt Additional Cpu Use, Mgmt Cpu 0 Use, Mgmt Cpu Use, SSL Tot Dec Bytes, SSL Tot Enc Bytes, SSL Tot SSL Info Session Hits, SSL Tot SSL Info Total Tx

Count, Sys Cpus, Tcp Cur Client Conn, Tcp Cur Client Conn Closing, Tcp Cur Client Conn Est, Tcp Cur Server Conn, Tcp Cur Server Conn Closing, Tcp Cur Server Conn Est, Tcp Err Rst, Tcp Tot Client Open, Tcp Tot Server Open, Tcp Tot Rx Bytes, Tcp Tot Rx Pkts, Tcp Tot Syn, Tcp Tot Tx Bytes, Tcp Tot Tx Pkts, Udp Tot Rx Bytes, Udp Tot Rx Pkts, Udp Tot Tx Bytes, Udp Tot Tx Pkts

- Memory Pool: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Schema Type, Time, CPU, Gslb Server, Gslb VServer, Interface, NetScaler, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, VServer Lb, VServer SSL, VServer User, Memory Pool: Mem Cur Alloc Size, Mem Err Alloc Failed, Mem Tot Available
- Monitoring Service Binding: Bind Entity Name, Entity Name, NetScalerId, SchemaType, Time, CPU, Gslb Server, Gslb VServer, Interface, Memory Pool, NetScaler, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, Vserver Lb, VServer SSL, VServer User, Mon Service Binding: RATE Mon Tot Probes, Mon Tot Probes
- Interface: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Schema Type, Time, CPU, Gslb Server, Gslb VServer, Memory Pool, NetScaler, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, Vserver Lb, VServer SSL, VServer User, Interface: RATE NIC Tot Rx Bytes, RATE NIC Tot Rx Packets, RATE NIC Tot Tx Bytes, RATE NIC Tot Tx Packets, NIC Tot Rx Bytes, NIC Tot Rx Packets, NIC Tot Tx Bytes, NIC Tot Tx Packets
- VServer CS: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Schema Type, Time, CPU, Gslb Server, Gslb VServer, Memory Pool, NetScaler, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, Vserver Lb, VServer SSL, VServer User, VServer Cs: RATE Si Tot Request Bytes, RATE Si Tot Requests, RATE Si Tot Response Bytes, RATE Si Tot Responses, RATE Si Tot Clt Ttlb,RATE Si Tot Clt Ttlb Transactions, RATE Si Tot Pkt Rcvd, RATE Si Tot Pkt Sent, RATE Si Tot Ttlb Frustrating Transactions, RATE Si Tot Ttlb Tolerating Transactions, RATE Vsvr Tot Hits, Si Cur State, Si Tot Request Bytes, Si Tot Requests, Si Tot Response Bytes, Si Tot Responses, Si Tot Clt Ttlb, Si Tot Clt Ttlb Transactions, Si Tot Pkt Rvd, Si Tot Pkt Sent, Si Tot Ttlb Frustrating Transactions, Si Tot Tlb Tolerating Transactions, Vsvr Tot Hits, Vsvr Tot Req Resp Invalid, Vsvr Tot Req Resp Invalid Dropped

Journaux du navigateur sécurisé

- Application Post:
  - Logs before the published application: Authentication, Browser, Change Id, Created, Customer Name, Destination URL, E-Tag, Gateway Service Product Id, Session Id, Legacy Icon, Application Name, Policies, Published Application Id, Region, Resource Zone, Resource Zone Id, Subscription, Session Idle Timeout, Session Idle Timeout Warning, Watermark, Whitelist External, Whitelist Internal, Whitelist Redirect

  - Journaux après l'application publiée : Authentification, Navigateur, ID de modification, Créé, Nom du client, Destination, E-Tag, ID produit du service de passerelle, ID de session, Icône héritée, Nom de l'application, Stratégies, ID de l'application publiée, Région, Zone de ressource, ID de zone de ressource, Abonnement, Délai d'inactivité de session, Avertissement de délai d'inactivité de session, filigrane, URL externe de liste blanche, URL interne de liste blanche, URL de redirection de liste blanche

- Application Delete:

  - Logs before the published application: Authentication, Browser, Change Id, Created, Customer Name, Destination URL, E-Tag, Gateway Service Product Id, Session Id, Legacy Icon, Application Name, Policies, Published Application Id, Region, Resource Zone, Resource Zone Id, Subscription, Session Idle Timeout, Session Idle Timeout Warning, Watermark, Whitelist External, Whitelist Internal, Whitelist Redirect
  - Journaux après l'application publiée : Authentification, Navigateur, ID de modification, Créé, Nom du client, Destination, E-Tag, ID produit du service de passerelle, ID de session, Icône héritée, Nom de l'application, Stratégies, ID de l'application publiée, Région, Zone de ressource, ID de zone de ressource, Abonnement, Délai d'inactivité de session, Avertissement de délai d'inactivité de session, filigrane, URL externe de liste blanche, URL interne de liste blanche, URL de redirection de liste blanche

- Application Update:

  - Logs before the published application: Authentication, Browser, Change Id, Created, Customer Name, Destination URL, E-Tag, Gateway Service Product Id, Session Id, Legacy Icon, Application Name, Policies, Published Application Id, Region, Resource Zone, Resource Zone Id, Subscription, Session Idle Timeout, Session Idle Timeout Warning, Watermark, Whitelist External, Whitelist Internal, Whitelist Redirect
  - Journaux après l'application publiée : Authentification, Navigateur, ID de modification, Créé, Nom du client, Destination, E-Tag, ID produit du service de passerelle, ID de session, Icône héritée, Nom de l'application, Stratégies, ID de l'application publiée, Région, Zone de ressource, ID de zone de ressource, Abonnement, Délai d'inactivité de session, Avertissement de délai d'inactivité de session, filigrane, URL externe de liste blanche, URL interne de liste blanche, URL de redirection de liste blanche

- Entitlement Create:

  - Logs before the entitlement creation: Approved, Customer Id, Data Retention Days, End Date, Grace Period Days, Session Id, Product SKU, Quantity, Serial Numbers, Start Date, State, Type
  - Logs after the entitlement creation: Approved, Customer Id, Data Retention Days, End

Date, Grace Period Days, Session Id, Product SKU, Quantity, Serial Numbers, Start Date, State, Type

- Entitlement Update:
  - Logs before the entitlement update: Approved, Customer Id, Data Retention Days, End Date, Grace Period Days, Session Id, Product SKU, Quantity, Serial Numbers, Start Date, State, Type
  - Logs after the entitlement update: Approved, Customer Id, Data Retention Days, End Date, Grace Period Days, Session Id, Product SKU, Quantity, Serial Numbers, Start Date, State, Type
- Session Access Host: Accept Host, Client IP, Date Time, Host, Session, User Name
- Session Connect:
  - Logs before the session connection: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
  - Logs after the session connection: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
- Session Launch:
  - Logs before the session launch: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
  - Logs after the session launch: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
- Session Tick:
  - Logs before the session tick: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
  - Logs after the session tick: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name

Journaux de Microsoft Graph Security

- Tenant Id
- User Id
- Indicator Id
- Indicator UUID

- Event Time
- Create Time
- Category of alert
- Logon Location
- Logon IP
- Logon Type
- User Account Type
- Vendor Information
- Vendor Provider Information
- Vulnerability States
- Vulnerability Severity

Journaux de Microsoft Active Directory

- Tenant Id
- Collect Time
- Type
- Directory Context
- Groups
- Identité
- User Type
- Account Name
- Bad Password Count
- City
- Common Name
- Company
- Pays
- Days Until Password Expiry
- Department
- Description

- Nom d'affichage
- Distinguished Name
- E-mail
- Fax Number
- First Name
- Group Category
- Group Scope
- Home Phone
- Initials
- IP Phone
- Is Account Enabled
- Is Account Locked
- Is Security Group
- Last Name
- Manager
- Member of
- Mobile Phone
- Pager
- Password Never Expires
- Physical Delivery Office Name
- Post Office Box
- Postal Code
- Primary Group Id
- État
- Street Address
- Title
- User Account Control
- User Group List
- Nom d'utilisateur principal
- Work Phone

Journaux Citrix Analytics for Performance

- actionid
- actionreason
- actiontype
- adminfolder
- agentversion
- allocationtype
- applicationid
- applicationname
- applicationpath
- applicationtype
- applicationversion
- associateduserfullnames
- associatedusername
- associatedusernames
- associateduserupns
- authenticationduration
- autoreconnectcount
- autoreconnecttype
- AvgEndpointThroughputBytesReceived
- AvgEndpointThroughputBytesSent
- blobcontainer
- blobendpoint
- blobpath
- brokerapplicationchanged
- brokerapplicationcreated
- brokerapplicationdeleted
- brokeringdate
- brokeringduration

- brokerloadindex
- brokerregistrationstarted
- browsername
- catalogchangeevent
- catalogcreatedevent
- catalogdeletedevent
- catalogid
- catalogname
- catalogsync
- clientaddress
- clientname
- clientplatform
- clientsessionvalidatedate
- clientversion
- collecteddate
- connectedviahostname
- connectedviaipaddress
- connectionid
- connectioninfo
- connectionstate
- connectiontype
- controllerdnsname
- cpu
- cpuindex
- createddate
- currentloadindexid
- currentpowerstate
- currentregistrationstate
- currentsessioncount

- datetime
- deliverygroupadded
- deliverygroupchanged
- deliverygroupdeleted
- deliverygroupid
- deliverygroupmaintenancemodechanged
- deliverygroupname
- deliverygroupsync
- deliverytype
- deregistrationreason
- desktopgroupdeletedevent
- desktopgroupid
- desktopgroupname
- desktopkind
- disconnectcode
- disconnectreason
- disk
- diskindex
- dnsname
- domainname
- effectiveloadindex
- enddate
- errormessage
- establishmentdate
- eventreporteddate
- eventtime
- exitcode
- failurecategory
- failurecode

- failuredata
- failuredate
- failurereason
- failuretype
- faultstate
- functionallevel
- gpoenddate
- gpostartdate
- hdxenddate
- hdxstartdate
- hôte
- hostedmachineid
- hostedmachinename
- hostingservername
- hypervisorconnectionchangedevent
- hypervisorconnectioncreatedevent
- hypervisorid
- hypervisorname
- hypervisorsync
- icartt
- icarttms
- id
- idletime
- inputbandwidthavailable
- inputbandwidthused
- instancecount
- interactiveenddate
- interactivestartdate
- ipaddress

- isassigned
- isinmaintenancemode
- ismachinephysical
- ispendingupdate
- ispreparing
- isremotepc
- issecureica
- lastderegisteredcode
- launchedviahostname
- launchedviaipaddress
- lifecyclestate
- LinkSpeed
- logonduration
- logonenddate
- logonscriptsenddate
- logonscriptsstartdate
- logonstartdate
- long
- machineaddedtodesktopgroupevent
- machineassignedchanged
- machinecatalogchangedevent
- machinecreatedevent
- machinedeletedevent
- machinederegistrationevent
- machinednsname
- machinefaultstatechangeevent
- machinehardregistrationevent
- machineid
- machinemaintenancemodechangeevent

- machinename
- machinepvdstatechanged
- machineregistrationendedevent
- machineremovedfromdesktopgroupevent
- machinerole
- machinesid
- machineupdatedevent
- machinewindowsconnectionsettingchanged
- memory
- memoryindex
- modifieddate
- NGSConnector.ICAConnection.Start
- NGSConnector.NGSSyntheticMetrics
- NGSConnector.NGSPassiveMetrics
- NGSConnector.NGSSystemMetrics
- network
- networkindex
- networklatency
- networkinfoperiodic
- NetworkInterfaceType
- ostype
- outputbandwidthavailable
- outputbandwidthused
- path
- percentcpu
- persistentuserchanges
- powerstate
- processname
- profileloadenddate

- profileloadstartdate
- protocol
- provisioningschemeid
- provisioningtype
- publishedname
- registrationstate
- serversessionvalidatedate
- sessioncount
- sessionend
- sessionfailure
- sessionid
- sessionidlesince
- sessionindex
- sessionkey
- sessionstart
- sessionstate
- sessionsupport
- sessiontermination
- sessiontype
- sid
- SignalStrength
- siteid
- sitename
- startdate
- totalmemory
- triggerinterval
- triggerlevel
- triggerperiod
- triggervalue

- usedmemory
- userid
- userinputdelay
- username
- usersid
- vdalogonduration
- vdaprocessdata
- vdaresourcedata
- version
- vmstartenddate
- vmstartstartdate
- windowsconnectionsetting
- xd.SessionStart

Vue d'ensemble de la sécurité technique

April 12, 2024

Le service Analytics hébergé dans Citrix Cloud collecte des données sur les produits du portefeuille Citrix et les produits tiers. Ces produits sont appelés sources de données. Citrix Analytics prend en charge les sources de données dans le cloud et sur site. Les informations contenues dans ce document s'appliquent à Citrix Analytics et à ses sources de données.

Flux de données

Citrix Analytics découvre automatiquement les sources de données Citrix Cloud qui sont abonnées aux clients. Toutefois, les sources de données locales nécessitent une configuration supplémentaire pour s'intégrer à Citrix Analytics. Par exemple, vous devez ajouter vos sites Citrix Virtual Apps and Desktops à Citrix Workspace avant que Citrix Analytics puisse découvrir les sites. De même, Citrix Gateway sur site nécessite que vous configuriez un agent Citrix ADM. Pour plus d'informations sur l'activation de Citrix Analytics sur les sources de données, consultez Activer Analytics sur les sources de données Citrix.

Vous pouvez intégrer quelques produits tiers tels que Microsoft Graph Security et Microsoft Active Directory à Citrix Analytics. Pour plus d'informations, consultez les rubriques suivantes :

- Activer Analytics sur la sécurité de Microsoft Graph
- Intégrez Analytics à Microsoft Active Directory

Citrix Analytics peut également envoyer des informations de veille sur les risques à un environnement Splunk appartenant au client. Cette intégration nécessite le déploiement et la configuration du **module complémentaire Citrix Analytics pour Spunk** dans l'environnement Splunk. Pour plus d'informations, consultez la section Intégration de Splunk.

Sans le consentement du client, Citrix Analytics ne traite aucun événement reçu des sources de données. Pour traiter les événements provenant des sources de données, l'administrateur Analytics doit activer le traitement des données. Pour plus d'informations sur la collecte, le stockage et la conservation des données par Analytics, consultez Gouvernance des données.

Configuration réseau requise

- **Configuration requise pour les services Citrix Cloud** : pour utiliser les services Citrix Cloud, vous devez être en mesure de vous connecter aux adresses Citrix requises via le port HTTPS 443. Pour plus d'informations, consultez Exigences en matière de connectivité Internet.
- **Configuration requise pour Citrix Analytics** : vérifiez la configuration système requise avant d'utiliser Citrix Analytics. Outre la configuration requise pour Citrix Cloud, les adresses de point de terminaison suivantes doivent être accessibles via le port HTTPS 443 pour utiliser le service Citrix Analytics.

Point de terminaison	Région des États-Unis	Région de l'Union européenne	Région Asie-Pacifique Sud
Interface utilisateur d'administration	`https://analytics.cloud.com/`	`https://analytics-eu.cloud.com/`	`https://analytics-aps.cloud.com/`
Interface utilisateur d'administration (CDN)	`https://cas-api-cdn-ep.azureedge.net/`	`https://cas-api-cdn-ep-eu.azureedge.net/`	`https://cas-api-cdn-ep-aps.azureedge.net/`
Services d'API	`https://api.analytics.cloud.com/`	`https://api.analytics-eu.cloud.com/`	`https://api.analytics-aps.cloud.com/`
Services d'API (analyse des performances)	`https://api-a.was.cloud.com/`	`https://api-eu-a.was.cloud.com/`	`https://api-ap-s-a.was.cloud.com/`

Point de terminaison	Région des États-Unis	Région de l'Union européenne	Région Asie-Pacifique Sud
	https://api-b.was.cloud.com/	https://api-eu-b.was.cloud.com/	https://api-ap-s-b.was.cloud.com/
Obtenir une adresse IP publique	https://locus.analytics.cloud.com/	https://locus.analytics.cloud.com/	https://locus.analytics.cloud.com/
Event Hub (ne s'applique pas à l'agent Citrix ADM)	https://citrixanalyticseh-alias.servicebus.windows.net/ https://citrixanalyticseh2-alias.servicebus.windows.net/	https://citrixanalyticseheu-alias.servicebus.windows.net/	https://citrixanalyticsehaps-alias.servicebus.windows.net/
Event Hub (pour l'agent Citrix ADM)	https://cas-eh-ns-alias.servicebus.windows.net/ ethttps://cas-eh-ns2-alias.servicebus.windows.net/	https://cas-eh-ns-eu-alias.servicebus.windows.net/	https://cas-eh-ns-aps-alias.servicebus.windows.net/
Chargement en masse	https://casstoragebulk.blob.core.windows.net/	https://casstorebulkeu.blob.core.windows.net/	https://casstorebulkaps.blob.core.windows.net/

> **Remarque**
>
> Citrix Analytics a arrêté la prise en charge de TLS 1.0 et TLS 1.1 pour la plupart des points de terminaison précédents.

- **Installation de Citrix Cloud Connector** : certaines sources de données telles que Citrix Endpoint Management, Citrix Virtual Apps and Desktops et Microsoft Active Directory nécessitent

que vous installiez un Citrix Cloud Connector sur votre emplacement de ressources. Le Citrix Cloud Connector est un canal de communication entre Citrix Cloud et vos emplacements de ressources. Après avoir installé Citrix Cloud Connector, vous devez configurer les paramètres du proxy Web. Pour de plus amples informations, consultez la section Configuration du pare-feu et du proxy d'un Cloud Connector.

- **Points de terminaison Citrix Analytics pour l'intégration SIEM** : pour intégrer Citrix Analytics à votre solution de gestion des informations et des événements de sécurité (SIEM), assurez-vous que les points de terminaison suivants figurent dans la liste verte de votre réseau :

Point de terminaison	Région des États-Unis	Région de l'Union européenne	Région Asie-Pacifique Sud

Brokers Kafka	`casnb-0.citrix.com:9094`
	`casnb-1.citrix.com:9094`
	`casnb-2.citrix.com:9094`
	`casnb-3.citrix.com:9094`
		`casnb-eu-0.citrix.com:9094`
		`casnb-eu-1.citrix.com:9094`
		`casnb-eu-2.citrix.com:9094`
			`casnb-aps-0.citrix.com:9094`
			`casnb-aps-1.citrix.com:9094`
			`casnb-aps-2.citrix.com:9094`

Gestion des identités et des accès

- Pour accéder à Citrix Analytics, vous devez utiliser votre compte Citrix Cloud. Par défaut, Citrix Cloud utilise le fournisseur d'identité Citrix pour gérer les informations d'identité de tous les utilisateurs de votre compte Citrix Cloud. Vous pouvez également utiliser d'autres fournisseurs d'identité, comme indiqué dans Gestion des identités et des accès.
- Citrix Analytics prend en charge les autorisations d'administrateur délégués. Vous pouvez attribuer une autorisation d'administrateur en lecture seule à un utilisateur pour gérer Analytics dans votre entreprise. Pour plus d'informations, consultez Gérer les rôles d'administrateur.

Résidence de données

Citrix Cloud gère le plan de contrôle pour Citrix Analytics. Les données reçues des sources de données sont stockées dans plusieurs environnements Microsoft Azure. Ces environnements sont situés aux États-Unis, dans l'Union européenne et dans les régions du sud de l'Asie-Pacifique. L'emplacement de stockage dépend de la région d'origine sélectionnée par les administrateurs Citrix Cloud lors de

l'intégration de leurs organisations à Citrix Cloud. Pour plus d'informations, consultez les rubriques suivantes :

- Considérations géographiques
- Gouvernance des données

Protection des données

Citrix Analytics reçoit les données des sources de données Citrix Cloud abonnées, des sources de données locales et des produits tiers. Les données reçues sont traitées uniquement si le client dispose d'un droit Citrix Cloud et que l'administrateur Analytics a explicitement activé le traitement des données pour chacune des sources de données abonnées.

Citrix Analytics protège les données des clients à l'aide des mesures de sécurité suivantes :

- Authentification Citrix Cloud pour les utilisateurs Analytics. Pour plus d'informations, consultez Gestion des identités et des accès.
- Contrôles d'accès aux données basés sur les locataires appliqués par le service de données et la couche d'accès aux données.
- Forte isolation des données par client ou locataire dans tous les magasins de données du lac de données et de l'entrepôt de données.
- Transfert de données cryptées TLS entre les différents microservices et magasins de données, applicable aux points de terminaison publics (APTS/entrées/sorties) de la plate-forme et au sein de la plate-forme.
- Des normes élevées en matière de points de terminaison TLS. Les protocoles TLS 1.0 et TLS 1.1 sont désactivés.
- Stockage des données chiffrées à l'aide de clés de cryptage et de secrets stockés dans des coffres à clés appropriés.
- Contrôles d'accès puissants à la gestion des utilisateurs pour les opérations de service et le support tout en protégeant les journaux
- Analyse des vulnérabilités, détection des intrusions, protection contre les programmes malveillants, analyse des rootkits utilisés avec Azure Security Center.

Comme pour tous les services Citrix Cloud, la collecte de données est strictement soumise au contrat de service utilisateur final (EUSA). Pour plus d'informations, consultez les accords suivants :

- Contrats d'utilisation
- Stratégie de confidentialité Citrix

- Contrat de traitement des données Citrix
- Annexe sur la sécurité des Services Citrix
- Citrix Cloud Services : contenu client et gestion des journaux
- Informations de confidentialité et de conformité Citrix

Responsabilité de sécurité

Responsabilité de Citrix

Citrix est responsable de la sécurisation de toutes les infrastructures et données résidant dans les environnements cloud gérés par Citrix qui hébergent Citrix Analytics. Citrix est responsable de l'application de mises à jour logicielles régulières et de correctifs sur l'environnement cloud pour remédier aux vulnérabilités de sécurité.

Responsabilité du client

Les clients Citrix sont responsables de la sécurisation de leurs sources de données, des points d'application des stratégies et des systèmes de gestion des informations et des événements de sécurité (SIEM) intégrés à Citrix Analytics, notamment :

- Sources de données sur site détenues et gérées par les clients :
  - **Sources de données locales** : Citrix Gateway, Citrix Virtual Apps and Desktops, Microsoft Active Directory
  - **SIEM** : Splunk et tout autre produit tiers qui utilise les brokers Kafka pour lire les événements de Citrix Analytics.
- Informations d'identification d'administrateur fournies par le client pour gérer les services Citrix Cloud, y compris Citrix Analytics.
- Les comptes d'administrateur appartenant au client qui reçoivent des e-mails ou des notifications de la part des services Citrix Cloud.
- Informations d'identification d'administrateur fournies par le client pour le déploiement et l'intégration des agents tels que les agents Citrix ADM. L'accès à ces agents doit être restreint car ils stockent les clés localement pour communiquer avec Citrix Analytics.
- Informations d'identification générées par Citrix Analytics pour configurer le **module complémentaire Citrix Analytics pour Splunk**.
- Les appareils des utilisateurs finaux fonctionnant sous Windows, Mac, Android, iOS pour se connecter à Citrix Cloud ou Citrix Workspace et intégrés aux sources de données.

Pour plus d'informations sur les dispositions de sécurité, consultez les documents suivants :

- Guide de déploiement sécurisé pour la plate-forme Citrix Cloud
- Documentation Citrix Workspace
- Présentation technique de la sécurité pour Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service)
- Considérations de sécurité pour Citrix Virtual Apps and Desktops
- Sécuriser votre documentation de déploiement StoreFront
- Présentation technique de la sécurité pour Citrix Endpoint Management
- Documentation sur le service Citrix Secure Private Access
- Guide de déploiement sécurisé pour Citrix ADC
- Configuration système requise pour Citrix ADM

Configuration système requise

September 21, 2023

Avant de commencer à utiliser Citrix Analytics, vous devez consulter les informations de licence, la configuration logicielle requise et la configuration du navigateur.

Abonnements Citrix Analytics

Vous devez disposer d'abonnements valides pour utiliser les produits Analytics suivants :

- Citrix Analytics for Security
- Citrix Analytics for Performance

Pour de plus amples informations, consultez la section Services Citrix Cloud.

Exigences en matière de sources

Les sources de données sont les produits qui envoient des événements à Citrix Analytics. En fonction des offres Citrix Analytics que vous utilisez, les sources de données varient. Consultez les articles suivants pour consulter les sources de données prises en charge par chaque offre :

- Sources de données prises en charge par Citrix Analytics for Security
- Sources de données prises en charge par Citrix Analytics for Performance

Navigateurs pris en charge

Pour accéder à Citrix Analytics, votre poste de travail doit disposer du navigateur Web pris en charge suivant :

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

Gérer les rôles d'administrateur pour Citrix Analytics

May 2, 2023

Par défaut, un administrateur Citrix Cloud dispose d'autorisations d'accès complètes à tous les services abonnés sur son compte Citrix Cloud. Avec les autorisations d'accès complètes, l'administrateur peut utiliser toutes les fonctionnalités et fonctionnalités d'un service abonné.

En tant qu'administrateur Citrix Cloud disposant d'un accès complet, vous pouvez inviter d'autres administrateurs à accéder à votre compte Citrix Cloud pour gérer les services abonnés de votre organisation. Vous pouvez ensuite définir leurs autorisations d'accès et leur permettre de gérer des fonctionnalités spécifiques dans les services auxquels vous êtes abonné.

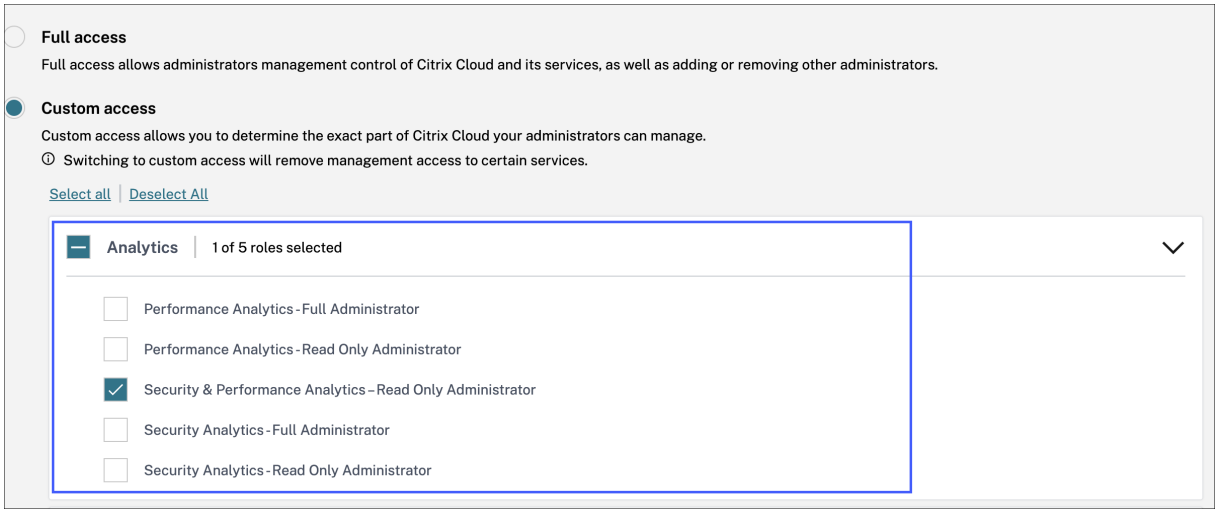
Les nouveaux administrateurs peuvent être ajoutés de deux manières :

1. Individuellement en tant qu'utilisateurs de Citrix Identity et d'Azure AD/Active Directory. Pour plus d'informations, consultez Gérer les administrateurs Citrix Cloud.
2. Utilisation de groupes dans Azure Active Directory. Pour plus d'informations, consultez Gérer les groupes d'administrateurs.

Les administrateurs peuvent se connecter à Citrix Cloud à l'aide de leurs comptes Citrix Cloud, Active Directory ou Azure Active Directory, accéder à des fonctionnalités spécifiques et effectuer des tâches en fonction de leurs rôles.

Pour Citrix Analytics, vous pouvez attribuer les rôles personnalisés suivants à vos administrateurs :

Rôle	Autorisation
Performance Analytics - Administrateur complet	Attribue une autorisation d'accès complet aux administrateurs Citrix Cloud de Performance Analytics.
Performance Analytics - Administrateur en lecture seule	Attribue une autorisation d'accès en lecture seule aux administrateurs Citrix Cloud de Performance Analytics.
Security & Performance Analytics - Administrateur en lecture seule	Attribue des autorisations d'accès en lecture seule aux administrateurs Citrix Cloud de Security Analytics et Performance Analytics.
Security Analytics - Administrateur complet	Attribue une autorisation d'accès complet aux administrateurs Citrix Cloud de Security Analytics.
Security Analytics - Administrateur en lecture seule	Attribue une autorisation d'accès en lecture seule aux administrateurs Citrix Cloud de Security Analytics.



Remarques

- Si vous sélectionnez plusieurs rôles pour un administrateur, le rôle dont l'accès est le plus élevé prend effet.
- Si l'accès est accordé à un utilisateur directement en tant qu'utilisateur et via un groupe Azure Active Directory, l'accès accordé individuellement à l'utilisateur prend effet.
- Les groupes Azure Active Directory peuvent uniquement être ajoutés en tant qu'administrateurs personnalisés. Le rôle d'administrateur à accès complet n'est pas disponible pour

> les groupes.
>
> - Les administrateurs ayant le rôle **Administrateur en lecture seule** qui était disponible auparavant sont renommés **Sécurité et performances - Administrateur en lecture seule**.
> - Les administrateurs dotés du rôle **Administrateur Security & Performance Analytics - Lecture seule** et **Performance Analytics - Administrateur en lecture seule** ne reçoivent aucune notification par e-mail de Citrix Analytics.

Pour plus d'informations sur les rôles spécifiques à l'offre, consultez les articles suivants :

- Gérer les rôles d'administrateur pour Performance Analytics
- Gérer les rôles d'administrateur pour Security Analytics

Mise en route

April 12, 2024

Ce document explique comment commencer à utiliser Citrix Analytics pour la première fois.

Étape 1 : Se connecter à Citrix Cloud

Pour utiliser Citrix Analytics, vous devez disposer d'un compte Citrix Cloud. Accédez à https://citrix.cloud.com et connectez-vous avec votre compte Citrix Cloud existant.

Si vous n'avez pas de compte Citrix Cloud, vous devez d'abord créer un compte Citrix Cloud ou rejoindre un compte existant créé par un autre membre de votre organisation. Pour obtenir des processus détaillés et des instructions sur la marche à suivre, consultez S'inscrire à Citrix Cloud.

Étape 2 : Accédez à Analytics

Vous pouvez accéder à Analytics de l'une des manières suivantes :

- **Demandez une version d'essai de l'offre Citrix Analytics**. Une fois connecté à Citrix Cloud, dans la section **Services disponibles**, sur la vignette **Analytics**, cliquez sur **Gérer** pour afficher la page de présentation d'Analytics.

  La page de présentation présente les offres d'analyse : **sécurité** et **performances**.

  - Pour les analyses de sécurité et les analyses de performance, cliquez sur **Demander un essai** pour utiliser la version d'essai de l'offre. Vous recevez un e-mail lorsque votre demande est approuvée et que la version d'essai est disponible. Vous pouvez utiliser l'essai

pendant une période maximale de 60 jours. Pour plus d'informations sur les essais de service, consultez la section Essais de service Citrix Cloud.

