Citrix Analytics for Security

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

June 18, 2024

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.

15 avril 2024

Nouveau rapport de synthèse

Vous avez désormais la possibilité de regrouper plusieurs rapports en un seul rapport de synthèse qui peut être programmé pour la période requise. Avec cette nouvelle fonctionnalité, vous ne fournissez à votre public que les informations graphiques nécessaires. Pour plus d'informations, voir Rapport de synthèse.

29 janvier 2024

Mises à jour des champs Workspace App Status

- **Recherche en libre-service** : vous pouvez désormais effectuer des requêtes pour connaître l'état de support d'une version de l'application Workspace en utilisant le nouveau champ d'état de **l'application Workspace** pour la source de données **Citrix Apps and Desktops**.
- **Utilisateurs** : la colonne **État de l'application Workspace** a été supprimée.

Pour plus d'informations, consultez la section Recherche en libre-service pour les applications et les postes de travail.

25 janvier 2024

Les incohérences dans l'interface utilisateur CAS ont été uniformisées

Les problèmes suivants ont été résolus dans la fonction de **recherche en libre-service** pour la source de données **Apps and Desktops** :

- Les événements qui étaient précédemment affichés de manière désordonnée au cours d'une session apparaissent désormais correctement.
- Les colonnes par défaut ont été mises à jour.

24 janvier 2024

Événements de profil utilisateur améliorés sur les environnements SIEM

Les événements de profil utilisateur exportés vers vos environnements SIEM incluent désormais :

- Informations sur les adresses IP
- Informations sur la localisation de Citrix Virtual Apps and Desktops et Citrix DaaS (anciennement Citrix Virtual Apps and Desktops service)

Ces nouvelles améliorations vous permettent d'identifier l'adresse IP du client utilisée pour accéder aux données de votre organisation et de recueillir des informations de localisation des utilisateurs à la fois auprès de Citrix Virtual Apps and Desktops et de Citrix DaaS.

Pour plus d'informations, consultez la section Données d'analyse des risques pour le SIEM.

1 décembre 2023

Page des paramètres de messagerie de l'administrateur pour les e-mails hebdomadaires et les alertes SIEM

La nouvelle fonctionnalité **Paramètres de messagerie de l'administrateur** vous permet de configurer les destinataires de la liste de distribution personnalisée pour les alertes système. Cette amélioration garantit que les administrateurs reçoivent uniquement les alertes système qui les concernent.

Pour plus d'informations, consultez la section Paramètres de messagerie de l'administrateur.

Tableau de bord des utilisateurs - Nouveau filtre de temps de comptage des utilisateurs actifs et mise à jour de la section Aperçu

Le nouveau filtre horaire du tableau de bord des **utilisateurs** vous permet de consulter et de modifier le nombre total d'utilisateurs actifs dans votre organisation pendant une période donnée, en tenant compte des sources de données pour lesquelles vous avez activé Citrix Analytics.

La section **Aperçu** améliorée du tableau de bord des **utilisateurs** affiche le nombre total d'utilisateurs de votre organisation, ainsi que le nombre d'utilisateurs actifs et inactifs actuellement connectés.

Pour plus d'informations, consultez Tableau de bord des utilisateurs.

Rapports personnalisés améliorés

- Vous pouvez désormais créer et planifier des rapports personnalisés à l'aide des événements et des informations disponibles dans Citrix Analytics for Security. Les rapports personnalisés vous aident à extraire des informations présentant un intérêt spécifique et à organiser les données graphiquement.
- Vous pouvez désormais utiliser les fonctionnalités améliorées de la plateforme Custom Report, qui incluent des rapports basés sur des requêtes de recherche en libre-service, des modèles, de meilleures visualisations, la couverture de toutes les sources de données et de tous les indicateurs, la planification des rapports et l'exportation de PDF.

Pour plus d'informations, consultez la section Rapports personnalisés.

30 novembre 2023

Suppression de toutes les fonctionnalités de ShareFile dans Citrix Analytics

Les fonctionnalités de détection de ShareFile suivantes sont supprimées :

- Partager des liens
- Indicateurs de risque associés
- Les stratégies et leurs occurrences
- Configurations d'exportation de données de Content Collaboration
- Rapports de Content Collaboration
- Source de données Content Collaboration sur la recherche
- Content Collaboration et recherches enregistrées
- Source de données Content Collaboration.

La suppression de ces fonctionnalités peut entraîner une incohérence temporaire dans le score de risque et les délais des utilisateurs. Toutes les autres fonctionnalités de Citrix Analytics restent les mêmes.

Découvrez comment ShareFile simplifie l'accès aux contrôles de sécurité directement depuis ShareFile.com.

22 septembre 2023

Source de données Citrix Secure Browser dans Custom Indicator

Vous pouvez désormais créer des indicateurs de risque pour la source de données Citrix Secure Browser afin de suivre l'activité d'un utilisateur dans le navigateur sécurisé. Pour plus d'informations, consultez la section Indicateurs personnalisés.

Amélioration du courrier électronique hebdomadaire grâce à l'exportation de données SIEM

L'e-mail hebdomadaire a été amélioré pour fournir un aperçu plus approfondi de la posture de sécurité de votre organisation en permettant l'exportation des données SIEM. Vous pouvez désormais intégrer et activer davantage de sources de données pour découvrir un large éventail d'événements concernant vos utilisateurs. L'e-mail hebdomadaire inclut les nouveaux ajouts suivants :

- La section récapitulative des données indique l'état de la consommation de données dans l'environnement SIEM.
- Recommandations pour les exportations de données basées sur l'état de consommation des exportations de données.

Pour plus d'informations, voir Notification hebdomadaire par e-mail.

Consommation des préférences de notification personnalisées de l'administrateur dans les e-mails

Citrix Analytics for Security respecte désormais les préférences de notification définies par les administrateurs personnalisés dans Citrix Cloud. Cette amélioration offre aux administrateurs personnalisés une plus grande flexibilité dans la gestion de leurs préférences de notification. Cette préférence est également exploitée lors de l'envoi d'e-mails de notification tels que des e-mails hebdomadaires, des e-mails d'action Notifier les administrateurs et des alertes pour les exportations de données.

Pour plus d'informations, voir Gérer les rôles d'administrateur pour Security Analytics.

4 juillet 2023

Assistance aux opérateurs OR dans le cadre de la recherche en libre-service et de l'indicateur personnalisé

L'opérateur **OR** est désormais disponible dans les fonctionnalités de **recherche en libre-service** et d'**indicateur de risque personnalisé**. Vous pouvez utiliser l'opérateur **OR** dans les modes de recherche tels que les requêtes de recherche en libre-service et d'indicateurs personnalisés.

Pour plus d'informations, consultez la section Opérateurs pris en charge dans les requêtes de recherche.

15 juin 2023

Activer la télémétrie du presse-papiers VDA

Un événement appelé VDA.Clipboard se déclenche lorsque vous lancez une opération de presse-papiers dans Citrix Apps and Desktops. Ces journaux du presse-papiers fournissent des informations essentielles telles que le nom du VDA, la taille du presse-papiers, le type de format du presse-papiers, l'adresse IP du client, le fonctionnement du presse-papiers, la direction du fonctionnement du presse-papiers et si l'opération du presse-papiers était autorisée. Les attributs de l'événement VDA Clipboard sont également disponibles dans les flux de travail de recherche en libre-service et d' indicateurs de risque personnalisés.

- **Recherche en libre-service** : vous pouvez générer des rapports, enregistrer des requêtes et consulter les événements VDA.Clipboard ainsi que tous les détails de ses attributs.
- **Indicateurs de risque personnalisés** : les attributs des événements du presse-papiers du VDA sont disponibles dans le flux de travail des indicateurs personnalisés. Vous pouvez utiliser ces paires clé/valeur d'événement pour configurer des déclencheurs d'indicateurs personnalisés et configurer des stratégies automatisées avec des actions.

Vous pouvez utiliser la **collection de métadonnées Clipboard Place pour la stratégie de surveillance de la sécurité** afin d'activer la télémétrie du presse-papiers et la transmission des journaux du presse-papiers à Citrix Analytics for Security. Cette stratégie est activée par défaut. Pour la désactiver, accédez à la page Policy et désactivez-la pour arrêter la collecte de données à partir des VDA.

Pour plus d'informations, consultez la section Activation de la télémétrie du presse-papiers pour Citrix DaaS.

14 juin 2023

Disponibilité du cycle de vie de l'application d'enregistrement de session et des événements de registre dans Citrix Analytics for Security

Les événements suivants **liés au cycle de vie des applications** et au **registre** issus de **l'enregistrement de session** sont désormais disponibles dans Citrix Analytics for Security :

- Citrix.EventMonitor.RegistryChange
- Citrix.EventMonitor.SessionLaunch
- Citrix.EventMonitor.SessionEnd
- Citrix.EventMonitor.Clipboard
- Citrix.EventMonitor.FileTransfer

Vous pouvez consulter ces événements, créer des indicateurs personnalisés et les exporter vers vos environnements SIEM.

Pour plus d'informations, consultez la section Types d'événements et champs pris en charge.

8 juin 2023

Problèmes résolus

- Certains événements d'ouverture de session qui sont envoyés à Citrix Analytics for Security n'ont pas de nom d'utilisateur. Cela se traduit par l'affichage de la colonne du nom d'utilisateur sous la forme **NA** pour certains événements sur la page de connexion des utilisateurs de Self Service Search and Access Assurance. Parfois, cela se traduit également par un nombre d'utilisateurs uniques égal à zéro, bien que le nombre total d'ouvertures de session soit différent de zéro dans le graphique des organisations d'enregistrement IP Access Assurance lorsque vous consultez les données sur une courte période, telle que la **dernière heure** ou le **dernier jour**. Ce problème est désormais résolu. [CAS-70954]
- Dans la recherche en libre-service pour Apps and Desktops, pour les événements utilisateur Session.Logon et Session.End, la dimension App-Name dans les requêtes de recherche est renseignée avec des noms de groupes de mise à disposition plutôt que le nom de l'application ou du bureau lancé, ce qui peut induire en erreur les administrateurs. La dimension App-Name est plus utile pour les requêtes sur les événements App.Start/App.End, car elle pointe vers les applications en cours de lancement. Pour plus de détails, reportez-vous à la section Recherche en libre-service pour Apps and Desktops. Ce problème est désormais résolu. [CAS-67968]
- Si votre organisation est intégrée à Citrix Cloud dans la région d'origine **Asie-Pacifique Sud**, les événements Content Collaboration ne sont pas visibles dans vos locataires Citrix Analytics. Ce problème est désormais résolu. [CAS-62317]
- Quelques versions de l'application Citrix Workspace et du client Citrix Receiver n'envoient pas d'événements spécifiques à Citrix Analytics. Par conséquent, Citrix Analytics ne peut pas fournir d'informations et générer des indicateurs de risque pour ces événements. Ce problème est désormais résolu. Pour plus d'informations, consultez Contrôle 6 : les événements relatifs aux applications et bureaux virtuels sont-ils transmis à Analytics ?. [CAS-16151]

29 mai 2023

Le module complémentaire Citrix Analytics pour Splunk est désormais disponible sur Splunk Cloud Platform

L'intégration de Splunk pour Citrix Analytics utilise le module complémentaire Citrix Analytics pour Splunk pour se connecter à l'environnement d'analyse et intégrer des données critiques dans votre environnement Splunk.

Auparavant, l'extension était approuvée par Splunk uniquement pour être installée sur la couche Splunk Enterprise et les clients étaient responsables de la configuration de l'extension dans leur environnement Splunk sur site. Avec la dernière version de 2.1.2, le module complémentaire est désormais compatible avec Splunk Cloud entre la plateforme Splunk et Splunk Cloud. Les clients qui utilisent des instances **Classic** avec des instances IDM ou **Victoria** peuvent bénéficier de cette amélioration de la compatibilité de la plateforme. Les clients ont désormais la possibilité de choisir entre Splunk Enterprise ou Splunk Cloud tout en envisageant le déploiement de notre module complémentaire pour faciliter l'intégration de Splunk.

Pour plus d'informations, consultez Splunk Integration.

Enregistrement d'événements de session dans SIEM

Les événements **d'enregistrement de session** peuvent désormais être exportés vers SIEM sous la forme d'événements **Risk Insight** et d'événements de **source de données** pour les applications et les postes de travail. Les types d'événements récemment ajoutés se trouvent dans l'étape Evénements de données à exporter sur la page **Exportations de données** .

Pour plus d'informations, consultez la section Stratégies et actions.

24 mai 2023

Informer l'utilisateur final d'une action globale

La fonctionnalité **Stratégies et actions** de Citrix Analytics prend désormais en charge l'action globale **Notifier l'utilisateur final**, qui peut être associée à un ou plusieurs déclencheurs d'indicateurs de risque intégrés ou personnalisés. Les administrateurs peuvent créer des stratégies à l'aide de **l'action Notifier l'utilisateur final** qui génère des notifications par e-mail destinées uniquement aux utilisateurs finaux. Cette action peut être utilisée dans divers cas d'utilisation de conformité, tels que la notification aux utilisateurs en cas d'utilisation non autorisée d'applications ou l'envoi d'alertes en cas de comportement suspect sur leurs comptes Citrix sans prendre de mesures perturbatrices. Les administrateurs peuvent personnaliser le corps et l'objet du message électronique en fonction du scénario spécifique.

Pour plus d'informations, voir Notifier l'utilisateur final.

4 mai 2023

Génération d'événements de test

La fonctionnalité de **génération d'événements de test** est créée pour aider les clients à tester rapidement leur pipeline Citrix Analytics - SIEM. Auparavant, si l'administrateur devait tester cette intégra-

tion, il devait attendre l'intégration de la source de données et l'activité des utilisateurs pour vérifier si les événements étaient générés par Citrix Analytics et donc reçus par son environnement SIEM. Ce n'est plus une nécessité. Il suffit de cliquer sur le bouton **Envoyer des données de test** pour envoyer un événement fictif dans l'environnement SIEM et d'utiliser la requête fournie pour vérifier si l'intégration SIEM de Citrix Analytics est définie comme prévu. Cela peut également fonctionner pour l'administrateur qui essaie de déboguer un flux de données perturbé, car cela peut aider à isoler le point de défaillance.

Pour plus d'informations, consultez la section Génération d'événements de test.

Génération d'alertes par e-mail SIEM

La fonctionnalité de génération d'alertes par e-mail SIEM simplifie considérablement le processus de résolution des problèmes liés à l'exportation de données. Citrix Analytics envoie des alertes système pour les activités susceptibles d'entraîner ou d'indiquer une interruption du flux de données SIEM. L'e-mail est distribué aux administrateurs Citrix Cloud, aux administrateurs complets de Security, aux administrateurs en lecture seule de Security et aux administrateurs en lecture seule de Security and Performance. Les différents types d'alertes qui sont envoyés sont les suivants :

1. **Alerte d'exportation de données SIEM - Le mot de passe a été réinitialisé**

   Cet e-mail est déclenché chaque fois que le mot de passe du compte est réinitialisé depuis la page Exportations de données. Si cela est fait uniquement sur l'interface graphique de Citrix Analytics for Security, cela peut entraîner une interruption du flux de données. Cette alerte indique l'heure à laquelle la réinitialisation du mot de passe a été effectuée, ce qui facilite grandement le retour à un flux de données réussi.

2. **Alerte d'exportation de données SIEM : arrêt du flux de données**

Cet e-mail est déclenché chaque fois que le client est confronté à un formulaire d'interruption du flux de données

- **Plus de 24 heures** : temps critique pour retrouver rapidement un flux de données efficace en utilisant les conseils de dépannage utiles contenus dans l'alerte ou en utilisant l'onglet **Résumé de l'exportation des données** avec **guide rapide**.
- **Plus de 7 jours** : la stratégie de conservation de Kakfa pour le sujet de chaque client est de sept jours, ce qui signifie qu'il est possible que certaines données sécurisées aient expiré. Il est impératif d'utiliser les outils de dépannage pour rétablir le flux de données vers le SIEM.
- **Plus de 30 jours** : cela signifie que le client a souffert de problèmes de sécurité et qu'il doit immédiatement s'attacher à rétablir le flux de données entre Citrix Analytics et l'environnement SIEM.

Pour plus d'informations, consultez la section Génération d'alertes par e-mail SIEM.

13 avril 2023

Problème résolu

L'application Windows Citrix Workspace envoie un nom de fichier, un chemin et une propriété de format vides à partir de la version 2203 et des versions ultérieures de l'application Citrix Workspace. Par conséquent, l'interface graphique de Citrix Analytics for Security affiche les valeurs NA pour les colonnes Nom du fichier de téléchargement, Chemin du fichier de téléchargement et Format de fichier de téléchargement. Ce problème est désormais résolu. [CAS-73498]

31 mars 2023

Événements d'enregistrement de session dans Citrix Analytics for Security

Dans Citrix Apps and Desktops, deux nouveaux types d'événements ont été ajoutés pour aider à identifier et à évaluer les événements basés sur l'enregistrement de session.

- Citrix.EventMonitor.RDPConnection
- Citrix.EventMonitor.UserAccountModification

Les administrateurs peuvent désormais facilement identifier et évaluer les risques de sécurité potentiels. Ils peuvent utiliser ces événements pour recueillir des informations sur des données vitales telles que les identifiants de processus, les adresses IP de destination et les descriptions des opérations des comptes utilisateurs. En outre, ces événements peuvent également être consultés sur la page des **indicateurs de risque personnalisés** et sur la page de **recherche en libre-service** .

- **Recherche en libre-service** : vous pouvez consulter ces événements ainsi que les détails de leurs attributs.
- **Indicateurs de risque personnalisés** : vous pouvez configurer n'importe quel indicateur personnalisé à l'aide de ces types d'événements.
  Pour plus d'informations, consultez la section Types d'événements et champs pris en charge.

Événements de App Protection dans Self-Service Search

Un nouvel événement appelé **AppProtection.ScreenCapture** se déclenche lorsque vous essayez de capturer une capture d'écran alors que vous êtes dans une session protégée sous la source de données Citrix Apps and Desktops. Les événements **AppProtection.ScreenCapture** sont également disponibles sur les pages de **recherche en libre-service** et d'**exportation de données**.

- **Recherche en libre-service** : vous pouvez consulter les résultats de **AppProtection.ScreenCapture** ainsi que tous les détails de ses attributs.

- **Exportations de données** : vous pouvez consulter le type d'événement **AppProtection.ScreenCapture** dans la section Exportations de données. Accédez à **Paramètres > Exportations de données > Configuration > Événements de données à exporter** sélectionnez **Applications et postes** de travail dans la catégorie Événements de source de données (facultatif).

Vous pouvez également afficher un nouvel attribut appelé **Stratégies App Protection** pour l'événement **Session.Logon**.

Pour plus d'informations, consultez la section Types d'événements et champs pris en charge.

30 mars 2023

Prise en charge des rôles personnalisés

Un administrateur peut être ajouté pour des rôles personnalisés à l'aide de groupes dans votre Active Directory ou Azure Active Directory ou en configurant une intégration Okta pour Citrix Analytics for Security. Cette intégration permet une approche rationalisée de la gestion des autorisations d'accès aux services pour tous les administrateurs de groupe.

Après avoir correctement ajouté un administrateur à Active Directory ou à Azure Active Directory, l'administrateur peut créer des groupes et attribuer un rôle personnalisé à un groupe spécifique. Les autorisations individuelles sont privilégiées par rapport aux autorisations de groupe si un administrateur est membre des deux.

Pour plus d'informations, consultez la section Support des rôles personnalisés.

Panneau de résolution des problèmes pour l'interface utilisateur SIEM

L'interface utilisateur des exportations de données a été améliorée avec les modifications suivantes :

- **Onglet Résumé** : L'onglet Résumé décrit les mesures des événements SIEM, l'état d'intégration des sources de données et l'état de consommation des données dans le scénario suivant :
  - **Données disponibles dans Citrix Analytics** : fournit l'état d'intégration des différentes sources de données.
  - **Événements disponibles pour la consommation du SIEM** : fournit le nombre d'informations envoyées à votre environnement SIEM.
  - **Consommation de données par SIEM** : fournit l'état de la consommation de données.
- **Onglet Configuration** : L'onglet **Configuration** contient les informations relatives à la configuration de votre compte, à la configuration de l'environnement SIEM et à la sélection des événements de données.

- **Guide rapide d'exportation de données** : les administrateurs peuvent désormais utiliser le **guide rapide**, qui simplifie la configuration et la gestion des intégrations SIEM. Le lien **Guide rapide d'exportation de données** est accessible depuis les onglets **Résumé** et **Configuration** .

Pour plus d'informations, voir Résolution des problèmes liés à l'exportation de données.

24 mars 2023

Modification de la vue du profil utilisateur

Les données de profil des utilisateurs relatives aux applications, aux emplacements, aux appareils et à l'utilisation des données ShareFile ne sont pas disponibles sur la page **Informations utilisateur** de la chronologie de l'utilisateur. Les informations utilisateur suivantes provenant d'Active Directory sont toujours disponibles :

- Intitulé du poste
- Adresse
- E-mail
- Phone
- Emplacement
- Organization

Aucune modification n'a été apportée aux données du profil utilisateur qui sont exportées vers SIEM. Pour plus d'informations, consultez la section Profil utilisateur.

Suppression des suggestions automatiques dynamiques de toutes les vues de recherche

La fonctionnalité de suggestion automatique pour les dimensions basées sur les données historiques du locataire est désormais obsolète pour les pages suivantes :

- Recherche en libre-service
- Indicateur de risque personnalisé

Toutefois, les suggestions statiques pour des dimensions telles que **Event-Type** et **Clipboard-Operations** sont toujours disponibles dans la zone de recherche.

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

21 mars 2023

Panneau de recommandations pour aider à intégrer la source de données StoreFront sur site

Un nouveau panneau de **recommandations** a été introduit sur la page **Sources de données** . Le panneau **Recommandations** de la page **Sources de données** explique à l'utilisateur l'importance d'intégrer des sources de données StoreFront sur site. Il permet à l'utilisateur d'intégrer facilement les sources de données StoreFront sur site et offre également la possibilité à l'utilisateur de consulter et de garantir l'intégration de toutes les sources de données disponibles.

Pour plus de détails, consultez la section Connexion à un déploiement StoreFront.

23 février 2023

Problèmes résolus

Les actions échouent pour les déploiements Citrix Apps and Desktop sur site où la version de Citrix Apps and Desktop > 1912. Ce problème a été observé à la fois dans les actions manuelles et basées sur des stratégies. Ce problème est désormais résolu. [CAS-69098]

La page Recherche en libre-service d'applications et de bureaux affiche plusieurs événements de démarrage et de fin d'application lorsque des applications virtuelles ne sont lancées qu'une seule fois. Ce problème se produit sur les versions clientes de l'application Citrix Workspace pour Linux. Ce problème est désormais résolu. [CAS-36236]

Les événements utilisateur du service Secure Private Access après le 4 avril 2022 et jusqu'à fin mai 2022 peuvent ne pas être disponibles dans vos clients Citrix Analytics. Ce problème est désormais résolu. [CAS-66897]

22 février 2023

Amélioration des notifications hebdomadaires par e-mail

Citrix Analytics envoie des notifications hebdomadaires par e-mail qui permettent de résumer les expositions aux risques de sécurité de votre entreprise. La notification hebdomadaire par e-mail a été améliorée avec les mises à jour suivantes :

- Fournit une vue de la répartition des risques des utilisateurs : nombre total d'utilisateurs découverts, nombre d'utilisateurs risqués et non risqués pendant une semaine
- Nombre total d'événements traités pendant une semaine
- Nombre total d'indicateurs déclenchés pendant une semaine
- Nombre total d'actions effectuées pendant une semaine

- Nombre total de sources de données activées pour le traitement des données

Pour plus de détails, consultez la section Notification hebdomadaire par e-mail.

Ajout du champ Download File Format pour le type d'événement app.saas.file.Download

Sur la page de recherche en libre-service de la source de données Apps and Desktops, un nouveau champ **Download File Format** a été ajouté pour le type d'événement App.saas.file.Download. Avec cette modification, vous pouvez désormais configurer des indicateurs de risque personnalisés pour le champ **Format de fichier de téléchargement** et également exporter le champ dans le cadre du format Exporter au format CSV.

Pour plus d'informations, consultez la section Recherche en libre-service d'applications et de bureaux.

Modification des champs dérivés du navigateur

Auparavant, la page de recherche en libre-service comportait les champs **Browser**, **Browser Major Version** et **Browser Minor Version** pour représenter les noms et les versions des navigateurs. Toutefois, par souci de clarté et d'exactitude, ces trois champs sont désormais obsolètes et remplacés par le **Browser Name** et **Browser Version** dans la recherche en libre-service, un modèle d'indicateur personnalisé et une source de données à télécharger au format CSV pour les applications et les ordinateurs de bureau.

Pour plus d'informations, consultez la section Recherche en libre-service d'applications et de bureaux.

16 février 2023

Problème résolu

Les e-mails hebdomadaires sont affectés pour certains clients de l'UE et de l'APS lors de la récupération du statut de masquage du nom d'utilisateur pour un locataire. Par conséquent, les administrateurs reçoivent 10 e-mails hebdomadaires identiques en raison de cette exception. Une fois l'exception survenue, les locataires suivants n'ont pas reçu l'e-mail hebdomadaire. Ce problème est désormais résolu. [CAS-76138]

3 février 2023

Support analytique pour le service Citrix Secure Private Access disponible dans l'Union européenne et dans les régions Asie-Pacifique Sud

Citrix Analytics for Security traite désormais les événements utilisateur à partir de Citrix Secure Private Access, disponible dans la région Union européenne et dans la région Asie-Pacifique Sud. Si votre organisation a intégré Citrix Cloud depuis la région de l'Union européenne ou de la région Asie-Pacifique Sud, vous pouvez consulter les informations sur les risques des utilisateurs qui utilisent le service Secure Private Access.

Pour plus d'informations, consultez la section Sources de données.

11 janvier 2023

Suppression de la fonctionnalité de filtrage Web de Secure Private Access

La fonctionnalité de filtrage Web a été supprimée de la catégorie Secure Private Access. Les fonctionnalités suivantes de Citrix Analytics for Security sont affectées par l'abandon du filtrage Web basé sur les catégories par Secure Private Access :

1. Les champs de données tels que le groupe de catégories, la catégorie et la réputation des URL ne sont plus disponibles sur le tableau de bord Citrix Analytics for Security.
2. L'indicateur Risky d'accès au site Web, qui repose sur les mêmes données, est également obsolète et n'est pas déclenché pour les clients.
3. Les indicateurs de risque personnalisés existants utilisant les champs de données (catégorie-groupe, catégorie et réputation des URL) et les stratégies associées ne sont plus déclenchés.
4. Les onglets **Accès utilisateur** et **Accès aux applications** .
5. Les exportations SIEM conservent les attributs urlcategory, urlcategorygroup et urlcategoryreputation depuis un certain temps avec les valeurs fictives suivantes :
    - 99999 pour la catégorie et le groupe de catégories
    - 0 pour Reputation

Pour plus d'informations, consultez la section Recherche en libre-service pour Secure Private Access.

27 décembre 2022

Modification de la liste déroulante des sources de données pour la recherche en libre-service

La liste des sources de données est modifiée pour refléter les **sessions** par défaut plutôt que **les applications et les postes** de travail sur la page de recherche en libre-service. De plus, la section Performances est déplacée vers le haut, suivie de la section Sécurité car les sources de données de performances n'étaient pas visibles.

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

13 décembre 2022

Amélioration du tableau de bord des utilisateurs

Le tableau de bord des utilisateurs a été remanié avec des résumés et des graphiques pour aider les administrateurs à surveiller le niveau de sécurité de l'organisation. La vue fournit non seulement des détails sur les utilisateurs découverts, les indicateurs de risque déclenchés et les actions appliquées, mais fournit également une courbe de tendance chronologique contenant des indicateurs critiques pour une meilleure évaluation des risques. Les administrateurs peuvent explorer les données qui les intéressent et accéder à des tableaux de bord pertinents avec le contexte approprié pour une analyse des risques plus rapide.

Pour plus d'informations, consultez Tableau de bord des utilisateurs.

5 décembre 2022

Tableau de bord de garantie d'accès - Logon Network

La section Logon Network vient d'être ajoutée et fournit les informations utilisateur suivantes :

- Les organisations associées aux adresses IP à partir desquelles les utilisateurs se sont connectés.
- Le total du sous-réseau public unique et du sous-réseau privé à partir duquel les utilisateurs se sont connectés.
- Les informations indiquant que l'utilisateur s'est connecté à l'aide de proxys et de services VPN privés.

À l'aide de ces informations supplémentaires, un administrateur peut valider les informations de connexion de l'utilisateur et s'assurer que l'ouverture de session de l'utilisateur répond aux attentes de sécurité de l'organisation.

Pour plus de détails, consultez Access Assurance Dashboard.

18 novembre 2022

Problème résolu

- Les indicateurs de géofence qui étaient déclenchés par erreur sans aucun événement source ont été corrigés. [CAS-73222]

8 novembre 2022

Renommer les actions

Certaines des actions utilisées dans Citrix Analytics for Security sont renommées pour plus de clarté. Ces actions sont les suivantes :

- **Avertir les administrateurs** - Avertir les administrateurs
- **Verrouiller l'utilisateur** - Verrouiller le compte utilisateur
- **Déconnecter l'utilisateur** : déconnecter les sessions actives
- **Déverrouiller l'utilisateur** - Déverrouiller le compte utilisateur
- **Désactiver l'utilisateur** - Désactiver le compte utilisateur

Pour plus d'informations, voir Quelles sont les actions ?

Problèmes résolus

- Si vous sélectionnez une option dans la liste déroulante des actions de la chronologie, vous ne pouvez pas déclencher d'action manuelle car les boutons Effacer et Appliquer ne sont pas visibles. Cette condition se produit dans la dernière version de Firefox. Ce problème est désormais résolu. [CAS-72051]
- Les catégories **HardDrive**, **harddrive** et **HDD** sont regroupées en une seule catégorie en tant que **Hard Disk Drive** pour le champ Type de périphérique de téléchargement de la source de données Self-Service Search for the Apps and Desktops. [CAS-67188]
- Parfois, des notifications dupliquées sont reçues de Microsoft Graph avec le même ID d'alerte, ce qui entraîne la création d'événements à risque dupliqués. Un mécanisme de déduplication est mis en œuvre dans les applications pour éviter ce problème. [CAS-66731]

19 octobre 2022

Sélection et exportation des événements de la date et de la source

Vous pouvez désormais tirer parti du nouveau flux de travail d'exportation des événements de données pour exporter les événements des sources de données, en plus des informations sur les risques générées par l'apprentissage automatique, des événements et des données associées.

Cela permet aux administrateurs des opérations de sécurité et de sécurité (SOC) de :

- Corrélez les données de Citrix Analytics avec les événements d'autres sources de données agrégés sur les informations de sécurité et la gestion des événements (SIEM)
- Contrôlez les événements de données qui sont acheminés vers les SIEM pour optimiser les coûts de stockage

Les événements de données sont transmis à vos intégrations SIEM et connecteurs de données existants, à égalité avec ce qui est disponible sur notre affichage de recherche d'événements en libre-service.

Pour plus d'informations, consultez la section Événements liés aux données exportés depuis Citrix Analytics for Security vers votre service SIEM.

18 octobre 2022

Autoriser l'administrateur à exécuter une action d'enregistrement de session dynamique sur les sites Citrix DaaS

Les administrateurs peuvent désormais exécuter des actions d'enregistrement de session dynamique sur les sites Citrix DaaS et enregistrer de manière dynamique les sessions virtuelles des utilisateurs. Ils peuvent configurer l'action avec une stratégie pour démarrer automatiquement l'enregistrement des sessions utilisateur au cas où une activité risquée d'un utilisateur donné serait détectée par Citrix Analytics for Security.

Pour plus d'informations, voir Quelles sont les actions ?

14 octobre 2022

Fournir des commentaires sur les indicateurs de risque utilisateur

Les administrateurs de Citrix Analytics for Security peuvent désormais signaler les indicateurs de risque utilisateur comme utiles ou non utiles en fournissant des commentaires sur le panneau de détails des indicateurs. Cette fonctionnalité permet aux administrateurs de signaler les faux positifs, de

réduire le bruit lié aux indicateurs fréquemment déclenchés et de partager du contexte supplémentaire avec d'autres administrateurs. Comme résultat supplémentaire, l'indicateur de risque inutile est masqué dans la chronologie de l'utilisateur et le score de risque de l'utilisateur est recalibré.

Pour plus d'informations, voir Fournir des commentaires sur les indicateurs de risque utilisateur.

26 septembre 2022

Garantie d'accès pour soutenir la liste de blocage de la géofence

Les onglets de localisation **sécurisée** et **risquée** sont ajoutés dans les paramètres de Geofence.

- Le géofencing sécurisé permet d'identifier et de restreindre l'accès en dehors d'une zone délimitée définie.
- Le géofencing de localisation à risque permet de détecter et de limiter les accès à risque des utilisateurs conformément au comportement connu de l'entreprise.

Les géofencings sûrs et risqués sont soutenus par leurs propres indicateurs de risque personnalisés préconfigurés.

Pour plus d'informations, voir Activer le géofencing.

Problèmes résolus

- API Citrix Cloud pour afficher le **nom du client** dans le corps de l'e-mail. Désormais, l'e-mail utilise le surnom pour afficher le **nom du client** dans le corps de l'e-mail envoyé aux administrateurs. [CAS-65350]
- La carte source de données Citrix Gateway est courante dans **Citrix Analytics for Security** et **Citrix Analytics for Performance**. Le traitement des données appelait en permanence le terminal Citrix Analytics for Security et était interrompu pour les clients disposant uniquement de droits **Citrix Analytics for Performance** . [CAS-70817]
- Lorsque plusieurs messages d'autorisation sont reçus simultanément de Citrix Cloud, une condition de course se produit lors de la mise à jour du cache Redis. Dans un tel scénario, un message d'autorisation est mis à jour dans le cache et le reste disparaît. Ce problème est désormais résolu pour mettre à jour tous les messages d'autorisation dans le cache. [CAS-70823]

13 septembre 2022

Amélioration du tableau de bord Sharelink

Le tableau de bord Sharelink a été remanié avec un résumé et une vue détaillée. La vue récapitulative comprend les principales actions actives et les actions les plus risquées. La vue détaillée fournit plus d'informations à l'administrateur avec l'introduction des attributs créés par, du nombre d'activités, du type d'authentification, de l'autorisation, du type de partage et du contenu. L'administrateur peut effectuer des recherches plus poussées et des filtres supplémentaires selon les besoins et modifier/-fournir le délai pour consulter les données qui l'intéressent.

Pour plus d'informations, consultez la section Tableau de bord Partager des liens.

9 septembre 2022

Amélioration des indicateurs de risque d'Impossible Travel

Les indicateurs de risque Impossible Travel ont été améliorés pour indiquer l'organisation d'enregistrement et le type de routage des adresses IP des clients. Ces nouveaux champs sont disponibles à la fois dans les vues détaillées des indicateurs de la chronologie utilisateur et dans les détails des indicateurs envoyés au SIEM.

Pour plus d'informations sur les stratégies par défaut, consultez les articles suivants :

- Évaluation continue des risques.
- Stratégies et actions

19 août 2022

Activer la télémétrie d'impression VDA

Un événement appelé VDA.Print se déclenche lorsqu'une tâche d'impression est lancée dans Citrix Apps and Desktops. Les événements VDA Print sont également disponibles sur les pages de **recherche en libre-service** et d'**indicateurs de risque personnalisés** .

- **Recherche en libre-service** : vous pouvez consulter les résultats de VDA.Print ainsi que tous les détails de ses attributs.
- **Indicateurs de risque personnalisés** : de nouveaux événements sont fournis pour la télémétrie d'impression VDA via EventHub et sont également disponibles dans Custom Indicator. Vous pouvez utiliser ces paires clé/valeur d'événement pour configurer des déclencheurs d'indicateurs personnalisés.

Pour activer la télémétrie d'impression et la transmission des journaux d'impression à Citrix Analytics for Security, vous devez créer des clés de registre et configurer votre VDA. Ces journaux d'impression fournissent des informations essentielles sur les activités d'impression, telles que les noms des imprimantes, les noms des fichiers d'impression et le nombre total de copies imprimées. En tant qu'administrateur de la sécurité, vous pouvez utiliser ces journaux pour analyser les risques et enquêter sur vos utilisateurs.

Pour plus d'informations, voir Activation de la télémétrie d'impression pour Citrix DaaS.

18 août 2022

Problème résolu

- Dans la recherche en libre-service pour les applications et les postes de travail et sur la page Connexions utilisateur sous le tableau de bord de localisation de l'assurance accès, la valeur de version de l'application Workspace a été renseignée sous la forme **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]

17 août 2022

Personnalisation de l'e-mail de l'utilisateur final par stratégie

Vous pouvez désormais personnaliser le contenu des e-mails envoyés aux utilisateurs finaux en fonction de la stratégie. Plus précisément, lorsque vous créez une stratégie avec l'action Demander la réponse de l'utilisateur final ou une action perturbatrice sur le compte de l'utilisateur (telle que Déconnecter l'utilisateur et Verrouiller l'utilisateur), le contenu des e-mails envoyés aux utilisateurs finaux lorsque la stratégie est appliquée est personnalisable.

Pour plus d'informations sur la personnalisation du courrier de l'utilisateur final par stratégie, consultez la section Stratégies et actions.

11 août 2022

De nouvelles questions concernant la **garantie d'accès** —**Géolocalisation** ont été ajoutées dans l'article **FAQ** . Pour plus de détails, consultez la FAQ.

Problème résolu

- Le bouton **Afficher toutes les notifications** a redirigé l'administrateur vers un lien e-mail `https://citrix.cloud.com/notifications` hebdomadaire contenant une faute de

frappe. [CAS-69236]

17 juin 2022

Le traitement des données est activé par défaut pour les nouveaux droits payants

Auparavant, les clients disposant de nouveaux droits payants sur Citrix Analytics for Security devaient activer le traitement des données dans la carte de site de sources de données spécifiques pour commencer à traiter les données de ces sources de données.

Dans cette version, lorsque les nouveaux droits payants à Citrix Analytics for Security sont fournis, le traitement des données est activé par défaut pour les services Citrix Cloud suivants :

- Citrix Secure Private Access
- Citrix Content Collaboration
- Citrix DaaS

Pour plus d'informations, reportez-vous à la section Mise en route.

09 juin 2022

Problème résolu

- Les indicateurs de risque Microsoft Graph générés par la protection d'identité Azure AD et Microsoft Defender for Endpoint peuvent être affichés plusieurs fois dans Security Analytics. Ce problème est désormais résolu. [CAS-66593,CAS-66731]

2 juin 2022

Problèmes résolus

- Dans la recherche en libre-service des stratégies, lorsque vous sélectionnez la dimension **Policy-Name** dans votre requête de recherche pour filtrer les événements, une liste de stratégies non valides a été suggérée ainsi que les stratégies valides pour Security Analytics. [CAS-66838]
- La taille du fichier de téléchargement des événements **File.Download** de Windows Citrix Receiver ne s'affichait pas correctement dans la recherche en libre-service. Ce problème est apparu parce que la valeur réelle était exprimée en Ko et que l'interface utilisateur traitait la valeur comme des octets, ce qui entraînait l'affichage de valeurs incorrectes aux utilisateurs. [CAS-67105]

24 mai 2022

Présentation des indicateurs de risque de déplacement impossible pour Content Collaboration, Citrix DaaS et Citrix Virtual Apps and Desktops, et des sources de données Gateway

Si l'utilisateur ouvre une session à partir de deux emplacements trop éloignés l'un de l'autre pour voyager dans le temps écoulé, Citrix Analytics détecte cette activité comme un scénario de voyage impossible et déclenche l'indicateur de risque **de voyage impossible** . Pour plus d'informations sur les indicateurs de risque de voyage impossible, consultez les articles suivants :

- Indicateurs de risque Citrix Content Collaboration
- Indicateurs de risque de Citrix Gateway
- Indicateurs de risque Citrix Virtual Apps and Desktops et Citrix DaaS

17 mai 2022

Virtual Apps and Desktops est renommé Apps and Desktops

Sur les tableaux de bord et les rapports Security Analytics et dans les données envoyées par Security Analytics à votre service SIEM, toutes les étiquettes Virtual Apps and Desktops sont désormais mises à jour en tant qu'applications et bureaux pour s'aligner sur le nouveau nom du produit.

Par exemple, sur la page Sources de données, les étiquettes Virtual Apps and Desktops sont renommées Apps and Desktops.

L'étiquette Apps and Desktops représente à la fois Citrix Virtual Apps and Desktops sur site et Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) dans votre organisation.

Problèmes résolus

Citrix Analytics ne découvre pas automatiquement les sites Citrix DaaS Cloud Monitor ou Director associés à votre compte Citrix Cloud. [CAS-66801]

5 avril 2022

Nouveautés

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.

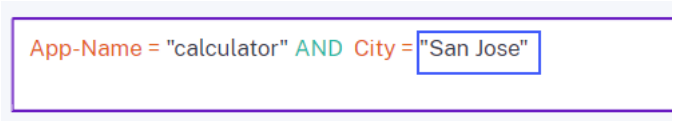
Par exemple, sur la page **Sources de données** et la page de **recherche en libre-service**, les étiquettes **Secure Workspace Access** de travail sont renommées **Accès privé sécurisé**.

21 mars 2022

Problème résolu

- Dans la page **Créer un indicateur de risque**, 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]

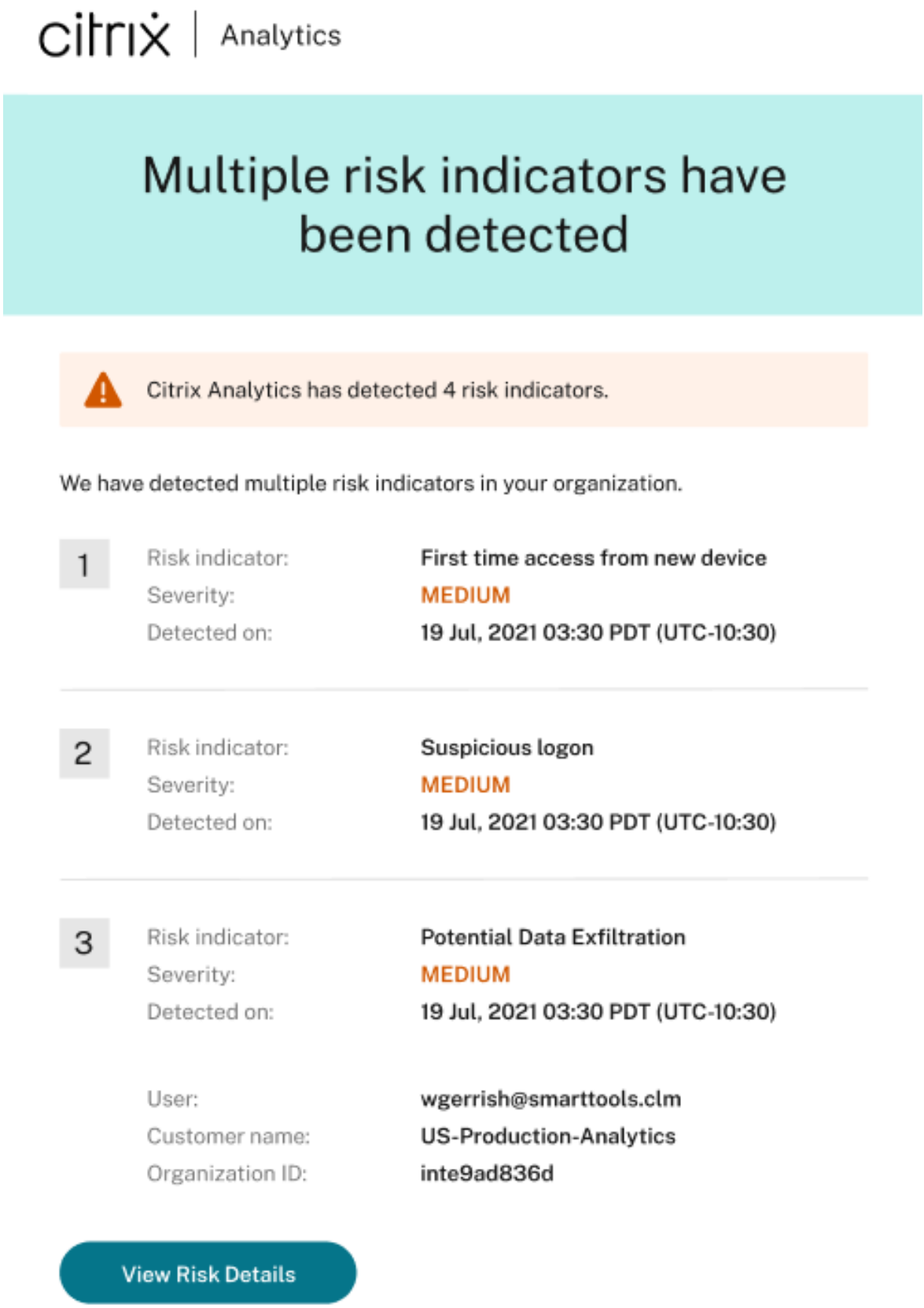
10 mars 2022

Nouveautés

Améliorations relatives à la notification

- La notification par e-mail pour l'action **Notifier les administrateurs** fournit désormais les détails des multiples indicateurs de risque associés à une stratégie déclenchée.
- Vous pouvez afficher le nom, le niveau de gravité et la date de déclenchement de chaque indicateur de risque associé à la stratégie.
- Cliquez sur **Afficher les détails du risque** pour ouvrir la page de chronologie de l'utilisateur dans Citrix Analytics et afficher le dernier indicateur de risque qui a déclenché la stratégie. Sur

la page de chronologie de l'utilisateur, vous pouvez également afficher tous les indicateurs de risque déclenchés pour l'utilisateur.