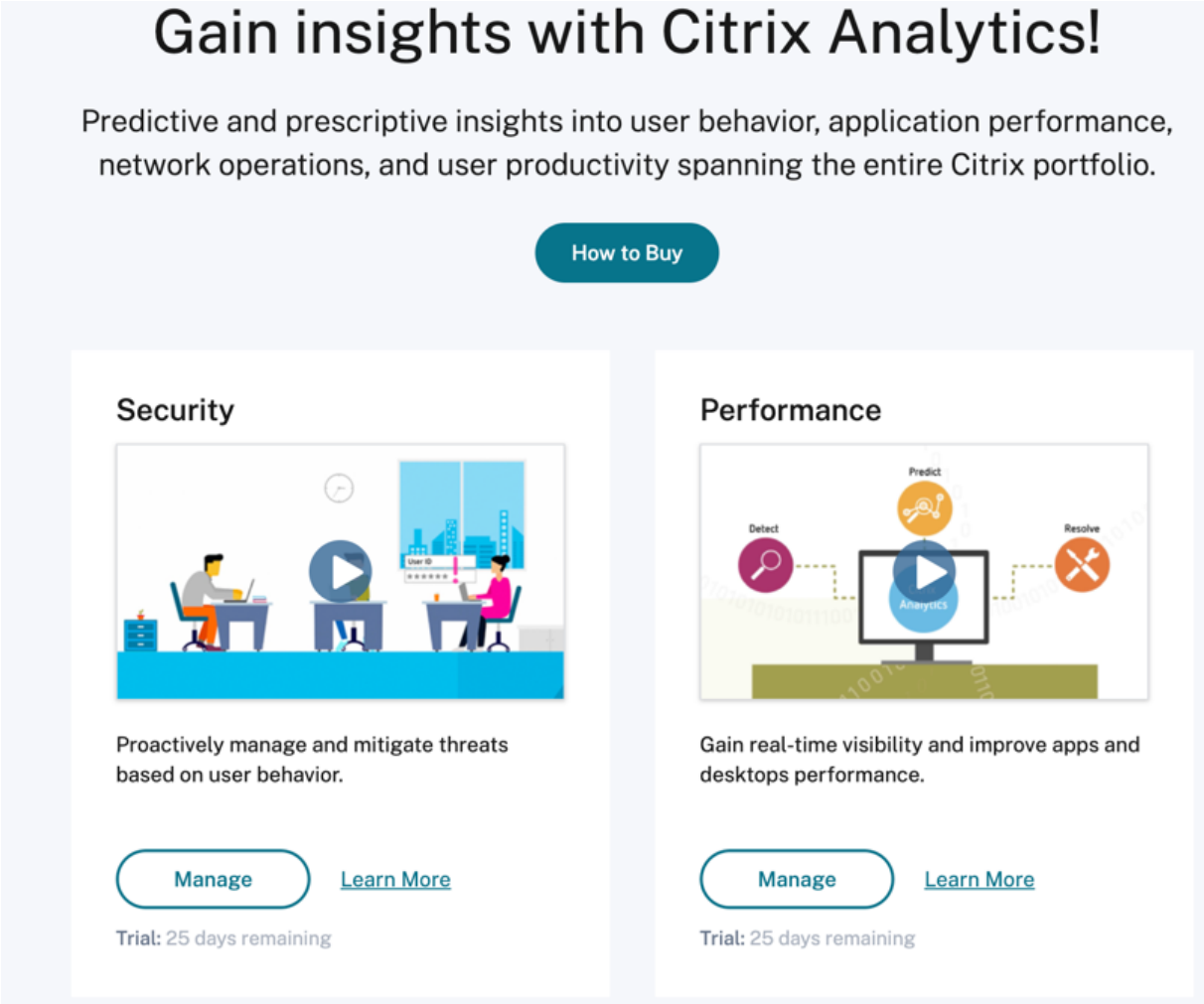
Sur la page Citrix Cloud, la vignette **Analytics** est déplacée vers la section **Mes services** .

- **Abonnez-vous à Citrix Analytics**. Vous pouvez acheter les abonnements Citrix Analytics suivants :
  - Citrix Analytics for Security
  - Citrix Analytics for Performance
  - Citrix Analytics pour la sécurité et les performances

  Citrix Analytics for Security et Citrix Analytics for Performance sont proposés en tant que service complémentaire avec les packages Citrix Workspace : Workspace Standard, Workspace Premium et Workspace Premium Plus. Pour de plus amples informations, consultez la section Services Citrix Cloud.

Étape 3 : Gérer Analytics

Pour les analyses de sécurité et les analyses de performance, une fois que vous avez souscrit les abonnements nécessaires ou que vous êtes autorisé à accéder à la version d'essai, sur la page d'aperçu d' Analytics, le bouton **Demander un essai** de l'offre passe à **Gérer**. Cliquez sur **Gérer** pour afficher le tableau de bord utilisateur correspondant à chaque offre.



Analytics découvre automatiquement les services Citrix Cloud (sources de données) associés à votre compte Citrix Cloud. Pour afficher les sources de données que vous avez découvertes, cliquez sur **Paramètres > Sources de données**, puis sur l'onglet requis, **Sécurité** ou **Performances**.

Pour plus d'informations sur chaque offre Analytics, consultez

- Citrix Analytics for Security
- Citrix Analytics for Performance

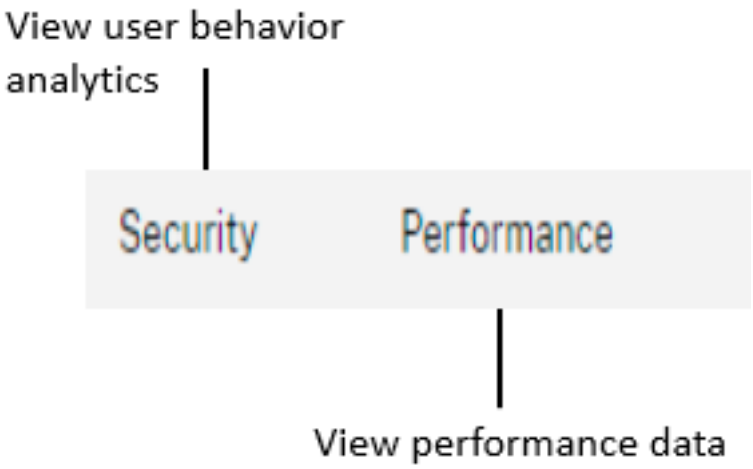
Familiarisation

May 6, 2022

Familiarisez-vous avec les principaux contrôles de l'interface utilisateur Analytics.

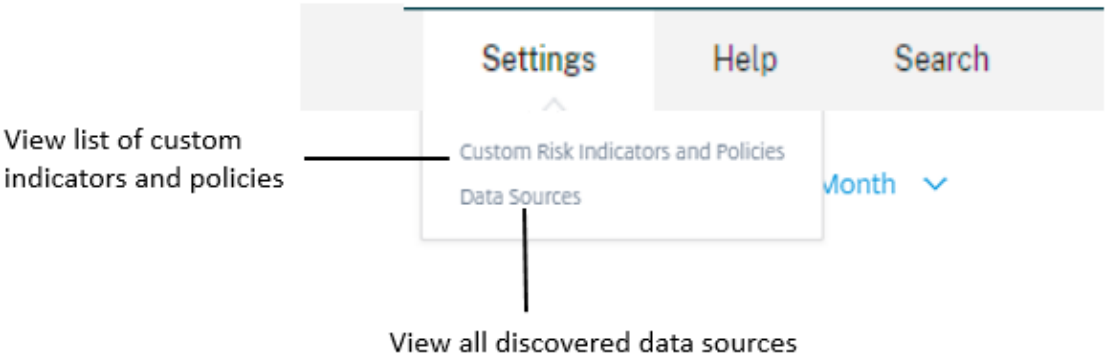
Barre supérieure

Accédez aux différentes offres Analytics dans la barre supérieure.

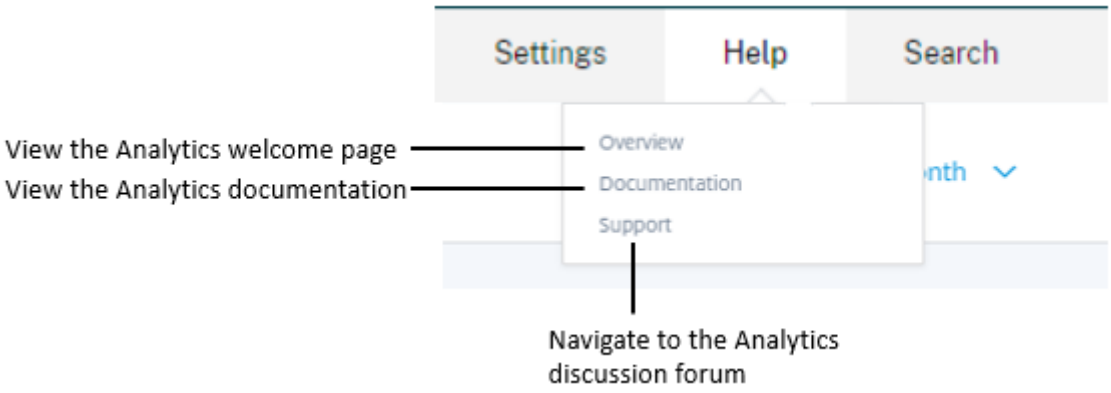


Menu Paramètres

Dans le menu **Paramètres**, accédez à la page Indicateurs et stratégies ou à la page Sources de données .

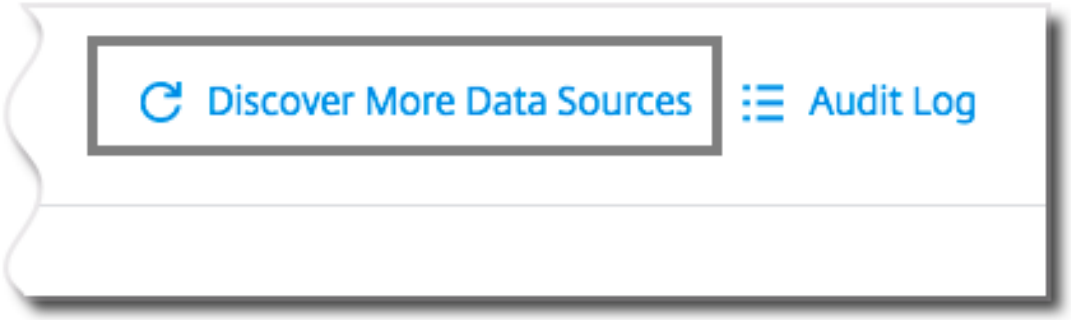


Menu d'aide



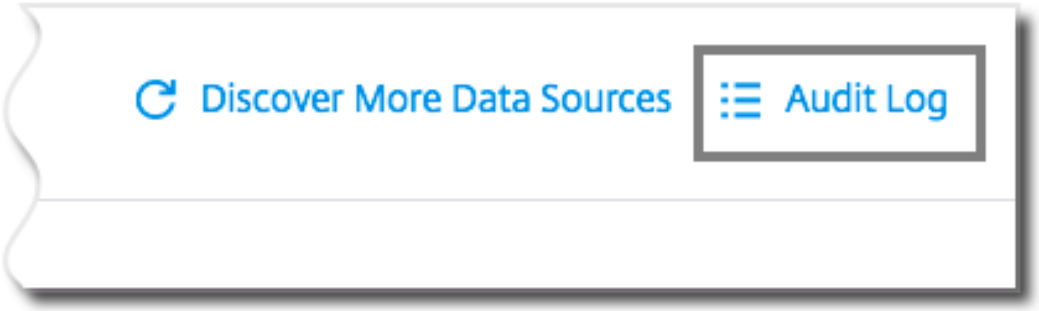
Découvrir d'autres sources de données

Découvrez les sources de données récemment ajoutées ou les sources de données précédemment supprimées.



Audit log

Accédez à la page Journal d'audit qui répertorie tous les événements générés sur Analytics.



Recherche en libre-service

December 7, 2023

Qu'est-ce que la recherche en libre-service ?

La fonction de recherche en libre-service vous permet de rechercher et de filtrer les événements utilisateur reçus de vos sources de données. Vous pouvez explorer les événements utilisateur sous-jacents et leurs attributs. Ces événements vous aident à identifier les problèmes de données et à les résoudre. La page de recherche affiche différentes facettes (dimensions) et mesures pour une source de données. Vous pouvez définir votre requête de recherche et appliquer des filtres pour afficher les événements qui correspondent à vos critères définis. Par défaut, la page de recherche en libre-service affiche les événements utilisateur du dernier jour.

Actuellement, la fonction de recherche en libre-service est disponible pour les sources de données suivantes :

- Authentication
- Gateway
- Secure Browser
- Secure Private Access
- Applications et bureaux
- Utilisateurs, machines et sessions de performance

Vous pouvez également effectuer une recherche en libre-service sur les événements qui ont respecté vos stratégies définies. Pour plus d'informations, consultez la section Recherche en libre-service de stratégies.

Comment accéder à la recherche en libre-service

Vous pouvez accéder à la recherche en libre-service en utilisant les options suivantes :

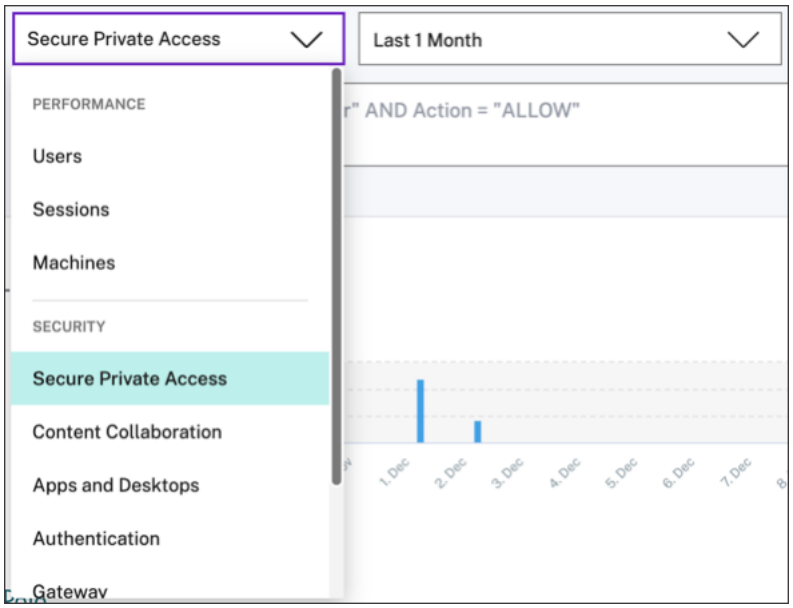
- **Barre supérieure** : cliquez sur **Rechercher** dans la barre supérieure pour afficher tous les événements utilisateur de la source de données sélectionnée.
- **Chronologie des risques sur une page de profil utilisateur** : cliquez sur **Recherche** d'événements pour afficher les événements de l'utilisateur concerné.

Recherche en libre-service depuis la barre supérieure

Utilisez cette option pour accéder à la page de recherche en libre-service depuis n'importe quel endroit de l'interface utilisateur.

1. Cliquez sur **Rechercher** pour afficher la page en libre-service.

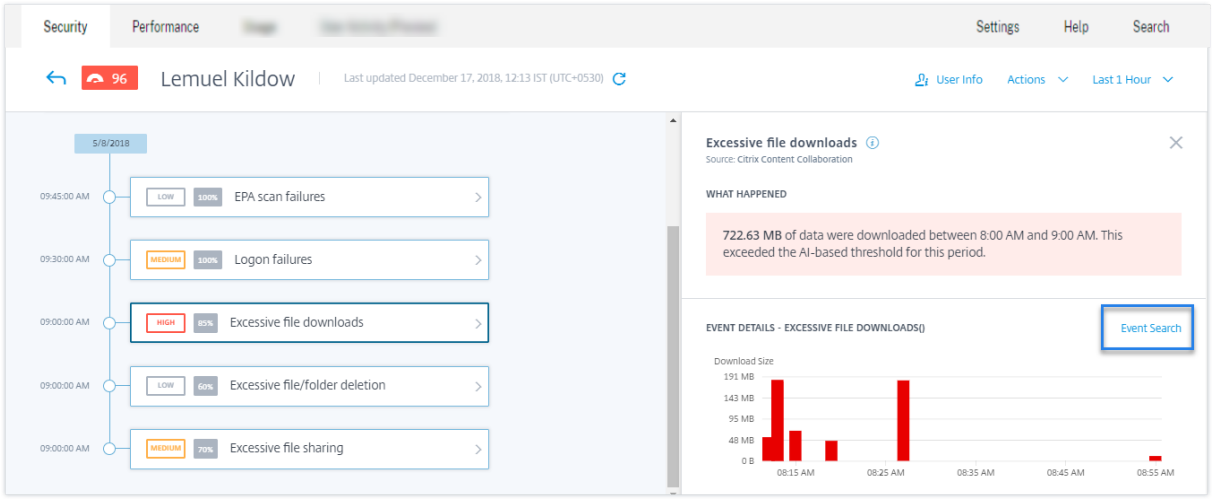
2. Sélectionnez la source de données et la période pour afficher les événements correspondants.



Recherche en libre-service à partir de la chronologie des risques de l'utilisateur

Utilisez cette option si vous souhaitez afficher les événements utilisateur associés à un indicateur de risque.

Lorsque vous sélectionnez un indicateur de risque dans la chronologie d'un utilisateur, la section Informations sur l'indicateur de risque s'affiche dans le volet droit. Cliquez sur **Recherche d'événements** pour explorer les événements associés à l'utilisateur et à la source de données (pour laquelle l'indicateur de risque est déclenché) sur la page de recherche en libre-service.



Pour plus d'informations sur la chronologie des risques utilisateur, voir Chronologie des risques.

Comment utiliser la recherche en libre-service

Utilisez les fonctionnalités suivantes sur la page de recherche en libre-service :

- Facettes pour filtrer vos événements.
- Zone de recherche pour entrer votre requête et filtrer les événements.
- Sélecteur de temps pour sélectionner la période.
- Détails de la chronologie pour afficher les graphiques des événements.
- Données d'événements pour afficher les événements.
- Exportez au format CSV pour télécharger vos événements de recherche sous forme de fichier CSV.
- Exportez le résumé visuel pour télécharger le rapport de synthèse visuel de votre requête de recherche.
- Tri sur plusieurs colonnes pour trier les événements par plusieurs colonnes.

Utiliser les facettes pour filtrer les événements

Les facettes sont le résumé des points de données qui constituent un événement. Les facettes varient en fonction de la source de données. Par exemple, les facettes de la source de données Secure Private Access sont la réputation, les actions, l'emplacement et le groupe de catégories. Alors que les facettes des applications et des bureaux sont le type d'événement, le domaine et la plate-forme.

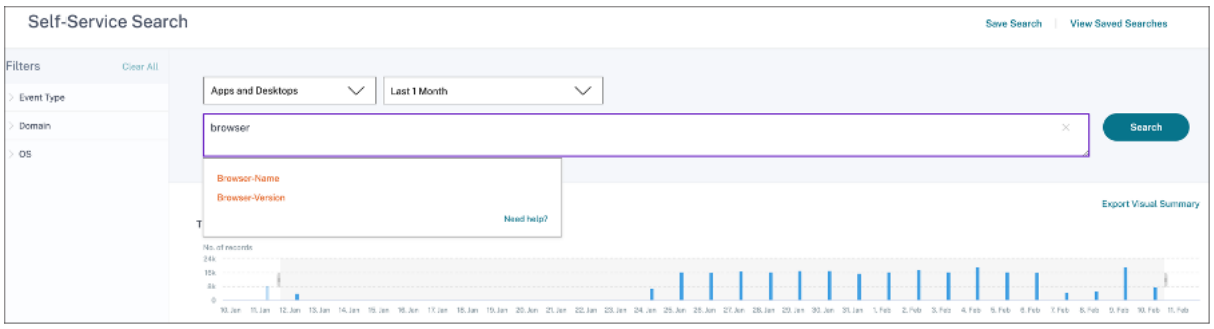
Sélectionnez les facettes pour filtrer les résultats de votre recherche. Les facettes sélectionnées sont affichées sous forme de jetons.

Pour plus d'informations sur les facettes correspondant à chaque source de données, consultez l'article de recherche en libre-service pour la source de données mentionnée plus haut dans cet article.

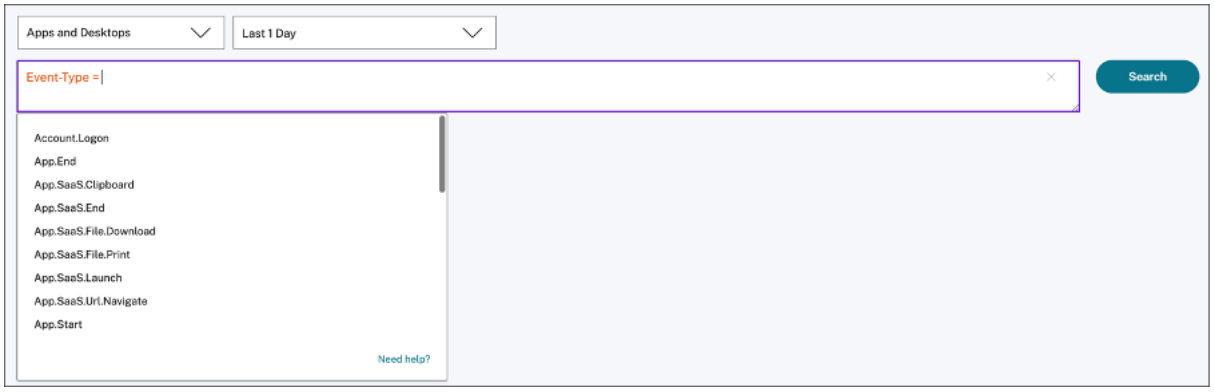
Utiliser la requête de recherche dans la zone de recherche pour filtrer les événements

Lorsque vous placez le curseur dans la zone de recherche, la zone de recherche affiche une liste de dimensions en fonction des événements utilisateur. Ces dimensions varient en fonction de la source de données. Utilisez les dimensions et les opérateurs valides pour définir vos critères de recherche et rechercher les événements requis.

Par exemple, dans la recherche en libre-service d'applications et de bureaux, vous obtenez les valeurs suivantes pour la dimension `Browser`. Utilisez la dimension pour saisir votre requête, sélectionnez la période, puis cliquez sur **Rechercher**.



Lorsque vous sélectionnez certaines dimensions comme `Event-Type` et `Clipboard-Operation` avec un opérateur valide, les valeurs de la dimension s'affichent automatiquement. Vous pouvez choisir une valeur parmi les options proposées ou en saisir une nouvelle en fonction de vos besoins.



Opérateurs pris en charge dans la recherche Utilisez les opérateurs suivants dans vos requêtes de recherche pour affiner vos résultats de recherche.

Opérateur	Description	Exemple	Sortie
	Attribuez une valeur à une dimension de recherche.	User-Name : John	Affiche les événements de l'utilisateur John.
=	Attribuez une valeur à une dimension de recherche.	User-Name = John	Affiche les événements de l'utilisateur John.
~	Recherchez des événements ayant des valeurs similaires.	User-Name ~ test	Affiche les événements ayant des noms d' utilisateur similaires.
" "	Enclenchez les valeurs séparées par des espaces.	User-Name = "John Smith"	Affiche les événements de l'utilisateur John Smith.
< >	Recherchez la valeur relationnelle.	Volume de données > 100	Affiche les événements dont le volume de données est supérieur à 100 Go.
AND	Recherchez les événements pour lesquels les conditions spécifiées sont vraies.	Nom d'utilisateur : Volume de données AND John > 100	Affiche les événements de l'utilisateur John dont le volume de données est supérieur à 100 Go.

Opérateur	Description	Exemple	Sortie
! ~	Vérifie les événements pour le modèle de correspondance que vous spécifiez. Cet opérateur NOT LIKE renvoie les événements qui ne contiennent pas le modèle correspondant dans la chaîne d' événements.	User-Name !~ John	Affiche les événements pour les utilisateurs, à l'exception de John, John Smith ou de tout autre utilisateur de ce type qui contient le nom correspondant « John ».
! =	Vérifie les événements pour obtenir la chaîne exacte que vous spécifiez. Cet opérateur NOT EQUAL renvoie les événements qui ne contiennent pas la chaîne exacte n' importe où dans la chaîne d'événements.	Country != USA	Affiche les événements pour les pays, à l' exception des États-Unis.
*	Recherchez les événements qui correspondent aux chaînes spécifiées. Actuellement, l' opérateur * n'est pris en charge qu'avec les opérateurs suivants : =, et ! =. Les résultats de la recherche respectent la casse.	User-Name = John*	Affiche les événements pour tous les noms d' utilisateurs commençant par John.
		User-Name = *John*	Affiche les événements de tous les noms d' utilisateurs contenant John.

Opérateur	Description	Exemple	Sortie
		User-Name = *Smith	Affiche les événements pour tous les noms d'utilisateurs qui se terminent par Smith.
		Nom d'utilisateur : John*	Affiche les événements pour tous les noms d'utilisateurs commençant par John.
		Nom d'utilisateur : *John*	Affiche les événements de tous les noms d'utilisateurs contenant John.
		Nom d'utilisateur : *Smith	Affiche les événements pour tous les noms d'utilisateurs qui se terminent par Smith.
		Nom d'utilisateur ! = John*	Affiche les événements pour tous les noms d'utilisateurs qui ne commencent pas par John.
		Nom d'utilisateur ! = *Smith	Affiche les événements pour tous les noms d'utilisateurs qui ne se terminent pas par Smith.

Opérateur	Description	Exemple	Sortie
`IN`	Attribuez plusieurs valeurs à une dimension de recherche pour obtenir les événements associés à une ou plusieurs valeurs. **Remarque** : Actuellement, vous pouvez utiliser cet opérateur avec les dimensions suivantes d'applications et de bureaux : `Device ID`, `Domain`, `Event-Type` et `User-Name`. Cet opérateur s'applique uniquement aux valeurs de chaîne.	User-Name IN (John, Kevin)	Retrouvez tous les événements liés à John ou Kevin.

Opérateur	Description	Exemple	Sortie
`NOT IN`	Attribuez plusieurs valeurs à une dimension de recherche et recherchez les événements qui ne contiennent pas les valeurs spécifiées. **Remarque** : Actuellement, vous pouvez utiliser cet opérateur avec les dimensions suivantes d'applications et de bureaux : `Device ID`, `Domain`, `Event-Type` et `User-Name`. Cet opérateur s'applique uniquement aux valeurs de chaîne.	User-Name NOT IN (John, Kevin)	Trouvez les événements pour tous les utilisateurs, à l'exception de John et Kevin.

Opérateur	Description	Exemple	Sortie
`IS EMPTY`	Vérifie la présence d'une valeur nulle ou vide pour une dimension. Cet opérateur fonctionne uniquement pour les dimensions de type chaîne telles que `App-Name`, `Browser` et `Country`. Il ne fonctionne pas pour les dimensions de type non chaîne (nombre) telles que `Upload-File-Size`, `Download-File-Size` et `Client-IP`.	Country IS EMPTY	Recherchez les événements pour lesquels le nom du pays n'est pas disponible ou est vide (non spécifié).
`IS NOT EMPTY`	Vérifie s'il n'y a pas de valeur nulle ou une valeur spécifique pour une dimension. Cet opérateur fonctionne uniquement pour les dimensions de type chaîne telles que `App-Name`, `Browser` et `Country`. Il ne fonctionne pas pour les dimensions de type non chaîne (nombre) telles que `Upload-File-Size`, `Download-File-Size` et `Client-IP`.	Country IS NOT EMPTY	Recherchez les événements pour lesquels le nom du pays est disponible ou spécifié.

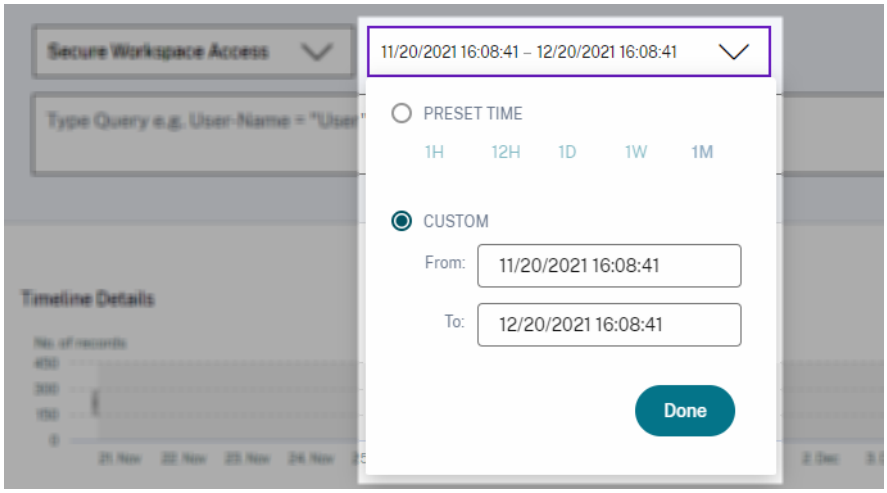
Opérateur	Description	Exemple	Sortie
OR	Recherche des valeurs pour lesquelles l'une ou les deux conditions sont vraies.	(User-Name = John* OU User-Name = *Smith) ET Event-Type = "Session.Logon"	Affiche les événements Session.Logon pour tous les noms d'utilisateur commençant par John ou se terminant par Smith.

> **Remarque**
>
> Pour l'opérateur **NOT EQUAL**, lorsque vous saisissez les valeurs des dimensions de votre requête, utilisez les valeurs exactes disponibles sur la page de recherche en libre-service d'une source de données. Les valeurs de dimension sont sensibles à la casse.

Pour plus d'informations sur la façon de spécifier votre requête de recherche pour la source de données, consultez l'article de recherche en libre-service de la source de données mentionné plus haut dans cet article.

Sélectionnez l'heure d'affichage de l'événement

Sélectionnez une heure prédéfinie ou saisissez une plage de temps personnalisée, puis cliquez sur **Rechercher** pour afficher les événements.

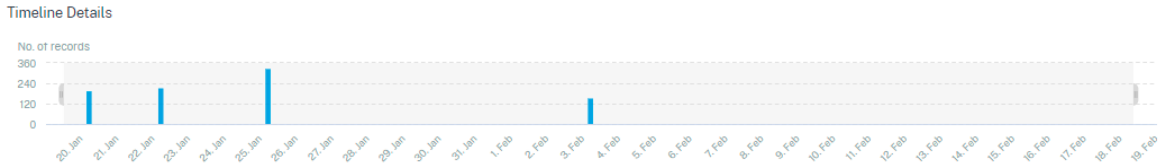


Afficher les détails de la chronologie

La chronologie fournit une représentation graphique des événements utilisateur pour la période sélectionnée. Déplacez les barres de sélection pour choisir la plage de temps et afficher les

événements correspondant à la plage de temps sélectionnée.

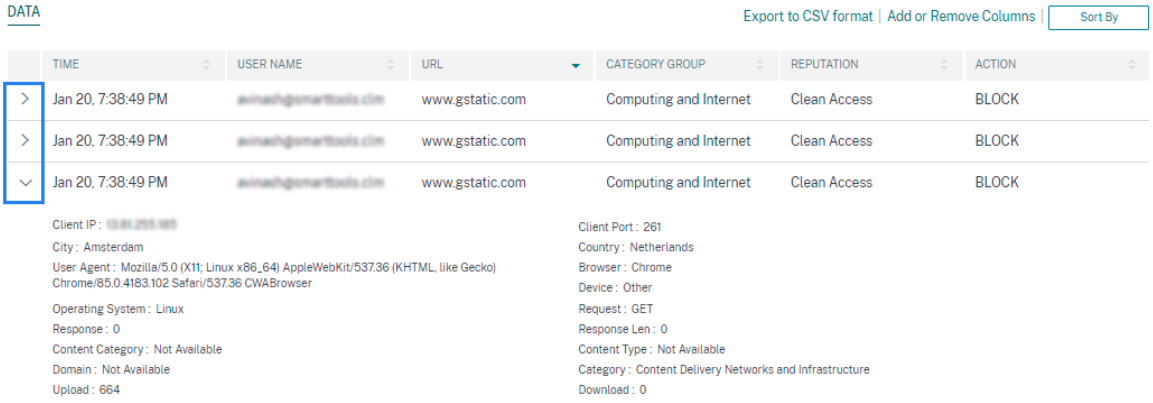
La figure montre les détails de la chronologie des données d'accès.