Pour plus d'informations sur l'action **Notifier les administrateurs**, consultez la section Stratégies et actions.

Problème résolu

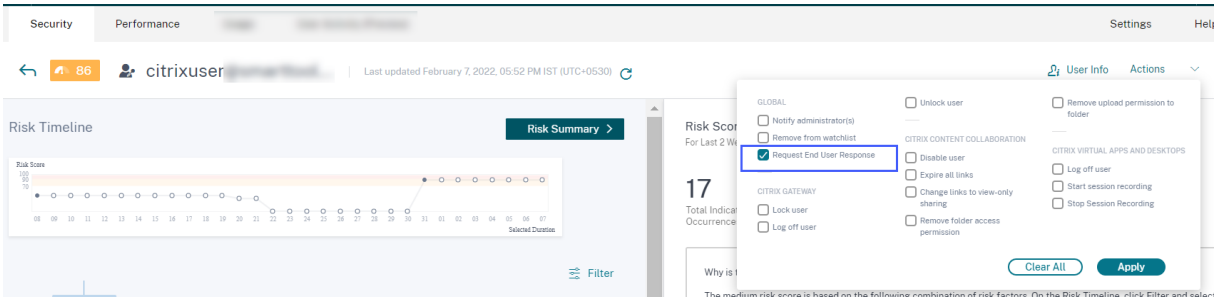
Citrix Analytics ne parvient pas à recevoir les événements utilisateur de la source de données Secure Workspace Access. Par conséquent, les événements utilisateur ne s'affichent pas dans la page de recherche en libre-service correspondante. En outre, vous ne pouvez pas créer d'indicateurs de risque personnalisés pour la source de données Secure Workspace Access. [CAS-64619]

3 mars 2022

Nouveautés

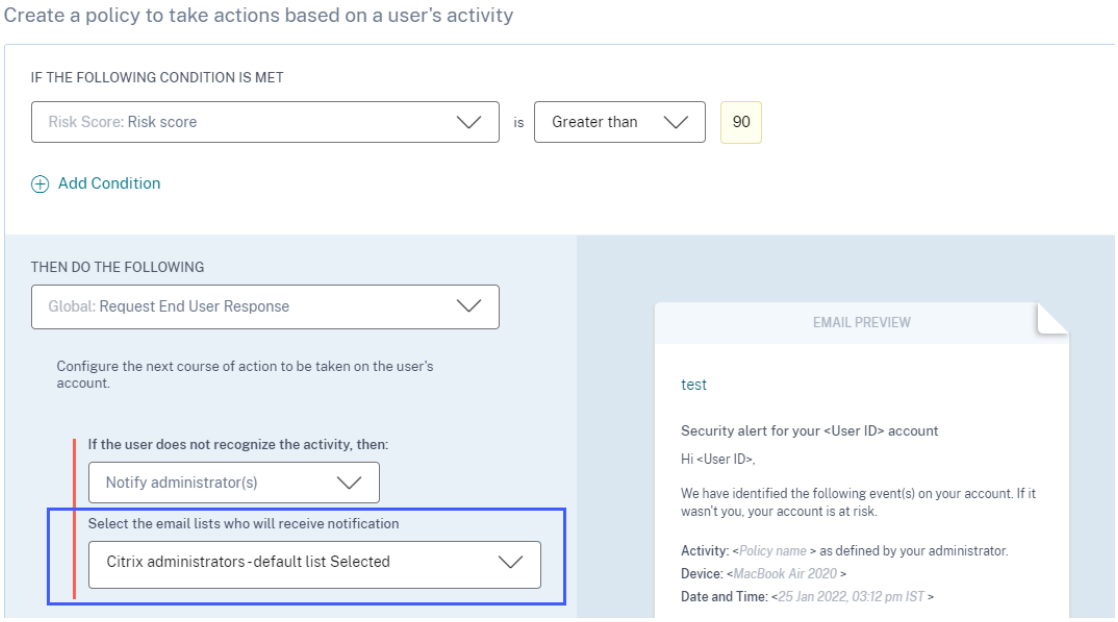
Appliquer la demande de réponse de l'utilisateur final manuellement Auparavant, vous pouviez appliquer l'action **Demander une réponse de l'utilisateur final** à un compte d'utilisateur uniquement en créant une stratégie.
Avec cette version, vous pouvez sélectionner l'action dans la liste **Actions** de la chronologie utilisateur et appliquer manuellement cette action à un indicateur de risque.

Pour plus d'informations sur l'action et sur la façon d'appliquer des actions manuellement, consultez Stratégies et actions.

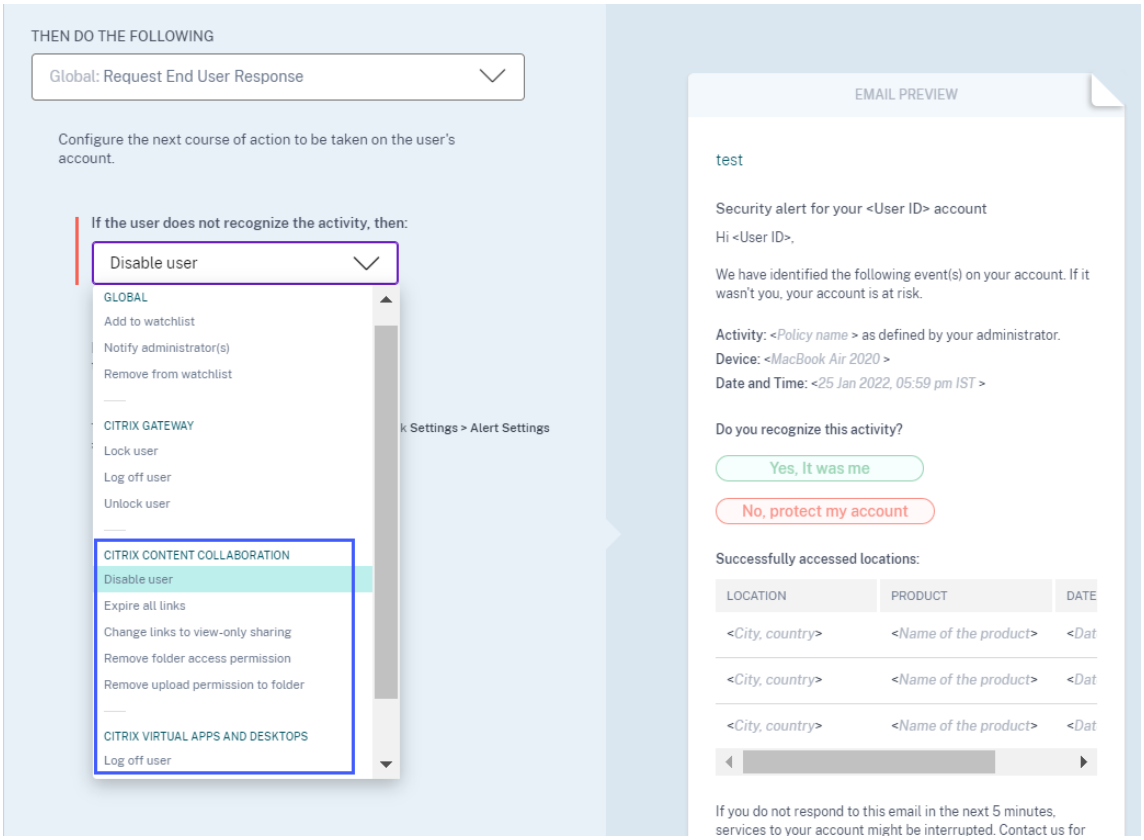


Demander des améliorations aux réponses des utilisateurs finaux pour la stratégie Lorsque vous créez une stratégie avec l'action **Demander une réponse de l'utilisateur final**, les améliorations suivantes s'affichent :

- Après avoir sélectionné **Notifier les administrateurs** comme action suivante, vous pouvez désormais afficher les listes de distribution par défaut et les listes de distribution d'e-mails créées parmi lesquelles vous pouvez choisir.



- Vous pouvez désormais sélectionner l'une des actions dans Citrix Content Collaboration ou Citrix Virtual Apps and Desktops et Citrix DaaS comme action suivante. Auparavant, vous ne pouviez sélectionner qu'une des actions globales ou des actions Citrix Gateway.



Pour plus d'informations sur cette action, consultez la section Stratégies et actions.

23 février 2022

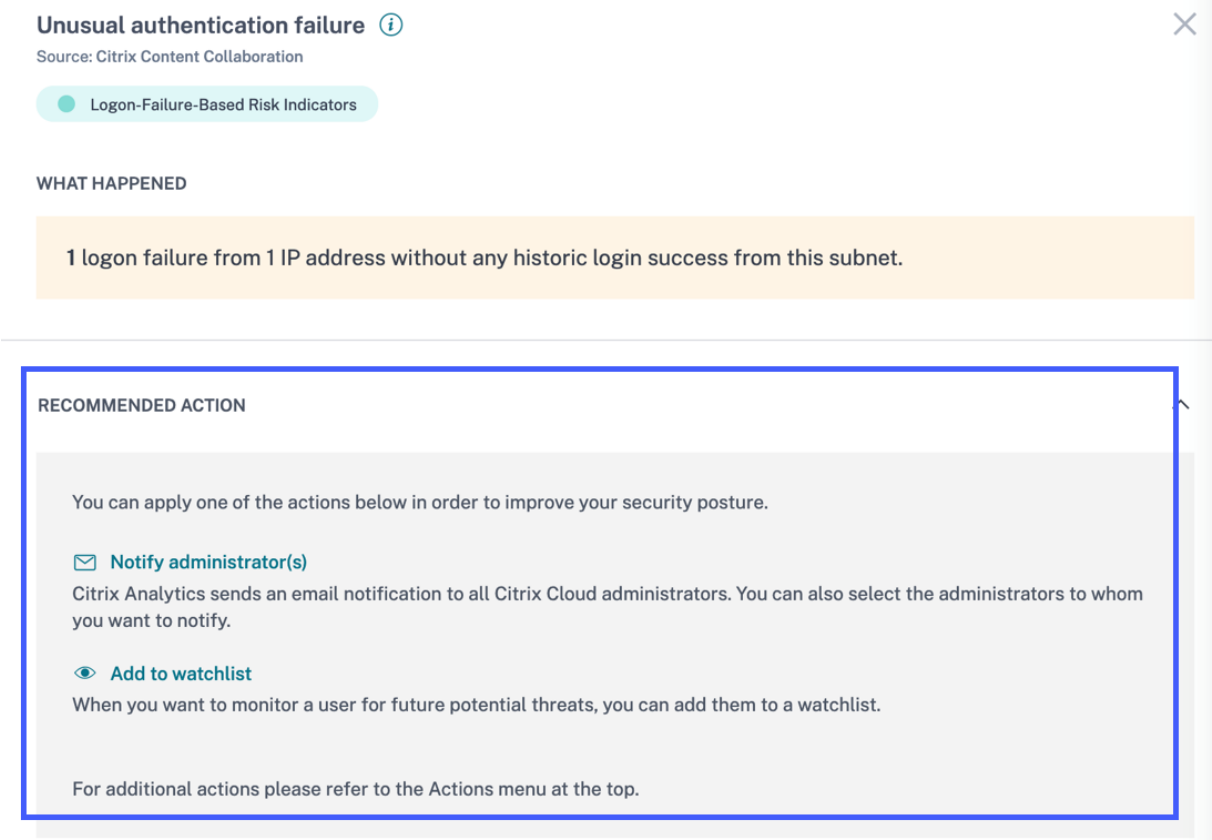
Nouveautés

Mesures recommandées pour un indicateur de risque Citrix Analytics vous suggère d'appliquer des actions telles que **Notifier les administrateurs**, **Ajouter à la liste**de suivi et **Créer une stratégie** lorsque les indicateurs de risque suivants sont déclenchés pour un utilisateur :

- Échec d'authentification inhabituel (source de données Content Collaboration)
- Échec d'authentification inhabituel (source de données Gateway)
- Ouverture de session suspecte (Citrix Virtual Apps and Desktops et source de données Citrix DaaS)

Lorsque vous accédez à la chronologie de l'utilisateur et que vous sélectionnez l'indicateur de risque, vous pouvez afficher toutes les actions suggérées dans la section **ACTION RECOMMANDÉE** .

Par exemple, dans l'indicateur de risque d'échec d'authentification inhabituel, vous pouvez afficher les actions recommandées suivantes :



Cette fonctionnalité fournit des conseils pour choisir une action que vous pouvez entreprendre en fonction de la gravité du risque posé par l'utilisateur. Cependant, vous pouvez également prendre

une mesure appropriée qui ne figure pas dans la liste recommandée et en fonction de votre analyse des risques.

Problème résolu

- Si votre organisation est intégrée à Citrix Cloud dans la région d'origine **Asie-Pacifique Sud**, Citrix Analytics peut ne pas recevoir d'événements utilisateur de la source de données d'authentification. Par conséquent, il est possible que vous ne voyiez pas les événements utilisateur dans la page de recherche en libre-service correspondante. Ce problème est résolu. [CAS-62300]

17 février 2022

Nouveautés

Amélioration de la collecte des données et des rapports pour les sources de données Citrix Virtual Apps and Desktops et Citrix DaaS Dans cette version, vous pouvez constater les modifications suivantes :

- Améliorations apportées à la collecte des données, à la corrélation et à la création de rapports sur les événements à partir des clients de l'application Citrix Workspace
- Amélioration de la qualité des événements reçus des utilisateurs et des versions client, qui peuvent être utilisés pour la recherche en libre-service, les indicateurs de risque personnalisés et la détection globale des risques.

Prise en charge des modèles contextuels pour les événements de session et les événements d'application dans Content Collaboration Sur la page de recherche en libre-service, vous pouvez désormais afficher les détails des seuls champs pertinents associés aux événements de fichier, de dossier, de session, de partage et d'utilisateur. Les champs non applicables aux événements sont supprimés.

Par exemple, vous pouvez afficher les détails suivants des `File.Copy` événements :

- ID de fichier
- ID de copie de fichier
- Chemin du fichier
- Chemin du fichier de destination
- Identifiant du flux
- ID de zone

Ces informations vous aident lors de l'enquête et de l'analyse des risques d'un compte utilisateur associé à un comportement à risque. Vous pouvez explorer les attributs spécifiques d'un événement qui semble risqué.

Pour plus d'informations sur les champs, voir Recherche en libre-service pour Content Collaboration.

10 février 2022

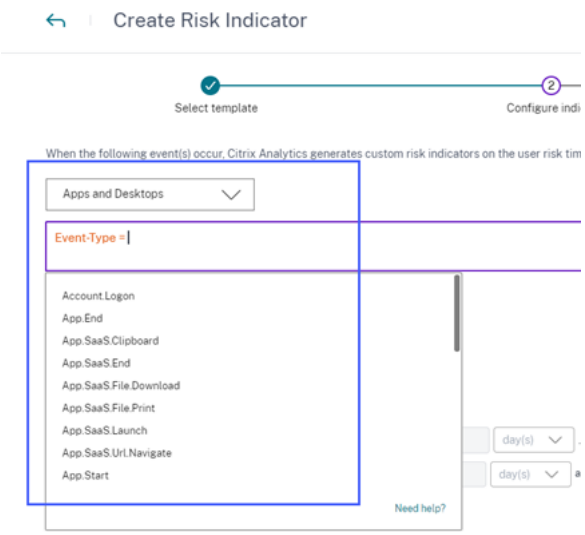
Nouveautés

Valeurs suggérées automatiquement pour les dimensions de l'indicateur de risque personnalisé Dans la page d'indicateur de risque personnalisé, lorsque vous sélectionnez une dimension et un opérateur valide dans la barre de condition, 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 `Event-Type` 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 section Indicateurs de risque personnalisés.



09 février 2022

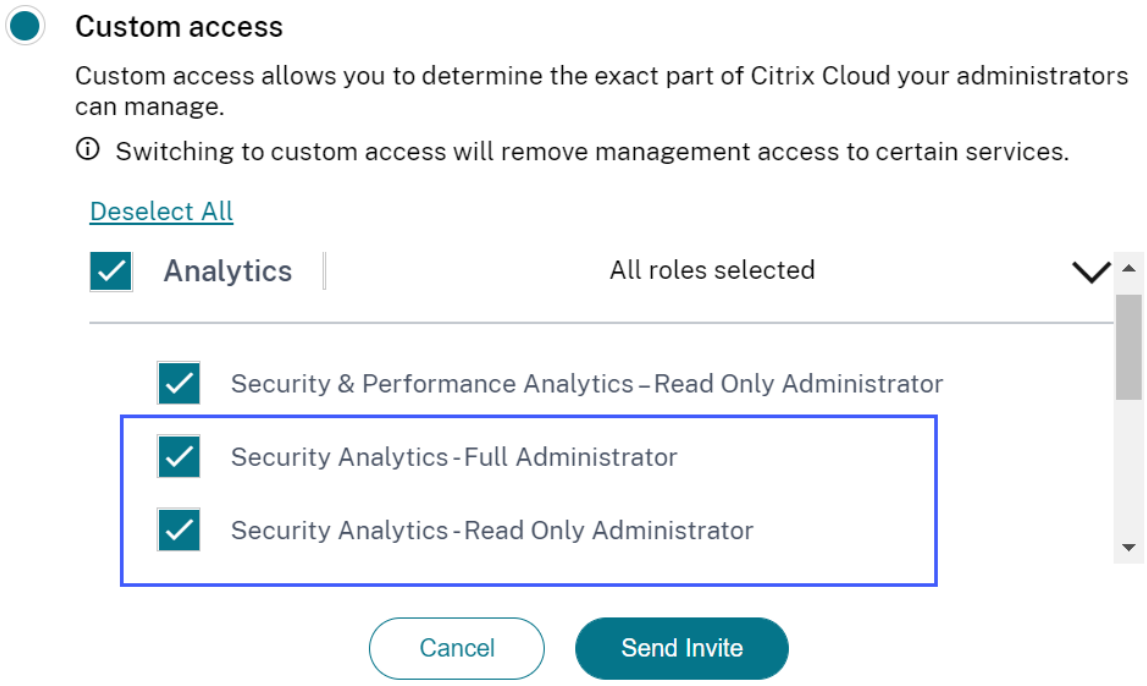
Nouveautés

Nouveaux rôles personnalisés pour les administrateurs En tant qu'administrateur Citrix Cloud disposant d'une autorisation d'accès total, vous pouvez inviter d'autres administrateurs à gérer Security Analytics dans votre organisation. Vous pouvez désormais attribuer les rôles personnalisés suivants aux administrateurs invités :

- Security Analytics - Administrateur complet
- Security Analytics - Administrateur en lecture seule

À l'aide du rôle personnalisé, vous pouvez fournir des autorisations d'accès en lecture seule ou complètes à vos administrateurs et leur permettre de gérer les différentes fonctionnalités de Security Analytics.

Pour plus d'informations sur les autorisations d'accès pour ces rôles personnalisés, voir Gérer les rôles d'administrateur pour Security Analytics.



Prise en charge des notifications par e-mail pour les administrateurs d'accès personnalisés Si vous êtes un administrateur Citrix Cloud avec des autorisations d'accès personnalisées (lecture seule ou accès complet) pour gérer Security Analytics, vous recevez désormais les notifications suivantes :

- Notifications hebdomadaires concernant les risques de sécurité détectés dans votre organisation. Pour plus d'informations, voir Notification hebdomadaire par e-mail.

- Notifications concernant les indicateurs de risque lorsque l'action **Notifier les administrateurs** est appliquée manuellement ou déclenchée par une stratégie. Pour plus d'informations, consultez la section Stratégies et actions.

28 janvier 2022

Nouveautés

Présentation des indicateurs de risque de connexion suspecte pour les sources de données Content Collaboration et Gateway Citrix Analytics for Security détecte désormais les ouvertures de session utilisateur de nature suspecte en fonction de plusieurs facteurs contextuels tels que :

- La localisation est jugée inhabituelle par rapport à l'utilisateur et à l'historique de l'organisation.
- L'appareil est considéré comme inhabituel par rapport à l'historique de l'utilisateur et de l'organisation
- Le réseau est considéré comme inhabituel en ce qui concerne l'historique de l'utilisateur et de l'organisation
- L'adresse IP est jugée suspecte en fonction des flux de renseignements sur les menaces IP

Lorsqu'un utilisateur se connecte à partir d'un contexte suspect basé sur la combinaison de ces facteurs, l'indicateur de risque est déclenché.

Cet indicateur de risque remplace l'indicateur de risque Accès à partir d'un emplacement inhabituel associé aux sources de données Citrix Content Collaboration et Citrix Gateway. Toutes les stratégies existantes basées sur l'indicateur de risque Accès à partir d'un emplacement inhabituel sont automatiquement liées au nouvel indicateur de risque : Ouverture de session suspecte.

Pour plus d'informations sur les indicateurs de risque, voir Connexion suspecte- Content Collaboration et Logon suspecte- Gateway.

Pour plus d'informations sur le schéma des indicateurs de risque, consultez Format de données Citrix Analytics pour SIEM.

20 janvier 2022

Nouveautés

Intégration avec Microsoft Azure Active Directory Vous pouvez désormais connecter votre Azure Active Directory à Citrix Analytics pour la sécurité pour :

- Importez les détails des utilisateurs et les groupes d'utilisateurs du domaine de votre organisation vers Citrix Analytics for Security.
- Enrichissez les profils des utilisateurs avec des détails supplémentaires tels que le titre du poste, l'organisation, l'emplacement du bureau, l'adresse e-mail et les coordonnées, qui vous aideront lors de l'enquête et de l'analyse des risques.

Pour plus d'informations, consultez Intégration Azure Active Directory.

18 janvier 2022

Nouveautés

Prise en charge des actions de lien de partage sur tous les indicateurs de risque Content Collaboration Auparavant, vous pouviez appliquer les actions de lien de partage - **Expirer tous les liens** et **Modifier le lien pour le partage en lecture seule** sur les indicateurs de risque basés sur des liens de partage suivants associés au service Content Collaboration :

- Téléchargement du lien de partage sensible anonyme
- Téléchargements de liens de partage excessifs
- Partage excessif de fichiers

Avec cette version, vous pouvez désormais appliquer les actions de lien de partage sur les indicateurs de risque basés sur les utilisateurs suivants associés au service Content Collaboration :

- Accès depuis un endroit inhabituel
- Accès excessif aux fichiers sensibles
- Chargements excessifs de fichiers
- Téléchargements excessifs de fichiers
- Suppression excessive de fichiers ou de dossiers
- Fichiers malveillants détectés
- Activité de ransomware suspectée
- Échecs d'authentification inhabituels

Vous pouvez également appliquer les actions du lien de partage sur les indicateurs de risque personnalisés associés au service Content Collaboration.

Pour plus d'informations sur les actions et les indicateurs de risque, consultez les articles suivants :

- Stratégies et actions

- Indicateurs de risque de Content
- Indicateurs de risque personnalisés

L'intégration avec SIEM est désormais disponible pour tous Vous pouvez intégrer Citrix Analytics for Security à vos services de gestion des informations et des événements de sécurité (SIEM) et exporter les données des utilisateurs de l'environnement informatique Citrix vers votre SIEM. L'intégration vous aide à corréler les données collectées auprès de différentes sources et à obtenir une vue globale de la sécurité de votre organisation.