Voir l'événement

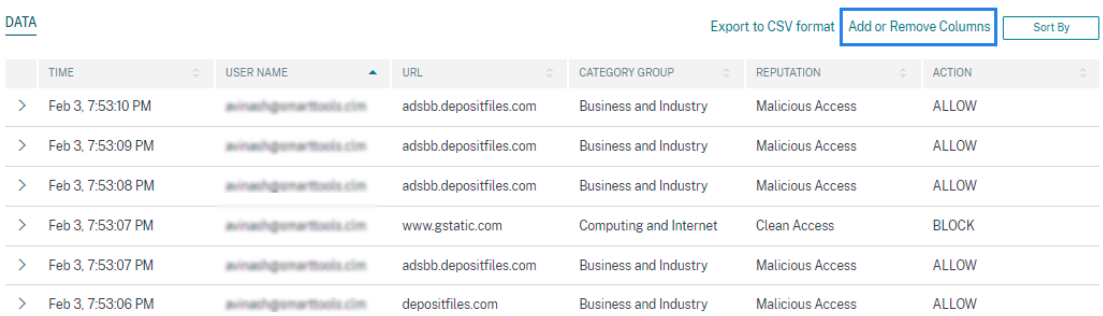
Vous pouvez consulter les informations détaillées sur l'événement utilisateur. Dans le tableau **DATA**, cliquez sur la flèche de chaque colonne pour afficher les détails de l'événement utilisateur.

La figure montre les détails concernant les données d'accès de l'utilisateur.

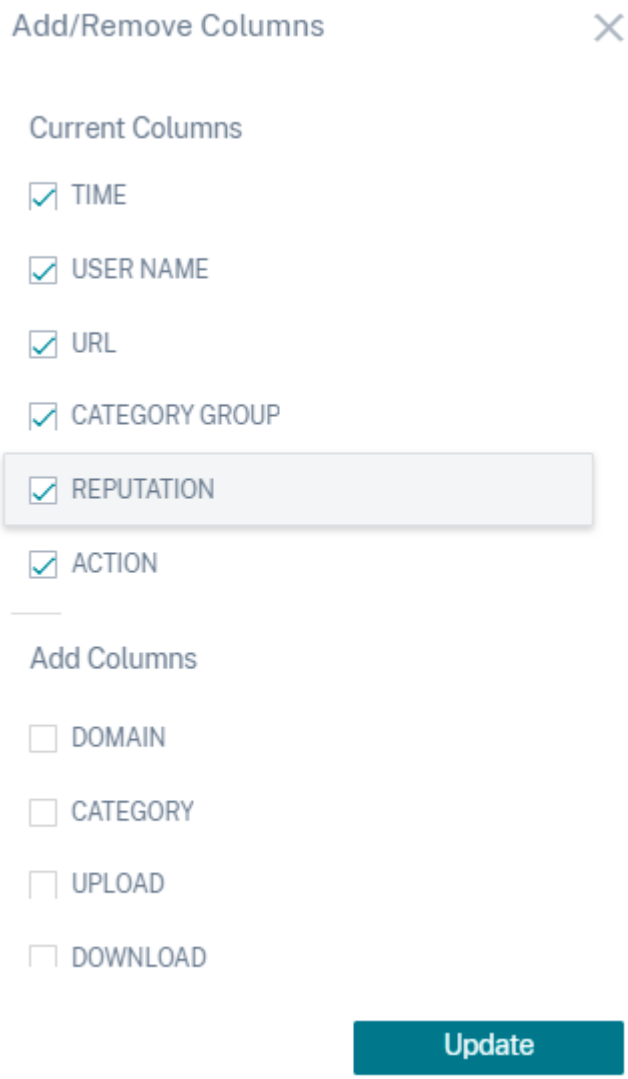


Ajouter ou supprimer des colonnes Vous pouvez ajouter ou supprimer des colonnes de la table d'événements pour afficher ou masquer les points de données correspondants. Procédez comme suit :

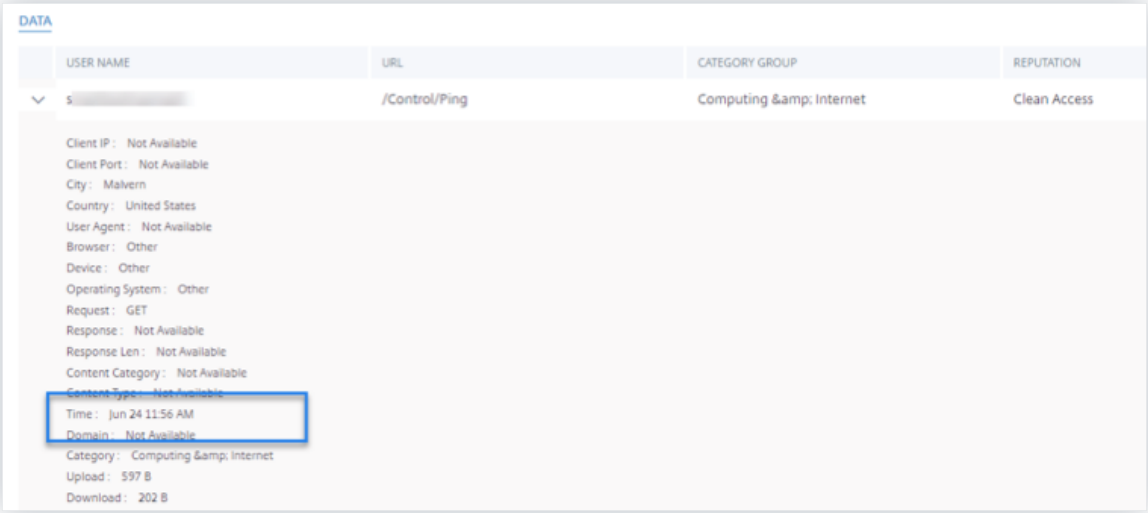
1. Cliquez sur **Ajouter ou supprimer des colonnes**.



2. Sélectionnez ou désélectionnez les éléments de données dans la liste, puis cliquez sur **Mettre à jour**.

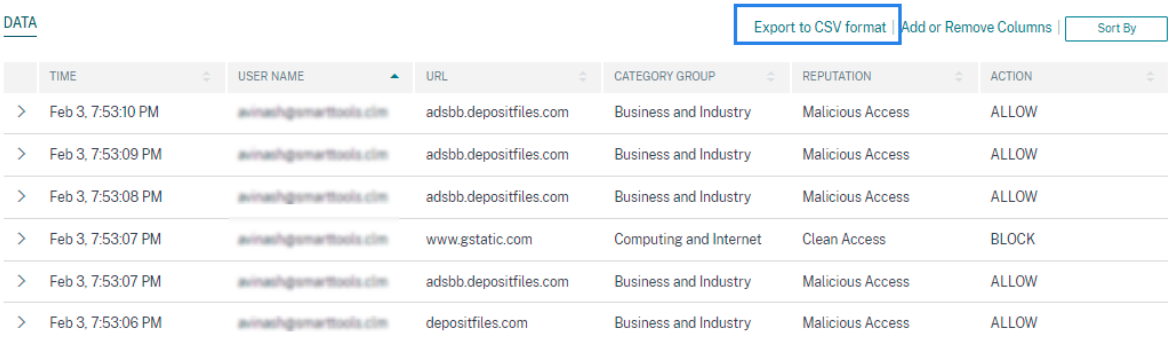


Si vous désélectionnez un point de données de la liste, la colonne correspondante est supprimée de la table des événements. Toutefois, vous pouvez afficher ce point de données en développant la ligne d'événement pour un utilisateur. Par exemple, lorsque vous désélectionnez le point de données **TIME** de la liste, la colonne **TIME** est supprimée de la table des événements. Pour afficher l'enregistrement de temps, développez la ligne d'événement d'un utilisateur.



Exportez les événements dans un fichier CSV

Exportez les résultats de la recherche dans un fichier CSV et enregistrez-le pour référence. Cliquez sur **Exporter au format CSV** pour exporter les événements et télécharger le fichier CSV généré. Vous pouvez exporter 100 000 lignes à l'aide de la fonctionnalité **Exporter au format CSV** .



Résumé visuel de l'exportation

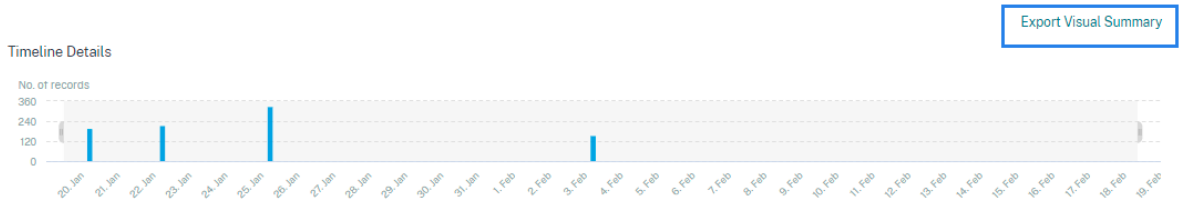
Vous pouvez télécharger le rapport de synthèse visuel de votre requête de recherche et en partager une copie avec d'autres utilisateurs, administrateurs ou votre équipe de direction.

Cliquez sur **Exporter le résumé visuel** pour télécharger le rapport de synthèse visuel au format PDF. Le rapport contient les informations suivantes :

- La requête de recherche que vous avez spécifiée pour les événements de la période sélectionnée.
- Les facettes (filtres) que vous avez appliquées aux événements pendant la période sélectionnée.

- Le résumé visuel, tel que les graphiques chronologiques, les graphiques à barres ou les graphiques des événements de recherche pour la période sélectionnée.

Pour une source de données, vous pouvez télécharger le rapport de synthèse visuel uniquement si les données sont affichées dans des formats visuels tels que des graphiques à barres ou des détails de la chronologie. Sinon, cette option n'est pas disponible. Par exemple, vous pouvez télécharger le rapport récapitulatif visuel des sources de données telles que les applications et les bureaux, les sessions, où vous voyez les données sous forme de détails de chronologie et de graphiques à barres. Pour les sources de données telles que Utilisateurs et Machines, les données s'affichent uniquement sous forme de tableau. Par conséquent, vous ne pouvez pas télécharger de rapport de synthèse visuel.

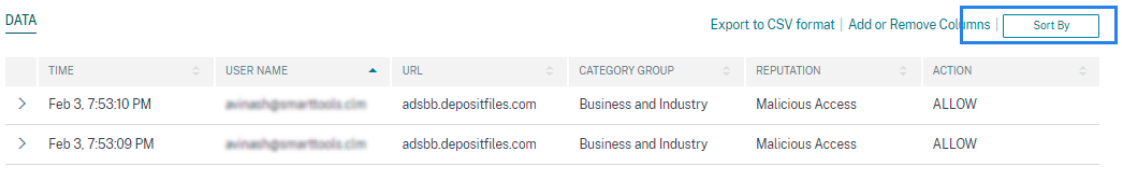


Tri multi-colonnes

Le tri aide à organiser vos données et offre une meilleure visibilité. Sur la page de recherche en libre-service, vous pouvez trier les événements utilisateur en fonction d'une ou de plusieurs colonnes. Les colonnes représentent les valeurs de divers éléments de données tels que le nom d'utilisateur, la date et l'heure et l'URL. Ces éléments de données varient en fonction des sources de données sélectionnées.

Pour effectuer un tri sur plusieurs colonnes, procédez comme suit :

1. Cliquez sur **Trier par**.

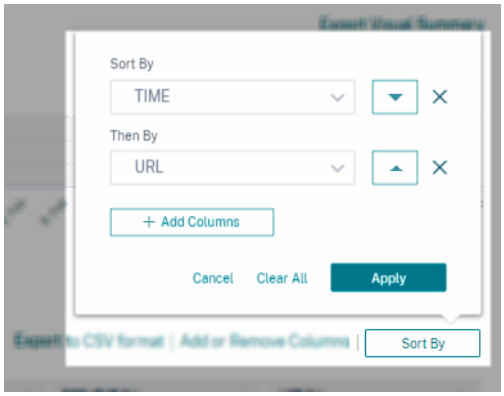


2. Sélectionnez une colonne dans la liste **Trier par** .
3. Sélectionnez l'ordre de tri : croissant (flèche vers le haut) ou décroissant (flèche vers le bas) pour trier les événements de la colonne.
4. Cliquez **sur+Ajouter des colonnes**.
5. Sélectionnez une autre colonne dans la liste **Then By** .
6. Sélectionnez l'ordre de tri : croissant (flèche vers le haut) ou décroissant (erreur vers le bas) pour trier les événements de la colonne.

> **Remarque**
>
> Vous pouvez ajouter jusqu'à six colonnes pour effectuer le tri.

7. Cliquez sur **Appliquer**.
8. Si vous ne souhaitez pas appliquer les paramètres précédents, cliquez sur **Annuler**. Pour supprimer les valeurs des colonnes sélectionnées, cliquez sur **Effacer tout**.

L'exemple suivant montre un tri sur plusieurs colonnes des événements Secure Private Access. Les événements sont triés par heure (du plus récent au plus ancien), puis par URL (par ordre alphabétique).



Vous pouvez également effectuer un tri sur plusieurs colonnes à l'aide de la touche **Maj** . Appuyez sur la **touche Maj** et cliquez sur les en-têtes de colonne pour trier les événements utilisateur.

Comment sauvegarder la recherche en libre-service

En tant qu'administrateur, vous pouvez enregistrer une requête en libre-service. Cette fonctionnalité permet de gagner du temps et d'économiser les efforts liés à la réécriture de la requête que vous utilisez souvent à des fins d'analyse ou de dépannage. Les options suivantes sont enregistrées avec la requête :

- Filtres de recherche appliqués
- Source de données et durée sélectionnées

Pour enregistrer une requête en libre-service, procédez comme suit :

1. Sélectionnez la source de données et la durée requises.
2. Tapez une requête dans la barre de recherche.
3. Appliquez les filtres requis.
4. Cliquez sur **Enregistrer la recherche**.
5. Spécifiez le nom pour enregistrer la requête personnalisée.

> **Remarque**
>
> Assurez-vous que le nom de la requête est unique. Sinon, la requête n'enregistre pas.

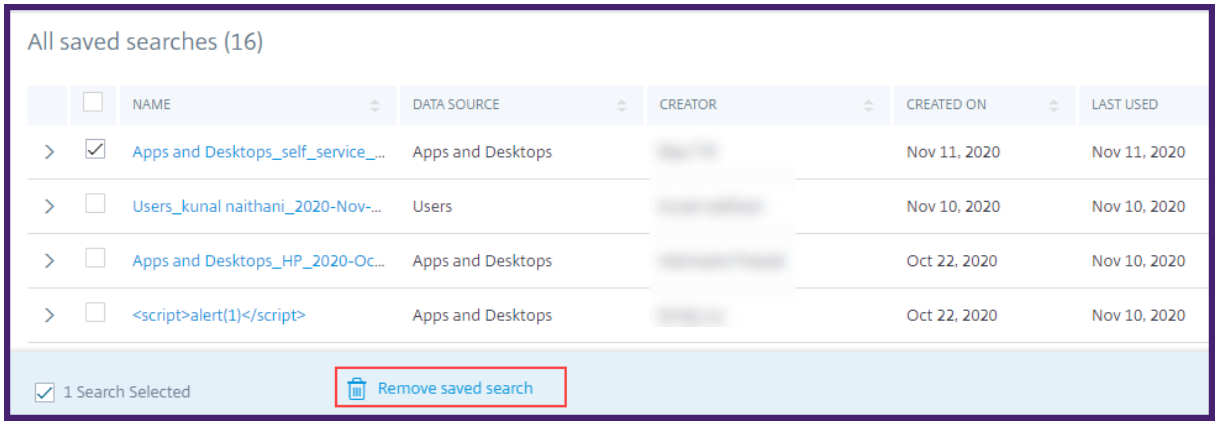
6. Activez le bouton **Planifier le rapport par e-mail** si vous souhaitez envoyer une copie du rapport de requête de recherche à vous-même et à d'autres utilisateurs à intervalles réguliers. Pour plus d'informations, consultez la rubrique Planifier un e-mail pour une requête de recherche.
7. Cliquez sur **Enregistrer**.

Pour afficher les recherches enregistrées, procédez comme suit :

1. Cliquez sur **Afficher les recherches enregistrées**.
2. Cliquez sur le nom de la requête de recherche.

Pour supprimer une recherche enregistrée :

1. Cliquez sur **Afficher les recherches enregistrées**.
2. Sélectionnez la requête de recherche que vous avez enregistrée.
3. Cliquez sur **Supprimer la recherche enregistrée**.



Pour modifier une recherche enregistrée :

1. Cliquez sur **Afficher les recherches enregistrées**.
2. Cliquez sur le nom de la requête de recherche que vous avez enregistrée.
3. Modifiez la requête de recherche ou la sélection des facettes en fonction de vos besoins.
4. Cliquez sur **Mettre à jour la recherche > Enregistrer** pour mettre à jour et enregistrer la recherche modifiée avec le même nom de requête de recherche.
5. Si vous souhaitez enregistrer la recherche modifiée sous un nouveau nom, cliquez sur la flèche vers le bas, puis sur **Enregistrer en tant que nouvelle recherche > Enregistrer sous**.

Si vous remplacez la recherche par un nouveau nom, la recherche est enregistrée en tant que nouvelle entrée. Si vous conservez le nom de recherche existant lors du remplacement, les données de recherche modifiées remplacent les données de recherche existantes.

> **Remarque**
>
> - Seul le propriétaire d'une requête peut modifier ou supprimer ses recherches enregistrées.
> - Vous pouvez copier l'adresse du lien de recherche enregistrée pour la partager avec un autre utilisateur.

Planifier un e-mail pour une requête de recherche

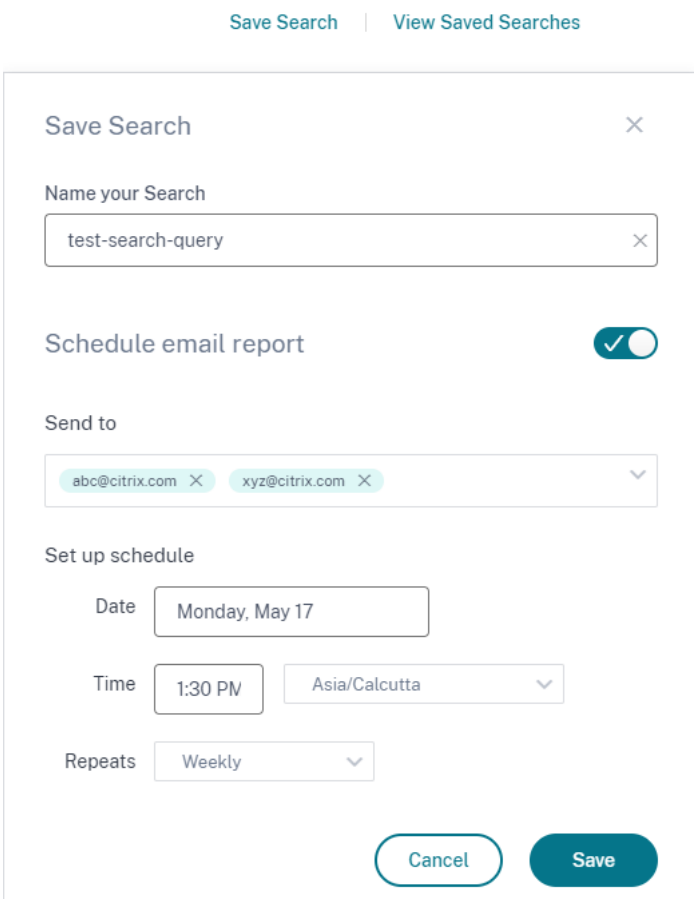
Vous pouvez envoyer une copie du rapport de requête de recherche à vous et à d'autres utilisateurs à intervalles réguliers en configurant un calendrier de remise des e-mails.

Cette option n'est disponible que si votre rapport de requête de recherche contient des données dans des formats visuels tels que des graphiques à barres et des détails de la chronologie. Sinon, vous ne pouvez pas planifier la livraison d'un e-mail. Par exemple, vous pouvez planifier un e-mail pour les sources de données telles que les applications et les bureaux, les sessions, où vous voyez les données sous forme de détails de chronologie et de graphiques à barres. Pour les sources de données telles que Utilisateurs et Machines, les données s'affichent uniquement sous forme de tableau. Par conséquent, vous ne pouvez pas programmer un e-mail.

Planifier un e-mail lors de l'enregistrement d'une requête de recherche

Lors de l'enregistrement d'une requête de recherche, configurez un calendrier de remise des e-mails comme suit :

1. Dans la boîte de dialogue **Enregistrer la recherche**, activez le bouton **Planifier le rapport par e-mail** .



2. Entrez ou collez les adresses e-mail des destinataires.

> **Remarque**
>
> Les groupes de messagerie ne sont pas pris en charge.

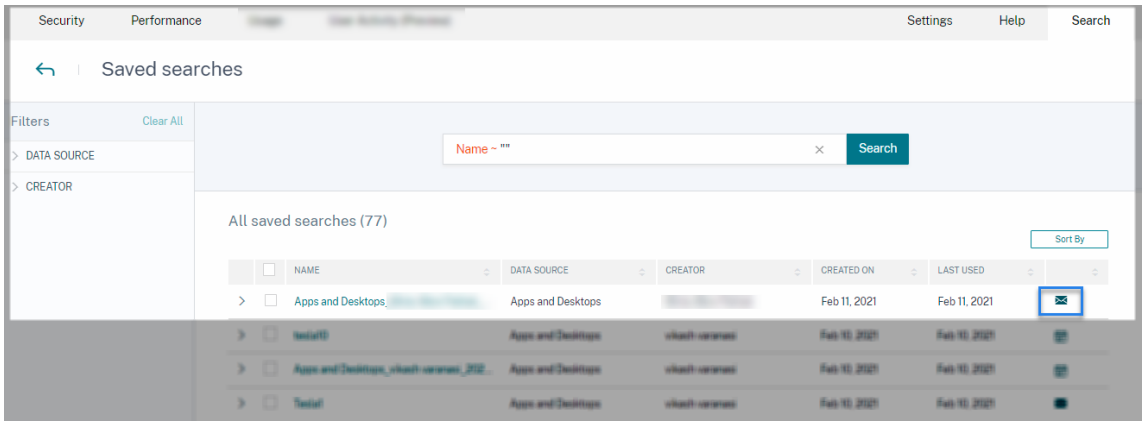
3. Définissez la date et l'heure de la livraison de l'e-mail.
4. Sélectionnez la fréquence de livraison : quotidienne, hebdomadaire ou mensuelle.
5. Cliquez sur **Enregistrer**.

Planifier un e-mail pour une requête de recherche déjà enregistrée

Si vous souhaitez définir un calendrier de remise des e-mails pour une requête de recherche que vous avez précédemment enregistrée, procédez comme suit :

1. Cliquez sur **Afficher les recherches enregistrées**.
2. Accédez à la requête de recherche que vous avez créée. Cliquez sur l'icône **Envoyer cette requête par e-mail** .

> **Remarque**
>
> Seul le propriétaire d'une requête peut planifier la livraison par e-mail de sa requête de recherche enregistrée.



3. Activez le bouton **Planifier le rapport par e-mail** .
4. Entrez ou collez les adresses e-mail des destinataires.

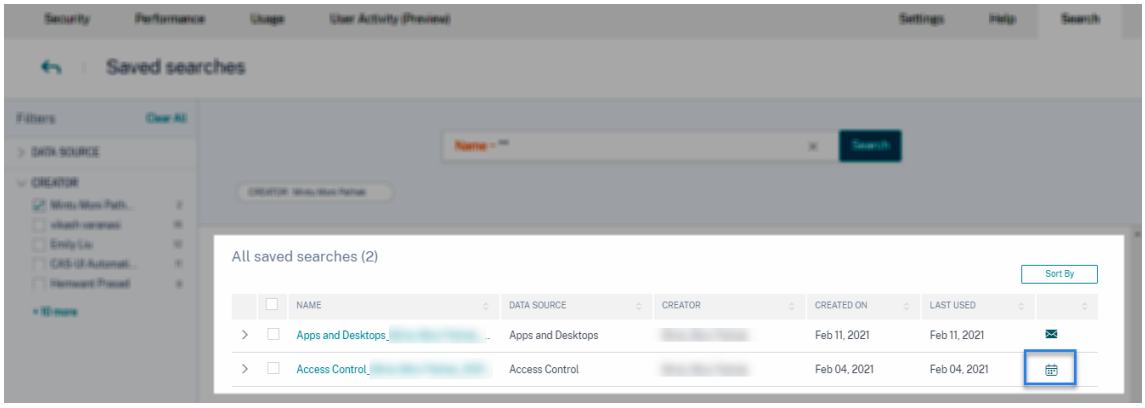
> **Remarque**
>
> Les groupes de messagerie ne sont pas pris en charge.

5. Définissez la date et l'heure de la livraison de l'e-mail.
6. Sélectionnez la fréquence de livraison : quotidienne, hebdomadaire ou mensuelle.
7. Cliquez sur **Enregistrer**.

Arrêter le calendrier de livraison d'un e-mail pour une requête de recherche

1. Cliquez sur **Afficher les recherches enregistrées**.
2. Accédez à la requête de recherche que vous avez créée. Cliquez sur l'icône **Afficher le calendrier de livraison des e-mails** .

> **Remarque**
>
> Seul le propriétaire d'une requête peut arrêter la planification des e-mails de sa requête de recherche enregistrée.



3. Désactivez le bouton **Planifier le rapport par e-mail** .
4. Cliquez sur **Enregistrer**.

Contenu de l'e-mail

Les destinataires reçoivent un e-mail de « Citrix Cloud - Notifications donotreplynotifications@citrix.com » concernant le rapport de requête de recherche. Le rapport est joint en tant que document PDF. L'e-mail est envoyé à un intervalle régulier défini par vous dans les paramètres du **rapport Planifier les e-mails** .

Le rapport sur les requêtes de recherche contient les informations suivantes :

- La requête de recherche que vous avez spécifiée pour les événements de la période sélectionnée.
- Les facettes (filtres) que vous avez appliquées aux événements.
- Le résumé visuel, tel que les graphiques chronologiques, les graphiques à barres ou les graphiques des événements de recherche.

Permissions pour les administrateurs d'accès complet et d'accès en lecture seule

- Si vous êtes un administrateur Citrix Cloud avec un accès complet, vous pouvez utiliser toutes les fonctionnalités disponibles sur la page **de recherche** .
- Si vous êtes un administrateur Citrix Cloud avec un accès en lecture seule, vous ne pouvez effectuer que les activités suivantes sur la page **de recherche** :
  - Affichez les résultats de la recherche en sélectionnant une source de données et la période.
  - Entrez une requête de recherche et affichez les résultats de la recherche.
  - Affichez les résultats de recherche enregistrés des autres administrateurs.

- Exportez le résumé visuel et téléchargez les résultats de la recherche sous forme de fichier CSV.

Pour plus d'informations sur les rôles d'administrateur, consultez Gérer les rôles d'administrateur pour Citrix Analytics.

Paramètres d'alerte

December 7, 2023

Citrix Analytics génère des alertes en fonction des critères de la stratégie d'alerte. Vous pouvez configurer pour recevoir des notifications d'alerte de la part de Citrix Analytics for Security and Performance par e-mail et Webhook.

- Liste de distribution par e-mail
- Webhook pour les notifications d'alerte

Vous pouvez formater la notification par e-mail pour les alertes provenant de Citrix Analytics for Security.

- Paramètres de messagerie de l'utilisateur final

Listes de distribution par e-mail

December 7, 2023

Lorsque vous appliquez l'action **Notifier les administrateurs** manuellement ou en créant une stratégie, une notification est envoyée aux administrateurs sélectionnés concernant l'indicateur de risque.

> **IMPORTANT**
>
> Vous pouvez sélectionner des administrateurs parmi les domaines Citrix Cloud et d'autres domaines autres que Citrix Cloud de votre organisation.

Pour envoyer des notifications aux groupes d'administrateurs appropriés, créez une liste de distribution à l'aide de leurs adresses e-mail.

Avec la liste de distribution par e-mail, vous pouvez effectuer les opérations suivantes :

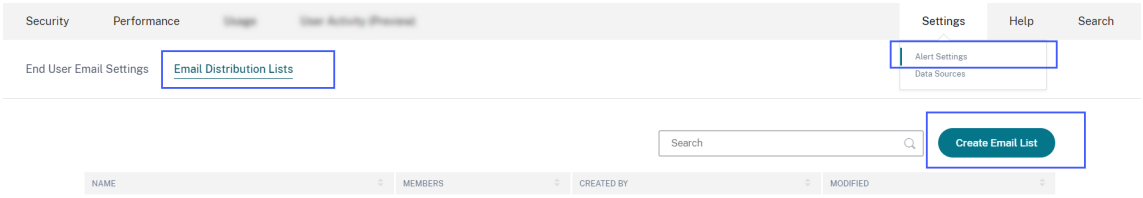
- Créez une liste de distribution d'e-mails commune avec des membres de différents domaines de votre organisation.

- Prévenez tous les membres en une seule fois.
- Économisez du temps et des efforts pour sélectionner les administrateurs de différents domaines.
- Gérez et gérez les listes de distribution d'e-mails en fonction de vos besoins, tels que l'ajout de nouveaux membres ou la suppression de membres existants.

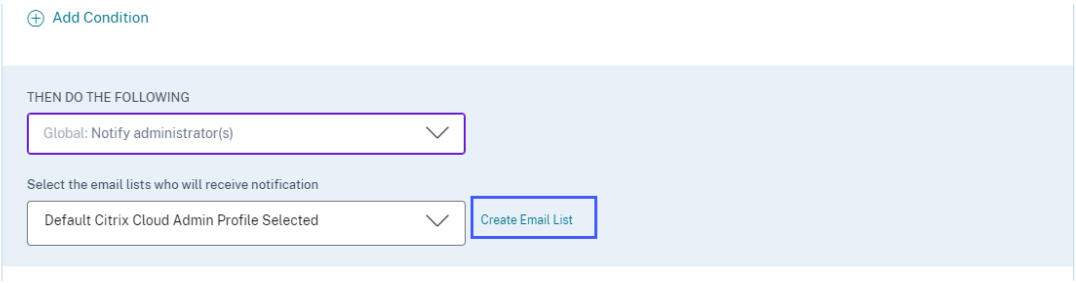
Créer une liste de distribution par e-mail

Pour créer une liste de distribution d'e-mails :

1. Cliquez sur **Paramètres > Paramètres d'alerte > Listes de distribution d'e-mails > Créer une liste**de diffusion.



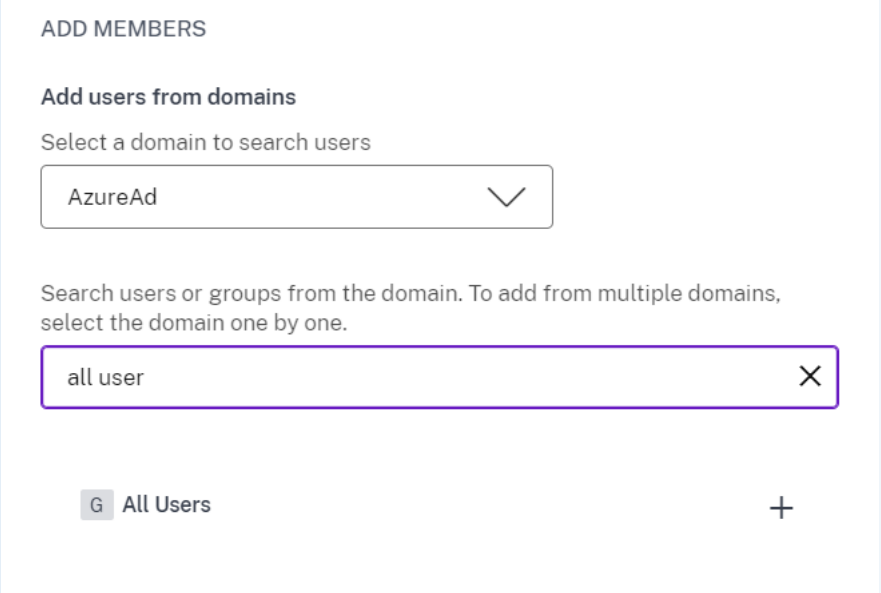
   Vous pouvez également créer une liste de distribution d'e-mails à partir d'une stratégie. Modifiez une stratégie existante ou créez une stratégie et sélectionnez l'action **Notifier les administrateurs** . Cliquez sur le lien **Créer une liste** de diffusion.



2. Entrez un nom et une description de la liste de diffusion des e-mails pour identifier son objectif.
3. Utilisez les options suivantes pour ajouter des membres à la liste de distribution des e-mails :
   - **Ajoutez des utilisateurs à partir de domaines**. Cette option nécessite que vos domaines soient connectés à Citrix Cloud.
   - **Ajoutez des utilisateurs par adresse e-mail**. Utilisez cette option si vous souhaitez ajouter des utilisateurs extérieurs aux domaines sélectionnés.
4. Pour ajouter des utilisateurs à partir de domaines, sélectionnez un domaine et recherchez les utilisateurs ou les groupes d'utilisateurs.

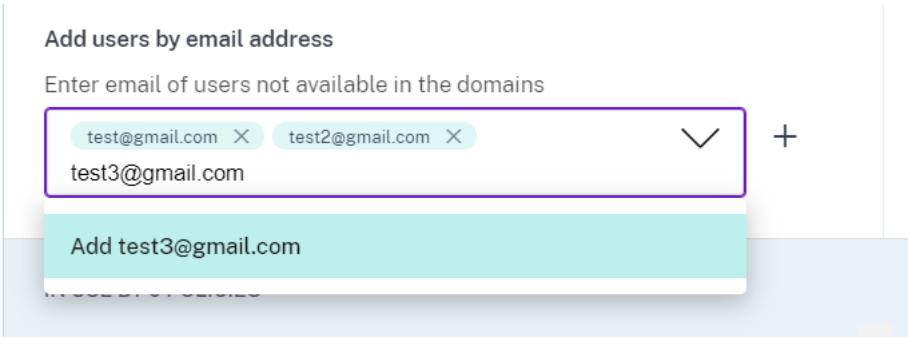
> **Remarque**
>
> Vous pouvez également ajouter des utilisateurs et des groupes d'utilisateurs provenant de plusieurs domaines en sélectionnant les domaines un par un. Pour chaque domaine, recherchez et ajoutez les utilisateurs ou le groupe d'utilisateurs.

5. Cliquez sur l'icône **Ajouter** en regard de l'utilisateur ou du groupe d'utilisateurs.



6. Pour ajouter des utilisateurs qui ne sont pas disponibles dans le domaine que vous avez sélectionné, saisissez les adresses e-mail des utilisateurs ou les listes de distribution des e-mails.

> **Remarque**
>
> Avant d'entrer dans une liste de distribution d'e-mails, assurez-vous de pouvoir y accéder depuis l'extérieur du réseau de votre organisation. Si vous ajoutez une liste de distribution d'e-mails interne à votre organisation, les membres de la liste ne peuvent pas recevoir de notifications de Citrix Analytics.



7. Cliquez sur **Créer une liste de diffusion**.

Afficher la liste de distribution par e-mail

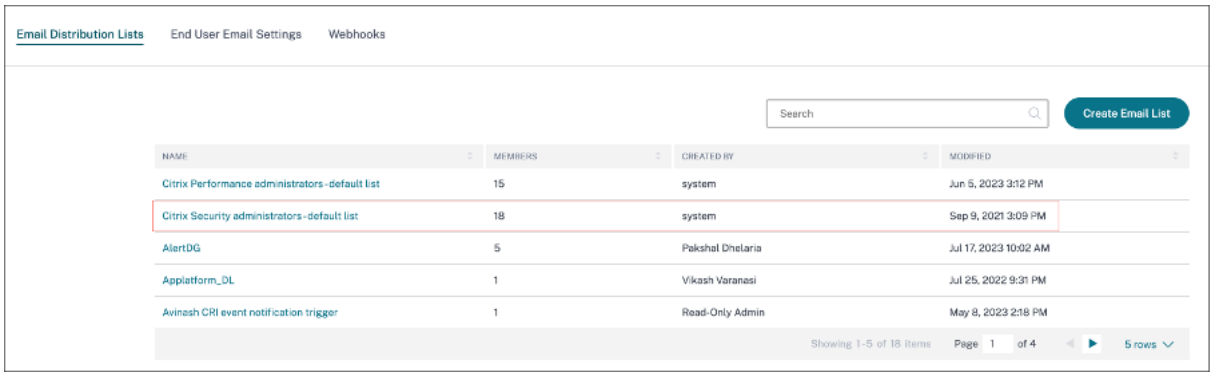
Pour afficher vos listes de distribution d'e-mails, cliquez sur **Paramètres > Paramètres d'alerte > Listes de distribution d'e-mails**.

La page affiche toutes les listes de distribution d'e-mails créées dans votre compte. Sélectionnez une liste de distribution d'e-mails pour afficher les membres ou modifier la liste.

Une liste de distribution d'e-mails créée par défaut s'affiche dans votre compte. Il contient les administrateurs Citrix Cloud dont l'option **Notifications par e-mail** est activée dans leurs comptes Citrix Cloud. Vous ne pouvez ni supprimer ni modifier la liste par défaut.

> **Remarque**
>
> Pour la liste de distribution des e-mails par défaut, Citrix Analytics met en cache les informations relatives aux administrateurs dont les notifications par e-mail sont activées. Le cache est actualisé toutes les 24 heures. Ainsi, si un administrateur modifie les préférences de notification par e-mail, cette modification est mise à jour dans Citrix Analytics après 24 heures.
>
> Par exemple, si un administrateur Citrix Cloud active ses notifications par e-mail, il commence à recevoir des notifications après 24 heures, et non instantanément. De même, si un administrateur Citrix Cloud désactive ses notifications par e-mail, il cesse de recevoir des notifications au bout de 24 heures.

La liste de distribution par défaut pour les administrateurs de sécurité inclut désormais les administrateurs complets et personnalisés dont l'option **Notifications par e-mail** est activée sur leurs comptes Citrix Cloud.



Modifier une liste de distribution d'e-mails

Pour modifier une liste de distribution d'e-mails :

1. Cliquez sur **Paramètres > Paramètres d'alerte > Listes de distribution des e-mails**.
2. Cliquez sur la liste de distribution des e-mails que vous souhaitez modifier.

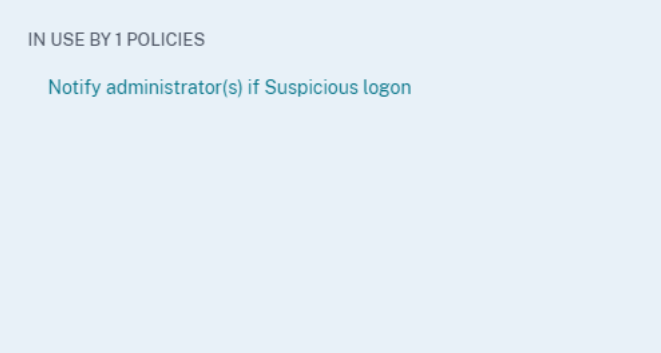
3. Dans la liste de distribution par e-mail, mettez à jour les informations requises telles que le nom, la description et l'ajout ou la suppression de membres.
4. Cliquez sur **Enregistrer**.

Supprimer une liste de distribution d'e-mails

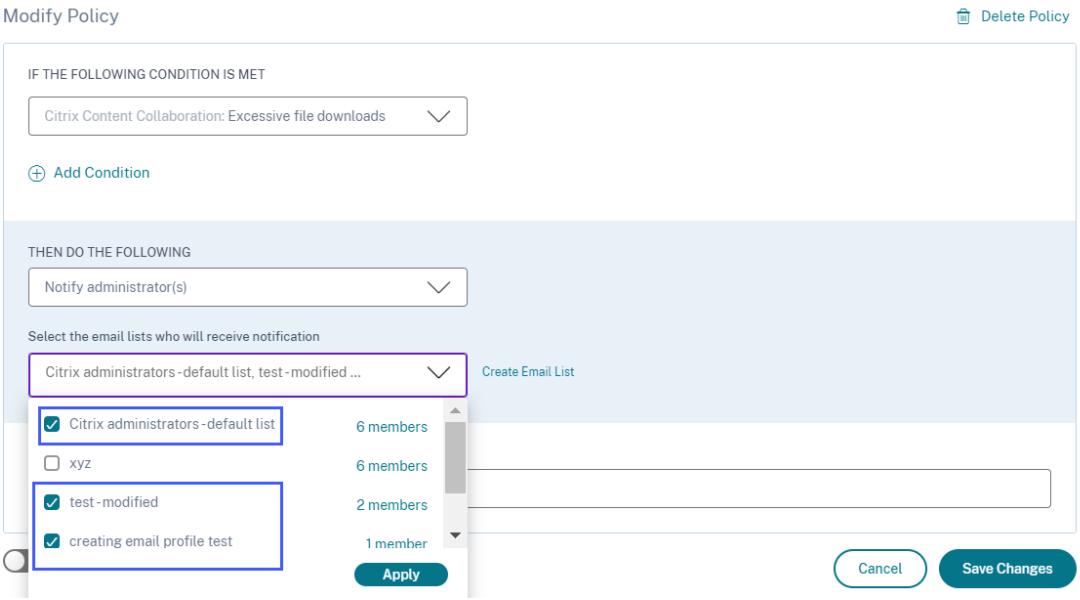
Vous pouvez supprimer une liste de distribution d'e-mails uniquement si elle n'est liée à aucune stratégie. S'il est lié à certaines stratégies, vous devez d'abord supprimer la liste de distribution des e-mails des stratégies associées.

Pour supprimer une liste de distribution d'e-mails :

1. Cliquez sur **Paramètres > Paramètres d'alerte > Listes de distribution des e-mails**.
2. Cliquez sur la liste de distribution des e-mails que vous souhaitez supprimer.
3. Dans la liste de distribution des e-mails, affichez les stratégies associées.



4. Cliquez sur la stratégie pour l'ouvrir et supprimer les listes de distribution d'e-mails. Vous pouvez également supprimer la stratégie si vous le souhaitez.



5. Cliquez sur **Enregistrer les modifications** et revenez à la liste de distribution des e-mails.
6. Ouvrez la liste de distribution des e-mails et cliquez sur l'icône **Supprimer** .

Webhook pour les notifications d'alerte

June 19, 2023

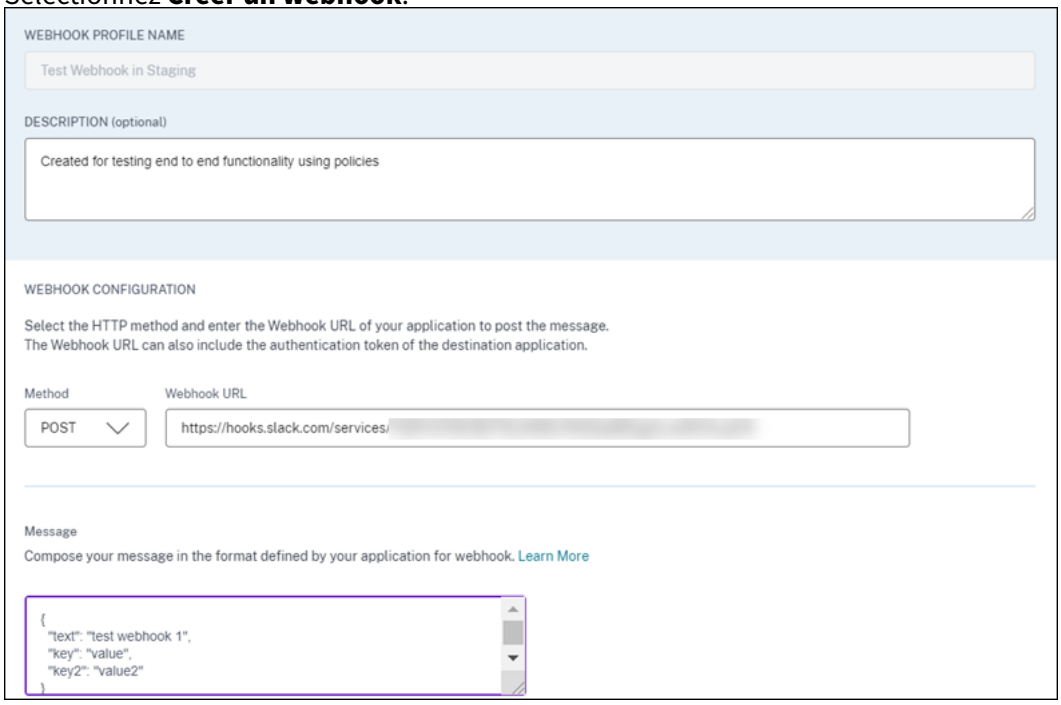
Vous pouvez utiliser des webhooks pour envoyer des notifications d'alerte Citrix Analytics à toutes les applications tierces dont les URL de webhook entrantes sont configurées. Les webhooks sont des callbacks HTTP qui permettent la messagerie en temps réel entre les applications du fournisseur de services et les applications grand public. Comme les notifications d'alerte sont envoyées en temps réel, vous êtes averti lorsque les événements se produisent.

Lorsque Citrix Analytics déclenche une alerte, le webhook associé envoie le message d'alerte à l'URL de l'application cible. L'alerte est envoyée sous la forme d'une charge utile JSON via la requête HTTP POST ou PUT. Par exemple, lorsqu'un utilisateur déclenche un indicateur de risque ou que les performances d'une machine VDI diminuent, vous pouvez configurer un webhook pour envoyer les notifications d'alerte à votre chaîne Slack.
La configuration de webhooks pour la gestion des alertes vous permet de recevoir des notifications en temps réel dans vos applications. Vous pouvez prendre des mesures opportunes pour atténuer les risques de sécurité ou améliorer les performances de votre déploiement de Citrix Virtual Apps and Desktops.

Créer un profil Webhook

Pour créer les profils de webhook sur Citrix Analytics, procédez comme suit :

1. Connectez-vous à Citrix Analytics.
2. En fonction de l'offre que vous avez souscrite, cliquez sur **Gérer** pour accéder à Security Analytics ou Performance Analytics.
3. Dans la barre supérieure, cliquez sur **Paramètres > Paramètres d'alerte > Webhook**.
4. Sélectionnez **Créer un webhook**.



5. Entrez un nom de profil et une description du webhook pour identifier son objectif.
6. Sélectionnez la méthode HTTP et l'URL du webhook de votre application pour envoyer le message d'alerte.

> **Remarque :**
> Les webhooks sortants sont généralement envoyés via la requête HTTP POST. Vous pouvez également inclure un jeton d'authentification dans l'URL du webhook de votre application.

7. Entrez le message concernant l'alerte que vous souhaitez envoyer à l'URL du webhook. Le message doit être structuré dans les formats tels que JSON ou XML tels que définis par l'application cible. Pour plus d'informations, consultez les exemples de webhook.
8. (Facultatif) Entrez les clés et les valeurs d'en-tête du message. L'en-tête peut inclure des jetons

d'authentification ou d'autres paires clé-valeur personnalisées pour envoyer en toute sécurité la charge utile à votre application.

9. Pour valider la configuration du webhook, cliquez sur **Tester**.
   Le test valide l'URL du webhook sortant, la structure de la charge utile et les clés d'en-tête. Si aucun problème n'est détecté dans votre configuration, le message « Test réussi » s'affiche.

Exemples de configuration de webhook

La section fournit des exemples de configuration de webhooks pour envoyer des alertes à des applications tierces telles que Slack et Microsoft Teams.

> **Remarque :**
> Reportez-vous à la documentation produit des applications tierces pour savoir comment obtenir l'URL du webhook et les configurations requises pour le webhook.

Envoyer un message d'alerte à Slack

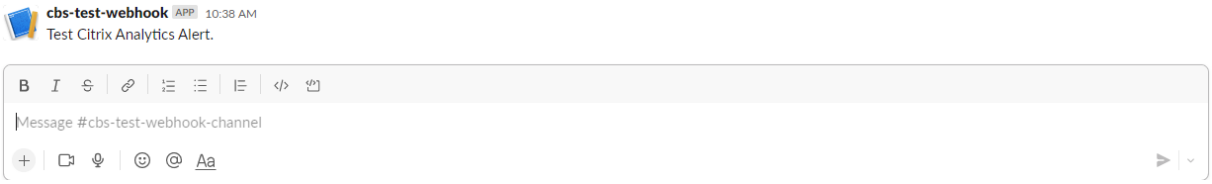
Sur Slack, assurez-vous d'avoir effectué les tâches suivantes avant d'envoyer une alerte :

1. Créez une application Slack pour Citrix Analytics si vous n'en avez pas déjà une.
2. Pour l'application, activez la fonction Webhook entrant et créez un Webhook entrant.
3. Sélectionnez le canal sur lequel l'application publie le message.
4. Lorsque vous autorisez l'application, vous obtenez l'URL du Webhook pour envoyer le message.
   Pour plus d'informations, consultez la section Démarrage avec les webhooks entrants.

Exemple de format de message

```
curl --location --request POST 'WEBHOOK URL'
--header 'Content-Type: application/json'--data-raw '{ "text": "Test
Citrix Analytics Alert." }
```

Résultat



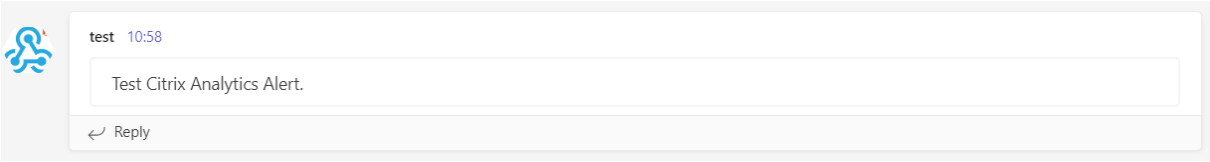
Envoyer un message d'alerte à Microsoft Teams

Sur Microsoft Teams, assurez-vous d'avoir effectué les tâches suivantes avant d'envoyer une alerte :

1. Créez un groupe Teams dans Teams si vous n'en avez pas déjà un.
2. Créez un connecteur Webhook. Reportez-vous aux étapes décrites dans l'article Créer et envoyer des messages .
3. Obtenez l'URL du webhook.

Exemple de format de message `curl --location --request POST 'WEBHOOK URL' --header 'Content-Type: application/json'--data-raw '{ "text": "Test Citrix Analytics Alert." }`

Résultat



Citrix Analytics pour la sécurité (Security Analytics)

February 9, 2024

Avec l'avantage de travailler depuis n'importe où, n'importe quand, n'importe quel appareil sur n'importe quel réseau, les données sensibles de l'entreprise sont davantage exposées que lorsque les utilisateurs travaillaient uniquement depuis un siège social isolé. Les utilisateurs malveillants ont une grande surface d'attaque à cibler. Les équipes informatiques sont chargées de fournir une expérience utilisateur exceptionnelle sans compromettre la sécurité. Citrix Analytics for Security peut aider à combler ce fossé en mettant l'accent sur la sécurité des utilisateurs.

Qu'est-ce que Security Analytics ?

Citrix Analytics for Security évalue en permanence le comportement des utilisateurs Citrix Virtual Apps and Desktops, des utilisateurs Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) et des utilisateurs de Citrix Workspace. Il applique des mesures visant à protéger les informations sensibles de l'entreprise. L'agrégation et la corrélation des données entre les réseaux, les applications virtualisées et les outils de bureau permettent de générer des informations précieuses et de prendre des mesures plus ciblées pour répondre aux menaces de sécurité des utilisateurs. En outre, l'apprentissage automatique prend en charge des approches hautement prédictives pour identifier les comportements malveillants des utilisateurs.

Fonctionnalités

- Des informations rationalisées provenant de tous les produits Citrix et des intégrations de partenaires. Pour plus d'informations, consultez la rubrique Recherche en libre-service.
- Les tableaux de bord faciles à utiliser fournissent une vue complète du comportement des utilisateurs. Pour plus d'informations, consultez Tableau de bord des utilisateurs.
- Détectez et atténuez les comportements malveillants des utilisateurs grâce à l'apprentissage automatique et à des stratégies personnalisées avec des actions automatisées Pour plus d'informations, consultez la section Stratégies et actions.
- La surveillance continue du comportement des utilisateurs après l'authentification initiale auprès des réseaux d'entreprise permet d'équilibrer une sécurité complète et une expérience utilisateur exceptionnelle. Pour plus d'informations, consultez la section Évaluation continue des risques.

Tableaux de bord

Vous pouvez afficher des détails sur le comportement des utilisateurs ou des entités sur les tableaux de bord de sécurité suivants :

- Utilisateurs : fournit une visibilité sur les modèles de comportement des utilisateurs au sein d'une organisation.
- Accès utilisateur : Résume le nombre de domaines à risque accédés et le volume de données téléchargées et téléchargées par les utilisateurs de votre réseau.
- Accès aux applications : Résume les détails des domaines, des URL et des applications auxquels les utilisateurs de votre réseau accèdent.

- Emplacement Access Assurance : Récapitule les détails d'accès et les détails d'ouverture de session des utilisateurs Citrix Virtual Apps and Desktops et des utilisateurs Citrix DaaS.
- Rapports : créez des rapports personnalisés en fonction des dimensions et des mesures disponibles à partir des sources de données intégrées.

Prochaine étape

- Configuration système requise : Configuration minimale qui doit être respectée avant de commencer.
- Sources de données : connaître les produits pris en charge par Analytics.
- Gouvernance des données : Connaître la collecte, le stockage et la conservation des journaux par Analytics.
- Pour commencer : Comment commencer à utiliser Analytics dans votre organisation.

Citrix Analytics for Performance (Analyse des performances)

September 21, 2023

Qu'est-ce que Performance Analytics ?

Performance Analytics est une offre Citrix Analytics qui vous permet de suivre, d'agréger et de visualiser les indicateurs de performance clés de votre environnement Apps and Desktops.

- Performance Analytics regroupe les mesures de performance du site dans des tableaux de bord d'expérience utilisateur et d'infrastructure faciles à consulter. Les tableaux de bord vous aident à analyser l'expérience utilisateur et à optimiser l'utilisation de vos sites Apps et Desktops.
- Performance Analytics prend en charge l'agrégation et la création de rapports multi-sites. Il regroupe les mesures de performance de vos configurations cloud et sur site. Ainsi, vous pouvez consulter les données de tous les sites de votre environnement sur une seule console.
- Performance Analytics quantifie les facteurs de performance des utilisateurs et classe les utilisateurs en fonction de ces facteurs. Il fournit des informations exploitables pour résoudre les pannes, les retards d'écran, les ouvertures de session retardées et d'autres indicateurs de performance.
- Performance Analytics vous permet de rechercher et de filtrer les mesures afin de les limiter aux utilisateurs ou sessions spécifiques confrontés à des problèmes de performances.

Comment utiliser Performance Analytics

Tableau de bord de l'expérience utilisateur

Le tableau de bord Expérience utilisateur affiche les performances du site concernant des facteurs tels que la réactivité de la session, la durée d'ouverture de session, les échecs de session et les reconnexions de session qui définissent ensemble l'expérience utilisateur.

Si vous prenez en charge plusieurs utilisateurs d'applications et de bureaux virtuels dans votre organisation et qu'ils rencontrent parfois des retards lors du lancement d'applications ou de bureaux, la mesure de durée d'ouverture de session peut vous fournir des informations sur le problème. L'exploration vers le bas peut vous aider à identifier les facteurs à l'origine des problèmes.

Tableau de bord de l'infrastructure

Le tableau de bord Infrastructure affiche l'état et la santé des machines de votre site. Lorsqu'ils sont utilisés ensemble, les tableaux de bord Utilisateur et Infrastructure peuvent vous aider à vérifier de manière proactive la disponibilité des ressources et à identifier les goulots d'étranglement des performances sur les sites.

- Si les tendances des utilisateurs ou des sessions affichent une baisse, ce qui indique une réduction du nombre d'utilisateurs ou de sessions connectés au site, utilisez cet indicateur pour vérifier si un hyperviseur a été redémarré ou si le nombre de machines est insuffisant.
- Si vous constatez plusieurs cas d'échec de lancement de sessions, faites une exploration vers le bas pour déterminer la cause de l'échec. Il peut s'agir d'une pénurie de licences ou de problèmes liés à la connexion de la machine au Delivery Controller.

> **Remarque :**
>
> Le**tableau de bord Infrastructure Analytics** est actuellement en version préliminaire.

Grâce à Performance Analytics, vous pouvez rapidement analyser les problèmes, les résoudre et les résoudre, et maintenir un niveau de service optimal des applications et des postes de travail.

Mise en route

Conditions préalables

1. Vérifiez si votre station de travail dispose d'un navigateur Web pris en charge répertorié dans l'article Navigateurs pris en charge . Pour plus d'informations sur la configuration système requise, consultez l'article Configuration système requise pour Citrix Analytics .

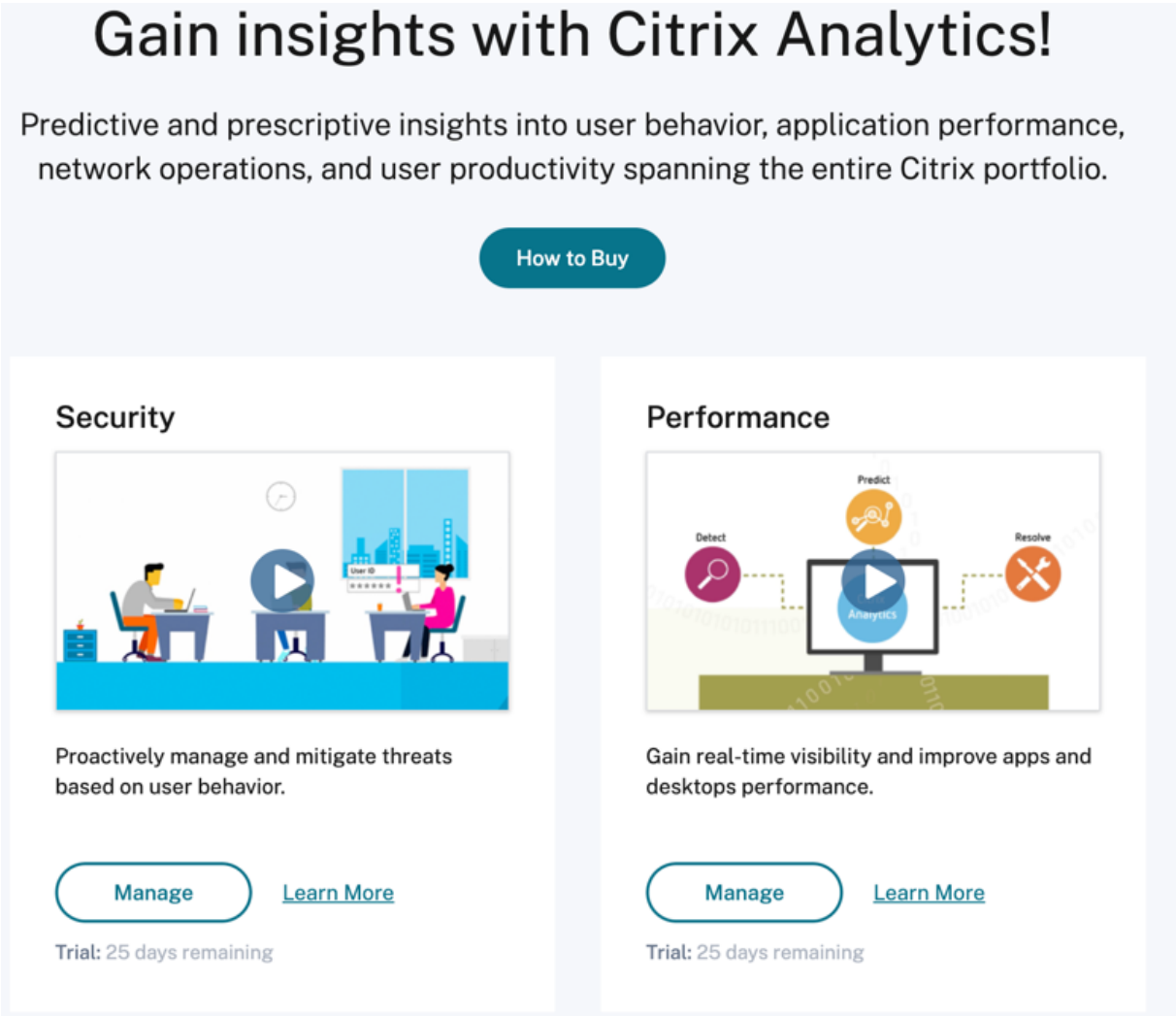
2. Vous devez disposer d'un compte Citrix Cloud pour utiliser le service Analytics. Pour obtenir des instructions détaillées sur la création d'un compte Citrix Cloud, consultez S'inscrire à Citrix Cloud. Accédez à https://citrix.cloud.com et connectez-vous avec votre compte Citrix Cloud.
3. Citrix Analytics for Performance est disponible sous forme d'offre par abonnement, en tant qu'offre autonome ou groupée avec Citrix Analytics for Security. Pour vous abonner à Citrix Analytics for Performance, reportez-vous à `https://www.citrix.com/products/citrix-analytics-performance.html)`.
4. Les versions prises en charge des sources de données sont disponibles dans l'article Sources de données .
5. Citrix Profile Management doit être installé sur toutes les machines.
6. Le service End User Experience Monitoring (EUEM) doit être en cours d'exécution et les stratégies correspondantes doivent être configurées sur toutes les machines. Pour plus de détails, consultez Paramètres de stratégie de surveillance des utilisateurs finaux.
7. La stratégie de **collecte de données VDA pour Performance Analytics** doit être définie sur **Autorisé** sur les machines pour permettre au service de surveillance de collecter des mesures de performance liées aux machines, telles que les statistiques de bande passante et de latence. Pour plus d'informations, consultez la section Stratégie de collecte de données pour Performance Analytics.
8. Activez la stratégie de surveillance des processus de Citrix Studio pour obtenir une meilleure visibilité sur les processus consommant beaucoup de ressources dans l'onglet **Statistiques de la machine > Processus** .
   Pour plus d'informations, voir Activer la surveillance des processus.
9. Garantir l'accessibilité aux URL suivantes à partir de tous les points de terminaison (ou des proxys, s'ils sont configurés) :

Point de terminaison	Région des États-Unis	Région de l'Union européenne	Région Asie-Pacifique Sud
Enregistrement des clés Citrix	`https://trust.citrixnetworkapi.net`	`https://trust.citrixnetworkapi.net`	`https://trust.citrixnetworkapi.net`
Citrix Cloud	`https://trust.citrixworkspacesapi.net`	`https://trust-eu.citrixworkspacesapi.net`	`https://trust-aps.citrixworkspacesapi.net`
Citrix Analytics	`https://api.was.cloud.com`	`https://api-eu.was.cloud.com`	`https://api-aps.was.cloud.com`

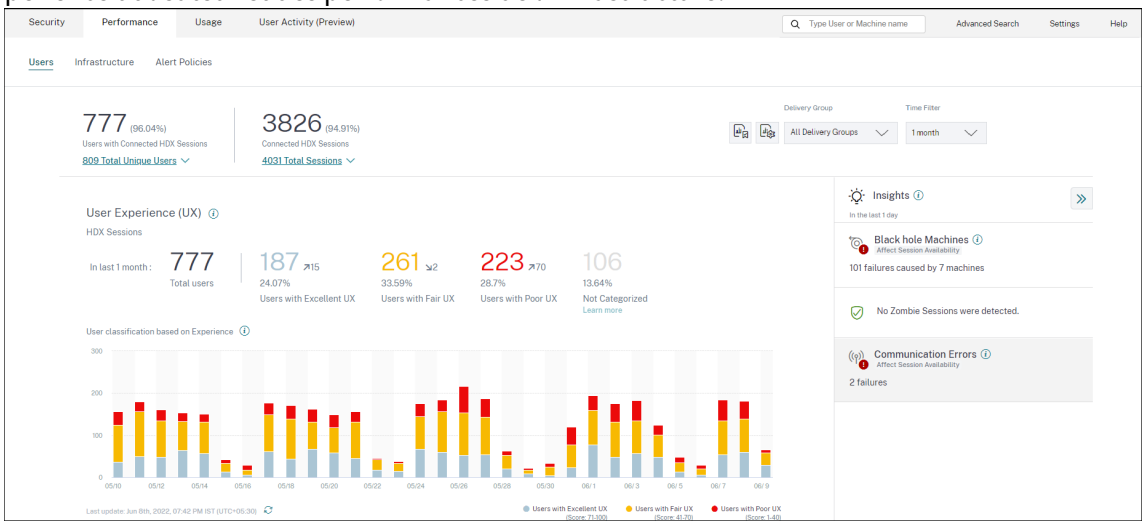
Point de terminaison	Région des États-Unis	Région de l'Union européenne	Région Asie-Pacifique Sud
Chargement en masse	https://citrixanalyticsehub-alias.servicebus.windows.net/	https://citrixanalyticsehub-alias.servicebus.windows.net/	https://citrixanalyticsehaps-alias.servicebus.windows.net/

Accès

1. Connectez-vous à Citrix Cloud. Recherchez la vignette du service Analytics et cliquez sur **Gérer**. La page de présentation affiche les offres disponibles dans le portefeuille Analytics.
2. Dans l'offre **Performance**, pour utiliser la version d'évaluation de l'offre, cliquez sur **Demander une évaluation**. Si vous avez acheté l'offre Citrix Analytics for Performance, cliquez sur le lien **Gérer** .