Actuellement, vous pouvez intégrer Citrix Analytics for Security aux services suivants :

- Splunk
- Sentinel
- Recherche élastique
- Autres services SIEM à l'aide d'un connecteur de données basé sur Kafka ou Logstash

Pour plus d'informations, voir Intégration de la gestion des informations et des événements de sécurité (SIEM).

23 décembre 2021

Nouveautés

Améliorations des indicateurs de risque liés Les améliorations suivantes sont apportées :

- Vous pouvez désormais créer une stratégie avec l'indicateur de risque de **téléchargement de lien de partage sensible anonyme** .
- L'indicateur de risque de **téléchargement d'actions sensibles anonymes** est renommé **Téléchargement de lien de partage sensible anonyme** pour le distinguer en tant qu'indicateur de risque de lien de partage.
- L'indicateur de risque de **téléchargements excessifs** est renommé **Téléchargements de liens de partage excessifs** pour le distinguer en tant qu'indicateur de risque de lien de partage et pour le différencier de l'indicateur de risque de **téléchargements excessifs de fichiers** basé sur l'utilisateur.

Pour plus d'informations, consultez la section Indicateurs de risque de lien de partage Citrix.

21 décembre 2021

Nouveautés

Envoyez des notifications concernant les indicateurs de risque à vos administrateurs non Citrix Cloud Vous pouvez désormais informer les administrateurs non Citrix Cloud de votre organisation avec l'action **Notifier les administrateurs** .

Pour informer ces administrateurs, créez une liste de distribution par e-mail. Sélectionnez les administrateurs dans la liste de distribution des e-mails soit à partir des domaines externes connectés à Citrix Cloud, soit en utilisant leurs adresses e-mail directement. Lors de l'application de **l'action Notifier** les administrateurs, sélectionnez la liste de distribution des e-mails qui contient les administrateurs non Citrix Cloud.

Pour plus d'informations, consultez la section Liste de distribution des e-mails.

20 décembre 2021

Nouveautés

Envoyez des notifications de réponse aux utilisateurs de Content Collaboration Outre vos utilisateurs Active Directory, vous pouvez désormais appliquer l'action **Demander une réponse de l'utilisateur final** à vos utilisateurs Content Collaboration.

Cette action envoie des notifications par e-mail aux utilisateurs lorsque Citrix Analytics détecte des activités inhabituelles sur leurs comptes Citrix. Pour plus d'informations sur l'action **Demander une réponse de l'utilisateur final**, consultez Stratégies et actions.

Access Control est renommé Secure Workspace Access Dans les tableaux de bord et les rapports **Security** Analytics, toutes les étiquettes de **contrôle d'accès** sont désormais mises à jour en tant que **Secure Workspace Access** pour s'aligner sur le nom du produit renommé.

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

Problème résolu

- Pour la source de données Apps and Desktops, lorsque vous téléchargez le rapport de recherche sous forme de fichier CSV, certaines valeurs de champ du fichier CSV sont affichées comme non disponibles (N/A) bien que leurs valeurs soient disponibles. Par exemple, les valeurs des champs tels que `Download File NameSession Launch Type`, et `Workspace App Version` sont affichées sur la page de **recherche en libre-service**, mais dans le fichier CSV

téléchargé, vous voyez ces valeurs comme non disponibles (N/A). Ce problème est désormais résolu. [CAS-62299]

09 décembre 2021

Nouveautés

Créez facilement vos indicateurs de risque personnalisés grâce à des modèles Vous pouvez désormais sélectionner un modèle en fonction de votre cas d'utilisation et créer un indicateur de risque personnalisé. Les modèles vous guident en fournissant des requêtes et des paramètres prédéfinis. Cela facilite vos efforts tout en créant un indicateur de risque personnalisé.

Pour plus d'informations, consultez la section Indicateurs de risque personnalisés.

07 décembre 2021

Problème résolu

- Sur Citrix Analytics for Security, vous ne recevez pas les événements des utilisateurs qui utilisent Citrix Secure Browser publié en septembre 2021. Le problème existe car la stratégie de **suivi du nom d'hôte** n'est pas visible dans Citrix Secure Browser après la publication de septembre 2021 et ne peut donc pas être activée pour s'intégrer à Citrix Analytics for Security. Ce problème est désormais résolu. [CAS-62254]

02 décembre 2021

Nouveautés

Indicateur de risque détecté des fichiers malveillants Vous pouvez désormais recevoir une alerte lorsqu'un utilisateur charge un fichier infecté dans Content Collaboration.

L'indicateur de risque détecte un fichier infecté par un logiciel malveillant tel qu'un cheval de Troie, un virus ou toute autre menace malveillante. Il fournit une visibilité sur les détails du fichier malveillant tels que le propriétaire du fichier, le nom du virus et l'emplacement du fichier.

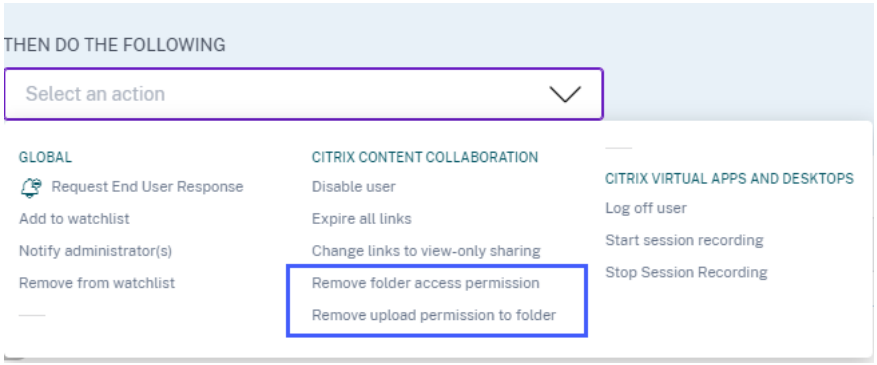
Le facteur de risque associé à l'indicateur de risque **détecté par les fichiers malveillants** est l'indicateur de risque basé sur les fichiers.

Pour plus d'informations sur l'indicateur de risque et les actions que vous pouvez appliquer, consultez l'indicateur de risque Fichiers malveillants détectés.

Nouvelles actions pour la source de données Content Collaboration Vous pouvez appliquer les actions suivantes lorsque l'indicateur de risque de **fichiers malveillants détectés** est déclenché pour un utilisateur :

- **Supprimer l'autorisation d'accès au dossier**. Vous pouvez bloquer l'autorisation d'accès de l'utilisateur qui télécharge le fichier infecté. L'utilisateur ne peut pas accéder au dossier dans lequel le fichier infecté a été téléchargé.
- **Supprimez l'autorisation de chargement sur le dossier**. Vous pouvez bloquer l'autorisation de chargement de l'utilisateur qui télécharge le fichier infecté. L'utilisateur ne peut pas télécharger de fichier dans le dossier dans lequel le fichier infecté a été chargé.

Pour plus d'informations sur les actions de Content Collaboration, voir Stratégies et actions.

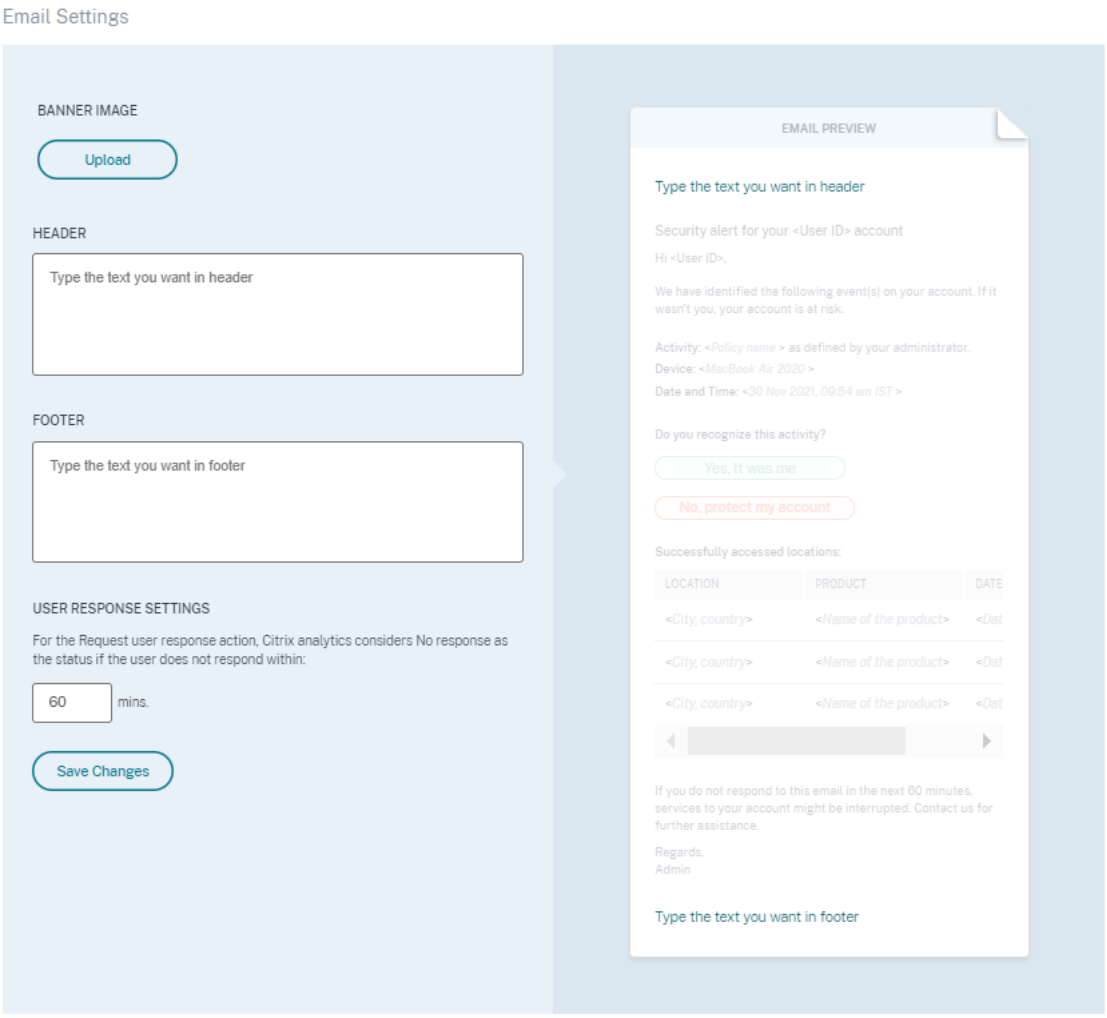


29 novembre 2021

Nouveautés

Amélioration des paramètres de messagerie pour les notifications utilisateur En tant qu'administrateur, vous pouvez désormais ajouter une image de bannière, un en-tête et un texte de pied de page dans le modèle d'e-mail de réponse de l'utilisateur. Ces champs renforcent la légitimité de votre e-mail, augmentant ainsi l'attention des utilisateurs et les réponses à votre e-mail.

Pour plus d'informations, consultez la section Paramètres de messagerie de l'utilisateur final.

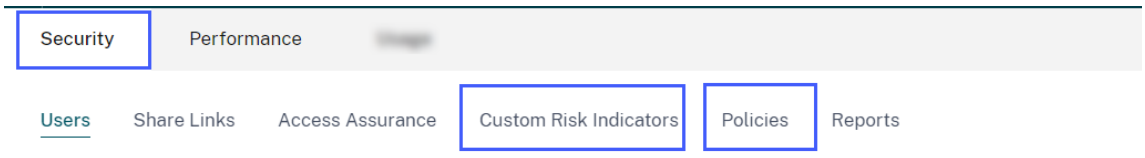


26 novembre 2021

Nouveautés

Modifications du menu des indicateurs de risque personnalisés et des stratégies Les liens de navigation des fonctionnalités suivantes sont mis à jour :

- Indicateurs de risque personnalisés : utilisez cette fonctionnalité en cliquant sur **Sécurité > Indicateurs de risque personnalisés**.
- Stratégies : utilisez cette fonctionnalité en cliquant sur **Sécurité > Stratégies**.



25 novembre 2021

Nouveautés

Amélioration de l'intégration de Security Information and Event Management (SIEM)

> **Remarque**
>
> Cette intégration est en préversion.

Vous pouvez désormais intégrer Citrix Analytics for Security aux services SIEM suivants :

- Sentinel
- Elasticsearch avec des services de visualisation tels que Kibana et un service SIEM tel que LogRythm
- Tout autre service SIEM utilisant le moteur de collecte de données Logstash

Selon les besoins de votre entreprise, importez les données des utilisateurs de Citrix Analytics for Security vers votre service SIEM. Cette intégration permet à vos équipes des opérations de sécurité de corréler, d'analyser et de rechercher des données provenant de journaux disparates au sein des services SIEM de votre organisation, les aidant ainsi à identifier et à corriger rapidement les risques de sécurité.

Pour plus d'informations, voir Intégration de la gestion des informations et des événements de sécurité (SIEM).

09 novembre 2021

Problème résolu

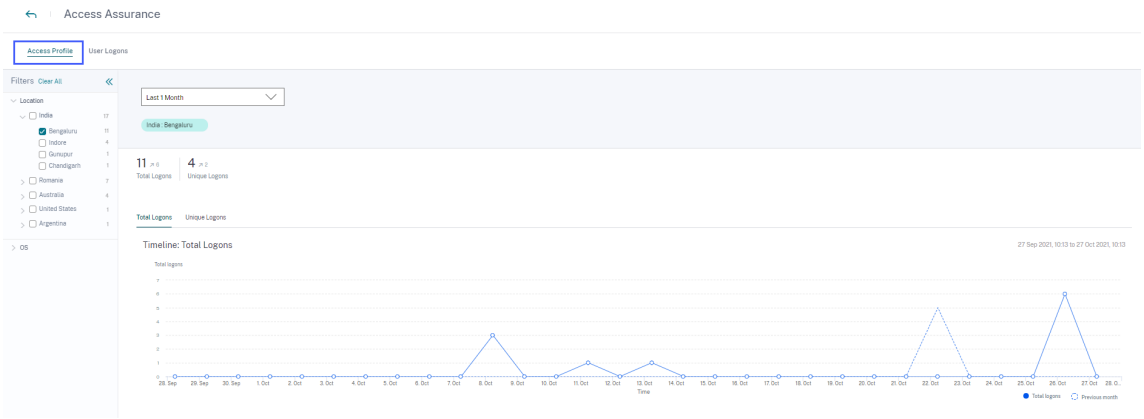
- Sur quelques locataires, les stratégies utilisateur ne fonctionnent pas. Ce problème s'est produit lorsque les alertes pour les applications virtuelles ont des valeurs de chaîne vides pour les domaines. Ce problème est désormais résolu. [CAS-60920]

02 novembre 2021

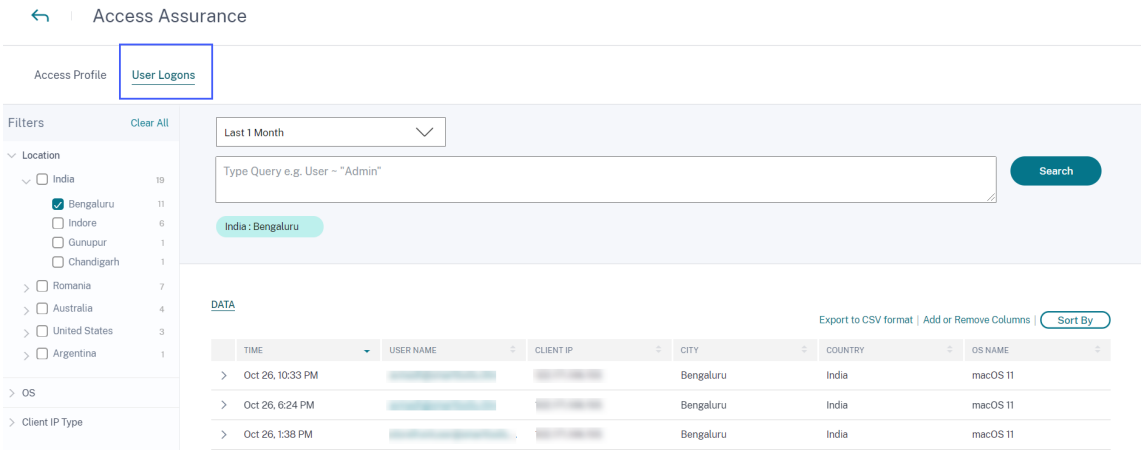
Nouveautés

Afficher les profils d'accès et les détails d'ouverture de session des utilisateurs Citrix Virtual Apps and Desktops et Citrix DaaS Sur le tableau de bord **Access Assurance Location**, vous pouvez afficher les profils d'accès et les détails d'ouverture de session des utilisateurs qui se sont connectés à des applications virtuelles et à des bureaux virtuels. Ces informations vous aident lors de l'investigation et de l'analyse des menaces.

- La page **Profil d'accès** fournit le résumé des accès utilisateur depuis les emplacements sélectionnés. Vous pouvez afficher l'analyse des tendances et les principaux événements d'accès du nombre total d'utilisateurs ainsi que les ouvertures de session uniques des utilisateurs.



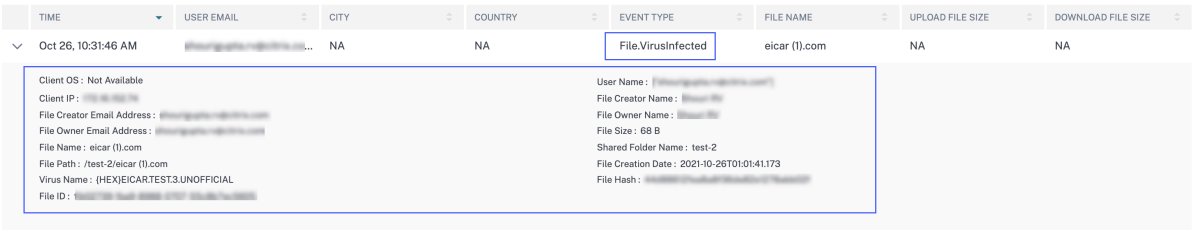
- La page Ouverture de **session utilisateur fournit les détails des ouvertures** de session utilisateur aux applications virtuelles et aux bureaux virtuels à partir des emplacements sélectionnés.



Pour plus d'informations, consultez le tableau de bord Emplacement Access Assurance.

Afficher les journaux des programmes malveillants sur la page de recherche en libre-service pour Content Collaboration Sur la page en libre-service de Content Collaboration, vous pouvez désormais afficher l'événement malveillant `File.VirusInfected` et ses journaux associés. Cet événement est déclenché lorsqu'un utilisateur de Content Collaboration télécharge un fichier infecté par un logiciel malveillant.

Pour plus d'informations, voir Recherche en libre-service pour Content Collaboration



Problème résolu

- Quelques utilisateurs de Content Collaboration sont incorrectement définis en tant que non-employés lors du traitement des événements dans Citrix Analytics. Par conséquent, les utilisateurs ne sont pas identifiés comme étant des utilisateurs découverts. Ce problème est désormais résolu. [CAS-59608]

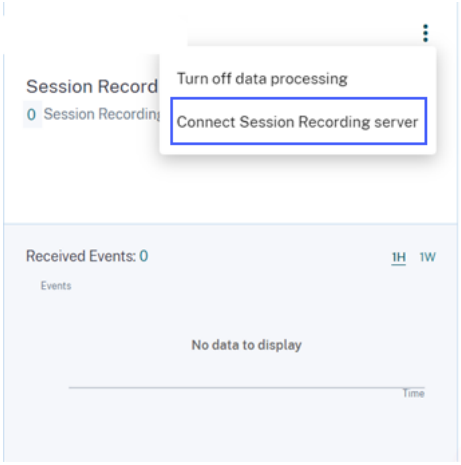
20 octobre 2021

Nouveautés

Intégration du serveur d'enregistrement de session Pour votre déploiement Citrix Virtual Apps and Desktops et Citrix DaaS, vous pouvez désormais configurer vos serveurs d'enregistrement de session pour envoyer les événements utilisateur à Citrix Analytics for Security. Ces événements utilisateur sont traités pour fournir des informations exploitables sur le comportement des utilisateurs.

Sur la page **Sources de données > Sécurité**, accédez à la carte de site **Virtual Apps and Desktops** . Sur la fiche de site **d'enregistrement de session**, cliquez sur des points de suspension verticaux (), puis sélectionnez **Connecter le serveur d'enregistrement de session**.

Pour plus d'informations, consultez la section Déploiement Connexion à l'enregistrement de session.



19 octobre 2021

Nouveautés

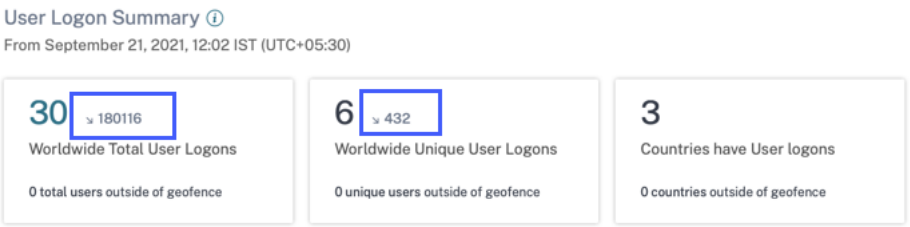
Améliorations apportées au modèle d'e-mail La notification par e-mail qu'un administrateur reçoit après avoir appliqué l'action **Notifier l'administrateur (s)** est améliorée afin de fournir de meilleures informations sur les événements à risque pour l'utilisateur.

- La notification fournit désormais des informations détaillées sur l'indicateur de risque déclenché ou la stratégie appliquée. Par exemple, vous pouvez afficher la gravité et l'heure de déclenchement des indicateurs de risque par défaut et personnalisés. La structure du contenu est améliorée pour une meilleure lisibilité.
- Les administrateurs peuvent désormais accéder à la chronologie des utilisateurs directement à partir de la notification par e-mail et afficher les détails des événements à risque.
- Une option de commentaire est ajoutée dans la notification. Cette option permet de collecter les réponses des administrateurs et d'améliorer continuellement le contenu de la notification en fonction des réponses.

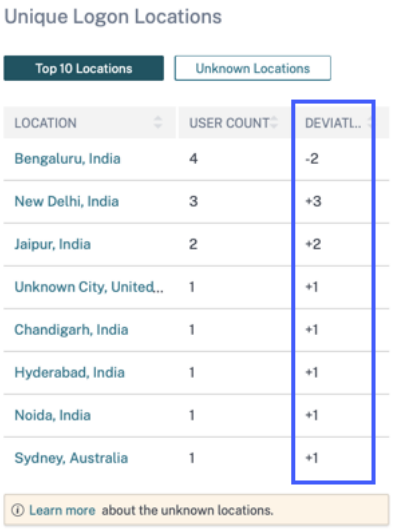
Pour plus d'informations sur l'action **Notifier les administrateurs**, consultez la section Stratégies et actions.

Améliorations du résumé de connexion utilisateur

- Vous pouvez désormais afficher la tendance à la hausse ou à la baisse des ouvertures de session utilisateur pour le nombre total d'ouvertures de session utilisateur dans le monde et les ouvertures de session utilisateur uniques dans le monde entier.



- La colonne **ÉCART** du tableau **Emplacements d'ouverture de session uniques** indique la modification à la hausse ou à la baisse des ouvertures de session utilisateur uniques pour un emplacement particulier.



Ces statistiques vous aident à comprendre comment les ouvertures de session des utilisateurs ont changé (positives ou négatives) par rapport à la période précédente. Il fournit une visibilité sur les interactions des utilisateurs avec vos déploiements Citrix Virtual Apps and Desktops et Citrix DaaS.

Pour plus d'informations, consultez Tableau de bord de localisation Access Assurance.

Problème résolu

- Sur le tableau de bord **Emplacement Access Assurance**, les fiches **Récapitulatif des ouvertures de session utilisateur** n'affichent pas les mesures d'ouverture de session utilisateur (nombre total d'ouvertures de session utilisateur dans le monde, ouvertures de session utilisateur uniques dans le monde et pays ayant des ouvertures de session utilisateur) lorsqu'aucun utilisateur ne se connecte depuis l'extérieur des zones de géofence. Ce problème est désormais résolu. [CAS-59595]

01 octobre 2021

Nouveautés

Afficher les journaux d'audit sur la recherche en libre-service pour Content Collaboration
Dans la recherche en libre-service de Content Collaboration, vous pouvez désormais afficher les journaux d'audit. Ces journaux fournissent des informations sur les autorisations et les actions appliquées aux comptes d'utilisateurs par les administrateurs de Content Collaboration. À l'aide de ces données, vous pouvez vérifier si les administrateurs de Content Collaboration ont pris des mesures valides sur leurs comptes d'utilisateurs. En tant qu'administrateur de la sécurité, il vous aide lors de l'investigation et de l'analyse des risques.

Pour plus d'informations sur les journaux d'audit, voir Recherche en libre-service pour Content Collaboration.

Problème résolu

Les administrateurs qui se connectent à Citrix Cloud à l'aide d'Azure AD ne peuvent pas accéder au service Citrix Analytics lorsque l'ID de session expiré précédent est accompagné du nouvel ID de session. Ce problème est désormais résolu. [CAS-59385]

29 septembre 2021

Nouveautés

Le tableau de bord de localisation Access Assurance est désormais disponible Le tableau de bord fournit une visibilité sur l'emplacement de vos utilisateurs Citrix Virtual Apps and Desktops et Citrix DaaS. Vous pouvez identifier les utilisateurs dont les emplacements sont inhabituels en activant le géofencing et en appliquant les actions appropriées pour prévenir toute menace.

Pour afficher le tableau de bord, cliquez sur **Sécurité > Access Assurance**. Sélectionnez la période pendant laquelle vous souhaitez afficher les détails du lieu.

Pour plus d'informations, consultez Tableau de bord de localisation Access Assurance.

15 septembre 2021

Nouveautés

Améliorations des indicateurs de risque personnalisés

- Lorsqu'un indicateur de risque personnalisé est déclenché, il s'affiche immédiatement sur la chronologie de l'utilisateur . Toutefois, le résumé des risques et le score de risque de l'utilisateur sont mis à jour après quelques minutes (environ 15 à 20 minutes).
- Si vous modifiez les attributs tels que la condition, la catégorie de risque, la gravité et le nom d'un indicateur de risque personnalisé existant, sur la chronologie de l'utilisateur, vous pouvez toujours afficher les occurrences précédentes de l'indicateur de risque personnalisé (avec les anciens attributs) qui ont été déclenchées pour l'utilisateur.
- Si vous supprimez un indicateur de risque personnalisé, sur la chronologie de l'utilisateur, vous pouvez toujours afficher les occurrences précédentes de l'indicateur de risque personnalisé qui ont été déclenchées pour l'utilisateur.

Pour plus d'informations, consultez la section Indicateurs de risque personnalisés.

14 septembre 2021

Nouveautés

Présentation de l'indicateur de risque d'ouverture de session suspecte Citrix Analytics for Security détecte désormais les ouvertures de session utilisateur de nature suspecte en fonction de plusieurs facteurs contextuels tels que :

- La localisation est jugée inhabituelle par rapport à l'utilisateur et à l'historique de l'organisation.
- L'appareil est considéré comme inhabituel par rapport à l'historique de l'utilisateur et de l'organisation
- Le réseau est considéré comme inhabituel en ce qui concerne l'historique de l'utilisateur et de l'organisation
- L'adresse IP est jugée suspecte en fonction des flux de renseignements sur les menaces IP

Lorsqu'un utilisateur de Citrix Virtual Apps and Desktops et Citrix DaaS se connecte à partir d'un contexte suspect en fonction de la combinaison de ces facteurs, l'indicateur de risque est déclenché.

Cet indicateur de risque remplace l'indicateur de risque **Accès à partir d'un emplacement inhabituel** associé à la source de données Citrix Virtual Apps and Desktops. Toutes les stratégies existantes basées sur l'indicateur de risque **Accès à partir d'un emplacement inhabituel** sont automatiquement liées au nouvel indicateur de risque : Ouverture de **session suspecte**.

Pour plus d'informations sur l'indicateur de risque, consultez les sections Indicateurs de risque Citrix Virtual Apps and Desktops et Citrix DaaS.

Amélioration des messages SIEM Citrix Analytics for Security envoie désormais les détails du schéma de l'indicateur de risque d'**ouverture de session suspecte** à votre service SIEM. Vous pouvez afficher le schéma du récapitulatif de l'indicateur et les détails de l'événement de l'indicateur de risque d'**ouverture de session suspecte** . Pour plus d'informations, consultez la section Format de données Citrix Analytics pour SIEM.

Problème résolu

- Pour la recherche en libre-service Apps and Desktops, la valeur IP du client est manquante dans le fichier CSV téléchargé. Ce problème est désormais résolu. [CAS-58426]

19 août 2021

Nouveautés

Présentation de l'application Citrix Analytics pour Splunk

> **Remarque**
>
> L'application est en prévisualisation.

L'application Citrix Analytics pour Splunk vous permet d'afficher les données collectées à partir de Citrix Analytics for Security sous la forme de tableaux de bord pertinents sur votre Splunk. Les tableaux de bord fournissent des informations sur les événements à risque de vos utilisateurs. Vous pouvez également mettre en corrélation les données Citrix Analytics avec les journaux collectés à partir de diverses autres sources de données. La corrélation vous aide à trouver des relations entre les événements et à prendre des mesures opportunes pour protéger votre environnement informatique.

Pour télécharger l'application, accédez à Splenkbase. Installez l'application sur votre tête de recherche Splunk.

Pour plus d'informations, consultez l'application Citrix Analytics pour Splunk.

Schéma d'indicateur de risque personnalisé pour SIEM Dans votre service SIEM, vous pouvez désormais consulter le schéma des indicateurs de risque personnalisés créés pour Citrix Virtual Apps and Desktops et Citrix DaaS. Ces données vous aident à mieux comprendre la posture de risque de sécurité de votre organisation.

Pour plus d'informations sur le schéma d'indicateur de risque personnalisé, consultez la section Format de données Citrix Analytics pour SIEM.

Prise en charge de Citrix Director en tant que source de données Vous pouvez désormais configurer vos sites locaux sur Citrix Director pour envoyer des événements à Security Analytics. Ces événements sont utilisés pour découvrir les utilisateurs connectés à Security Analytics et déterminer les versions de l'application Workspace installées sur les appareils des utilisateurs.

Par défaut, le traitement des données est activé après la découverte des sites. Sur la carte de **surveillance**, vous pouvez afficher tous les sites connectés.

Pour plus d'informations sur la façon de configurer vos sites sur Director, consultez Citrix Virtual Apps and Desktops et Source de données Citrix DaaS.

Prise en charge de la géolocalisation dans le tableau de bord de localisation Access Assurance Vous pouvez désormais utiliser les **paramètres de géolocalisation** dans le tableau de bord pour sélectionner et activer les zones geofence. Après avoir activé le geofence, la carte affiche les zones

geofence (pays) et les connexions de l'utilisateur depuis l'extérieur et l'intérieur de la clôture géographique. Cette fonctionnalité utilise la **session CVAD démarrée en dehors de l'indicateur de risque de géofence** pour surveiller les ouvertures de session des utilisateurs.

Pour plus d'informations, consultez Tableau de bord de localisation Access Assurance.

État de l'application Workspace sur la page Utilisateurs Sur la page **Utilisateurs**, vous pouvez désormais afficher l'état des clients de l'application Citrix Workspace pris en charge par Citrix Analytics. La page affiche l'état suivant :

- Pris en charge
- Prise en charge partielle
- Non pris en charge
- Non disponible
- Inactif

L'état vous aide à identifier toutes les versions de client non prises en charge utilisées par les utilisateurs et à recommander aux utilisateurs de mettre à niveau leurs clients vers une version prise en charge. Une version client prise en charge envoie les événements utilisateur à Citrix Analytics.

> **Remarque**
>
> Pour afficher l'état de l'application Citrix Workspace, vous devez embarquer votre source de données Citrix Director. Dans le cas contraire, l'état de chaque utilisateur de Citrix Virtual Apps and Desktops et Citrix DaaS est indiqué comme **Inactif**.

Pour plus d'informations, consultez le tableau de bord Utilisateurs.

Prise en charge de l'opérateur IS EMPTY Lors de la création d'un indicateur de risque personnalisé, vous pouvez désormais utiliser l'opérateur **IS EMPTY** dans votre condition pour vérifier la 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 section Indicateurs de risque personnalisés.

Cotation de risque améliorée Dans la chronologie de l'utilisateur, vous pouvez désormais afficher le résumé des risques d'un utilisateur. Le résumé des risques fournit des informations sur les facteurs de risque associés aux événements utilisateur. Le facteur de risque vous aide à identifier le type d'anomalies dans les événements utilisateur et à déterminer le score de risque. Les facteurs de risque sont les suivants :

- Indicateurs de risque basés sur les appareils
- Indicateurs de risque basés sur la localisation
- Indicateurs de risque basés sur IP
- Indicateurs de risque basés sur les échecs de connexion
- Indicateurs de risque basés sur des données
- Indicateurs de risque basés sur les fichiers
- Indicateurs de risque personnalisés
- Autres indicateurs de risque

Sur la chronologie de l'utilisateur, vous pouvez désormais appliquer le filtre pour afficher les événements utilisateur en fonction des facteurs de risque.

Pour plus d'informations, consultez les rubriques suivantes :

- Indicateurs de risque utilisateur Citrix
- Chronologie et profil des risques utilisateur

29 juillet 2021

Fonctionnalité obsolète

Actions obsolètes associées à Citrix Endpoint Management Les actions suivantes sont supprimées de la source de données Citrix Endpoint Management. Vous ne pouvez plus appliquer ces actions sur les indicateurs de risque ni créer de stratégies à l'aide de ces actions.

- Verrouiller un appareil
- Notifier l'administrateur Endpoint Management
- Notifier un utilisateur
- Révoquer un appareil
- Wipe device

Dans vos stratégies existantes, si ces actions sont déjà utilisées, elles sont automatiquement remplacées par l'action **Ajouter à la liste de suivi** . Et vous pouvez surveiller ces utilisateurs à partir de la liste de suivi.

14 juillet 2021

Nouveautés

Prise en charge de l'opérateur IS NOT EMPTY Lors de la création d'un indicateur de risque personnalisé, vous pouvez désormais utiliser l'opérateur **IS NOT EMPTY** dans votre état 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.

Par exemple, la condition suivante détecte les événements d'ouverture de session utilisateur de tout pays où la valeur du pays n'est pas nulle. En d'autres termes, le nom du pays est spécifié.

```
Event-Type = "Session.logon" AND Country IS NOT EMPTY
```

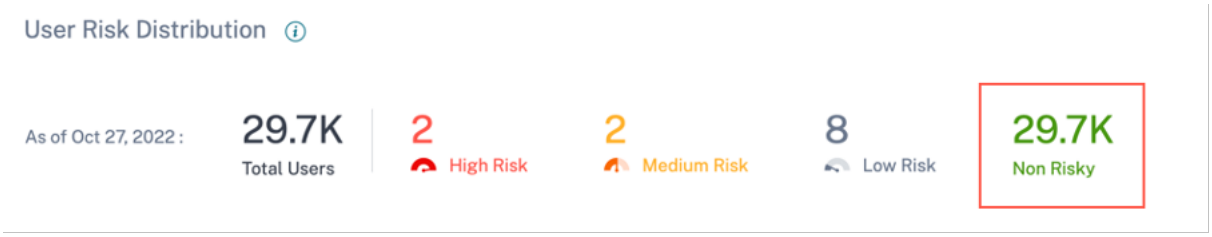
Pour plus d'informations, consultez la section Indicateurs de risque personnalisés.

06 juillet 2021

Nouveautés

Afficher les utilisateurs non risqués sur le tableau de bord Utilisateurs Dans le tableau de bord **Utilisateurs**, vous pouvez désormais afficher le nombre d'utilisateurs non risqués pour la période sélectionnée. Ces utilisateurs découverts sont identifiés comme étant non risqués sur la base du score de risque zéro pour la période sélectionnée. Cliquez sur la fiche **Utilisateurs non risqués** pour afficher tous les utilisateurs dont le score de risque est nul.

Pour plus d'informations, consultez Tableau de bord des utilisateurs.



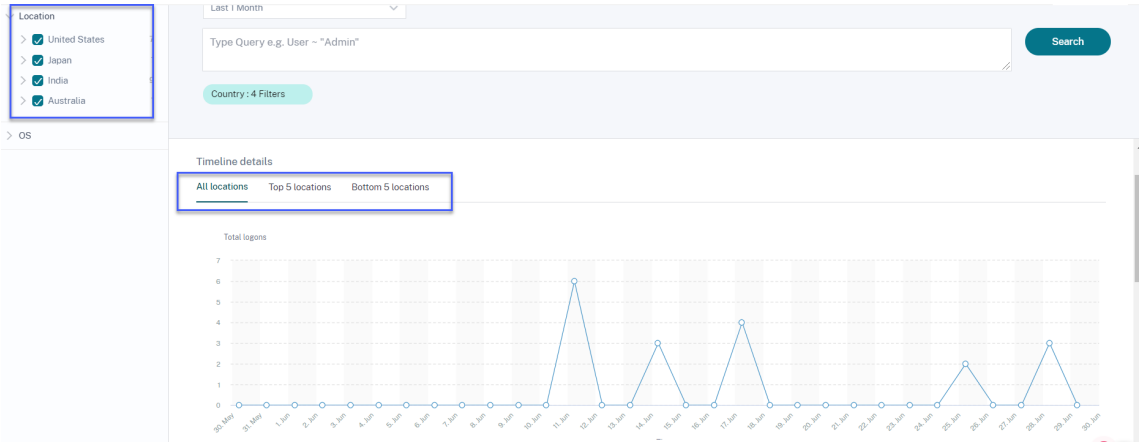
01 juillet 2021

Nouveautés

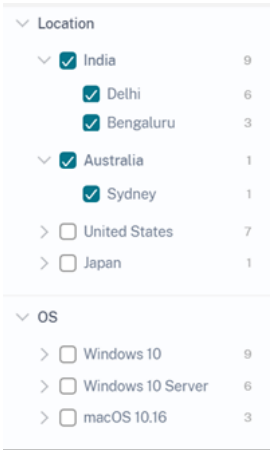
Améliorations du tableau de bord de localisation Access Assurance

- Dans le tableau **Top 10 des emplacements d'ouverture de session uniques**, vous pouvez afficher le nombre d'ouvertures de session uniques d'utilisateurs à partir d'emplacements inconnus. Cette liste est un sous-ensemble des 10 principaux emplacements d'ouverture de session uniques. Vous pouvez également trouver les raisons pour lesquelles les emplacements sont inconnus et les moyens possibles d'obtenir les emplacements des utilisateurs.

- Sur la page **Emplacement d'accès**, si vous sélectionnez plusieurs emplacements, vous pouvez afficher et comparer les détails de la chronologie des ouvertures de session des utilisateurs de tous les emplacements, des cinq premiers emplacements et des cinq derniers emplacements.

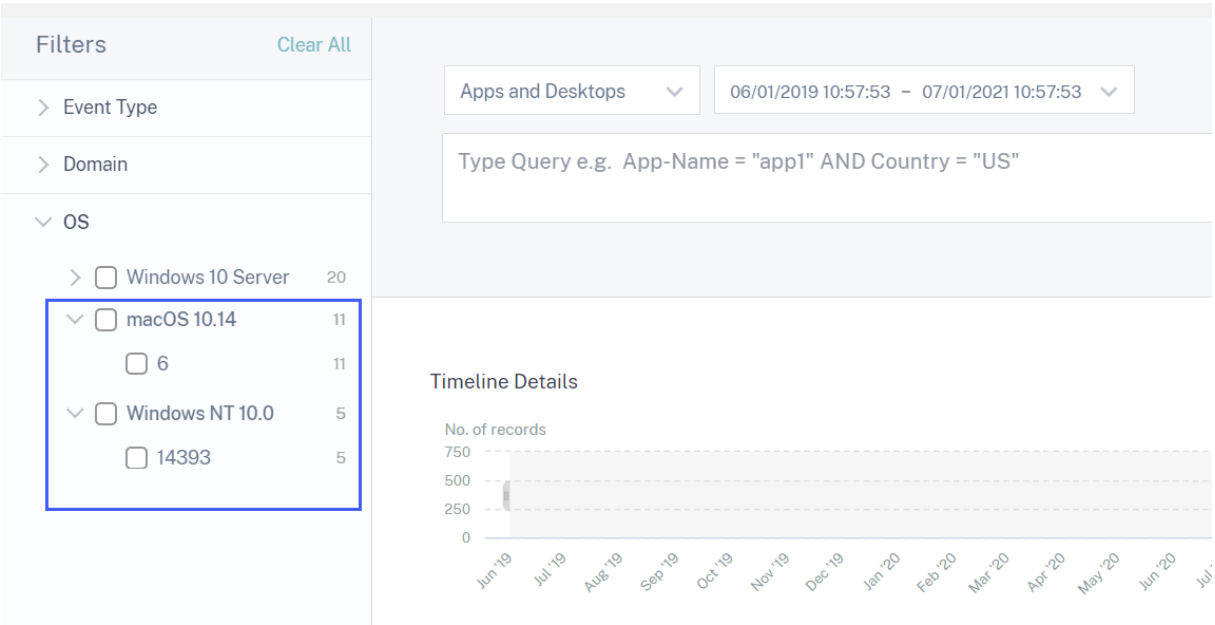


- Sur la page **Emplacement d'accès**, vous pouvez utiliser les facettes imbriquées telles que le pays et ses villes, les systèmes d'exploitation, les versions principales et secondaires. Ces facettes vous permettent de filtrer les événements de manière granulaire.



Pour plus d'informations, consultez la section Emplacement de la garantie d'accès.

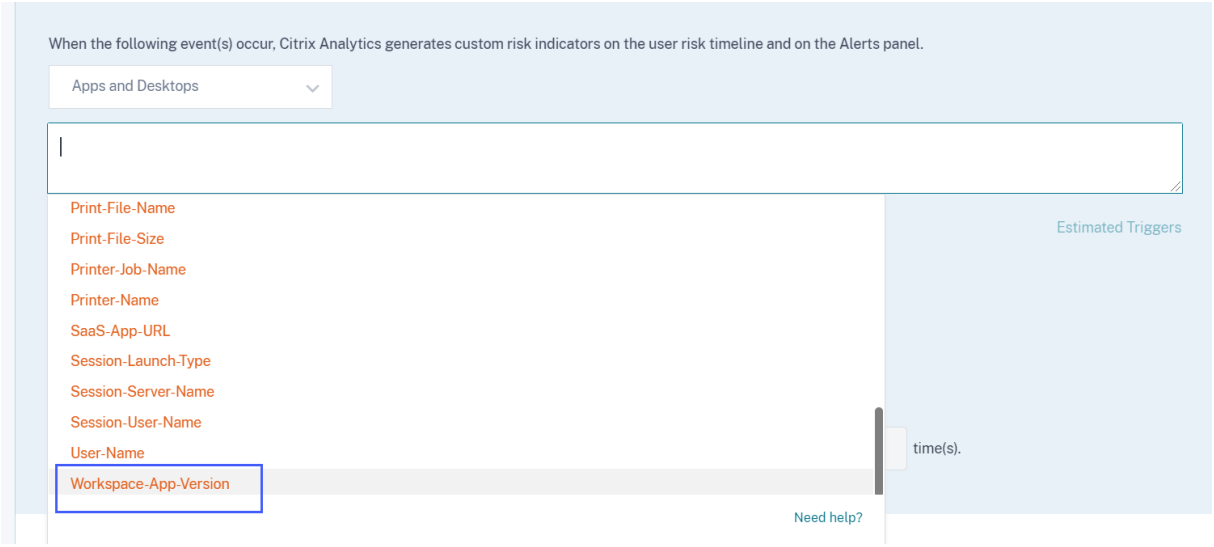
Mise à jour de la facette du système d'exploitation dans la recherche en libre-service pour Virtual Apps and Desktops Vous pouvez désormais filtrer les événements Apps and Desktops à l'aide de la facette du système d'exploitation imbriqué. Sélectionnez la version principale et la version secondaire associées à un système d'exploitation et filtrez les événements de manière granulaire. Pour plus d'informations, consultez la section Recherche en libre-service d'applications et de bureaux.



30 juin 2021

Nouveautés

Ajout de la version de l'application Workspace dans l'état d'indicateur de risque personnalisé pour les applications Pour la source de données **Apps and Desktops**, vous pouvez désormais utiliser la dimension **Workspace-App-Version** pour définir votre condition tout en créant un indicateur de risque personnalisé. Pour plus d'informations sur la dimension, consultez la section Recherche en libre-service d'applications et de bureaux.



23 juin 2021

Nouveautés

Améliorations apportées aux messages SIEM Les champs suivants sont désormais ajoutés au schéma des indicateurs de risque :

- `indicator_vector_name`- Indique le vecteur de risque associé à un indicateur de risque. Les vecteurs de risque sont les indicateurs de risque basés sur l'appareil, les indicateurs de risque basés sur l'emplacement, les indicateurs de risque basés sur les échecs de connexion, les indicateurs de risque basés sur IP, les indicateurs de risque basés sur les données, les indicateurs de risque basés sur les fichiers et d'autres indicateurs de risque.
- `indicator_vector_id`- L'identifiant associé à un vecteur de risque. ID 1 = indicateurs de risque basés sur l'appareil, ID 2 = indicateurs de risque basés sur la localisation, ID 3 = indicateurs de risque basés sur l'échec de la connexion, ID 4 = indicateurs de risque basés sur IP, ID 5 = indicateurs de risque basés sur IP, ID 6 = indicateurs de risque basés sur les données, ID 7 = Autres indicateurs de risque et ID 999 = Non disponible.