1. Citrix Analytics for Performance s'ouvre avec des tableaux de bord affichant l'analyse de l'expérience utilisateur et des performances de l'infrastructure.



Accès depuis la région Asie-Pacifique Sud Citrix Analytics for Performance est désormais intégré automatiquement pour les clients d'essai et les clients abonnés dans la région Asie-Pacifique Sud (APS). Pour plus d'informations sur les régions prises en charge dans Citrix Cloud, consultez la section Considérations géographiques.

Pour accéder à Performance Analytics à partir de la région APS, choisissez la région Sud de l'Asie-Pacifique lors de l'intégration de votre locataire à Citrix Cloud. Ouvrez une session sur Citrix Cloud et sélectionnez votre locataire dans la région APS de Citrix Cloud. Utilisez l'URL `https://analytics-aps.cloud.com` pour accéder à votre service Citrix Analytics Cloud.

- Citrix Analytics for Performance stocke désormais les événements utilisateur et les métadonnées de votre organisation dans la région Asie-Pacifique Sud lorsque vous la choisissez comme région d'origine. Pour plus d'informations, voir Gouvernance des données.
- Pour plus d'informations sur la configuration réseau requise pour la région Sud de l'Asie-Pacifique, voir Vue d'ensemble de la sécurité technique.

Configuration des sources de données

Vous pouvez utiliser Performance Analytics pour surveiller les sites locaux ou Cloud. Vous pouvez utiliser cette offre que vous soyez un client local pur, un client Cloud ou un client hybride avec un mélange de sites sur site et de sites cloud.

Performance Analytics détecte automatiquement votre Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service).
Si vous êtes un client local,

- Commencez par embarquer vos sites Citrix Virtual Apps and Desktops à Performance Analytics.
- Pour obtenir des informations relatives au réseau sur Performance Analytics, vous devez également intégrer votre Citrix Gateway local.

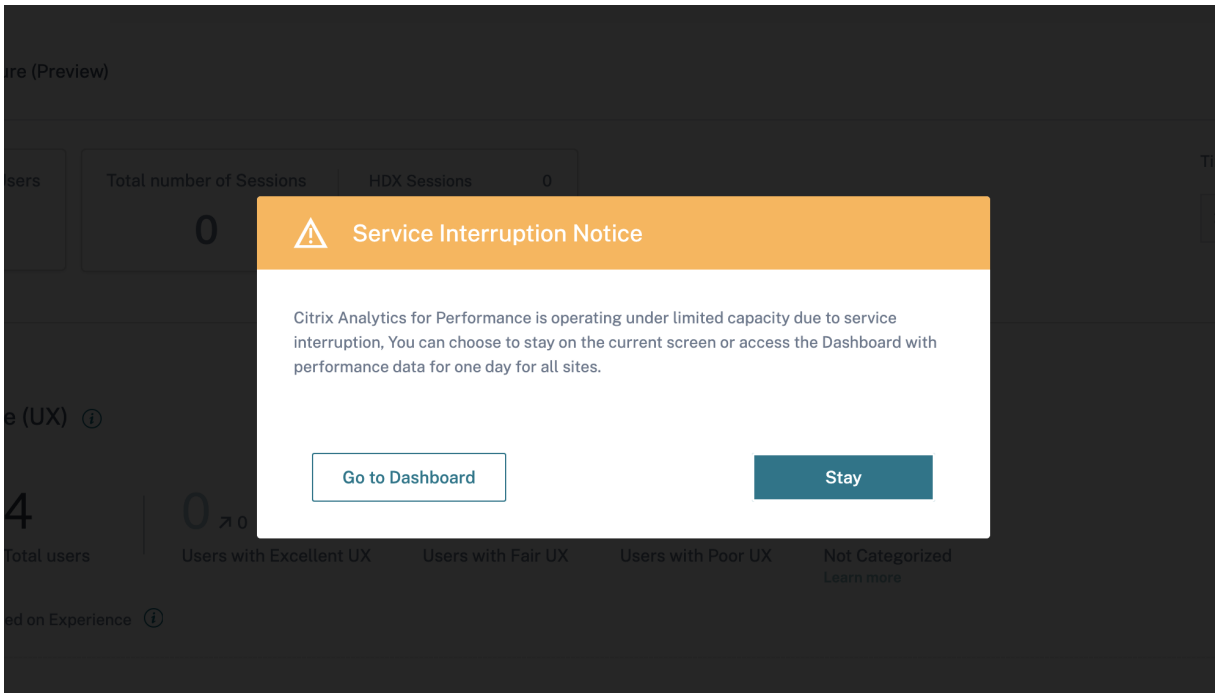
Configurez les sources de données requises comme décrit dans l'article Sources de données .

> **Remarque :**
>
> - Citrix Analytics for Performance collecte et stocke les journaux des points de données répertoriés dans Journaux collectés pour Citrix Analytics for Performance.
> - Les limites recommandées pour le service Citrix Analytics for Performance sont répertoriées dans l'article Limites .

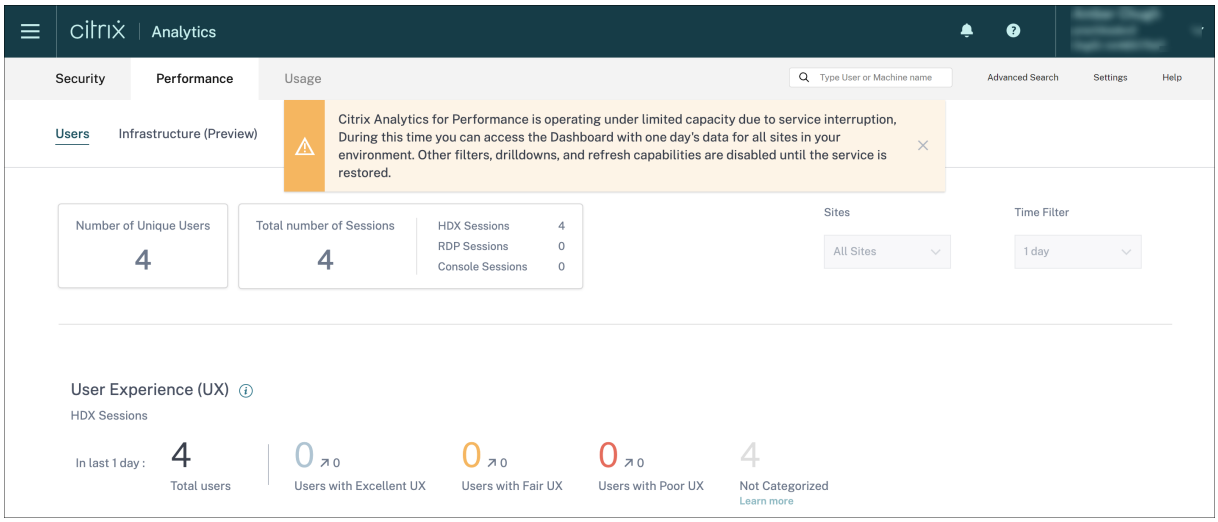
Continuité du service

En cas d'interruption de service, Citrix Analytics for Performance fonctionne avec une capacité limitée.

L'administrateur peut choisir de **rester** et d'afficher les données disponibles sur l'écran actuel ou d'**accéder au tableau de bord** en mode rétrogradé.



En mode rétrogradé, l'utilisateur est basculé vers le tableau de bord contenant les données de tous les sites de la journée écoulée.
Tous les filtres et les descentes sont désactivés jusqu'à ce que le service reprenne son fonctionnement normal dans les deux cas.



Cette mise à jour améliore la résilience du produit et aide à s'aligner sur le contrat de niveau de service.

Résolution des problèmes liés à Citrix Analytics pour la sécurité et les performances

December 7, 2023

Cette section explique comment résoudre les problèmes suivants que vous pouvez rencontrer lorsque vous utilisez Citrix Analytics pour la sécurité.

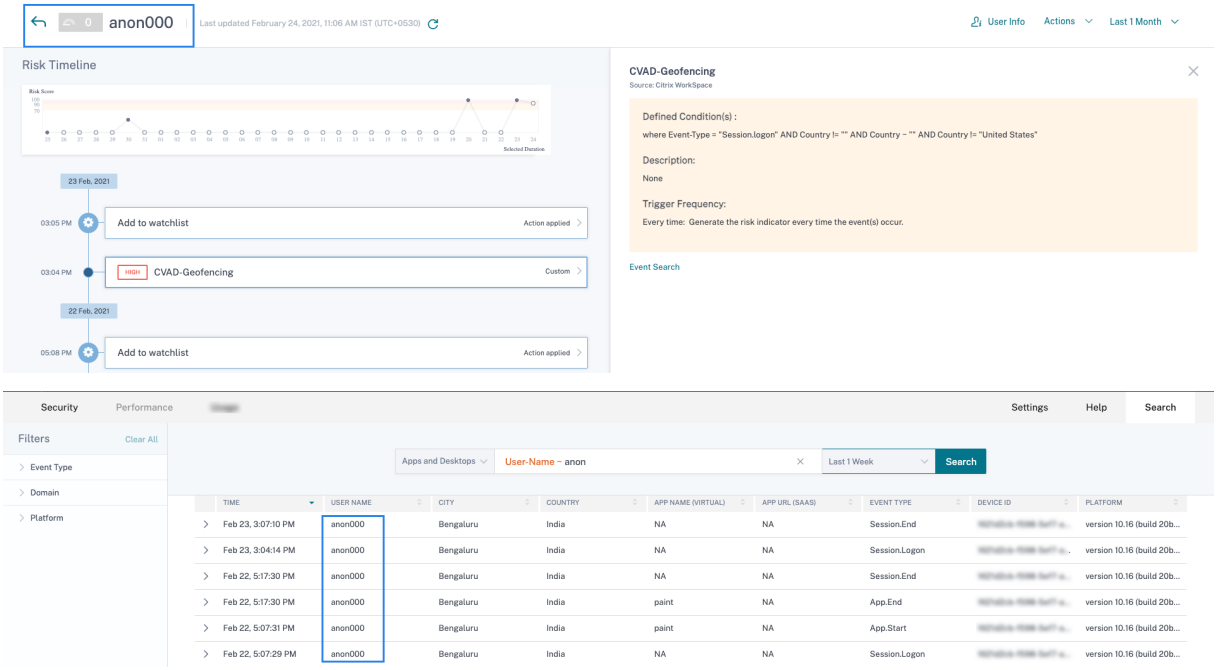
- Vérifiez que les utilisateurs anonymes sont des utilisateurs légitimes.
- Résoudre les problèmes de transmission d'événements à partir d'une source de données.
- Déclenchez des événements Virtual Apps and Desktops, des événements SaaS et vérifiez la transmission des événements à Citrix Analytics for Security.
- Impossible dese connecter au serveur d'enregistrement de session.
- Problèmes de configuration avec le module complémentaire Citrix Analytics pour Splunk

Vérifiez que les utilisateurs anonymes sont des utilisateurs légitimes

August 22, 2022

En tant qu'administrateur, vous remarquerez peut-être que certains de Citrix Virtual Apps and Desktops
utilisateurs et Citrix DaaS (anciennement le Citrix Virtual Apps and Desktops Service) apparaissent comme anonymes sur Citrix Analytics for Security. Ces utilisateurs sont identifiés comme des utilisateurs découverts. Mais leurs noms d'utilisateur apparaissent sous la forme anonXYZ (où « XYZ » représente un nombre à trois chiffres) sur les pages suivantes :

- Utilisateurs
- Chronologie de l'utilisateur
- Utilisateurs risqués
- Recherche en libre-service pour la source de données Apps and Desktops



Lorsque vous voyez de tels utilisateurs, vous voudrez peut-être savoir :

- Qui sont ces utilisateurs ?
- Ces utilisateurs sont-ils de nature légitime ou malveillante ?
- Comment les vérifier ?
- Quelles actions dois-je appliquer pour ces utilisateurs ?

Vous voyez des utilisateurs anonymes dans votre environnement informatique Citrix dans les scénarios suivants :

- Lorsqu'un utilisateur utilise une application de navigateur sécurisée publiée
- Lorsqu'un utilisateur utilise un magasin non authentifié

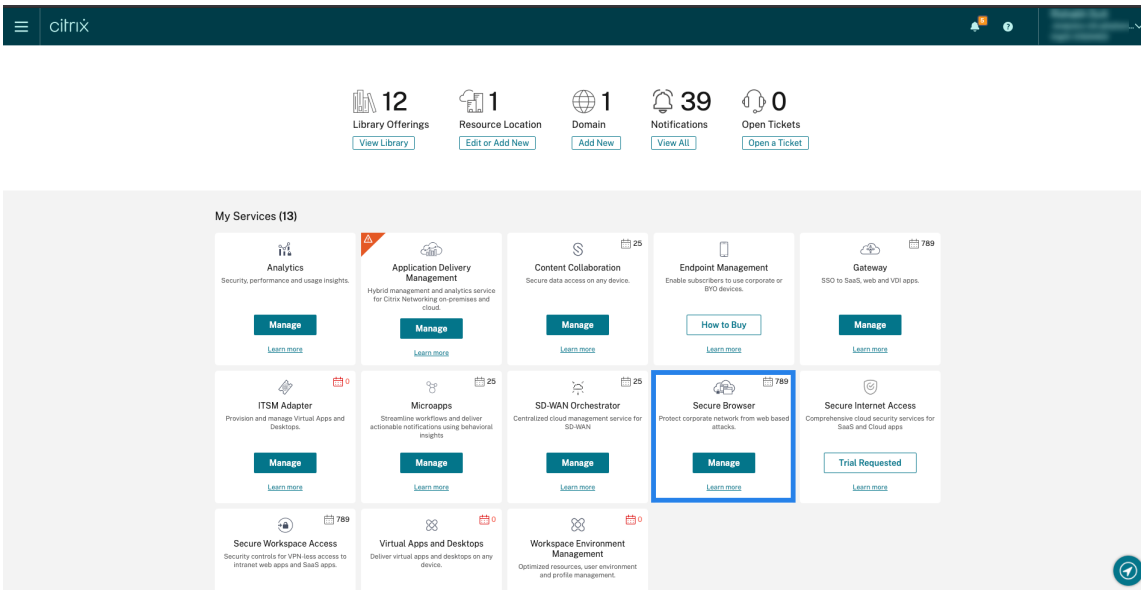
Utilisateur utilisant des applications de navigateur sécurisées publiées

Les applications de navigateur sécurisé sont des applications Web publiées à l'aide du service Citrix Secure Browser. Ces applications isolent vos événements de navigation Web et protègent votre réseau d'entreprise contre les attaques basées sur les navigateurs. Pour plus d'informations, consultez la section Secure Browser Service.

Les applications de navigateur sécurisées utilisent la fonctionnalité de session anonyme de Citrix DaaS.

Pour vérifier si Secure Browser est configuré dans votre compte Citrix Cloud :

1. Connectez-vous à Citrix Cloud.
2. Sur la carte **Secure Browser**, cliquez sur **Gérer**.



3. Sur la page **Gérer**, recherchez les applications de navigateur sécurisées publiées.

Si un utilisateur accède à un magasin StoreFront via des sites Citrix Receiver pour Web à l'aide d'un navigateur Web et utilise les applications de navigateur sécurisées publiées, l'identité de l'utilisateur est masquée. Par conséquent, Citrix Analytics affiche l'utilisateur comme étant anonyme.

Si un utilisateur accède à un magasin StoreFront via une application Citrix Receiver ou Citrix Workspace installée sur son appareil et utilise les applications de navigateur sécurisées publiées, Citrix Analytics affiche l'utilisateur en tant que nom d'utilisateur spécifié dans StoreFront.

Vous pouvez donc considérer l'utilisateur comme un utilisateur légitime de votre organisation. Vous n'avez pas besoin d'appliquer d'action si aucun comportement à risque n'est associé à l'utilisateur.

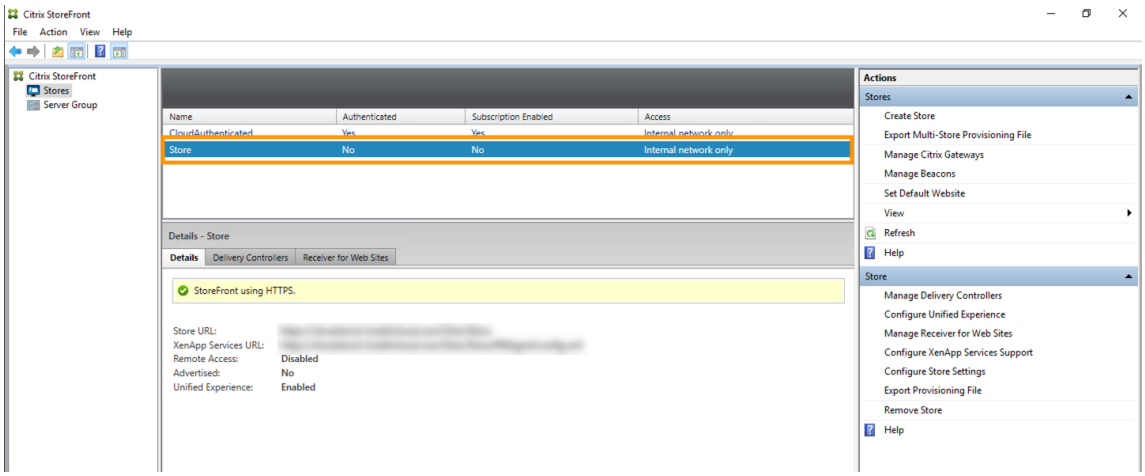
Utilisateur utilisant un magasin non authentifié

Le magasin non authentifié est une fonctionnalité de Citrix StoreFront et s'applique aux magasins gérés par le client. Cette fonctionnalité prend en charge l'accès pour les utilisateurs non authentifiés

(anonymes).

Pour vérifier si votre organisation possède un magasin non authentifié :

1. Lancez Citrix Studio.
2. Cliquez sur **Stores**.
3. Pour vos magasins, vérifiez l'état d'authentification dans la colonne Authentifié.



Si un magasin n'est pas authentifié et que l'utilisateur accède à ce magasin non authentifié, l'identité de l'utilisateur reste anonyme. Par conséquent, Citrix Analytics affiche l'utilisateur comme étant anonyme. Vous pouvez considérer cet utilisateur comme un utilisateur légitime de votre organisation. Vous n'avez pas besoin d'appliquer d'action si aucun comportement à risque n'est associé à l'utilisateur.

Résoudre les problèmes de transmission d'événements à partir d'une source de données

April 12, 2024

Cette section vous permet de résoudre les problèmes de transmission de données dans Citrix Analytics for Security. Lorsqu'une source de données ne parvient pas à transmettre des événements utilisateur avec précision, vous pouvez rencontrer des problèmes tels que la non-découverte des utilisateurs et des indicateurs de risque.

Checklist

Séquence	Chèques
1	Avez-vous le droit d'utiliser Security Analytics ?
2	La source de données est-elle prise en charge dans votre région d'origine ?
3	Votre environnement répond-il à toutes les exigences du système ?
4	Est-ce que toutes les sources de données sont découvertes et que le traitement des données est activé sur Analytics ?
5	Les activités des utilisateurs sur la source de données transmettent-elles des événements avec précision à Analytics ?
6	Les événements des applications et des bureaux virtuels sont-ils transmis à Analytics ?
7	Les événements utilisateur apparaissent-ils sur la page de recherche en libre-service dans Analytics ?
8	Les utilisateurs sont-ils découverts par Analytics ?

Contrôle 1- Avez-vous le droit d'utiliser Security Analytics ?

Citrix Analytics for Security est une offre basée sur un abonnement. Pour plus d'informations, reportez-vous à la section Mise en route.

Contrôle 2 : la source de données est-elle prise en charge dans votre région d'origine ?

Citrix Analytics for Security est pris en charge dans les régions d'origine suivantes :

- États-Unis (US)
- Union européenne (UE)
- Asie-Pacifique Sud (APS)

Selon l'emplacement de votre organisation, vous pouvez intégrer Citrix Cloud dans l'une des régions d'origine.

Toutefois, certaines sources de données ne sont pas prises en charge dans toutes les régions d'origine. La [ou les sources de données]((/en-us/security-analytics/data-sources.html)sont les produits à partir

desquels Citrix Analytics for Security reçoit des événements utilisateur.

Si votre organisation est intégrée à Citrix Cloud dans une région d'origine où une source de données n'est pas prise en charge, vous n'obtenez pas les événements utilisateur de la source de données.

Utilisez le tableau suivant pour afficher les sources de données et les régions dans lesquelles elles sont prises en charge.

Source de données	Supporté dans la région des États-Unis	Soutenu dans la région UE	Supporté dans la région APS
Citrix Endpoint Management	Oui	Oui	Oui
Citrix Gateway (local)	Oui	Oui	Oui
Fournisseur d'identité Citrix	Oui	Oui	Oui
Citrix Secure Browser	Oui	Oui	Oui
Citrix Secure Private Access	Oui	Non	Non
Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service)	Oui	Oui	Oui
Citrix Virtual Apps and Desktops sur site	Oui	Oui	Oui
Microsoft Active Directory	Oui	Oui	Oui
Microsoft Graph Security	Oui	Oui	Oui

Contrôle 3 : votre environnement répond-il à toutes les exigences du système ?

Citrix Analytics peut prendre quelques minutes pour recevoir les événements utilisateur provenant des sources de données. Si vous ne voyez aucun événement utilisateur sur les cartes de site de la source de données, assurez-vous que votre environnement répond aux conditions préalables et à la configuration système requise.

Conditions préalables

1. Tous vos abonnements Citrix Cloud doivent être actifs. Sur la page Citrix Cloud, assurez-vous que tous les services Citrix Cloud sont actifs.

2. Si vous utilisez des sites locaux de Citrix Virtual Apps and Desktops, vous devez ajouter vos sites à Citrix Workspace et configurer l'agrégation de sites. Citrix Analytics détecte automatiquement les sites ajoutés à Citrix Workspace. Pour plus d'informations, consultez la rubrique Agréger des applications et bureaux virtuels locaux dans des espaces de travail.
3. Si vous utilisez un déploiement StoreFront pour vos sites, configurez vos serveurs StoreFront pour permettre à l'application Citrix Workspace d'envoyer des événements utilisateur à Citrix Analytics. Assurez-vous que la version StoreFront est 1906 ou ultérieure. Si vous ne configurez pas le serveur StoreFront, Citrix Analytics ne parvient pas à recevoir des événements utilisateur en provenance de locaux de Citrix Virtual Apps and Desktops. Pour configurer le déploiement StoreFront, consultez l'article sur le service Citrix Analytics dans la documentation StoreFront.
4. Les de Citrix Virtual Apps and Desktops utilisateurs et Citrix DaaS les utilisateurs doivent utiliser la version spécifiée des applications Citrix Workspace ou Citrix Receiver sur leurs terminaux. Dans le cas contraire, Analytics ne reçoit pas les événements utilisateur en provenance des points de terminaison utilisateur. La liste des versions prises en charge de l'application Citrix Workspace ou de Citrix Receiver est disponible dans les sources de données Citrix Virtual Apps and Desktops et Citrix DaaS.
5. Pour recevoir les événements des utilisateurs à partir d'une session Secure Browser publiée, activez le paramètre **Hostname Tracking** dans le Secure Browser. Par défaut, ce paramètre est désactivé. Pour plus d'informations, consultez Gérer les navigateurs sécurisés publiés.
6. Intégrez vos sources de données comme indiqué dans les articles suivants :
    - Source de données de Citrix Endpoint Management
    - Source de données de Citrix Gateway
    - Source de données Citrix Secure Private Access
    - Source de données Citrix Virtual Apps and Desktops et Citrix DaaS
    - Intégration de Microsoft Active Directory
    - Intégration de Microsoft Graph Security

Contrôle 4 : toutes les sources de données sont-elles découvertes et le traitement des données est-il activé dans Analytics ?

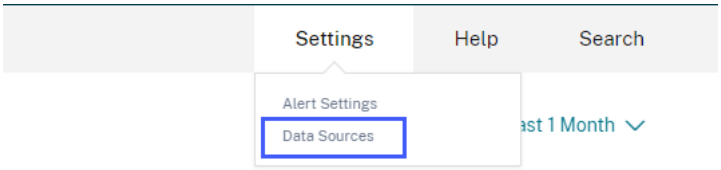
Assurez-vous que toutes vos sources de données sont découvertes et que vous avez activé le traitement des données pour elles. Si vous n'activez pas le traitement des données pour une source de données, les utilisateurs utilisant la source de données ne sont pas découverts. Cette situation peut créer un risque potentiel pour la sécurité.

L'activation du traitement des données garantit que Citrix Analytics traite vos événements utilisateur. Les événements sont envoyés à Citrix Analytics uniquement lorsque les utilisateurs utilisent activement la source de données.

> **Remarque**
>
> Citrix Analytics n'extrait pas activement les données de votre environnement.

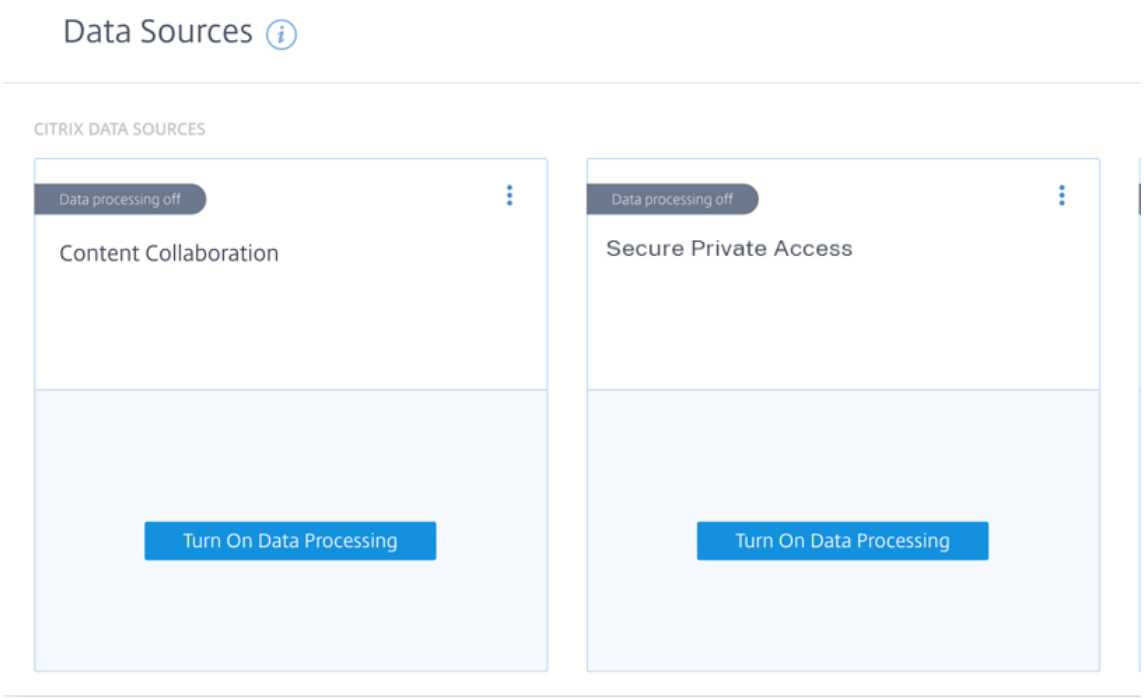
Pour découvrir vos sources de données et activer les analyses, procédez comme suit :

1. Cliquez sur **Paramètres** > **Sources de données** > **Sécurité** pour afficher vos sources de données découvertes. Citrix Analytics découvre automatiquement les sources de données auxquelles vous avez souscrit à votre compte Citrix Cloud.

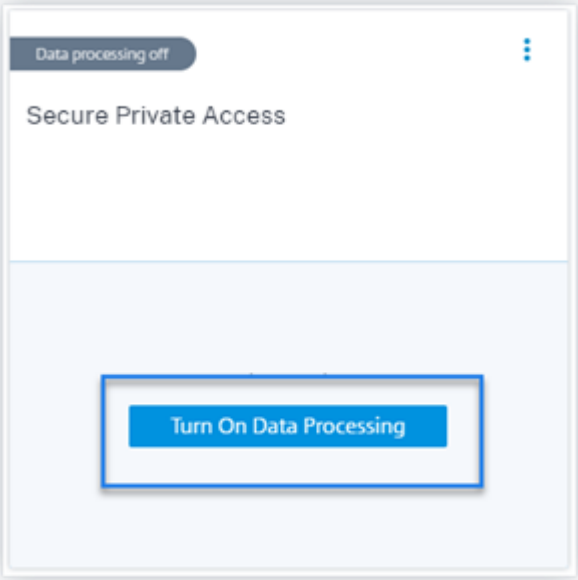


2. Sur la page **Sources de données**, les sources de données découvertes apparaissent sous forme de fiches de site. Par défaut, le traitement des données est désactivé.