Pour plus d'informations, consultez la section Format de données Citrix Analytics pour SIEM.

07 juin 2021

Nouveautés

Améliorations apportées à l'action Notifier les administrateurs Lorsque vous appliquez l'action **Notifier les administrateurs** à un indicateur de risque ou que vous créez une stratégie avec cette action, vous pouvez désormais sélectionner les administrateurs qui reçoivent une notification concernant le comportement à risque de l'utilisateur. Pour plus d'informations sur cette action, consultez la section Stratégies et actions.

Ajout de la prise en charge de l'action de partage en lecture seule Si un utilisateur partage des fichiers de manière excessive, Citrix Analytics déclenche l'indicateur de risque de **partage de fichiers excessif** . À partir de la chronologie des risques de l'utilisateur, vous pouvez désormais appliquer l'action **Modifier les liens vers le partage en lecture seule** à l'indicateur de risque de **partage de fichiers excessif** . Vous pouvez également appliquer l'action sur un lien de partage particulier sur la chronologie des risques liés au lien de partage. Cette action empêche les autres utilisateurs de télécharger, de copier ou d'imprimer les fichiers associés aux liens de partage. Pour plus d'informations sur cette action, consultez la section Stratégies et actions.

18 mai 2021

Nouveautés

Migration des indicateurs de risque par défaut vers des indicateurs de risque personnalisés Les indicateurs de risque par défaut suivants sont migrés vers des indicateurs de risque personnalisés préconfigurés.

Indicateur de risque de défaut	Source de données	Indicateur de risque personnalisé préconfiguré
Premier accès à partir d'un nouvel appareil	Citrix Virtual Apps and Desktops et Citrix DaaS	Accès au CVAD pour la première fois depuis un nouvel appareil
Premier accès à partir d'une nouvelle adresse IP	Citrix Gateway	Accès Gateway pour la première fois à partir d'une nouvelle adresse IP

Avec cette migration vers les indicateurs de risque personnalisés, les indicateurs de risque par défaut et les algorithmes de machine learning associés sont déconseillés.

Les indicateurs de risque personnalisés correspondants sont déclenchés en fonction des conditions préconfigurées suivantes :

- Lorsqu'un utilisateur accède pour la première fois à partir d'un nouvel appareil ou d'un appareil existant qui n'a pas été utilisé depuis au moins 90 jours.
- Lorsqu'un utilisateur se connecte pour la première fois à partir d'une nouvelle adresse IP ou d'une adresse IP existante qui n'a pas été utilisée depuis au moins 90 jours.

En plus des conditions préconfigurées, vous pouvez désormais ajouter vos propres conditions pour ces indicateurs de risque personnalisés afin d'identifier les menaces dans votre environnement Citrix. Cette option vous permet de configurer l'indicateur de risque personnalisé en fonction de vos besoins en matière de sécurité. Vous pouvez également créer des stratégies pour appliquer des actions sur les événements risqués détectés par ces indicateurs de risque personnalisés.

Toutefois, sur la ligne de temps de l'utilisateur, vous pouvez toujours afficher les indicateurs de risque par défaut précédemment déclenchés et leurs événements.

Les stratégies associées à ces indicateurs de risque par défaut sont automatiquement liées aux indicateurs de risque personnalisés préconfigurés correspondants.

Pour plus d'informations, consultez la section Indicateurs et stratégies de risque personnalisés préconfigurés.

Améliorations apportées à la recherche en libre-service pour Gateway

- Le filtre **Type d'événement** est maintenant renommé en **Type d'enregistrement**. Sélectionnez l'un des types d'enregistrement suivants pour filtrer vos événements : VPN_AI, VPN_IF et VPN_ST.
- Dans la table **DATA**, développez une ligne pour un événement utilisateur pour afficher le type d'événement correspondant. Les types d'événements peuvent être les suivants : Authentification, Fichier ICA ou Déconnexion de session.

Le tableau suivant décrit la corrélation entre les types d'enregistrement et les types d'événements.

Type d'enregistrement	Type d'événement
VPN_AI	Authentification
VPN_IF	Fichier ICA
VPN_ST	Déconnexion de session

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

Problème résolu

- L'indicateur de risque personnalisé est déclenché en fonction de la sensibilité à la casse des valeurs conditionnelles. Par exemple, dans les événements utilisateur contenant des ID d'appareil dans la liste autorisée, vous constatez le comportement suivant :
  - Si vous saisissez la valeur de la `Device-ID` dimension en minuscules, l'indicateur personnalisé est déclenché.

    ```
    Event-Type = Session.Logon AND Device-ID NOTIN ("1621d2cb-f598-5ef7-a5bf-81747496ed2e")
    ```

  - Si vous saisissez la valeur de la `Device-ID` dimension en majuscules pour le même appareil, l'indicateur personnalisé ne se déclenche pas.

    ```
    Event-Type = Session.Logon AND Device-ID NOTIN ("1621D2CB-F598-5EF7-A5BF-81747496ED2E")
    ```

  Ce problème est désormais résolu et l'indicateur de risque personnalisé est déclenché indépendamment de la sensibilité à la casse des valeurs conditionnelles.

  [CAS-50153]

29 avril 2021

Nouveautés

Détails des événements pour un indicateur de risque personnalisé Sur la page de chronologie des risques de l'utilisateur, vous pouvez désormais afficher les événements qui ont déclenché un indicateur de risque personnalisé. Auparavant, vous ne pouvez afficher que les conditions définies, la description et la fréquence de déclenchement d'un indicateur de risque personnalisé. Cliquez sur **Recherche d'événements** pour afficher les détails des événements associés à l'utilisateur et l'indicateur de risque.
Pour plus d'informations, consultez la section Indicateurs de risque personnalisés.

Problème résolu

- Un administrateur n'est pas en mesure de créer des indicateurs de risque personnalisés même après que son autorisation d'accès est passée de l'administrateur en lecture seule à l'administrateur complet. [CAS-49628]

16 avril 2021

Nouveautés

Améliorations apportées aux messages SIEM Vous pouvez consulter les améliorations suivantes concernant le format du schéma de l'indicateur de risque :

- L'adresse IP du client est désormais disponible dans le schéma pour tous les indicateurs de risque de lot. Auparavant, l'adresse IP du client n'était disponible que pour quelques indicateurs de risque de lot :
  - Échec de l'analyse EPA
  - Échec excessif de l'authentification
  - Ouverture de session à partir d'une adresse IP suspecte
  - Accès depuis un endroit inhabituel
  - Échec d'authentification inhabituel
  - Téléchargement anonyme de partage sensible
  - Exfiltration potentielle des données
- Si une valeur de champ de type de données entier n'est pas disponible, la valeur attribuée est **-999**. Par exemple, `"latitide"= -999`.
- Si une valeur de champ de type de données de chaîne n'est pas disponible, la valeur attribuée est **NA**. Par exemple, `"city"= "NA"`.

Pour plus d'informations, consultez la section Format de données Citrix Analytics pour SIEM.

26 mars 2021

Nouveautés

Restriction sur les messages SIEM Citrix Analytics envoie un maximum de 1 000 détails d'événements pour chaque occurrence d'indicateur de risque à votre service SIEM. Ces événements sont envoyés dans un ordre chronologique d'occurrence. Pour plus d'informations, consultez la section Format de données Citrix Analytics pour SIEM.

Ajout des champs ID de source de données et ID de catégorie d'indicateur dans les messages SIEM Les champs suivants sont ajoutés dans le schéma récapitulatif de l'indicateur et dans le schéma des détails de l'événement de l'indicateur.

Champ	Description
`data_source_id`	ID associé à une source de données. ID 0 = Citrix Content Collaboration, ID 1 = Citrix Gateway, ID 2 = Citrix Endpoint Management, ID 3 = Citrix Virtual Apps and Desktops, ID 4 = Citrix Access Control
`indicator_category_id`	ID associé à une catégorie d'indicateurs de risque. ID 1 = Exfiltration de données, ID 2 = menaces internes, ID 3 = utilisateurs compromis

Pour plus d'informations, consultez la section Format de données Citrix Analytics pour SIEM.

18 mars 2021

Nouveautés

Tableau de bord de localisation Access Assurance

> **Remarque**
>
> La fonctionnalité est en prévisualisation.

Le tableau de bord **Access Assurance Location** fournit une vue d'ensemble des emplacements à partir desquels les utilisateurs de Citrix Virtual Apps and Desktops et Citrix DaaS se sont connectés pendant une période donnée. Citrix Analytics reçoit ces événements d'ouverture de session utilisateur de l'application Citrix Workspace installée sur les appareils des utilisateurs.

Pour afficher le tableau de bord, cliquez sur **Sécurité > Access Assurance**.

Vous pouvez consulter les informations suivantes pour une période sélectionnée :

- Nombre total d'ouvertures de session utilisateur à partir d'un emplacement particulier et entre les différents emplacements.
- Nombre total d'ouvertures de session utilisateur uniques dans les emplacements.
- Nombre total de pays depuis lesquels les utilisateurs se sont connectés.
- Top 10 des emplacements avec des ouvertures de session utilisateur uniques.

Pour plus d'informations, consultez la section Emplacement de la garantie d'accès.

Prise en charge du programme NOT LIKE (! ~) opérateur Pour la requête de recherche en libre-service et la condition de l'indicateur de risque personnalisé, 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.

Version traduite du système d'exploitation Pour la source de données Citrix Virtual Apps and Desktops et Citrix DaaS, la dimension **Plateforme** est désormais traduite en dimensions **OS-Major-Version**, **OS-Minor-Version**et **OS-Extra-Details** . En fonction des détails du système d'exploitation d'un utilisateur, Citrix Analytics affiche ces dimensions sur la page de recherche en libre-service.

Vous pouvez utiliser ces dimensions pour définir les conditions d'un indicateur de risque personnalisé.

Pour les indicateurs de risque personnalisés précédemment créés, si vous avez utilisé la dimension **Platform** comme condition, Citrix Analytics remplace automatiquement la dimension **Platform** par la version **majeure** du système d'ordinateur, la version **mineure** du système d'analyse et les **détails supplémentaires d'OS**. Cette mise à jour n'affecte pas l'intégrité de la condition définie.

Pour plus d'informations sur les nouvelles dimensions, consultez la rubrique Recherche en libre-service d'Virtual Apps and Desktops.

Mise à jour des champs de données pour les applications et les bureaux Dans la recherche en libre-service d'applications et de bureaux, affichez les champs de données mis à jour en fonction du modèle contextuel.

Pour plus d'informations, consultez la section Recherche en libre-service d'applications et de bureaux.

Fonctionnalité obsolète

Suppression des événements VPN_AF et VPN_SU de la page de recherche en libre-service Sur la page de recherche en libre-service de la source de données Citrix Gateway, les types d'enregistrement suivants sont désormais supprimés.

Type d'enregistrement	Nom de l'enregistrement
VPN_SU	Enregistrement de mise à jour de session
VPN_AF	Enregistrement d'échec du lancement de l'application

Vous ne pouvez donc pas filtrer et afficher vos événements en fonction de ces types d'enregistrement. Tous les indicateurs de risque personnalisés basés sur ces types d'enregistrements cessent de fonctionner.

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

11 mars 2021

Nouveautés

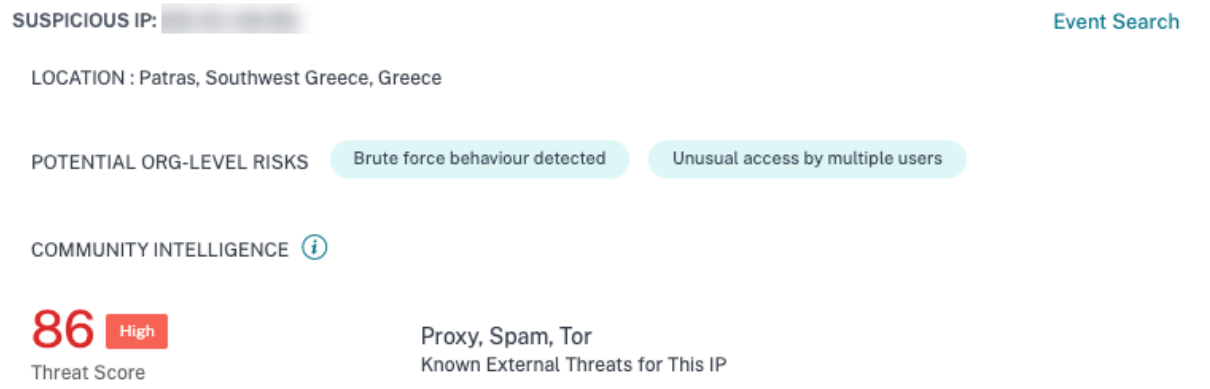
Horodatage actuel du schéma de score de risque utilisateur Un nouveau champ `last_update_timestam` est ajouté dans le format du schéma de score de risque utilisateur. Ce champ indique l'heure à laquelle le score de risque a été mis à jour pour la dernière fois. Pour plus d'informations sur le format du schéma, consultez Schéma de score de risque utilisateur.

03 mars, 2021

Nouveautés

Améliorations apportées à l'indicateur de risque d'ouverture de session à partir d'une adresse IP suspecte Sur la page de chronologie des risques de l'utilisateur, une nouvelle section **IP sus-**

pecte s'affiche pour l'indicateur de risque Ouverture de **session à partir d'une adresse IP suspecte** . Cette section fournit les informations suivantes :



- Adresse IP à partir de laquelle une activité de connexion suspecte est détectée.
- Emplacement de l'utilisateur.
- Tout modèle d'activité IP suspecte que Citrix Analytics a récemment détecté dans votre organisation.
- Flux de renseignements au niveau de la communauté concernant l'adresse IP.

Pour plus d'informations, consultez l'indicateur de risque d'ouverture de session à partir d'une adresse IP suspecte .

Améliorations apportées à l'indicateur de risque d'accès à partir d'un emplacement inhabituel

- Dans l'indicateur de risque Accès à partir d'un emplacement inhabituel pour Citrix Content Collaboration, la colonne **TOOL NAME** a été ajoutée dans la table des événements. Suppression de la colonne **DEVICE BROWSER** de la table des événements. Pour plus d'informations, consultez la section Indicateurs de risque Citrix Content Collaboration.
- Dans l'indicateur de risque d'accès depuis une localisation inhabituelle pour Citrix Virtual Apps and Desktops et Citrix DaaS, ajoutez les colonnes **DEVICE ID** et **RECEIVER TYPE** dans le tableau des événements. Pour plus d'informations, consultez la section Indicateurs de risque Citrix Virtual Apps and Desktops.

Format de données de Citrix Analytics pour SIEM Cet article décrit le schéma des données traitées générées par Citrix Analytics pour votre service SIEM.

Problème résolu

- Pour un utilisateur Content Collaboration, si la valeur `Is Employee<!--NeedCopy-->` est NULL, l'utilisateur n'est pas affiché dans la liste des utilisateurs découverts. [CAS-47815]

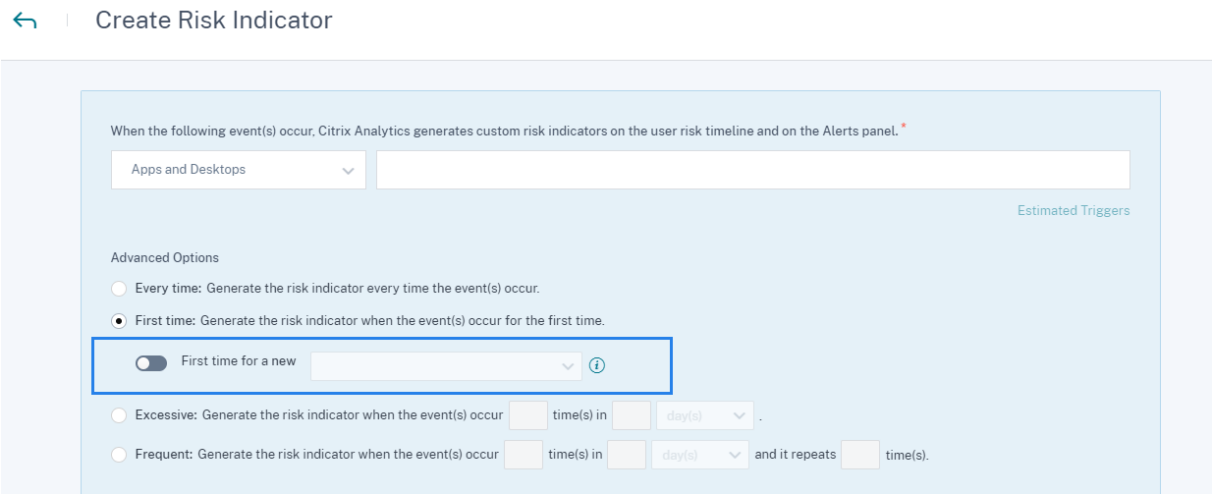
February 18, 2021

Nouveautés

Prise en charge du premier accès à partir d'une nouvelle entité dans l'indicateur de risque personnalisé Vous pouvez désormais créer un indicateur de risque qui se déclenche lorsque Citrix Analytics reçoit des événements d'une nouvelle entité pour la première fois. Voici quelques exemples d'entités : Client IP, City et Country.

Sur la page **Créer un indicateur**, cliquez sur l'option **Première fois** . Activez le bouton **Première fois pour un nouveau** bouton et sélectionnez une entité valide dans la liste en fonction de la source de données. Il n'est pas nécessaire d'attribuer une valeur spécifique à l'entité. Par exemple, si vous sélectionnez **Ville** dans la liste, Citrix Analytics déclenche un indicateur de risque chaque fois que les utilisateurs se connectent à partir d'une nouvelle ville pour la première fois.

Pour plus d'informations, consultez la section Création d'un indicateur de risque personnalisé.



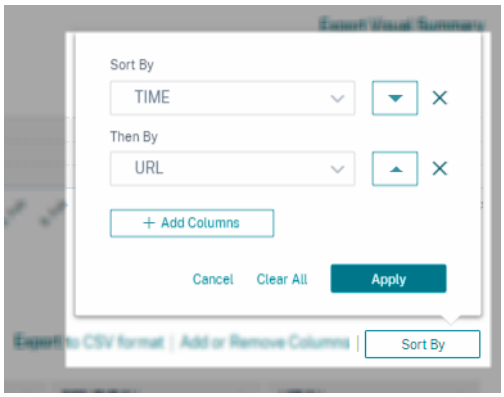
Limite maximale de création d'un indicateur de risque personnalisé Vous pouvez désormais créer des indicateurs de risque personnalisés jusqu'à une limite maximale de 50. Si vous atteignez cette limite maximale, vous devez supprimer ou modifier tout indicateur de risque personnalisé existant pour créer un indicateur de risque personnalisé.

Pour plus d'informations, consultez la section Indicateurs de risque personnalisés.

Données de localisation des utilisateurs provenant de Citrix Virtual Apps and Desktops et Citrix DaaS Sur la page **Informations utilisateur**, Citrix Analytics affiche désormais l'emplacement de l'utilisateur à partir de la source de données Citrix Virtual Apps and Desktops et Citrix DaaS.

Pour plus d'informations sur l'emplacement de l'utilisateur, consultez Profil utilisateur.

Tri multi-colonnes Sur la page de recherche en libre-service, vous pouvez désormais trier les événements utilisateur par plusieurs colonnes. Cliquez sur **Trier par**, ajoutez les colonnes et l'ordre de tri. Cliquez sur **Appliquer** pour trier les événements utilisateur. Vous pouvez ajouter jusqu'à six colonnes pour effectuer un tri sur plusieurs colonnes.



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

Fonctionnalités obsolètes

L'indicateur de risque de défaillance d'autorisation excessive est obsolète L'indicateur de risque Citrix Gateway - **Défaillance d'autorisation excessive** est obsolète. Vous ne pouvez consulter que les données historiques liées à cet indicateur.

Les modifications suivantes sont applicables dans le cadre de cette dépréciation :

- Citrix Analytics ne génère plus ces indicateurs de risque.
- Citrix Analytics ne génère plus de stratégies avec ces indicateurs de risque comme conditions.
- Stratégies par défaut avec ces indicateurs de risque, car les conditions ne prennent plus effet.

Pour plus d'informations, consultez la section Indicateurs de risque Citrix Gateway.

27 janvier 2021

Nouveautés

Améliorations apportées à l'indicateur de risque Accès à partir d'un emplacement inhabituel
Pour Citrix Content Collaboration, Citrix Gateway et Citrix Virtual Apps and Desktops, l'indicateur de risque **Accès à partir d'un emplacement inhabituel** est désormais déclenché lorsque l'utilisateur se connecte à partir d'une adresse IP associée à un nouveau pays ou d'une nouvelle ville anormalement éloignée de toute connexion précédente emplacement. D'autres facteurs incluent le niveau global de mobilité de l'utilisateur et la fréquence relative des connexions depuis la ville pour tous les utilisateurs de votre organisation. Dans tous les cas, l'historique de localisation des utilisateurs est basé sur les 30 jours précédents d'activité de connexion.

Pour plus d'informations sur l'indicateur de risque, consultez les rubriques suivantes :

- Indicateurs de risque Citrix Content Collaboration
- Indicateurs de risque de Citrix Gateway
- Indicateurs de risque Citrix Virtual Apps and Desktops et Citrix DaaS

January 20, 2021

Problème résolu

- Pour la source de données Apps and Desktops avec StoreFront local, le traitement des données échoue bien que le déploiement StoreFront soit correctement connecté.

  [CAS-46656]

19 janvier 2021

Problème résolu

- Dans la page d'indicateur de risque personnalisé, après avoir corrigé une condition non valide dans le champ de recherche, le lien **Estimate Trigger** ne répond pas.

  Par exemple, vous saisissez une condition *Client-IP = 10.10.10.10*non valide. Après avoir corrigé cette condition et tapé *Client-IP = « 10.10.10.10 »*, le lien **Estimate Trigger** ne répond pas.

  Solution : actualisez la page des indicateurs personnalisés, puis créez l'indicateur personnalisé avec une condition valide.

  [CAS-46316]

January 13, 2021

Nouveautés

Une nouvelle version du module complémentaire Citrix Analytics pour Splunk est disponible Le module complémentaire Citrix Analytics version 2.1.0 pour Splunk est désormais disponible. Accédez à la page des téléchargements pour télécharger le fichier.

Ajout de la prise en charge de Splunk Cloud Inputs Data Manager (IDM) et de Splunk 8.1 64 bits Vous pouvez désormais intégrer Citrix Analytics for Security avec Splunk Cloud IDM et Splunk 8.1 64 bits. Pour plus d'informations, consultez la section Intégration de Splunk.

Prise en charge dépréciée

Suppression du support pour Splunk 7.1 64 bits Vous ne pouvez plus intégrer Citrix Analytics for Security avec Splunk 7.1 64 bits. Pour plus d'informations sur les versions Splunk prises en charge, voir Intégration de Splunk.

11 janvier 2021

Problème résolu

- Sur la fiche de site Virtual Apps and Desktops, l'étiquette **Utilisateurs clients pris en charge** est renommée en **Événements reçus des utilisateurs**. Le libellé **Utilisateurs clients non pris en charge** est renommé « **Impossible de recevoir des événements de la part des utilisateurs** ».