> **Important**
>
> Citrix Analytics traite vos données après avoir donné votre consentement.



3. Cliquez **sur Activer le traitement des données** sur la carte de site pour laquelle vous souhaitez que Citrix Analytics traite les événements. Par exemple, sur la fiche de Citrix Secure Private Access site, cliquez **sur Activer le traitement des données**.



4. Une fois que vous avez activé le traitement des données, Citrix Analytics traite les événements de la source de données. Le statut de la fiche du site passe à Traitement des données. Vous pouvez afficher le nombre d'utilisateurs et les événements reçus en fonction de la période sélectionnée.

5. Pour toutes les sources de données découvertes, suivez les étapes spécifiées dans Mise en route pour activer les analyses.

Contrôle 5 : les activités des utilisateurs sur la source de données transmettent-elles des événements avec précision à Analytics ?

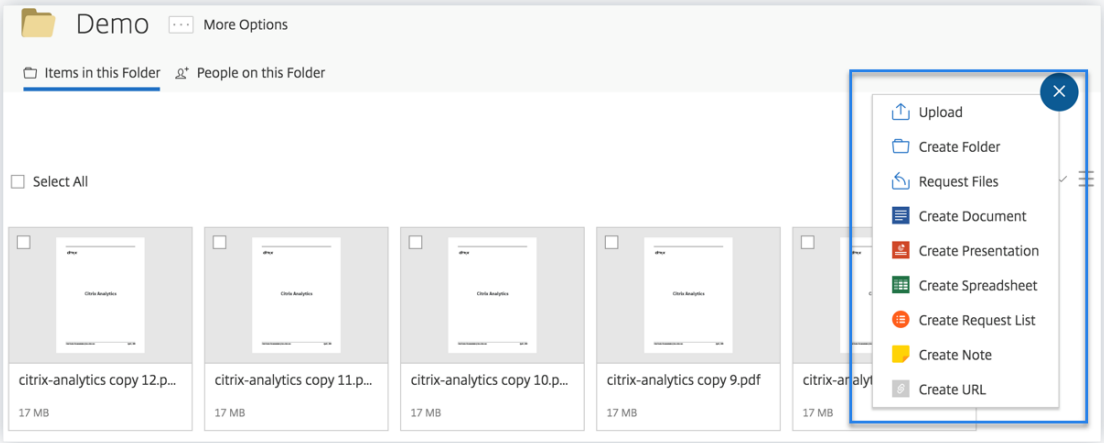
Citrix Analytics reçoit des événements utilisateur provenant des sources de données lorsque les utilisateurs utilisent activement les sources de données. Les utilisateurs doivent effectuer certaines activités sur la source de données pour générer des événements. Par exemple, pour recevoir des événements depuis la source de données Apps and Desktops, les utilisateurs d'Apps and Desktops doivent partager, charger ou télécharger certains fichiers.

> **Remarque**
>
> Citrix Analytics n'extrait pas activement les données de votre environnement.

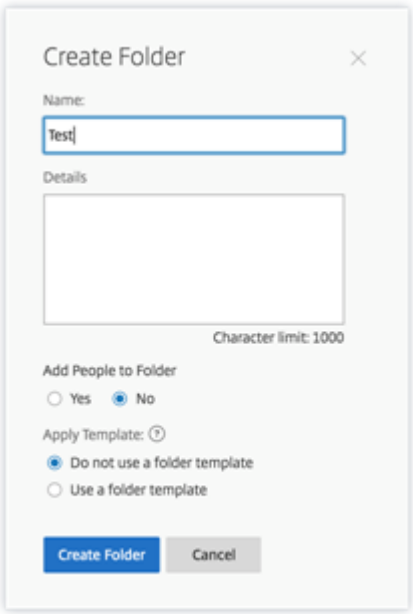
Si vous ne voyez aucun événement utilisateur dans Citrix Analytics pour votre source de données, il est fort probable que les utilisateurs ne soient pas actifs à ce moment-là.

Pour vérifier que Citrix Analytics reçoit correctement les événements utilisateur, effectuez l'activité suivante. Cette activité utilise la source de données Citrix Apps and Desktops. Vous pouvez effectuer une activité similaire en utilisant d'autres produits Citrix (sources de données) en fonction de votre abonnement.

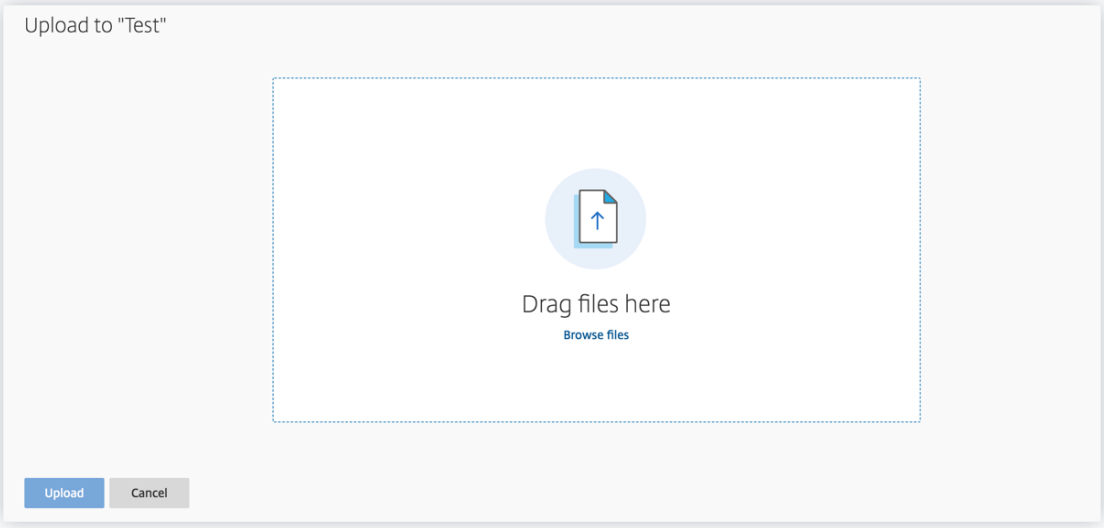
1. Ouvrez une session sur le service Citrix Apps and Desktops.
2. Effectuez certaines activités habituelles de l'utilisateur, telles que créer un dossier, télécharger des fichiers, télécharger des fichiers ou supprimer des fichiers.



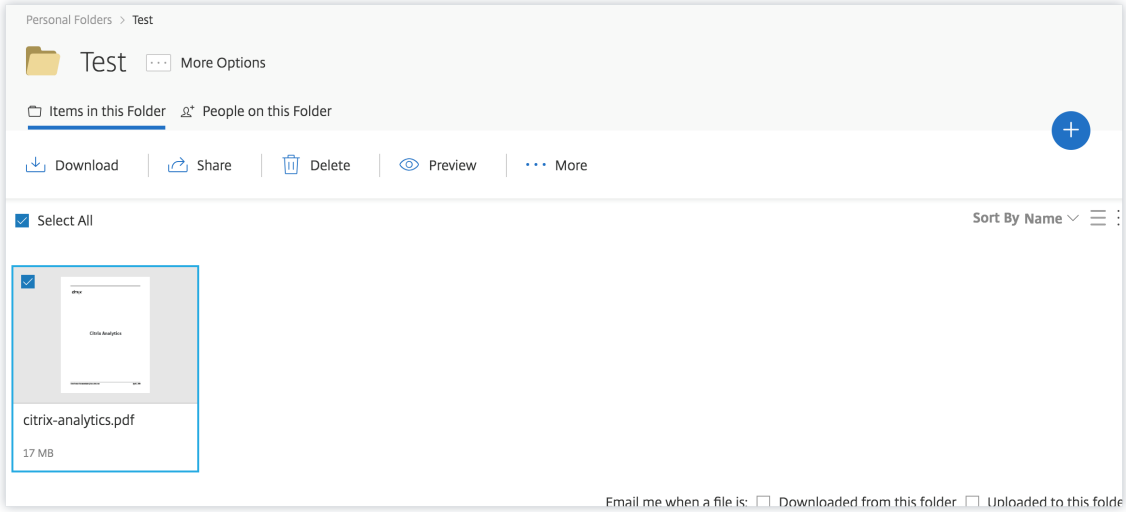
3. Par exemple, créez un dossier Test.



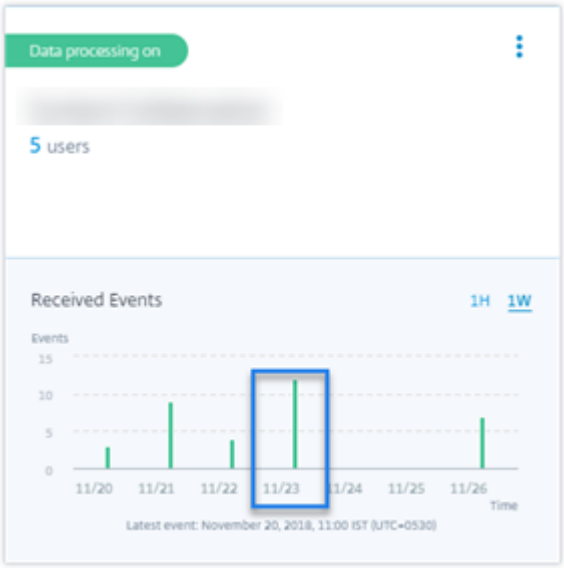
4. Téléchargez des fichiers locaux.



5. Supprimez certains fichiers du dossier.



6. Revenez à Citrix Analytics et consultez la fiche **Apps and Desktops** sur la page Source de données. Citrix Analytics reçoit les événements utilisateur depuis la source de données Apps and Desktops et les affiche sur la fiche du site.



Contrôle 6 : les événements des applications et des bureaux virtuels sont-ils transmis à Analytics ?

Certaines versions de l'application Citrix Workspace ou du client Citrix Receiver ne parviennent pas à envoyer les événements utilisateur à Citrix Analytics. Lorsque les utilisateurs lancent des applications et des bureaux virtuels via ces clients, Citrix Analytics ne parvient pas à découvrir les utilisateurs tant qu'ils n'ont pas effectué les événements pris en charge.

Par exemple, l'application Citrix Workspace pour Linux 2006 ou version ultérieure n'envoie pas les événements de ***lancement d'application SaaSet de fin d'application SaaS*** à Citrix Analytics. Un util-

isateur qui lance une application SaaS à l'aide de l'application Citrix Workspace pour Linux n'est pas détecté sur Citrix Analytics.

Événements pris en charge

Reportez-vous au tableau suivant pour vérifier les événements utilisateur pris en charge par chaque version du client.

- **Oui**- L'événement est envoyé par le client à Citrix Analytics.
- **Non**- L'événement n'est pas envoyé par le client à Citrix Analytics.
- **NA**- L'événement n'est pas applicable au client.

Événement	Application Workspace pour Windows 1907 ou version ultérieure	Application Workspace pour Mac 1910.2 ou version ultérieure	Application Workspace pour Linux 2006 ou version ultérieure	Application Workspace pour Android - Dernière version disponible sur Google Play	Application Workspace pour iOS : dernière version disponible dans l'App Store d'Apple	Application Workspace pour Chrome - Dernière version disponible dans le Chrome Web Store	Application Workspace pour HTML5 2007 ou version ultérieure
Ouverture de session de compte	Oui	Oui	Oui	Oui	Oui	Non	Non
Ouverture de session	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Lancement de session	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Fin de session	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Démarrage de l'application	Oui	Oui	Oui	Non	Oui	Oui	Oui

Événement	Application Workspace pour Windows 1907 ou version ultérieure	Application Workspace pour Mac 1910.2 ou version ultérieure	Application Workspace pour Linux 2006 ou version ultérieure	Application Workspace pour Android - Dernière version disponible sur Google Play	Application Workspace pour iOS : dernière version disponible dans l'App Store d'Apple	Application Workspace pour Chrome - Dernière version disponible dans le Chrome Web Store	Application Workspace pour HTML5 2007 ou version ultérieure
Fin de l'application	Oui	Oui	Oui	Non	Oui	Oui	Oui
Téléchargement de fichier	Oui	Oui	Oui	Non	Non	Oui	Oui
Impression	Non	Oui	Oui	Non	Non	Oui	Oui
Lancement de l'application SaaS	Oui	Oui	Non	Non	Non	Non	Non
Fin de l'application SaaS	Oui	Oui	Non	Non	Non	Non	Non
Navigation dans les URL des applications SaaS	Oui	Oui	Non	Non	Non	Non	Non
Accès au presse-papiers des applications SaaS	Oui	Oui	Non	Non	Non	Non	Non

Événement	Application Workspace pour Windows 1907 ou version ultérieure	Application Workspace pour Mac 1910.2 ou version ultérieure	Application Workspace pour Linux 2006 ou version ultérieure	Application Workspace pour Android - Dernière version disponible sur Google Play	Application Workspace pour iOS : dernière version disponible dans l'App Store d'Apple	Application Workspace pour Chrome - Dernière version disponible dans le Chrome Web Store	Application Workspace pour HTML5 2007 ou version ultérieure
Téléchargement de fichiers SaaS App	Oui	Oui	Non	Non	Non	Non	Non
Impression de fichiers d'applications SaaS	Oui	Oui	Non	Non	Non	Non	Non

En fonction de l'état de transmission des événements, vous pouvez rencontrer les problèmes suivants :

- Lorsque les utilisateurs se connectent à leurs clients de Citrix Virtual Apps and Desktops ou Citrix DaaS utilisent les clients, ils peuvent ne pas être découverts dans Citrix Analytics tant qu'ils n'ont pas effectué un événement (activité) pris en charge. Par exemple, considérez deux événements utilisateur : App Start et SaaS App Launch. Un utilisateur qui utilise l'application Citrix Workspace pour iOS reçoit l'événement App Start mais pas l'événement SaaS App Launch. Ainsi, lorsque l'utilisateur lance des applications virtuelles, l'événement App Start est transmis à Citrix Analytics et l'utilisateur est découvert. Toutefois, si l'utilisateur lance une application SaaS, Citrix Analytics ne reçoit pas l'événement SaaS App Launch et l'utilisateur n'est pas découvert. Pour plus d'informations sur les utilisateurs découverts, consultez la section Utilisateurs découverts.
- Les événements marqués comme **Non** dans le tableau n'apparaissent pas sur la page de recherche en libre-service. Pour plus d'informations sur l'utilisation de la page en libre-service, consultez la rubrique A propos de la recherche en libre-service.

Conseil

Pour profiter au maximum des avantages d'Analytics, Citrix recommande ce qui suit :

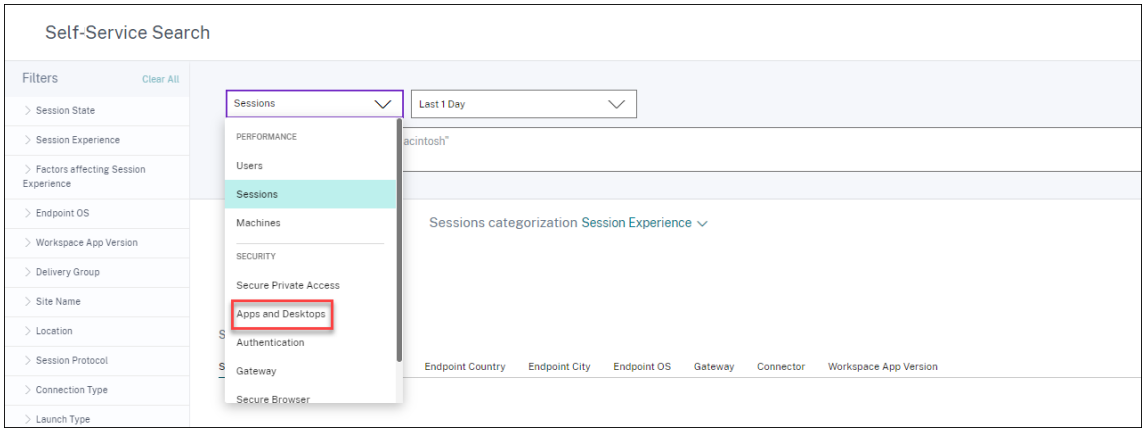
- **Utilisateur Windows** : connectez-vous à votre Citrix Virtual Apps and Desktops et Citrix DaaS application Citrix Workspace pour Windows 1907 ou version ultérieure.
- **Utilisateur Mac** : connectez-vous à Citrix Virtual Apps and Desktops et Citrix DaaS l'aide de l' application Citrix Workspace pour Mac 1910.2 ou version ultérieure.

Contrôle 7 : les événements utilisateur apparaissent-ils sur la page de recherche en libre-service dans Analytics ?

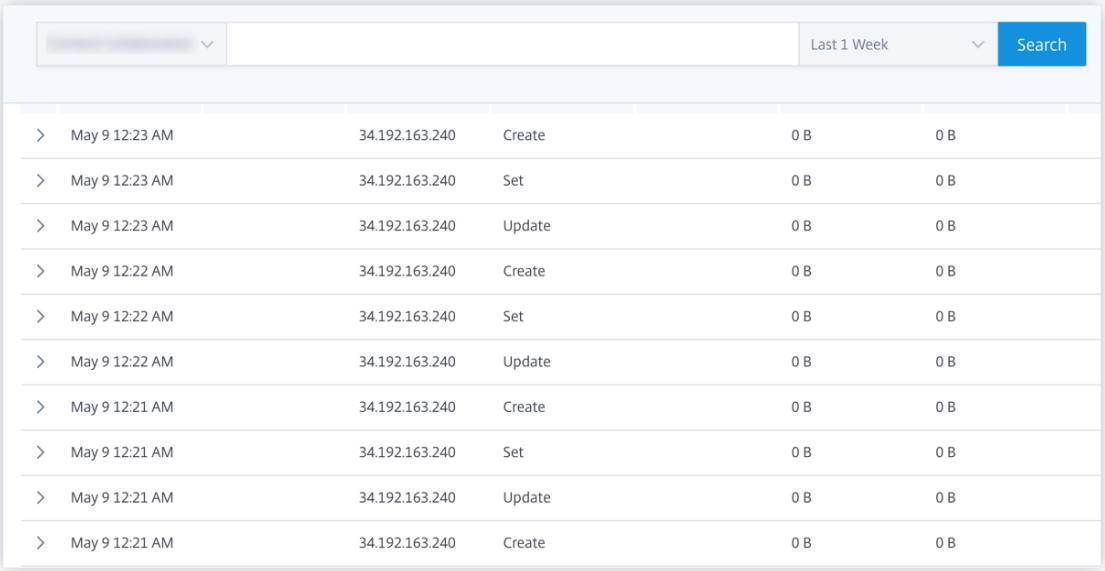
Effectuez cette dernière vérification pour vous assurer que les événements sont transmis avec précision à Citrix Analytics.

1. Dans la barre supérieure, cliquez sur **Recherche avancée** pour accéder à la page de recherche en libre-service.

2. Sélectionnez la source de données pour afficher la page de recherche correspondante et les événements.



3. Pour afficher les données associées aux événements Apps and Desktops, sélectionnez **Apps and Desktops** dans la liste, sélectionnez la période, puis cliquez sur **Rechercher**.



Pour plus d'informations, consultez la rubrique Recherche en libre-service.

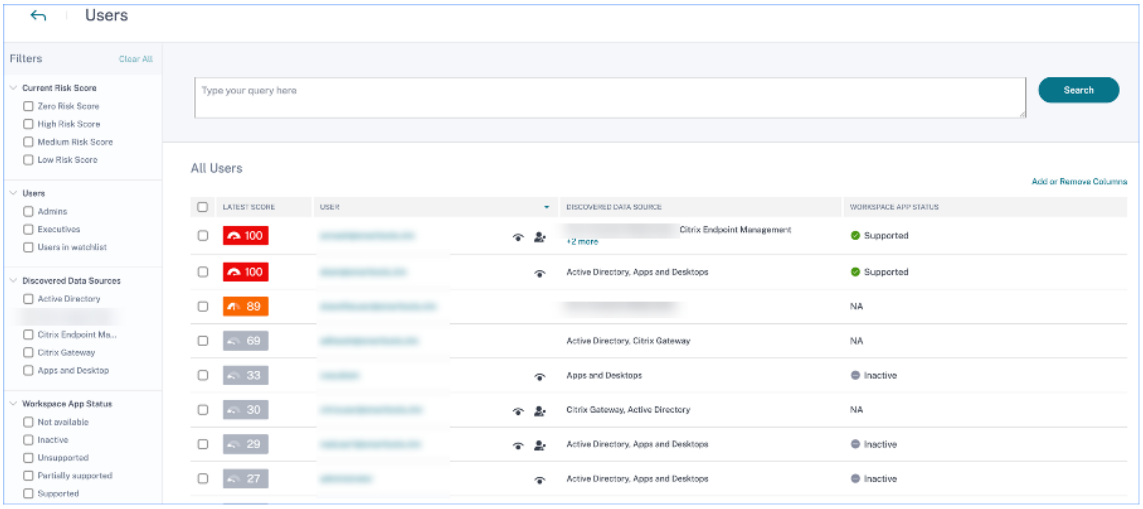
Contrôle 8 : les utilisateurs sont-ils découverts par Analytics ?

Lorsque les événements commencent à être transmis à Citrix Analytics, les utilisateurs qui les génèrent sont découverts et affichés sur le tableau de bord des **utilisateurs** . Ce processus prend généralement quelques minutes avant de pouvoir les afficher sur le tableau de bord.

1. Cliquez sur le lien **Utilisateurs découverts** dans le tableau de bord **Utilisateurs** pour afficher la liste complète des utilisateurs découverts par Citrix Analytics.

2. La page **Utilisateurs** affiche la liste de tous les utilisateurs découverts au cours des 31 derniers jours. Sélectionnez la période pour afficher les occurrences des indicateurs de risque.

> **Remarque**
>
> Si vous essayez de définir une valeur supérieure à 31 jours, le système affiche un message d'erreur indiquant : **Plage de dates non valide. La plage maximale autorisée entre la date de début et la date de fin est de 31 jours**.



Si les événements sont transmis avec succès, votre environnement Citrix Analytics fonctionne comme prévu. Des indicateurs de risque sont générés lorsque des anomalies sont détectées.

Déclencher des événements Virtual Apps and Desktops, des événements SaaS et vérification de la transmission des événements

April 12, 2024

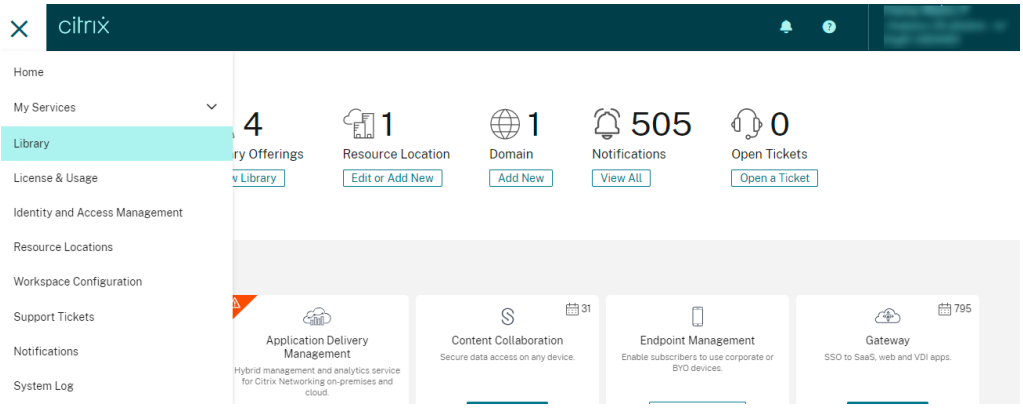
Cette section décrit les procédures permettant de déclencher des événements Apps and Desktops, des événements SaaS et de vérifier que Citrix Analytics for Security reçoit activement ces événements utilisateur.

Conditions préalables

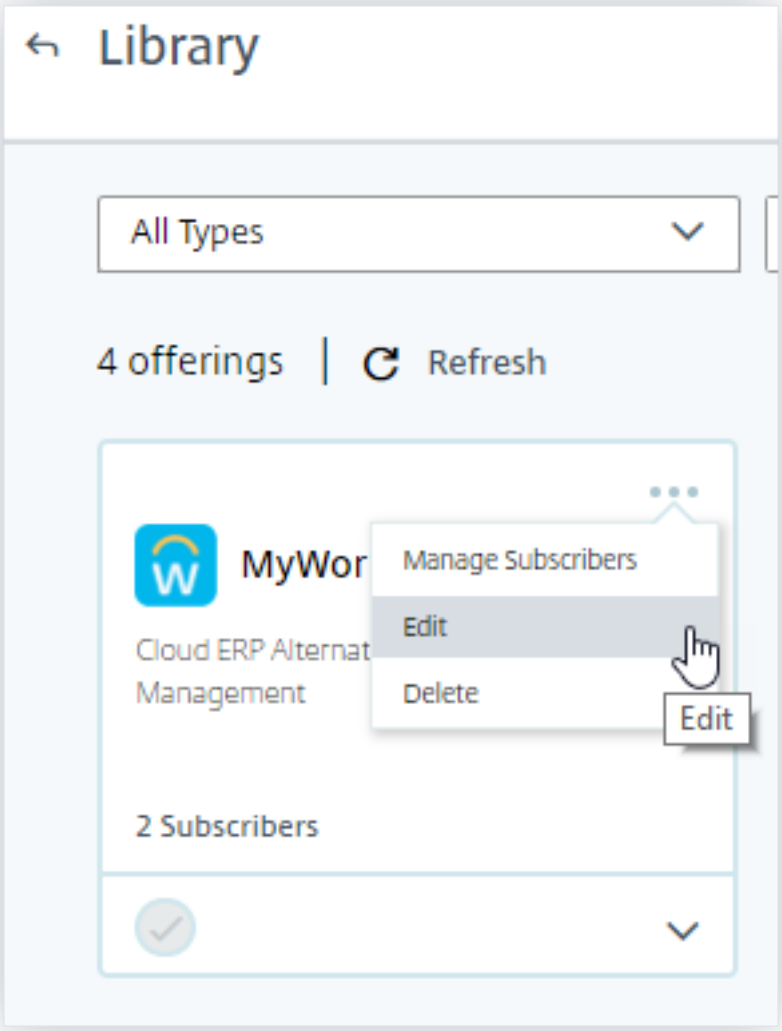
- Si vous utilisez des sites locaux de Citrix Virtual Apps and Desktops, intégrez vos sites locaux à Citrix Analytics et activez le traitement des données à partir de la fiche de site. Si vous utilisez Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service), activez le traitement des données directement à partir de la carte de site. Pour plus d'informations, consultez Citrix Virtual Apps and Desktops et Source de données Citrix DaaS.
- Utilisez les versions appropriées de l'application Citrix Workspace ou de Citrix Receiver sur les terminaux des utilisateurs afin que les événements soient envoyés avec précision à Citrix Analytics. Pour plus d'informations, consultez Citrix Virtual Apps and Desktops et Source de données Citrix DaaS.
- Avant de déclencher l'événement d'impression à partir de votre bureau virtuel, assurez-vous qu'une imprimante est configurée et provisionnée dans votre environnement Apps and Desk-

tops. Pour plus d'informations sur la gestion d'une imprimante, reportez-vous à la section Impression.

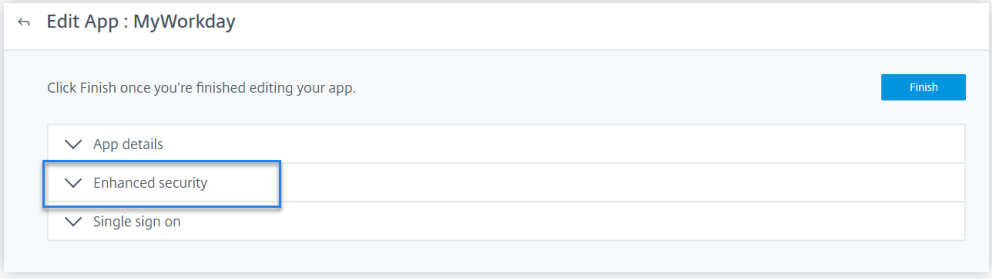
- Pour déclencher les événements SaaS tels que le lancement d'applications SaaS, la navigation par URL d'application SaaS, le téléchargement de fichiers d'applications SaaS, vous devez utiliser une application SaaS configurée à partir de Workspace. Les applications SaaS les plus utilisées sont Salesforce, Workday, Concur, GoTo Meeting.
  - Si aucune application SaaS n'est configurée, vous devez configurer et publier une application SaaS. Pour plus d'informations, consultez la section Prise en charge des applications Software as a Service. Lors de la configuration d'une application SaaS, assurez-vous que les options de sécurité suivantes sont désactivées :
    - Restreindre l'accès au presse-papiers
    - Restreindre l'impression
    - Restreindre la navigation
    - Limiter le téléchargement
  - Si vous souhaitez utiliser une application SaaS déjà configurée à partir de votre espace de travail pour déclencher les événements, assurez-vous que les options de sécurité améliorées spécifiées sont désactivées pour l'application SaaS :
    1. Accédez à votre compte Citrix Cloud et sélectionnez **Bibliothèque**.



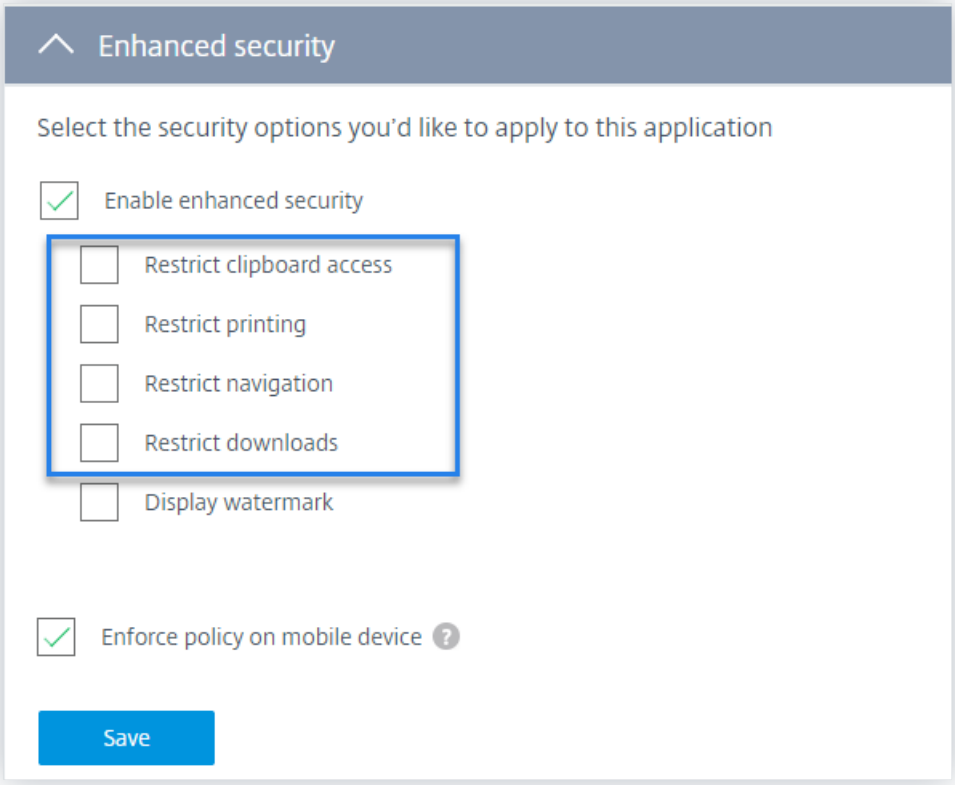
    2. Sur la page **Bibliothèque**, identifiez l'application SaaS que vous souhaitez utiliser pour vérifier les événements. Par exemple, Workday.
    3. Cliquez sur les points de suspension, puis sélectionnez **Modifier**.