  [CAS-44773]

December 17, 2020

Nouveautés

Utilisez des indicateurs de risque personnalisés préconfigurés et une stratégie pour bloquer l'accès depuis des emplacements inhabituels (géofencing) Citrix fournit une liste d'indicateurs de risque personnalisés préconfigurés et une stratégie qui vous aident à surveiller la sécurité de votre infrastructure Citrix. Grâce à ces indicateurs et à une stratégie, vous pouvez bloquer l'accès utilisateur provenant de pays hors de leur pays d'exploitation habituel. Par défaut, le pays est défini sur « États-Unis ». Vous pouvez définir votre pays requis pour le géofencing.

Voici les indicateurs de risque personnalisés préconfigurés et une stratégie :

- La session CVAD débute en dehors du périmètre de géofencing
- GW-Geofence crossing
- CCC-Geofence crossing
- Début de la session en dehors de la clôture géographique

Pour plus d'informations, consultez la section Indicateurs et stratégies de risque personnalisés préconfigurés.

Afficher les emplacements accessibles dans l'e-mail de réponse utilisateur Au lieu de l'adresse IP d'une machine utilisateur, l'e-mail de réponse de l'utilisateur affiche désormais tous les emplacements auxquels l'utilisateur a accédé au cours des 15 dernières minutes. L'emplacement est affiché dans le `<City>,<Country><!--NeedCopy-->` format. Si la ville ou le pays n'est pas disponible, la valeur correspondante est affichée comme « Inconnu ».

Pour plus d'informations, consultez la section Demander une réponse utilisateur.

Indicateur de risque de Content Collaboration renommé - Premier accès depuis un nouvel emplacement L'indicateur de risque Citrix Content Collaboration Le **premier accès à partir d'un nouvel emplacement** est renommé **Accès depuis un emplacement inhabituel**.

Pour plus d'informations, consultez Accès à partir d'un emplacement inhabituel.

Fonctionnalités obsolètes

Feedback sur les indicateurs de risque Le mécanisme de rétroaction des indicateurs de risque est supprimé. Si l'indicateur de risque Content Collaboration - Accès depuis un emplacement inhabituel est déclenché de manière incorrecte, vous ne pouvez plus le signaler comme un faux positif et fournir des commentaires.

December 07, 2020

Nouveautés

Améliorations de l'indicateur de risque potentiel d'exfiltration de données Les améliorations suivantes sont apportées à l'indicateur de risque :

- Les informations de la section **WHAT HAPPENED** sont mises à jour. Le format de l'heure est mis à jour pour maintenir la cohérence.
- Les informations de localisation de l'appareil apparaissent dans la liste des événements.

Pour plus d'informations sur l'indicateur de risque, voir Exfiltration potentielle de données.

Améliorations de l'indicateur de risque Content Collaboration - Premier accès depuis un nouvel emplacement Dans la chronologie des risques utilisateur, sélectionnez **Premier accès depuis un nouvel emplacement** pour afficher les informations suivantes :

- **Emplacements de connexion** : affiche une vue cartographique géographique des emplacements habituels et inhabituels à partir desquels l'utilisateur s'est connecté.
- **Nombre de connexions depuis des emplacements habituels - 30 derniers jours** : affiche un graphique à secteurs des 6 premiers emplacements habituels à partir desquels l'utilisateur s'est connecté au cours des 30 derniers jours. Il affiche également le nombre d'événements de connexion de ces emplacements.
- **Détails de l'événement pour un emplacement inhabituel** : fournit la liste des événements de connexion de l'emplacement inhabituel pour l'utilisateur.

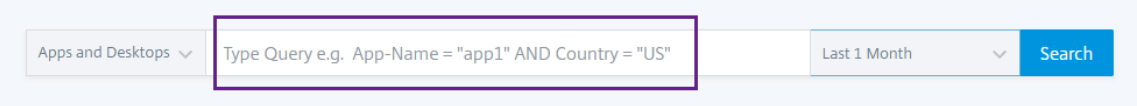
Pour plus d'informations sur l'indicateur de risque, voir Premier accès depuis un nouvel emplacement.

30 novembre 2020

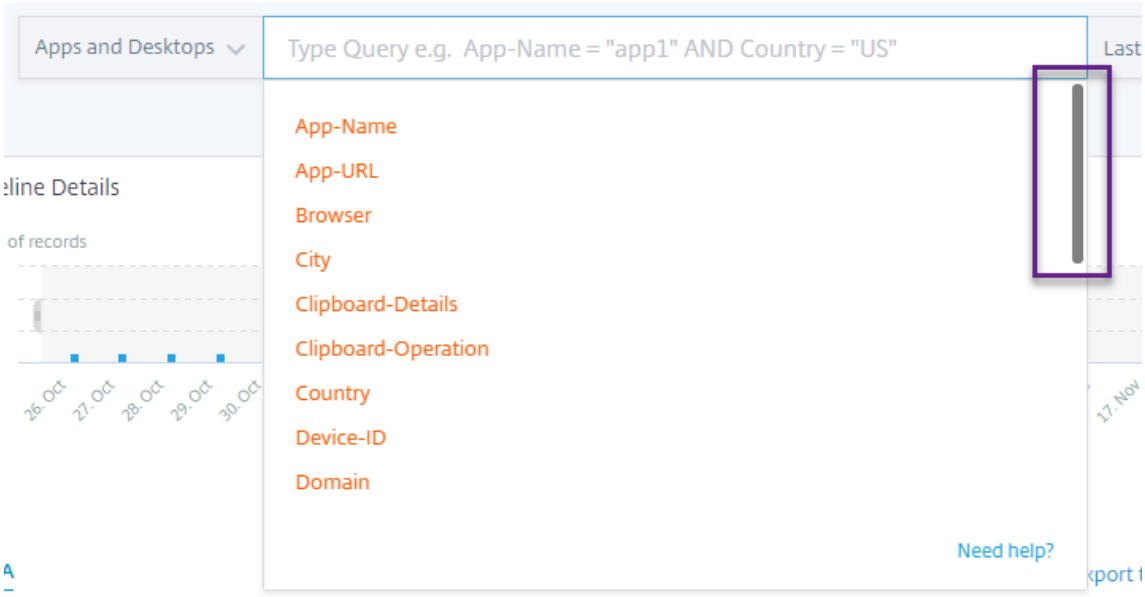
Nouveautés

Amélioration de la page de recherche en libre Les améliorations suivantes sont apportées pour améliorer la convivialité de la page de recherche en libre-service :

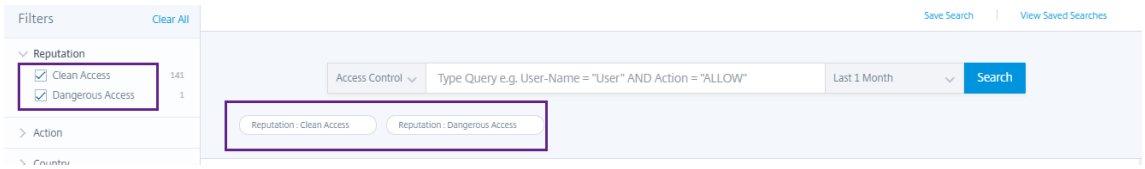
- La zone de recherche affiche un exemple de requête pour indiquer comment saisir votre propre requête.



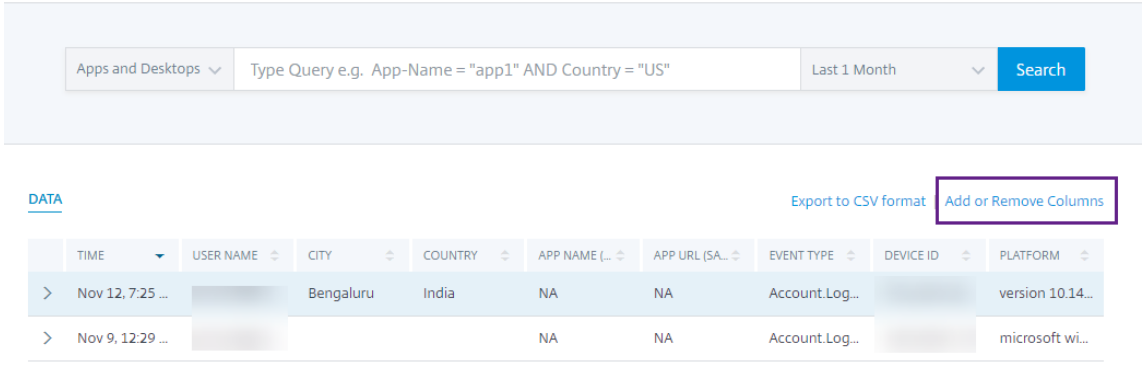
- Sous macOS, la barre de défilement de la liste des dimensions apparaît désormais par défaut.



- Les filtres appliqués apparaissent désormais sous forme de jetons.



- L'étiquette **Ajouter ou supprimer des colonnes** remplace l'icône **+** .



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

Amélioration des stratégies La page **Stratégies** affiche désormais les stratégies associées aux sources de données qui ont été découvertes et connectées à Citrix Analytics. Cette page n'affiche pas les stratégies pour lesquelles une condition est définie pour les sources de données non découvertes. La désactivation du traitement des données pour une source de données déjà connectée n'affecte pas les stratégies existantes sur la page **Stratégies** .

Pour plus d'informations, consultez la section Configurer des stratégies et des actions.

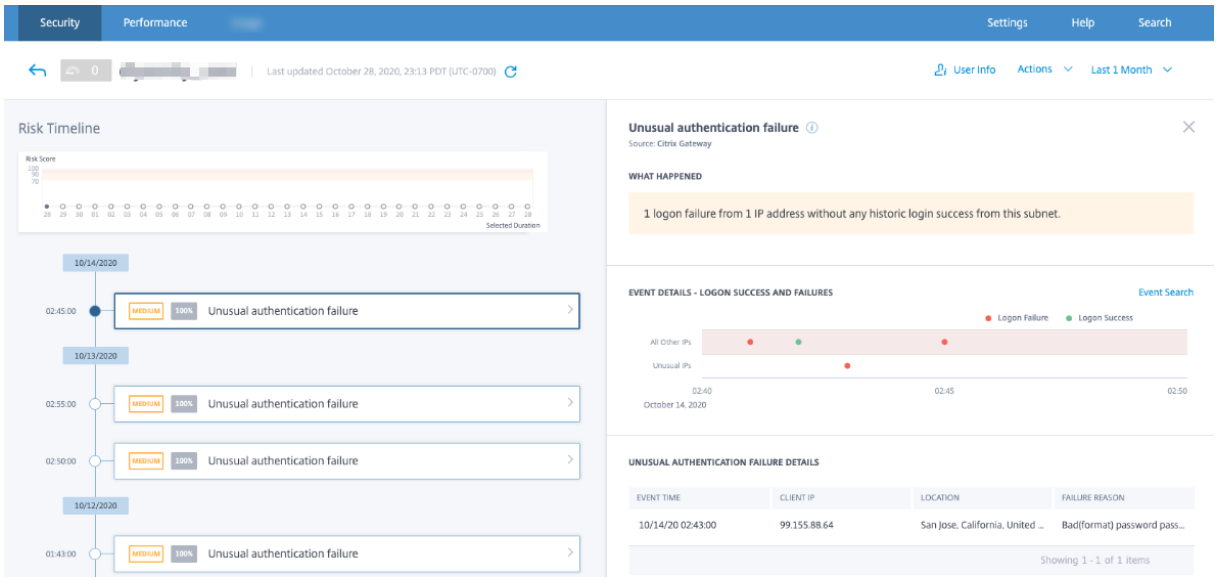
04 novembre 2020

Nouveautés

Échec d'authentification inhabituel : indicateur de risque Citrix Gateway Citrix Analytics détecte les menaces basées sur l'accès lorsqu'un utilisateur a des échecs de connexion à partir d'une adresse IP inhabituelle et déclenche l'indicateur de risque **d'échec d'authentification inhabituel** .

Cet indicateur de risque est déclenché lorsqu'un utilisateur de votre organisation a des échecs de connexion à partir d'une adresse IP inhabituelle qui est contraire à son comportement habituel.

Pour plus d'informations, consultez la section Indicateurs de risque Citrix Gateway.



20 octobre 2020

Problème résolu

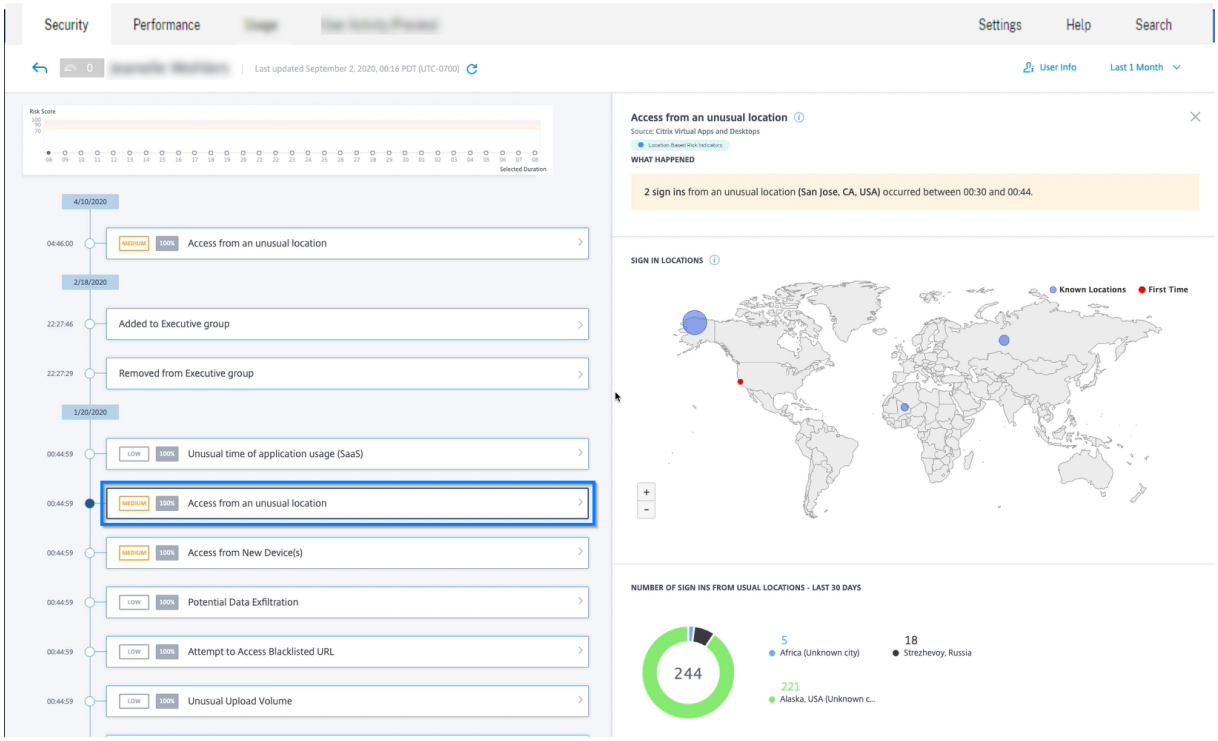
- L'indicateur de risque **Premier accès depuis un nouvel appareil** avec **l'action Déconnexion de l'utilisateur** appliquée ne fonctionne pas comme prévu.

  [CAS-40743]

15 octobre 2020

Nouvelles fonctionnalités

Accès depuis un emplacement inhabituel : indicateur de risque Citrix Virtual Apps and Desktops et Citrix DaaS Citrix Analytics détecte les menaces basées sur l'accès en fonction des connexions inhabituelles de Citrix Workspace et déclenche l'indicateur de risque correspondant.



Pour plus d'informations, consultez les sections Indicateurs de risque Citrix Virtual Apps and Desktops et Citrix DaaS.

Améliorations du tableau de bord Share Link

- La colonne SHARE URL est maintenant remplacée par la colonne SHARE ID. Chaque URL de partage est désormais identifiée par un ID de partage.
- La sélection de l'heure sur le tableau de bord est supprimée. Désormais, ce tableau de bord affiche tous les liens de partage entre l'état actif et l'état expiré au lieu d'une période sélectionnée.
- Tous les liens de partage sont triés dans l'ordre des liens actifs, puis des liens expirés. Par défaut, le lien de partage avec le nombre d'indicateurs de risque le plus élevé apparaît en haut de la liste.

- Les liens risqués affichent désormais les liens actifs qui présentent un comportement risqué. Il n'affiche pas les liens expirés. Par défaut, le lien risqué avec le nombre d'indicateurs de risque le plus élevé apparaît en haut de la liste.
- La vue des tendances de la carte Liens de partage risqués et de la fiche Tous les liens de partage est supprimée.

Pour plus d'informations, consultez la section Tableau de bord Partager des liens.

Améliorations de la chronologie des risques de Share Link La chronologie des risques affiche désormais l'ID de partage au lieu de l'URL du partage. Pour plus d'informations, voir Chronologie des risques de lien de partage.

Fonctionnalités obsolètes

L'accès à partir d'un appareil doté d'un indicateur de risque de système d'exploitation (OS) non pris en charge est obsolète L'indicateur de risque Citrix Virtual Apps and Desktops - **L'accès à partir d'un appareil doté d'un système d'exploitation (SE) non pris en charge** est obsolète. Vous ne pouvez consulter que les données historiques liées à cet indicateur.

Les modifications suivantes sont applicables dans le cadre de cette dépréciation :

- Analytics ne génère plus ces indicateurs de risque.
- Analytics ne génère plus de stratégies avec ces indicateurs de risque comme conditions.
- Stratégies par défaut avec ces indicateurs de risque, car les conditions ne prennent plus effet.

Pour plus d'informations, consultez les sections Indicateurs de risque Citrix Virtual Apps and Desktops et Citrix DaaS.

10 septembre 2020

Nouvelles fonctionnalités

Liste de contrôle pour StoreFront Citrix Analytics affiche désormais une liste des conditions préalables que vous devez respecter avant de télécharger le fichier de configuration StoreFront. Consultez la liste de contrôle et assurez-vous que toutes les exigences minimales sont sélectionnées. Si la configuration minimale n'est pas sélectionnée, vous ne pouvez pas télécharger le fichier de configuration. Pour plus d'informations, consultez la section Source de données Citrix Virtual Apps and Desktops.

Recherche en libre-service - prise en charge de NOT EQUAL (! =) opérateur Vous pouvez maintenant utiliser la fonction NOT EQUAL (! =) dans votre requête dans les fonctionnalités suivantes :

- Indicateur de risque personnalisé
- Recherche en libre-service

Vous pouvez utiliser cet opérateur pour les conditions suivantes :

Source de données	Dimensions
Content Collaboration	Pays, ville, système d'exploitation client
Contrôle d'accès	Pays, Ville, Action, URL, Catégorie d'URL, Réputation, Navigateur, OS, Appareil
Applications et bureaux	Pays, ville, nom de l'application, fonctionnement du presse-papiers, navigateur, système d'exploitation
Gateway	Étape d'authentification, IP du client

À l'aide de l'opérateur, créez une expression d'indicateur personnalisée avec une seule valeur telle que « Country ! = XYZ » et affichez la liste des utilisateurs. Créez ensuite une stratégie pour appliquer des actions telles que Ajouter à la liste de suivi, Notifier l'administrateur ou Désactiver l'utilisateur. Vous pouvez également utiliser l'opérateur dans la recherche en libre-service des sources de données spécifiées pour filtrer les événements utilisateur.

Lorsque vous saisissez les valeurs des dimensions de votre requête, utilisez les valeurs exactes affichées sur la page de recherche en libre-service d'une source de données. Les valeurs de dimension sont sensibles à la casse.

08 septembre 2020

Nouvelles fonctionnalités

Corrélation des utilisateurs Analytics établit désormais une corrélation avec les utilisateurs découverts à partir de diverses sources de données. Ce mécanisme élimine la plupart des utilisateurs dupliqués de la liste des utilisateurs découverts. Les utilisateurs découverts dans Analytics affichent désormais la liste des utilisateurs uniques ainsi que leurs sources de données et les indicateurs de risque.

Par exemple, l'utilisateur « Joe Smith » peut avoir plusieurs identifiants utilisateur : JosephSM joe.smith@citrix.com et joe.smith, en fonction des sources de données. Analytics identifie désormais cet utilisateur avec un nom d'identificateur unique. Tous les autres identificateurs d'utilisateur sont

corrélés et les événements reçus pour Joe Smith à partir de diverses sources de données sont liés à ce nom unique.
Pour plus d'informations, consultez la section Utilisateurs découverts

Problème résolu

Dans la liste **Actions**, après avoir sélectionné les options d'action et cliqué sur **Appliquer**, un message d'erreur s'affiche.

[CAS-39914]

11 août 2020

Problèmes résolus

- Vous n'êtes pas en mesure d'intégrer Microsoft Graph Security à Citrix Analytics. Ce problème s'est produit car le portail Microsoft n'a pas pu être redirigé vers Citrix Analytics.

[CAS-38021]

31 juillet 2020

Problèmes résolus

- L'option **Déclencheurs estimés** de l'indicateur de risque personnalisé ne prédit pas les instances de l'indicateur de risque personnalisé pour le dernier jour.

[CAS-38129]

09 juillet 2020

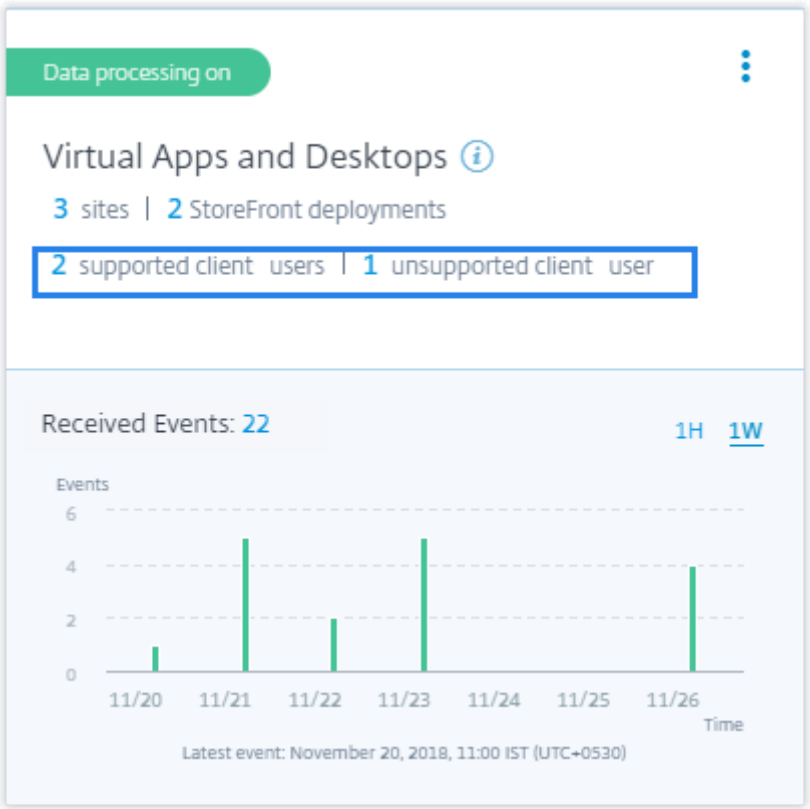
Nouvelles fonctionnalités

La fiche de site Virtual Apps and Desktops affiche les utilisateurs avec des clients pris en charge et non pris en charge Sur la fiche de site, vous pouvez désormais afficher le nombre d'utilisateurs qui utilisent des versions prises en charge et non prises en charge de l'application Citrix Workspace ou des clients Citrix Receiver sur leurs points de terminaison.