4. Sur la page **Modifier l'application**, cliquez sur la flèche vers le bas pour renforcer la sécurité.



5. Assurez-vous que les options de sécurité suivantes ne sont pas sélectionnées.



Problème connu

Quelques versions de l'application Citrix Workspace et de Citrix Receiver ne parviennent pas à envoyer certains événements à Citrix Analytics. Par conséquent, Citrix Analytics ne peut pas fournir d'informations et générer des indicateurs de risque pour ces événements. Pour plus d'informations sur le problème et sa solution de contournement, consultez le problème connu CAS-16151.

Procédure

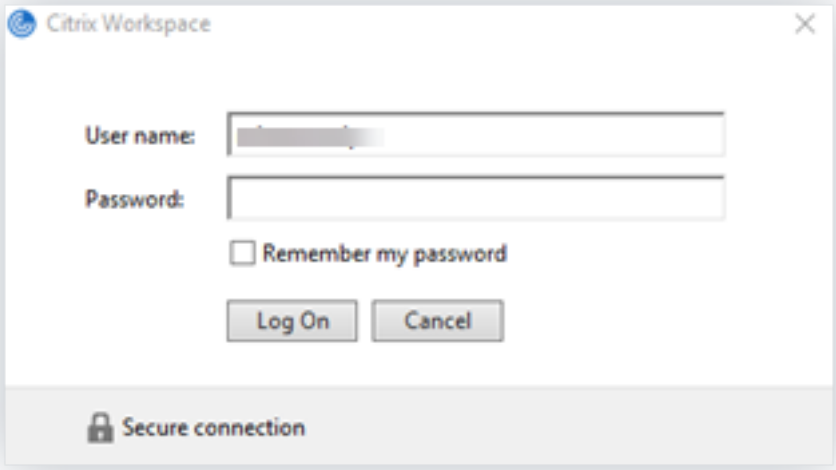
Effectuez les étapes suivantes dans l'ordre pour déclencher les événements dans votre environnement Apps and Desktops et vérifier que Citrix Analytics for Security reçoit activement ces événements.

> **Remarque**
>
> - Les événements peuvent prendre un certain temps pour atteindre Citrix Analytics. Actualisez la page Citrix Analytics si vous ne voyez pas les événements déclenchés.
> - Pour déclencher les événements SaaS, cette procédure utilise l'application Workday à titre

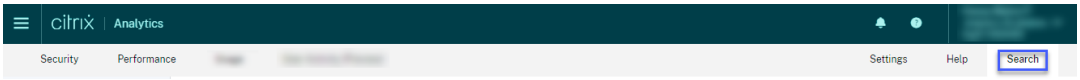
> d'exemple. Vous pouvez utiliser toutes les applications SaaS configurées depuis votre espace de travail pour déclencher les événements SaaS.

- **Ouverture de session de compte**

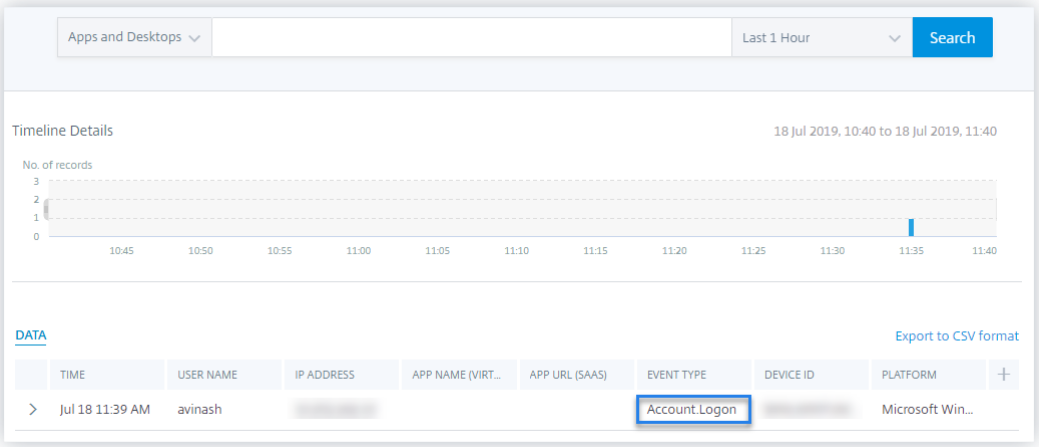
  1. Lancez l'application Citrix Workspace ou Citrix Receiver pour accéder à votre Workspace ou StoreFront.
  2. Entrez vos informations d'identification pour vous connecter à l'application Citrix Workspace ou à Citrix Receiver.



  3. Accédez à Citrix Analytics.
  4. Cliquez sur **Rechercher** et sélectionnez **Apps and Desktops** dans la liste.

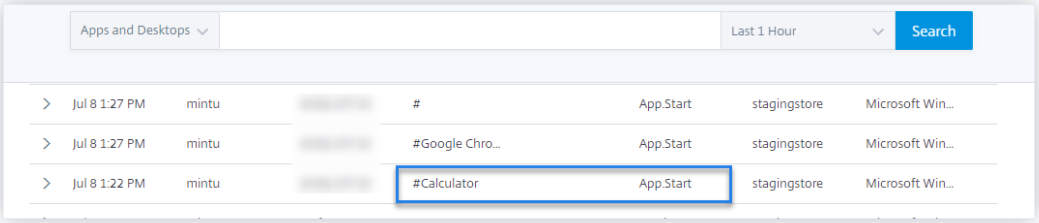


  5. Dans la page de recherche, affichez les données de l'événement **Account.Logon** . Développez la ligne pour afficher les détails de l'événement.



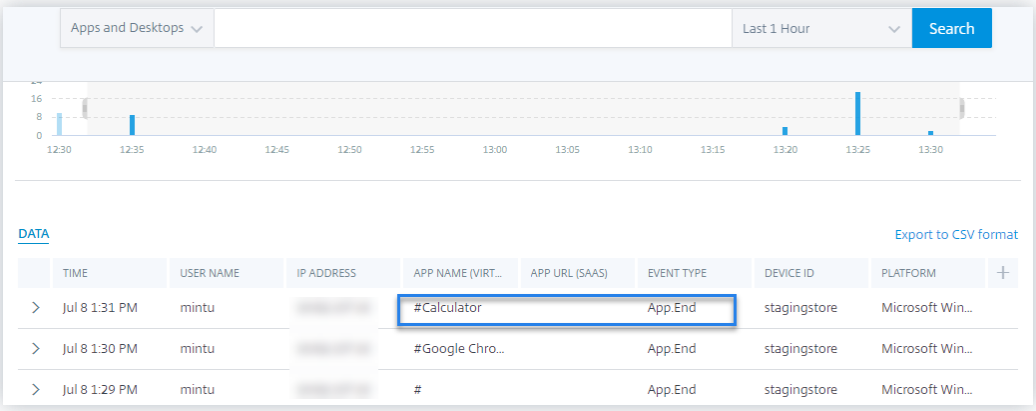
- **Démarrage de l'application**

  1. Lancez l'application Citrix Workspace ou Citrix Receiver pour accéder à votre Workspace ou StoreFront.
  2. Lancez une application telle que la calculatrice.
  3. Accédez à Citrix Analytics.
  4. Cliquez sur **Rechercher** et sélectionnez **Applications et postes de travail**.
  5. Dans la page de recherche, affichez les données de l'événement **App.Start** . Développez la ligne pour afficher les détails de l'événement.



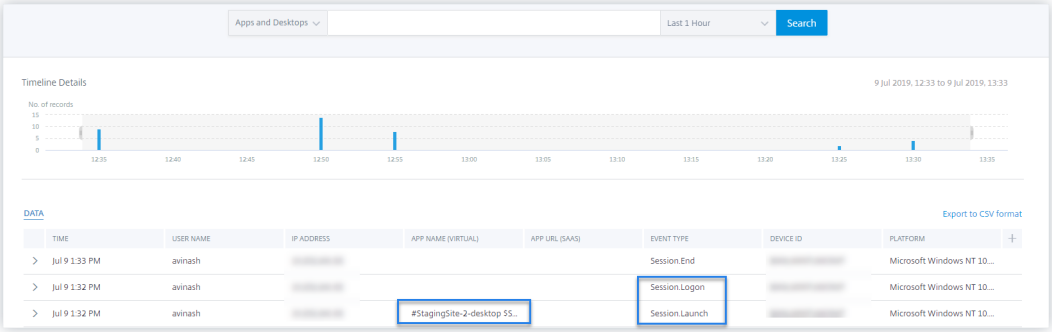
- **Fin de l'application**

  1. Fermez la calculatrice que vous avez déjà lancée dans votre espace de travail ou StoreFront.
  2. Accédez à Citrix Analytics.
  3. Cliquez sur **Rechercher** et sélectionnez **Applications et postes de travail**.
  4. Dans la page de recherche, affichez les données des événements **App.End** . Développez la ligne pour afficher les détails de l'événement.



- **Ouverture de session et lancement de session**

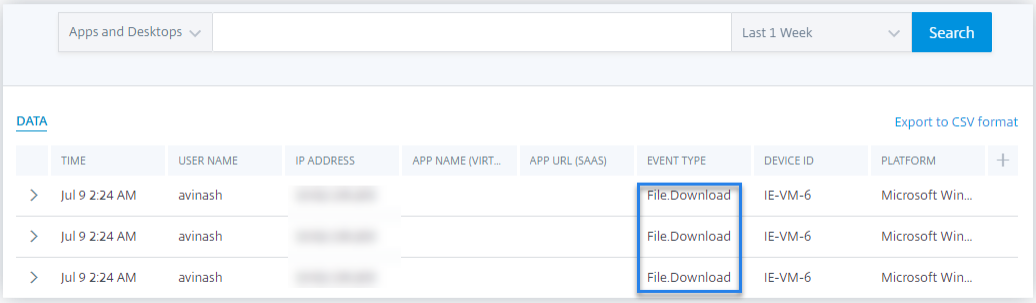
  1. Lancez l'application Citrix Workspace ou Citrix Receiver pour accéder à votre Workspace ou StoreFront.
  2. Lancez votre bureau virtuel.
  3. Accédez à Citrix Analytics.
  4. Cliquez sur **Rechercher** et sélectionnez **Applications et postes de travail**.
  5. Dans la page de recherche, affichez les données des événements **Session.Logon** et **Session.Launch** . Développez la ligne pour afficher les détails de l'événement.



- **Téléchargement de fichier**

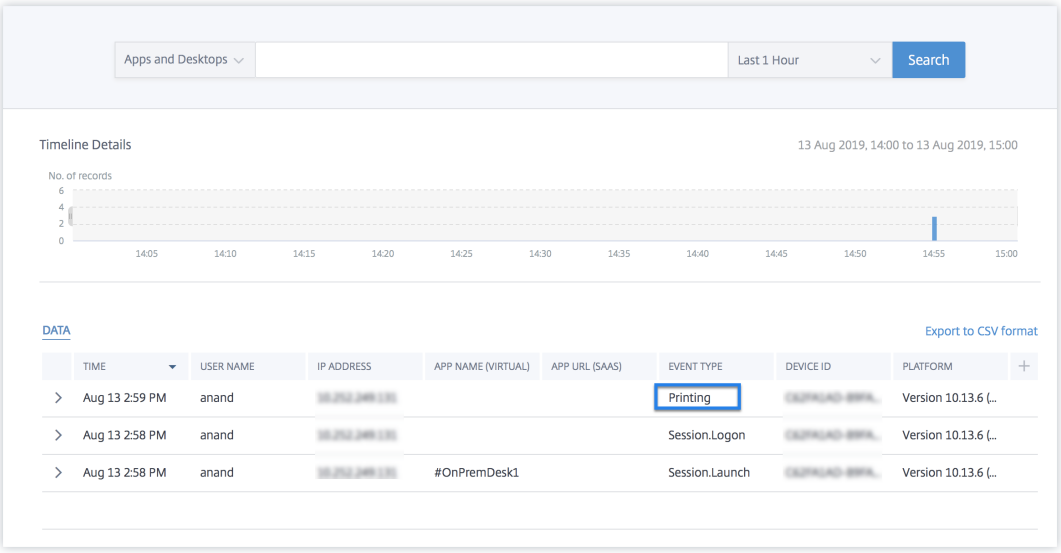
  1. Lancez l'application Citrix Workspace ou Citrix Receiver pour accéder à votre Workspace ou StoreFront.
  2. Lancez votre bureau virtuel.
  3. Copiez un fichier depuis votre bureau virtuel vers votre ordinateur local.
  4. Accédez à Citrix Analytics.
  5. Cliquez sur **Rechercher** et sélectionnez **Applications et postes de travail**.

6. Dans la page de recherche, affichez les données de l'événement **File.Download** . Développez la ligne pour afficher les détails de l'événement.



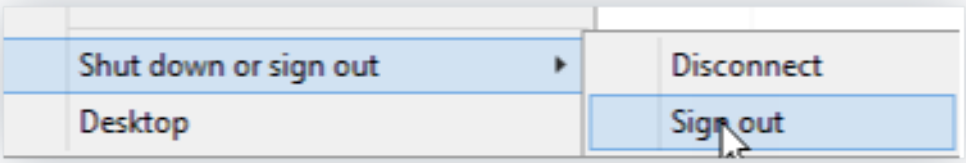
- **Impression**

1. Lancez l'application Citrix Workspace ou Citrix Receiver pour accéder à Workspace
2. Lancez votre bureau virtuel.
3. Imprimez un document à l'aide d'une imprimante configurée avec votre bureau virtuel.
4. Accédez à Citrix Analytics.
5. Cliquez sur **Rechercher** et sélectionnez **Applications et postes de travail**.
6. Dans la page Rechercher, affichez les données de l'événement **Impression** . Développez la ligne pour afficher les détails de l'événement.

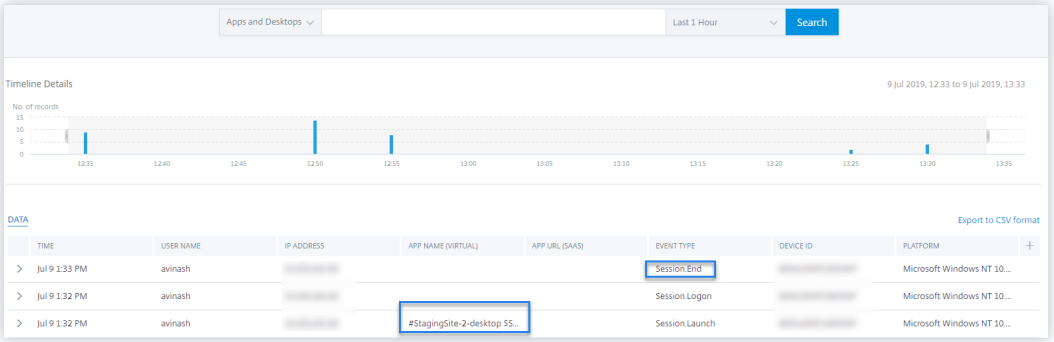


- **Fin de session**

1. Déconnectez-vous de votre bureau virtuel. Par exemple, si vous utilisez un bureau virtuel Windows, sélectionnez l'option **Déconnexion** .



2. Accédez à Citrix Analytics.
3. Cliquez sur **Rechercher** et sélectionnez **Applications et postes de travail**.
4. Dans la page de recherche, affichez les données de l'événement **Session.End** . Développez la ligne pour afficher les détails de l'événement.

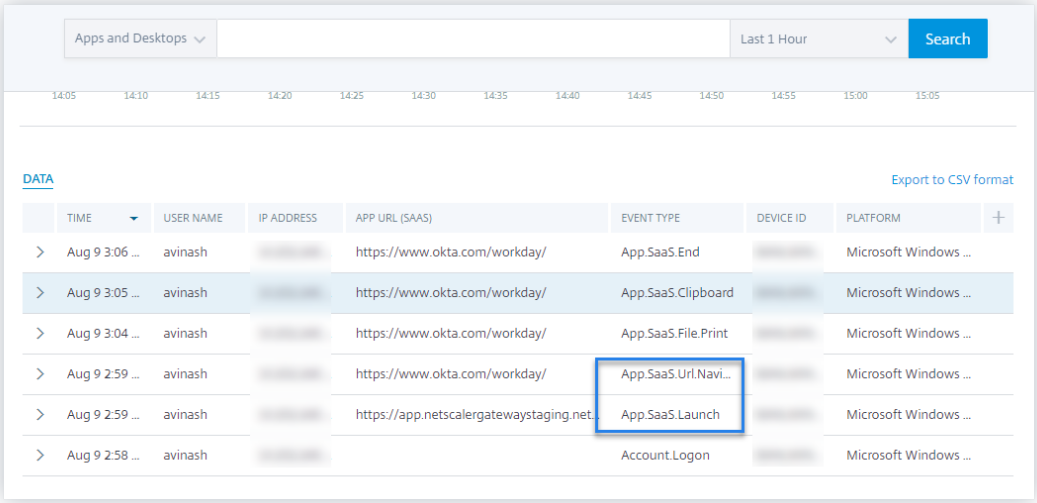


- **Lancement d'applications SaaS et navigation dans les URL des applications SaaS**

1. Lancez l'application Citrix Workspace ou Citrix Receiver pour accéder à votre Workspace ou StoreFront.
2. Lancez une application SaaS telle que Workday et attendez que la page Workday soit chargée. Naviguez parmi les pages Web de Workday.

> **Remarque**
>
> Assurez-vous que l'option **Restreindre la navigation** est désactivée dans la section Sécurité renforcée. Pour plus d'informations, consultez **la section Prérequis**.

3. Accédez à Citrix Analytics.
4. Cliquez sur **Rechercher** et sélectionnez **Applications et postes de travail**.
5. Dans la page de **recherche**, affichez les données des événements **App.Saas.Launch** et **App.Saas.Url.Navigation** . Développez la ligne pour afficher les détails de l'événement.

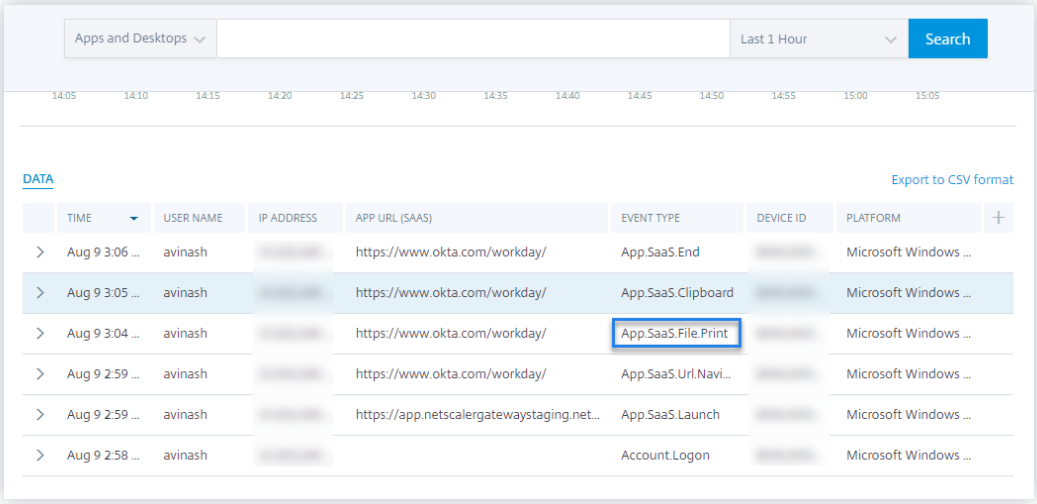


- **Impression de fichiers d'applications SaaS**

  1. Imprimez la page Workday que vous êtes en train de consulter.

     > **Remarque**
     >
     > Assurez-vous que l'option **Restreindre l'impression** est désactivée dans la section Sécurité renforcée. Pour plus d'informations, consultez les **conditions préalables**.

  2. Accédez à Citrix Analytics.
  3. Cliquez sur **Rechercher** et sélectionnez **Applications et postes de travail**.
  4. Dans la page de recherche, affichez les données de l'événement **App.Saas.File.Print** . Développez la ligne pour afficher les détails de l'événement.

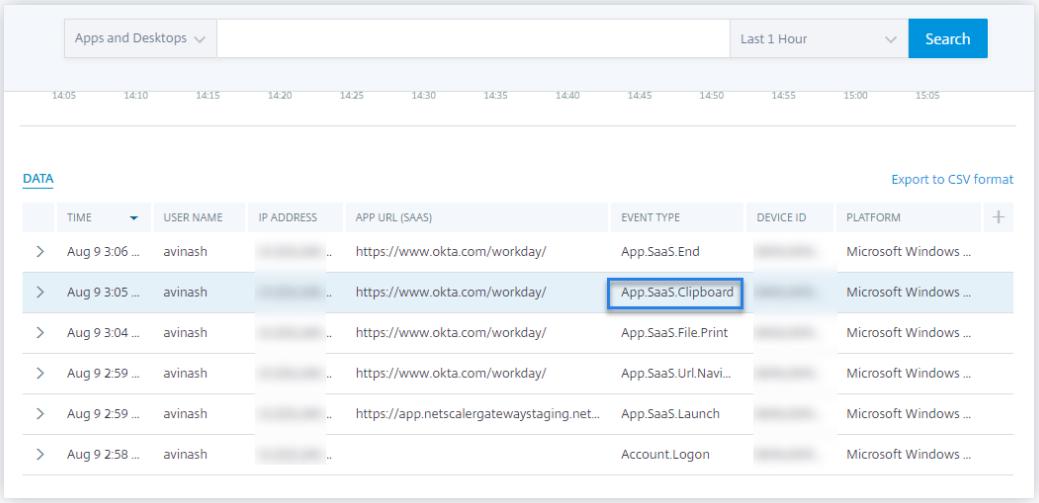


- **Accès au presse-papiers des applications SaaS**

1. Sur la page Workday, copiez du texte dans le presse-papiers de votre système.

> **Remarque**
>
> Assurez-vous que l'option **Restreindre l'accès au presse-papiers** est désactivée dans la section Sécurité renforcée. Pour plus d'informations, consultez les **conditions préalables**.

2. Accédez à Citrix Analytics.
3. Cliquez sur **Rechercher** et sélectionnez **Applications et postes de travail**.
4. Dans la page de recherche, affichez les données de l'événement **App.Saas.Clipboard** . Développez la ligne pour afficher les détails de l'événement.

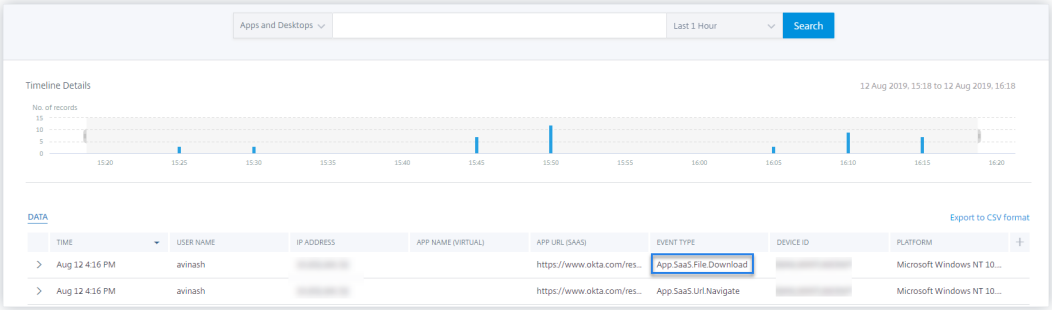


- **Téléchargement de fichiers SaaS App**

1. Sur la page Workday, recherchez un document public tel qu'un livre blanc et téléchargez le document.

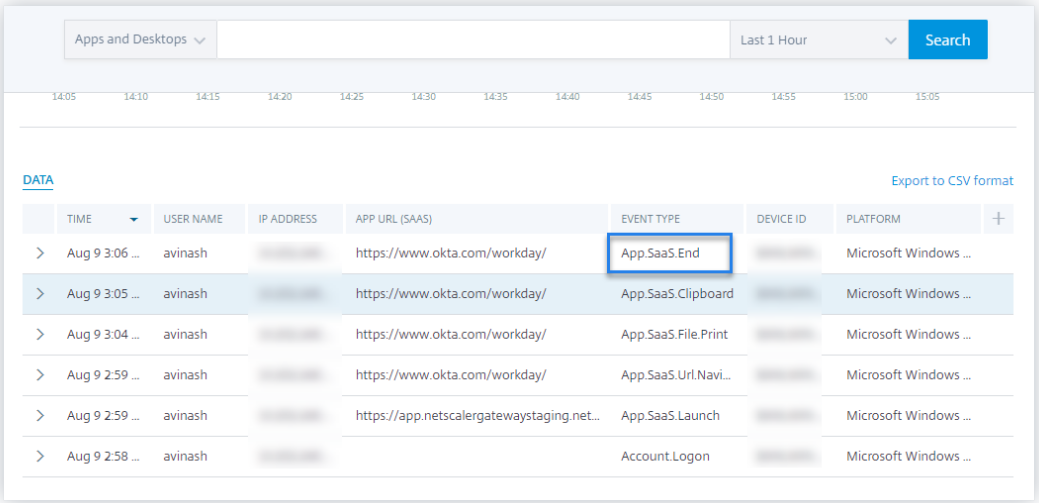
> **Remarque**
>
> Assurez-vous que l'option **Restreindre les téléchargements** est désactivée dans la section Sécurité renforcée. Pour plus d'informations, consultez les **conditions préalables**.

2. Accédez à Citrix Analytics.
3. Cliquez sur Rechercher et sélectionnez **Applications et postes de travail**.
4. Dans la page Rechercher, affichez les données de l'événement **App.saas.File.Download** . Développez la ligne pour afficher les détails de l'événement.



- **Fin de l'application SaaS**

  1. Fermez la page Workday.
  2. Accédez à Citrix Analytics.
  3. Cliquez sur **Rechercher** et sélectionnez **Applications et postes de travail**.
  4. Dans la page de recherche, affichez les données de l'événement **App.Saas.end** . Développez la ligne pour afficher les détails de l'événement.



- **VDA.Print**

  Conditions préalables

  Avant de déclencher l'événement d'impression, consultez la section Activation de la télémétrie d'impression pour Citrix DaaS.

  Pour déclencher un événement d'impression, effectuez les actions suivantes :

  1. Ouvrez un document texte avec le bloc-notes ou toute autre application où l'impression est autorisée.
  2. Cliquez sur **Fichier > Imprimer** ou appuyez sur **Ctrl + P**.

3. Dans Sélectionner une imprimante, choisissez votre imprimante, puis cliquez sur **Appliquer**, puis sur Imprimer.

- **VDA. Presse-papiers**

  Conditions préalables

  Avant de déclencher l'événement d'impression, consultez la section Activation de la télémétrie du presse-papiers pour Citrix DaaS.

  Pour déclencher un événement dans le presse-papiers, effectuez les actions suivantes :

  1. Ouvrez un document texte à l'aide du bloc-notes ou de tout autre éditeur de texte.
  2. Sélectionnez le contenu à copier.
  3. Cliquez avec le bouton droit sur Copier ou appuyez sur Ctrl+C.

Impossible de se connecter au serveur d'enregistrement de session configuré

July 14, 2022

Votre serveur d'enregistrement de session ne parvient pas à se connecter à Citrix Analytics après la configuration. Par conséquent, le serveur configuré n'apparaît pas sur la carte de site **Enregistrement de session** .

Pour résoudre ce problème, procédez comme suit :

1. Sur votre serveur d'enregistrement de session configuré, exécutez la commande PowerShell suivante pour vérifier l'identification de la machine cliente (CMID).

```
Get-WmiObject -class SoftwareLicensingService | select
    Clientmachineid
```

2. Si CMID est vide, ajoutez les fichiers de registre suivants dans les chemins d'accès spécifiés.

Nom de Registre	Chemin du registre	Type de clé	Valeur
AuditorUniqueID	Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\	Chaîne	Entrez votre UUID.

Nom de Registre	Chemin du registre	Type de clé	Valeur
EnableCASUseAuditorComputerID	HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/SmartAuditor/Server/	REG_DWORD	1

3. Redémarrez les services suivants :
    - Service d'analyse de l'enregistrement de session Citrix
    - Gestionnaire de stockage d'enregistrement de session Citrix

Problèmes de configuration avec le module complémentaire Citrix Analytics pour Splunk

July 14, 2022

Paramètres du module complémentaire Citrix Analytics non disponibles

Après avoir installé le module complémentaire Citrix Analytics pour Splunk sur votre environnement Splunk Forwarder ou Splunk Standalone, vous ne voyez pas les paramètres du **module complémentaire Citrix Analytics** sous **Paramètres > Entrées de données**.

Reason

Ce problème se produit lorsque vous installez le module complémentaire Citrix Analytics pour Splunk dans un environnement Splunk non pris en charge.

Corrections

Installez le module complémentaire Citrix Analytics pour Splunk dans un environnement Splunk pris en charge. Pour plus d'informations sur les versions prises en charge, consultez la section Intégration Splunk.

Aucune donnée disponible sur les tableaux de bord Splunk

Après avoir installé et configuré le module complémentaire Citrix Analytics pour Splunk sur votre environnement Splunk Forwarder ou Splunk Standalone, vous ne voyez aucune donnée de Citrix Analytics dans vos tableaux de bord Splunk.

Chèques

Pour résoudre ce problème, vérifiez les points suivants dans votre environnement Splunk Forwarder ou Splunk Standalone :

1. Assurez-vous que les conditions préalables à l'intégration Splunk sont remplies.
2. Accédez à **Paramètres > Entrées de données > Module complémentaire Citrix Analytics**. Assurez-vous que les détails de configuration de Citrix Analytics sont disponibles.
3. Si les détails de configuration sont disponibles, exécutez la requête suivante pour rechercher dans les journaux toute erreur liée au module complémentaire Citrix Analytics pour Splunk :

   ```
   index=_internal sourcetype=splunkd log_level=ERROR component=
      ExecProcessor cas_siem_consumer
   ```

4. Si vous ne trouvez aucune erreur, le module complémentaire Citrix Analytics pour Splunk fonctionne comme prévu. Si vous trouvez des erreurs dans les journaux, cela peut être dû à l'une des raisons suivantes :

   - Impossible d'établir la connexion entre votre environnement Splunk et les points de terminaison Citrix Analytics Kafka. Ce problème peut être dû aux paramètres du pare-feu.

     Correctifs : contactez votre administrateur réseau pour résoudre ce problème.

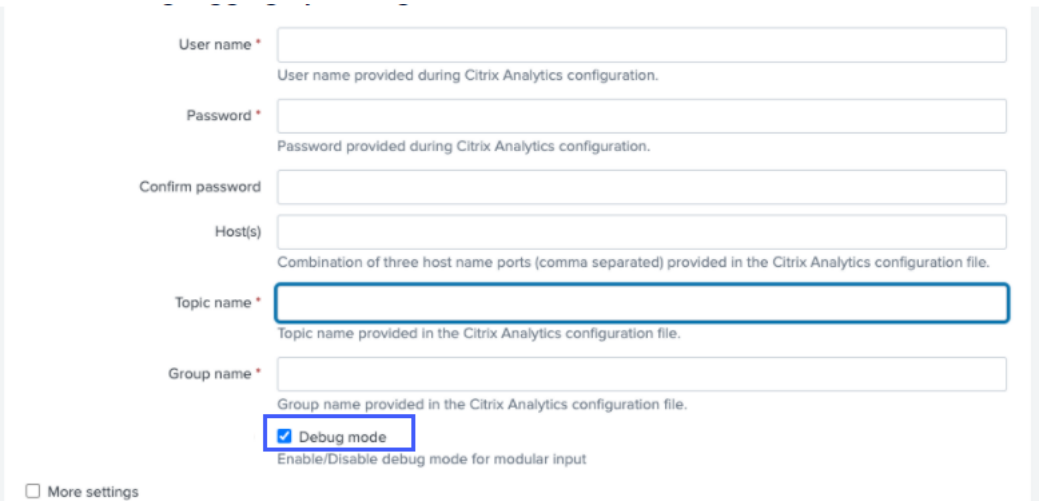
   - Détails de configuration incorrects dans **Paramètres > Entrées de données > Module complémentaire Citrix Analytics**.

     Correctifs : assurez-vous que les détails de configuration de Citrix Analytics tels que le nom d'utilisateur, le mot de passe, les points de terminaison d'hôte, la rubrique et le groupe de consommateurs sont correctement saisis conformément au fichier de configuration Citrix Analytics. Pour plus d'informations, consultez la section Configurer le module complémentaire Citrix Analytics pour Splunk.

5. Si vous ne parvenez pas à trouver la cause du problème dans les journaux précédents et que vous souhaitez approfondir vos recherches :

   a) Activez le **mode de débogage** dans **Paramètres > Entrées de données > Module complémentaire Citrix Analytics**.

> Remarque
>
> Par défaut, le **mode de débogage** est désactivé. L'activation de ce mode génère trop de journaux. Utilisez donc cette option uniquement lorsque cela est nécessaire et désactivez-la après avoir terminé votre tâche de débogage.



b) Recherchez les journaux de débogage générés à l'emplacement suivant et recherchez les erreurs éventuelles :

```
$SPLUNK_HOME$/var/log/splunk.Filename
    splunk_citrix_analytics_add_on_debug_connection.log
```

c) (Facultatif) Utilisez le script `splunk cmd python cas_siem_consumer_debug.py` de débogage disponible avec le module complémentaire Citrix Analytics pour Splunk. Ce script génère un fichier journal qui contient les détails de votre environnement Splunk et les vérifications de connectivité. Vous pouvez utiliser les détails pour déboguer le problème. Exécutez le script à l'aide de la commande suivante :

```
cd $SPLUNK_HOME$/etc/apps/TA_CTXS_AS/bin/; /opt/splunk/bin/
    splunk cmd python cas_siem_consumer_debug.py
```

Message d'erreur

Dans les journaux liés au module complémentaire Citrix Analytics pour Splunk, l'erreur suivante peut s'afficher :

```
ERRORKafkaError{ code=_TRANSPORT,val=-195,str="Failed to get metadata
: Local: Broker transport failure"}
```

Cette erreur est due à un problème de connectivité réseau ou à un problème d'authentification.

Pour déboguer le problème :

1. Dans votre environnement Splunk Forwarder ou Splunk Standalone, activez le **mode Débogage** pour obtenir les journaux de débogage. Reportez-vous à l'étape 5.a précédente.
2. Exécutez la requête suivante pour rechercher les problèmes d'authentification dans les journaux de débogage :

```
index=_internal source="*
    splunk_citrix_analytics_add_on_debug_connection.log*" "
    Authentication failure"
```

3. Si vous ne trouvez aucun problème d'authentification dans les journaux de débogage, l'erreur est due à un problème de connectivité réseau.
4. Recherchez et résolvez le problème à l'aide de telnet ou du script de débogage mentionné à l'étape précédente 5.c.

La mise à niveau du module complémentaire échoue à partir d'une version antérieure à la version 2.0.0

Dans votre environnement Splunk Forwarder ou Splunk Standalone, lorsque vous mettez à niveau le module complémentaire Citrix Analytics pour Splunk vers la dernière version à partir d'une version antérieure à la version 2.0.0, la mise à niveau échoue.

Corrections

1. Supprimez les fichiers et dossiers suivants situés dans le dossier `/bin` du dossier d'installation du module complémentaire Citrix Analytics pour Splunk :
   - `cd $SPLUNK_HOME$/etc/apps/TA_CTXS_AS/bin`
   - `rm -rf splunklib`
   - `rm -rf mac`
   - `rm -rf linux_x64`
   - `rm CARoot.pem`
   - `rm certificate.pem`
2. Redémarrez votre environnement Splunk Forwarder ou Splunk Standalone.

Impossible de connecter le serveur StoreFront à Citrix Analytics

January 4, 2023

Après avoir importé les paramètres de configuration de Citrix Analytics vers votre serveur StoreFront, le serveur StoreFront ne parvient pas à se connecter à Citrix Analytics.

Pour plus d'informations sur la façon d'importer des paramètres de configuration sur un serveur StoreFront, consultez Sites d'Virtual Apps and Desktops intégrés à l'aide de StoreFront.

L'assistant d'intégration CAS permet de vérifier et de résoudre les problèmes décrits dans cet article. Pour plus d'informations, consultez Assistant d'intégration de Citrix Analytics Service (CAS).

Pour résoudre le problème, procédez comme suit :

1. Sur le serveur StoreFront, effectuez une commande ping sur les points de terminaison spécifiques à la région de Citrix Analytics pour tester la connectivité entre le serveur StoreFront et le serveur Citrix Analytics. Assurez-vous également que les conditions préalables sont remplies.

   > **Remarque**
   >
   > Sur votre serveur StoreFront, vous pouvez tester la connectivité en envoyant un ping directement aux points de terminaison spécifiques à la région ou en ouvrant un navigateur Web et en accédant aux points de terminaison spécifiques à la région.

2. Activez la journalisation détaillée sur le serveur StoreFront pour suivre les journaux. Pour plus d'informations sur la journalisation détaillée, consultez l'article CTX139592.
3. Ouvrez le gestionnaire des services Internet (IIS) et vérifiez les points suivants :
   - Si le site StoreFront se trouve sous le site par défaut IIS, IIS redémarre le site StoreFront.
   - Si le site StoreFront se trouve dans d'autres pilotes ou s'il n'est pas sous le site par défaut, ouvrez la fenêtre de commande et tapez `iisreset`.
4. Exécutez la commande suivante pour importer les paramètres Citrix Analytics :

   ```
   Import-STFCasConfiguration -Path "configuration file path"
   ```

5. Exécutez la commande suivante pour vérifier les paramètres importés :

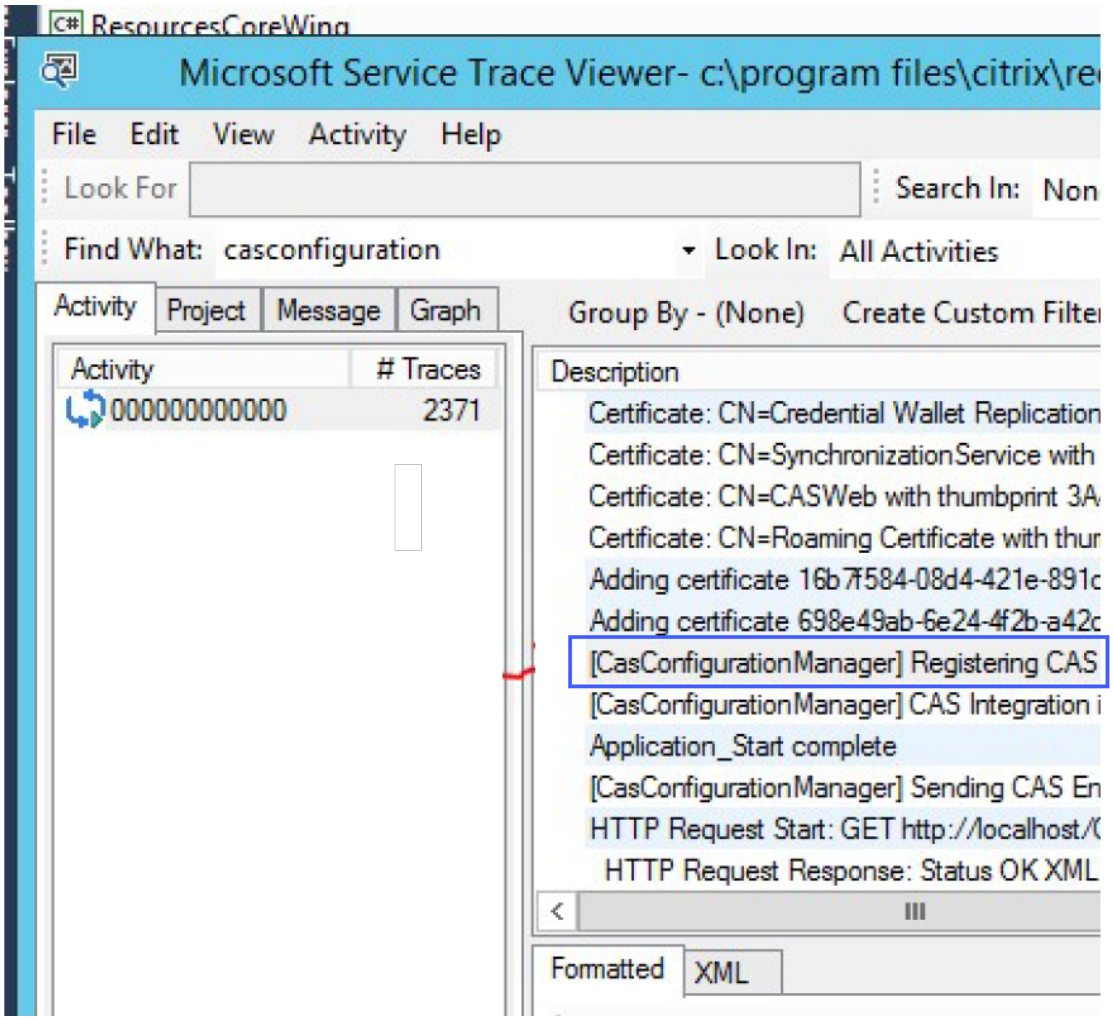
   ```
   Get-STFCasConfiguration
   ```

6. Si le site StoreFront se trouve dans d'autres pilotes ou s'il ne se trouve pas dans le site par défaut, ouvrez la fenêtre de commande. Tapez `iisreset` pour permettre au site StoreFront de lire les paramètres Citrix Analytics.
7. Obtenez les fichiers journaux détaillés StoreFront à partir de l'emplacement suivant :

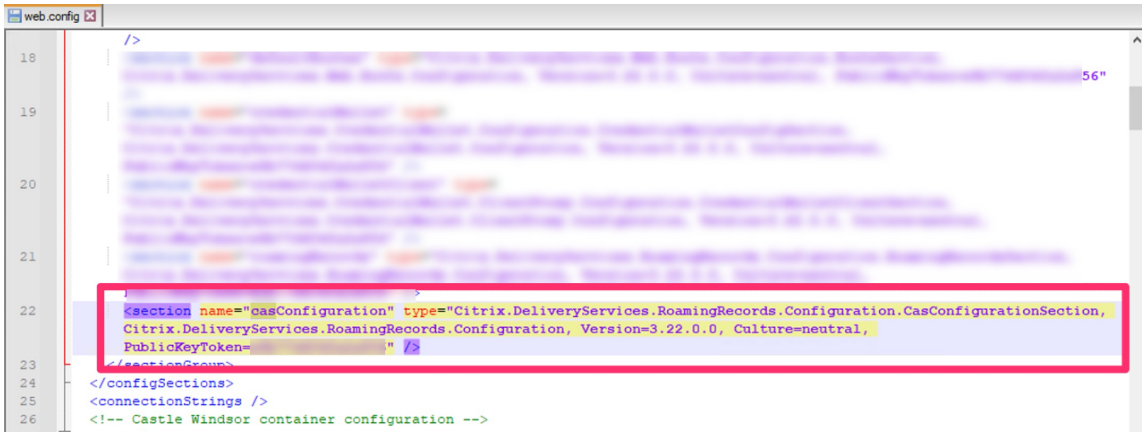
   ```
   C:\Program Files\Citrix\Receiver StoreFront\Admin\trace
   ```

   À l'emplacement mentionné ci-dessus, vous pouvez trouver plusieurs fichiers svclog qui peuvent être ouverts dans l'Observateur d'événements.

8. Utilisez Microsoft Service Trace Viewer pour ouvrir les journaux suivants :
   - Journaux StoreFront
   - Journaux détaillés des sites itinérants
9. Dans les journaux, assurez-vous que les sections **CASConfigurationManager** et les informations du serveur Citrix Analytics sont disponibles.



10. Si les sections CASConfigurationManager ne sont pas disponibles, ouvrez le fichier web.config pour le site itinérant qui se trouve dans le `roaming site\folder`.
11. Dans le fichier `web.config`, recherchez la section **CASConfiguration** et assurez-vous que les informations du serveur Citrix Analytics sont disponibles.



12. Sur les machines Windows Server sur lesquelles le serveur StoreFront est installé, assurez-vous de ce qui suit :

    - Le client TLS 1.2 est activé.
    - Au moins l'une des suites de chiffrement suivantes est activée :
        - `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`
        - `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`
        - `TLS_DHE_RSA_WITH_AES_256_GCM_SHA384`
        - `TLS_DHE_RSA_WITH_AES_128_GCM_SHA256`

    Pour plus d'informations sur la façon de configurer l'ordre des suites de chiffrement TLS, consultez la documentation Microsoft.

13. Si vous utilisez des machines Windows Server 2012, assurez-vous que l'échange Diffie-Hellman (ECDHE/DHE) est activé.

14. Assurez-vous que les machines Windows Server sur lesquelles le serveur StoreFront est installé doivent contenir les paramètres de registre mentionnés dans la documentation Microsoft.

    > **IMPORTANT**
    >
    > Mettez à jour les suites de chiffrement TLS/SSL à l'aide de la stratégie de groupe. Ne modifiez pas manuellement les suites de chiffrement TLS/SSL. Pour plus d'informations sur la façon d'utiliser la stratégie de groupe, consultez la documentation Microsoft.

    Par exemple, les paramètres de registre suivants doivent être disponibles sur votre ordinateur Windows Server :

    Client TLS 1.2 :

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
   SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client]
```



```
"Enabled"=dword:00000001
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
   SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client]
"DisabledByDefault"=dword:00000000

<!--NeedCopy-->
```

Les KEA de Diffie-Hellman :

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
   SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\Diffie-Hellman
   ]
"Enabled"=dword:ffffffff
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
   SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\ECDH]
"Enabled"=dword:ffffffff

<!--NeedCopy-->
```

Chiffrements AES-128/AES-256 :

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
   SecurityProviders\SCHANNEL\Ciphers\AES 128/128]
"Enabled"=dword:ffffffff
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
   SecurityProviders\SCHANNEL\Ciphers\AES 256/256]
"Enabled"=dword:ffffffff

<!--NeedCopy-->
```

Hashs SHA256/SHA384 :

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
   SecurityProviders\SCHANNEL\Hashes\SHA256]
"Enabled"=dword:ffffffff
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
   SecurityProviders\SCHANNEL\Hashes\SHA384]
"Enabled"=dword:ffffffff

<!--NeedCopy-->
```

FAQ

November 16, 2023

Source de données

Qu'est-ce qu'une source de données ?

Les sources de données sont les services et produits Citrix qui envoient des données à Citrix Analytics.

Pour en savoir plus : Source de données

Comment puis-je ajouter une source de données ?

Après vous être connecté à Citrix Analytics, sur l'écran de **bienvenue**, sélectionnez **Démarrer** pour ajouter une source de données à Citrix Analytics. Vous pouvez également ajouter une source de données en accédant à **Paramètres > Sources de données**.

Agent Citrix ADM

Quelles sont les ressources minimales requises pour installer un agent sur un hyperviseur sur site ?

8 Go de RAM, 4 processeurs virtuels, 120 Go de stockage, 1 interface réseau virtuelle, débit de 1 Gbit/s

Dois-je attribuer un disque supplémentaire à l'agent Citrix ADM lors du provisionnement ?

Non, il n'est pas nécessaire d'ajouter un disque supplémentaire. L'agent est utilisé uniquement comme intermédiaire entre Citrix Analytics et les instances du centre de données de votre entreprise. Il ne stocke pas les données d'inventaire ou d'analyse qui nécessiteraient un disque supplémentaire.

Quelles sont les informations d'identification par défaut pour se connecter à un agent ?

Les informations d'identification par défaut pour se connecter à l'agent sont `nsrecover`/`nsroot`. Cela vous connecte à l'invite shell de l'agent.

Comment modifier les paramètres réseau d'un agent si j'ai saisi une valeur incorrecte ?

Ouvrez une session sur la console de l'agent sur votre hyperviseur et accédez à l'invite du shell à l'aide des informations d'identification `nsrecover`/`nsroot`, puis exécutez la commande `networkconfig`.

Pourquoi ai-je besoin d'une URL de service et d'un code d'activation ?

L'agent utilise l'URL du service pour localiser le service et le code d'activation pour enregistrer l'agent auprès du service.

Comment puis-je saisir à nouveau l'URL du service si je l'ai mal saisie dans la console de l'agent ?

Ouvrez une session à l'invite du shell de l'agent en utilisant les informations d'identification `nsrecover`/`nsroot`, puis tapez : `deployment_type.py`. Ce script vous permet de saisir à nouveau l'URL du service et le code d'activation.

Comment puis-je obtenir un nouveau code d'activation ?

Vous pouvez obtenir un nouveau code d'activation auprès du service Citrix ADM. Ouvrez une session sur le service Citrix ADM et accédez à **Réseaux > Agents**. Sur la page **Agents**, dans la liste **Sélectionner une action**, sélectionnez **Générer le code d'activation**.

Puis-je réutiliser mon code d'activation avec plusieurs agents ?

Non, vous ne pouvez pas.

Combien d'agents Citrix ADM dois-je installer ?

Le nombre d'agents dépend du nombre d'instances gérées dans un centre de données et du débit total. Citrix vous recommande d'installer au moins un agent pour chaque centre de données.

Comment installer plusieurs agents Citrix ADM ?

Sur la page Sources de données, cliquez sur le signe plus (+) en regard de Citrix Gateway et suivez les instructions pour installer un autre agent.

Vous pouvez également accéder à l'interface graphique Citrix ADM et accéder à Réseaux > Agents, puis cliquer sur **Configurer l'agent** pour installer plusieurs agents.

Puis-je installer deux agents dans une configuration haute disponibilité ?

Non, vous ne pouvez pas.

Que dois-je faire si l'inscription de mon agent échoue ?

- Assurez-vous que votre agent a accès à Internet (configurez le DNS).
- Assurez-vous d'avoir correctement copié le code d'activation.
- Vérifiez que vous avez correctement saisi l'URL du service.
- Assurez-vous que les ports requis sont ouverts.

L'enregistrement a réussi, mais comment savoir si l'agent fonctionne correctement ?

Vous pouvez procéder comme suit pour vérifier si l'agent fonctionne correctement :

- Une fois l'agent enregistré avec succès, accédez à Citrix ADM et accédez à **Réseaux > Agents**. Vous pouvez consulter les agents découverts sur cette page. Si l'agent fonctionne correctement, l'état est indiqué par une icône verte. S'il n'est pas en cours d'exécution, l'état est indiqué par une icône rouge.
- Ouvrez une session sur l'invite shell de l'agent et exécutez les commandes suivantes : `ps -ax | grep mas` et `ps -ax | grep ulfd`. Assurez-vous que les processus suivants sont en cours d'exécution.

- Si l'un des processus n'est pas en cours d'exécution, exécutez la commande **masd restart**. Le démarrage de tous les démons peut prendre un certain temps (environ 1 minute).
- Assurez-vous qu'`agent.conf` il est créé `/mpsconfig` après l'enregistrement réussi de l'agent.

Intégration des instances Citrix Gateway

Les instances Citrix Gateway sont ajoutées à Citrix Analytics, mais comment savoir si Analytics est activé sur l'agent ?

Vous pouvez vérifier si Analytics est activé sur l'agent à l'aide de l'invite shell de l'agent. Si Analytics est correctement activé sur l'agent, le `turnOnEvent` paramètre sera défini sur `Y` dans le `/mpsconfig/telemetry_cloud.conf` fichier.

Ouvrez une session à l'invite shell de l'agent et exécutez la commande suivante : cat `/mpsconfig/telemetry_cloud.conf` et vérifiez la valeur du `turnOnEvent` paramètre.

J'ai accidentellement fermé l'assistant d'intégration de Citrix Gateway. Dois-je démarrer ma configuration depuis le début ?

Non. Citrix Analytics enregistre la progression et affiche la configuration incomplète sous forme de vignette dans la page **Sources de données > Paramètres** . Cliquez sur **Poursuivre l'installation** pour terminer la configuration.

Site d'intégration Virtual Apps and Desktops

Comment puis-je désactiver le traitement des données ?

Si vous souhaitez désactiver temporairement le traitement des données de votre site vers Citrix Analytics, cliquez simplement sur la fiche de **site**, puis sur **Désactiver le traitement des données**.

Lorsque j'ajoute mon site à Workspace et que je clique sur « Test STA », le test échoue. Que dois-je faire ?

Il y a peut-être un problème de connectivité entre votre Citrix Gateway et Cloud Connector. Pour résoudre les problèmes, consultez CTX232517 dans le centre de connaissances du support Citrix.

Où puis-je obtenir de l'aide concernant Citrix Analytics ?

Vous pouvez poser des questions et entrer en contact avec les experts de Citrix Analytics sur le forum de discussion Citrix Analytics à l'adresse https://discussions.citrix.com/forum/1710-citrix-analytics/.

Pour participer au forum, vous devez vous connecter avec votre identifiant Citrix.

Assurance d'accès —Géolocalisation

Comment les détails de géolocalisation sont-ils dérivés par Analytics ?

Citrix Analytics utilise l'adresse IP de l'appareil à partir duquel le client Workspace est lancé. Citrix Analytics utilise un fournisseur de données de géolocalisation IP tiers pour dériver l'emplacement d'un utilisateur à partir de son adresse IP. Lorsque vous effectuez une ouverture de session, votre emplacement (adresse IPv4) est résolu en un pays ou une ville, et le mappage est mis à jour périodiquement. Les organisations peuvent utiliser ces emplacements définis par les pays pour surveiller les modèles d'accès à partir de là où elles n'exercent pas leurs activités.

Quel est le niveau de précision de la localisation d'un utilisateur ?

Citrix Analytics utilise un fournisseur de données de géolocalisation IP tiers pour dériver l'emplacement d'un utilisateur à partir de son adresse IP. Les services GeoIP sont capables de trouver la bonne ville ou le bon emplacement la plupart du temps, mais les recherches GeoIP ne sont jamais totalement précises. Parfois, l'emplacement indiqué pour un utilisateur peut être différent de l'emplacement précis d'accès.

Selon la documentation IP GeoPoint, le niveau de couverture est d'environ 99,99 % des adresses IP allouées dans le monde (adresses IP routables IPv4). En termes de précision de localisation, il accompagne chacun des champs de localisation essentiels (pays, État, ville, code postal) d'un facteur de confiance.

Dans quels cas la détermination de l'emplacement est-elle inexacte ?

La précision des données de géolocalisation dépend de la manière dont l'appareil se connecte à Internet. Un appareil peut se connecter à Internet via :

- Passerelles mobiles
- VPN ou installation d'hébergement
- Serveur proxy ou anonymiseur régional ou international

Dans de tels cas, les données de géolocalisation ne sont pas exactes, quelle que soit l'utilisation du logiciel du fournisseur de géolocalisation IP.

Quelles sont les versions de l'application Citrix Workspace prises en charge ?

Des versions minimales de l'application Citrix Workspace sont requises pour que le système d'exploitation envoie l'attribut d'**adresse IP** à Citrix Analytics for Security. Reportez-vous au tableau matriciel ou aux emplacements identifiés comme non disponibles pour plus de détails.

Dans quels cas ne recevons-nous pas les détails géologiques ?

Pour afficher les détails de la géolocalisation, reportez-vous à la section Emplacements identifiés comme non disponibles pour plus de détails.

Quel service de géolocalisation Citrix Analytics utilise-t-il pour signaler l'emplacement d'un utilisateur ? Comment signaler un mauvais emplacement pour une adresse IP ?

Citrix Analytics utilise les services de géolocalisation basés sur des fichiers Neustar pour fournir des données de géolocalisation pour les accès entrants. Il dispose d'une page de correction IP ouverte au public qui peut être utilisée pour soumettre automatiquement une demande de correction. Une fois qu'une demande de correction est soumise, la demande est examinée par Neustar pour en vérifier l'exactitude et traitée.

Le fournisseur GeoIP aide à afficher des informations aussi précises que possible. Malheureusement, il peut y avoir des cas où les données GeoIP sont inexactes en raison de la nature innée de GeoIP.

Glossaire des termes

April 12, 2024

- **Actions** : réponses en boucle fermée à des événements suspects. Des mesures sont prises pour empêcher de futurs événements anormaux de se produire. En savoir plus.
- **Cloud Access Security Broker (CASB)** : point d'application des stratégies de sécurité sur site ou dans le cloud placé entre les consommateurs de services cloud et les fournisseurs de services cloud. Les CASB combinent et interjettent les stratégies de sécurité d'entreprise à mesure que les ressources basées sur le cloud sont accessibles Ils aident également les entreprises à étendre les contrôles de sécurité de leur infrastructure sur site au cloud.
- **NetScaler ADC (Application Delivery Controller)** : périphérique réseau résidant dans un centre de données, situé stratégiquement entre le pare-feu et un ou plusieurs serveurs d'applications. Gère l'équilibrage de charge entre les serveurs et optimise les performances et la sécurité des utilisateurs finaux pour les applications d'entreprise. En savoir plus.
- **Citrix ADM (Application Delivery Management)** : solution centralisée de gestion, d'analyse et d'orchestration du réseau. À partir d'une plate-forme unique, les administrateurs peuvent afficher, automatiser et gérer les services réseau pour les architectures d'applications évolutives. En savoir plus.
- **Agent Citrix ADM** : proxy qui permet la communication entre Citrix ADM et les instances gérées d'un centre de données. En savoir plus.
- **Citrix Analytics** : service cloud qui collecte des données sur les services et les produits (sur site et dans le cloud), et génère des informations exploitables, permettant aux administrateurs de gérer de manière proactive les menaces de sécurité des utilisateurs et des applications, d'améliorer les performances des applications et de prendre en charge les opérations continues. En savoir plus.
- **Citrix Cloud** : plate-forme qui se connecte aux ressources via Citrix Cloud Connector sur n'importe quel cloud ou infrastructure (sur site, cloud public, cloud privé ou cloud hybride). En savoir plus.
- **Citrix Gateway** : solution d'accès à distance consolidée qui consolide l'infrastructure d'accès à distance pour fournir une authentification unique sur toutes les applications, que ce soit dans un centre de données, dans le cloud ou fournies en tant que SaaS. En savoir plus.
- **Citrix Hypervisor** : plate-forme de gestion de la virtualisation optimisée pour les infrastructures de virtualisation des applications, des postes de travail et des serveurs. En savoir plus.
- **Application Citrix Workspace** (anciennement Citrix Receiver) : logiciel client qui fournit un accès transparent et sécurisé aux applications, aux bureaux et aux données depuis n'importe quel appareil, y compris les smartphones, les tablettes, les PC et les Mac. En savoir plus.
- **DLP (Data Loss Prevention)** : solution qui décrit un ensemble de technologies et de techniques d'inspection permettant de classer les informations contenues dans un objet tel qu'un fichier, un e-mail, un paquet, une application ou un magasin de données. En outre, l'objet peut égale-

ment être stocké, en cours d'utilisation ou sur un réseau. Les outils DLP peuvent appliquer dynamiquement des stratégies telles que consigner, signaler, classer, déplacer, étiqueter et chiffrer. Les outils DLP peuvent également appliquer des protections de gestion des droits sur les données d'entreprise. En savoir plus.

- **DNS (Domain Name System)** : service réseau utilisé pour localiser les noms de domaine Internet et les traduire en adresses IP (Internet Protocol). DNS mappe les noms de sites Web que les utilisateurs fournissent, à leurs adresses IP correspondantes fournies par les machines, pour localiser un site Web quel que soit l'emplacement physique des entités.
- **Traitement des données** : méthode de traitement des données d'une source de données vers Citrix Analytics. En savoir plus.
- **Source de données** : produit ou service qui envoie des données à Citrix Analytics. Une source de données peut être interne ou externe. [En savoir plus] /en-us/citrix-analytics/data-sources.html).
- **Exportation de données** : produit ou service qui reçoit des données de Citrix Analytics et fournit des informations. En savoir plus.
- **Utilisateurs découverts** : nombre total d'utilisateurs d'une organisation qui utilisent des sources de données. En savoir plus.
- **FQDN (nom de domaine complet)** : nom de domaine complet pour l'accès interne (StoreFront) et externe (NetScaler ADC).
- **Apprentissage automatique** : type de technologie d'analyse de données qui extrait des connaissances sans être explicitement programmée pour le faire. Les données provenant d'une grande variété de sources potentielles telles que les applications, les capteurs, les réseaux, les appareils et les appareils sont introduites dans un système d'apprentissage automatique. Le système utilise les données et applique des algorithmes pour créer sa propre logique afin de résoudre un problème, d'obtenir un aperçu ou de faire une prédiction.
- **Microsoft Graph Security** : passerelle qui connecte la sécurité des clients et les données organisationnelles. Fournit des alertes et des options de résolution faciles à consulter lorsqu'une action doit être prise. En savoir plus.
- **Analyse des performances** : service qui fournit une visibilité sur les détails de la session utilisateur au sein d'une organisation. En savoir plus.
- **Stratégie** : Ensemble de conditions à remplir pour qu'une action soit appliquée sur le profil de risque d'un utilisateur. En savoir plus.
- **Indicateur de risque** : Mesure qui fournit des informations sur le niveau d'exposition à un risque commercial auquel l'organisation est exposée à un moment donné. En savoir plus.
- **Score de risque** : valeur dynamique qui indique le niveau global de risque qu'un utilisateur

ou une entité pose à une infrastructure informatique sur une période de surveillance prédéterminée. En savoir plus.

- **Chronologie des risques** : enregistrement du comportement à risque d'un utilisateur ou d'une entité qui permet aux administrateurs d'étudier un profil de risque et de comprendre l'utilisation des données, l'utilisation des appareils, l'utilisation des applications et l'utilisation de l'emplacement. En savoir plus.
- **Utilisateur à risque** : Utilisateur qui a agi de manière risquée ou qui a présenté un comportement à risque. En savoir plus.
- Analyse**de la sécurité : analyse**avancée des données qui est utilisée pour obtenir des résultats de sécurité convaincants tels que la surveillance de la sécurité et la recherche des menaces. En savoir plus.
- **Accès privé sécurisé** : service qui fournit l'intégration de l'authentification unique, de l'accès à distance et de l'inspection du contenu dans une solution unique pour le contrôle d'accès de bout en bout. En savoir plus.
- **Splunk** : logiciel SIEM (Security Information and Event Management) qui reçoit des données intelligentes de Citrix Analytics et fournit des informations sur les risques commerciaux potentiels. En savoir plus.
- **UBA (User Behavior Analytics)** : Processus de base de l'activité et du comportement des utilisateurs combiné à une analyse des groupes de pairs, afin de détecter les intrusions potentielles et les activités malveillantes.
- **Liste de surveillance** : liste des utilisateurs ou des entités que les administrateurs souhaitent surveiller pour détecter les activités suspectes. En savoir plus.