- Cliquez sur le nombre d'utilisateurs des clients pris en charge pour afficher la page **Utilisateur** qui affiche tous les utilisateurs découverts.

- Cliquez sur le nombre d'utilisateurs des clients non pris en charge pour télécharger un fichier CSV. Le fichier répertorie les utilisateurs et leurs versions client non prises en charge. Analytics ne reçoit pas d'événements utilisateur des clients non pris en charge et n'ajoute donc pas les utilisateurs en tant qu'utilisateurs découverts. À l'aide du fichier CSV, vous identifiez les utilisateurs qui doivent mettre à niveau leurs clients vers une version prise en charge afin qu'Analytics puisse fournir des informations de sécurité sur leur comportement.

Pour afficher la liste des clients pris en charge, consultez Citrix Virtual Apps and Desktops et Source de données Citrix DaaS.



Accès à partir d'un indicateur de risque de localisation inhabituelle

- L'indicateur de risque Citrix Gateway **Premier accès depuis un nouvel emplacement** est renommé **Accès à partir d'un emplacement inhabituel**.
- Dans la chronologie du risque utilisateur, une carte géographique et un diagramme circulaire sont introduits dans la section Détails de l'événement.
  - **Emplacements de connexion** : Cette section affiche une vue cartographique géographique des emplacements habituels et inhabituels de l'utilisateur. Les emplacements habituels et inhabituels sont indiqués par un code couleur en haut à droite de la carte géographique. Vous pouvez zoomer sur la carte géographique pour voir de plus près l'

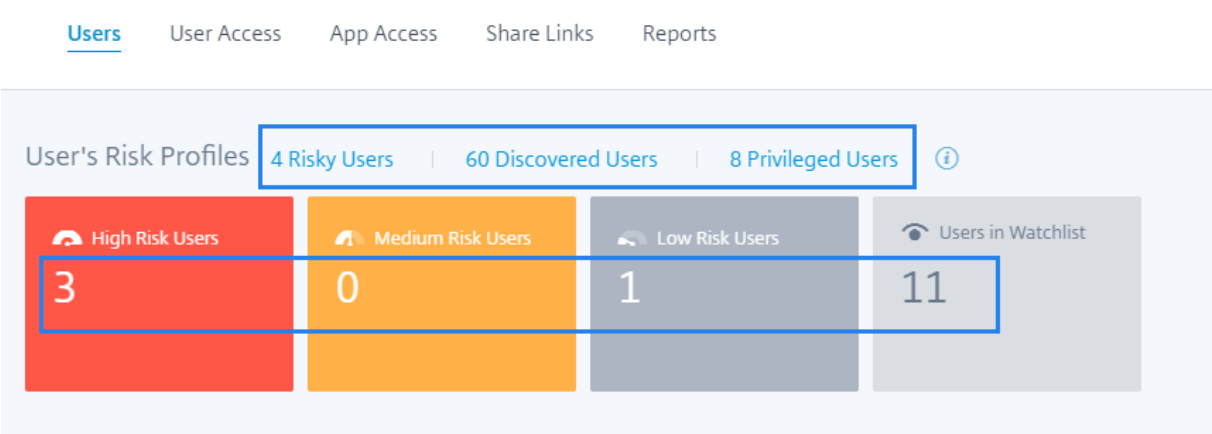
emplacement.

- **Emplacements habituels - 30 derniers jours** : Cette section affiche un graphique à secteurs qui donne une vue des 6 principaux emplacements habituels depuis lesquels l'utilisateur s'est connecté. Chaque emplacement est marqué par un code couleur différent. Vous pouvez trier la section par emplacement pour obtenir une vue détaillée de l'emplacement sélectionné.

Pour plus d'informations, consultez Accès à partir d'un emplacement inhabituel.

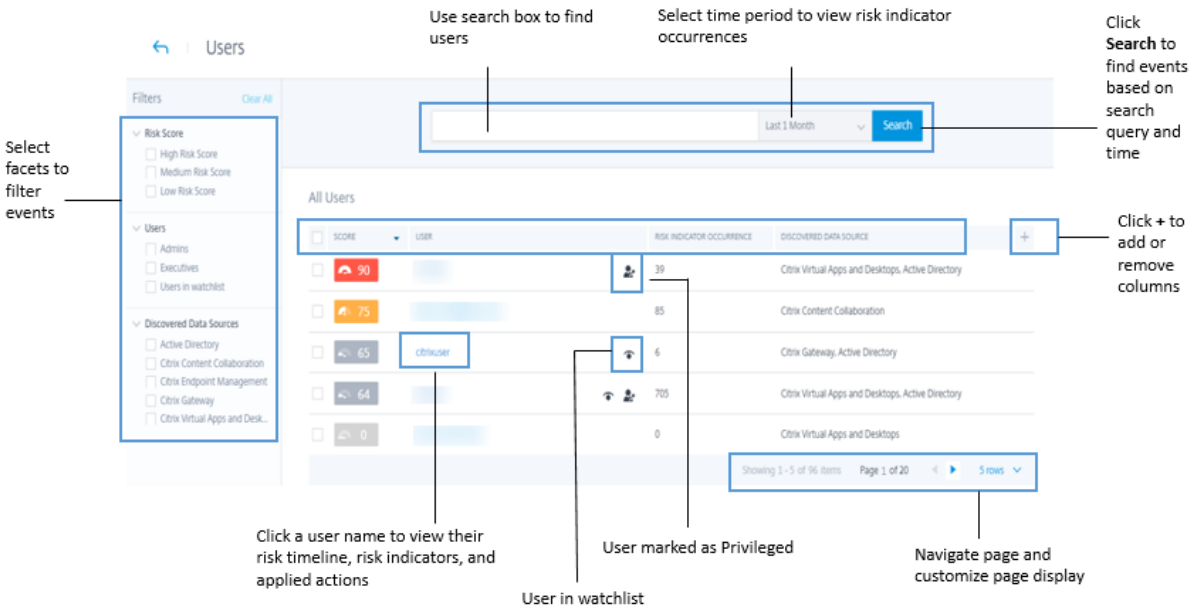
Données du tableau de bord des utilisateurs Le nombre d'utilisateurs à risque, d'utilisateurs découverts, d'utilisateurs privilégiés et d'utilisateurs dans la liste de suivi est affiché pour les 13 derniers mois, quelle que soit la période sélectionnée dans le tableau de bord **Utilisateurs** et la page **Utilisateurs** . Lorsque vous sélectionnez la période, les occurrences de l'indicateur de risque changent.

Pour plus d'informations, consultez Tableau de bord des utilisateurs.



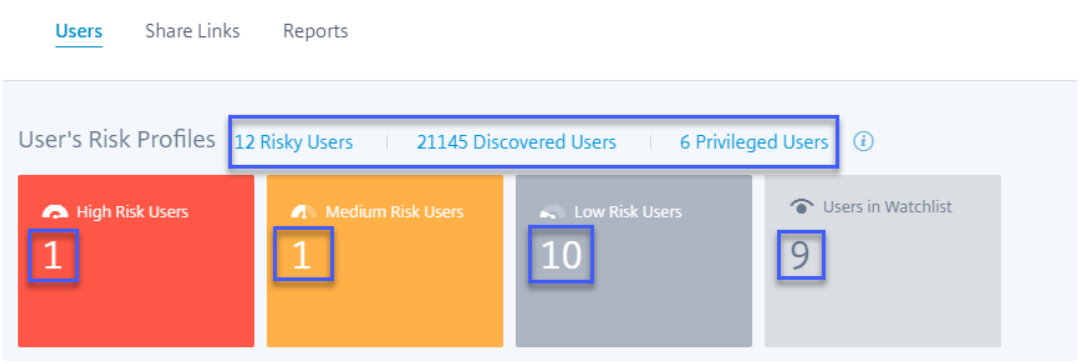
Page Utilisateurs repensée La page **Utilisateurs** a été améliorée pour une meilleure expérience utilisateur. Il fournit un résumé consolidé des événements utilisateur en fonction des scores de risque utilisateur, de la source de données et du type d'utilisateur.

Pour permettre une recherche plus ciblée, la page **Utilisateurs** contient la section **Filtres** dans le volet gauche et la barre de recherche en haut. Vous pouvez rechercher des événements utilisateur pour une durée prédéfinie ou une plage de temps personnalisée.



Pour afficher la page **Utilisateurs** :

- Accédez à **Sécurité > Utilisateurs** pour afficher le tableau de bord **Utilisateurs** et procédez comme suit :
  - Cliquez sur l'un des liens suivants ou sur les fiches.



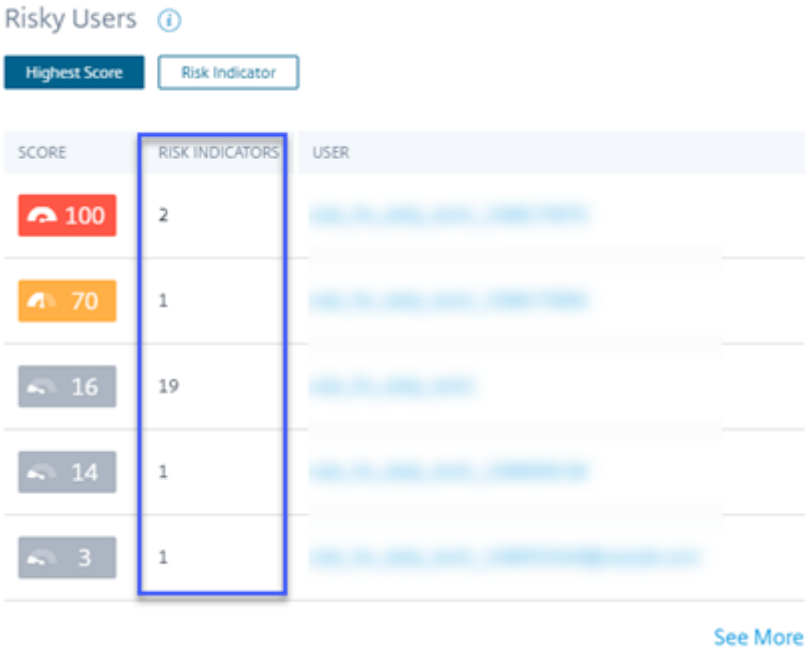
  - Dans le volet **Utilisateurs risqués**, cliquez sur **Voir plus**.
  - **Dans le volet Utilisateurs de la liste de suivi**, cliquez sur **Voir plus**.
  - Dans le volet **Utilisateurs privilégiés**, cliquez sur **Voir plus**.

- Accédez à **Paramètres > Sources de données > Sécurité**. Cliquez sur le nombre d'utilisateurs de n'importe quelle fiche de site de source de données.

Pour plus d'informations, consultez Tableau de bord des utilisateurs.

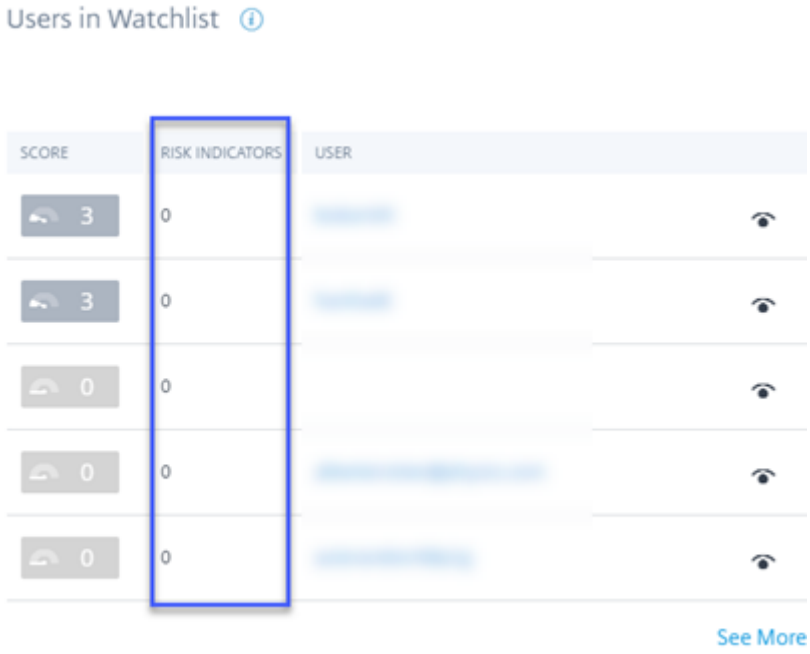
Améliorations du volet Utilisateurs risqués La colonne **Changement** est remplacée par la colonne **Indicateurs de risque** . La colonne **Indicateurs de risque** affiche le nombre total d'occurrences d'indicateurs de risque d'un utilisateur pendant une période spécifique.

Pour plus d'informations, consultez la section Utilisateurs risqués.



Améliorations apportées aux utilisateurs dans le volet Liste de suivi La colonne **Changement** est remplacée par la colonne **Indicateurs de risque** . La colonne **Indicateurs de risque** affiche le nombre total d'occurrences d'indicateurs de risque d'un utilisateur pendant une période spécifique.

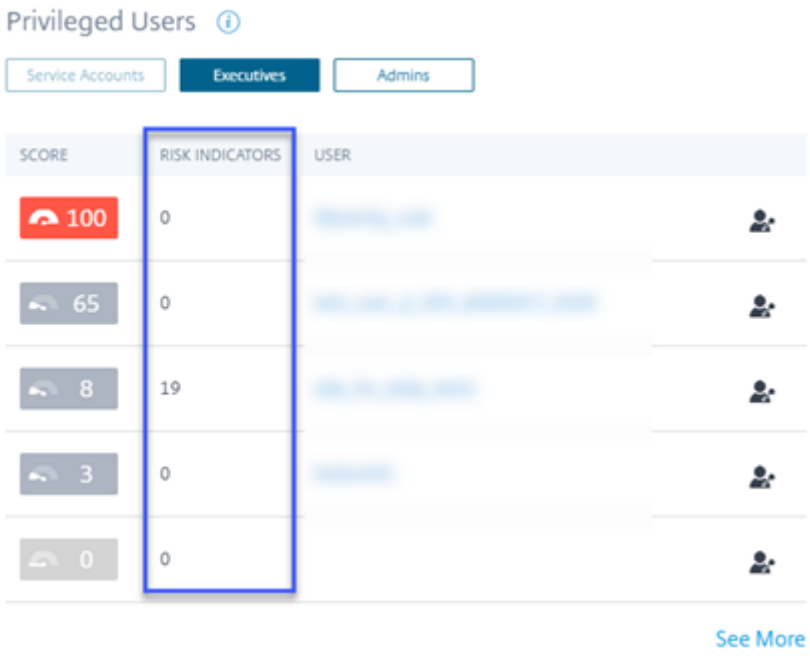
Pour plus d'informations, consultez la section Utilisateurs dans la liste de suivi.



Améliorations du volet Utilisateurs privilégiés

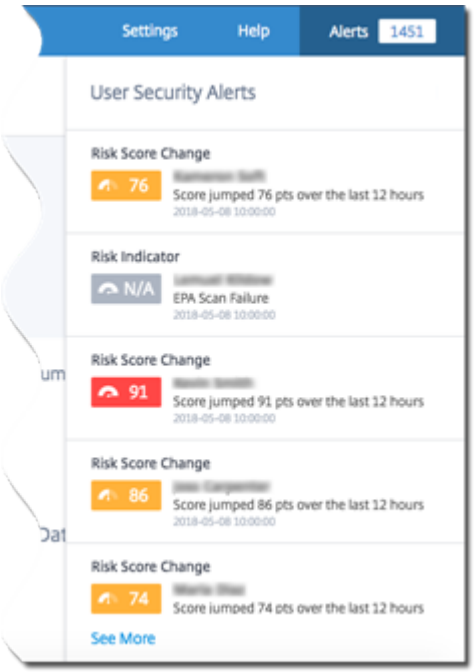
- La colonne **Changement** est remplacée par la colonne **Indicateurs de risque** . La colonne **Indicateurs de risque** affiche le nombre total d'occurrences d'indicateurs de risque d'un utilisateur pendant une période spécifique.
- Cliquez sur **Voir plus** pour afficher la page **Utilisateurs** . La page **Utilisateurs** qui affiche la liste des utilisateurs privilégiés administrateur et exécutif. Sur cette page, vous pouvez ajouter ou supprimer un utilisateur en tant qu'utilisateur privilégié.

Pour plus d'informations, consultez la section Utilisateurs privilégiés.

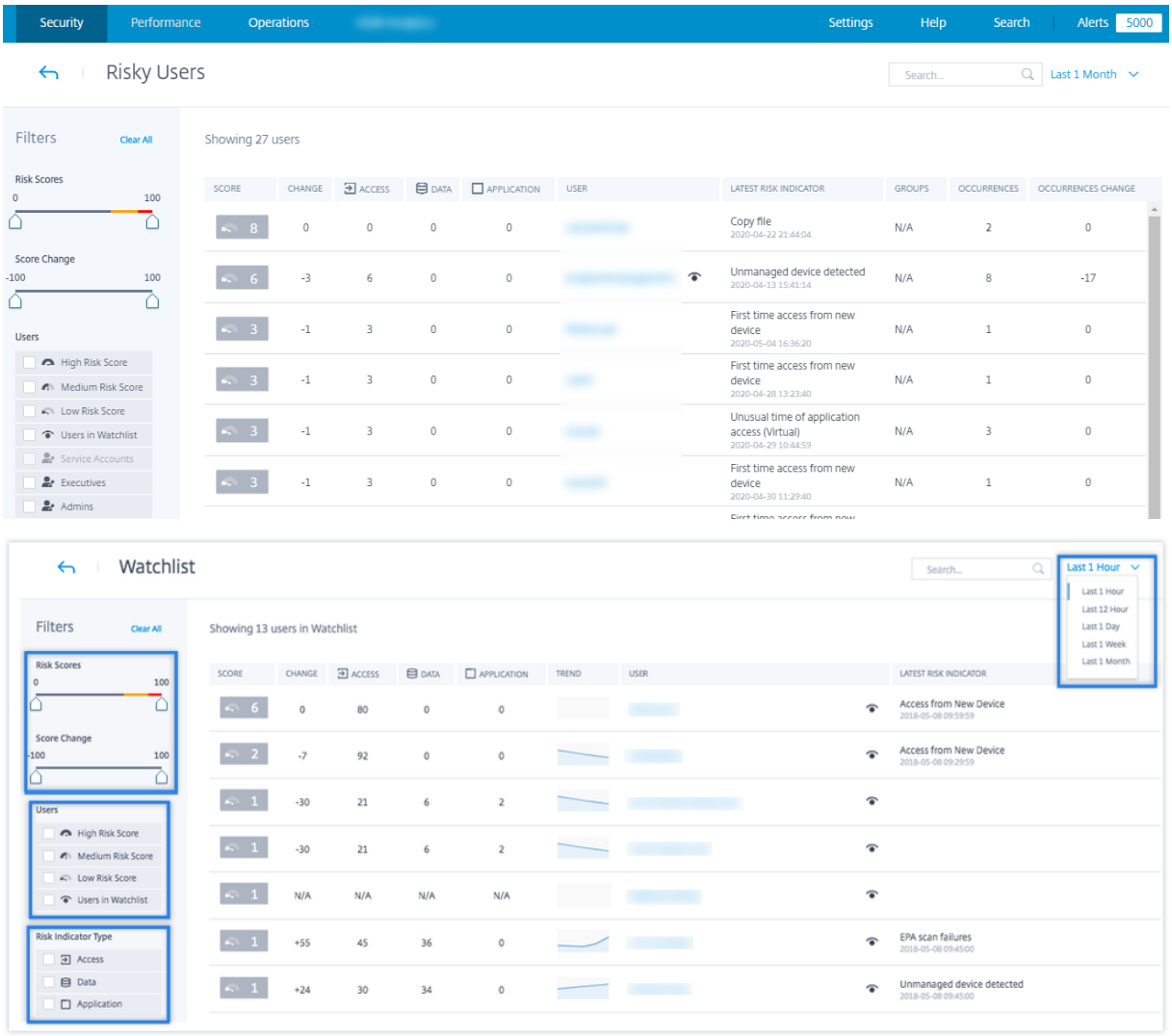


Fonctionnalités obsolètes

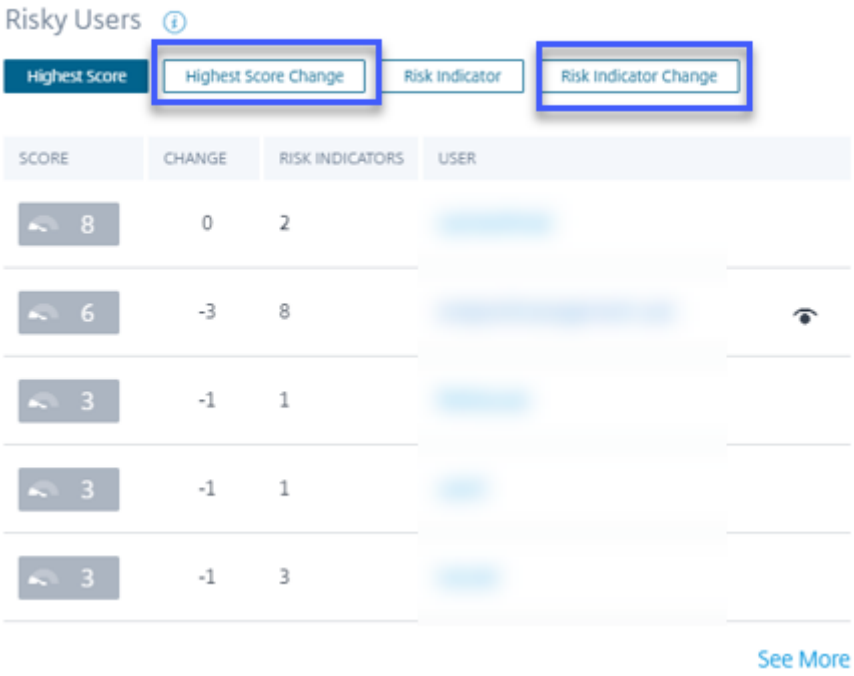
Alertes La fonctionnalité **Alertes** est désormais obsolète et n'est plus disponible dans l'interface utilisateur Analytics.



Page Utilisateurs à risque et liste de suivi Les pages **Utilisateurs risqués** et **Liste de suivi** sont obsolètes. Ils sont remplacés par la page **Utilisateurs** qui récapitule tous les événements utilisateur risqués et les utilisateurs de la liste de suivi.

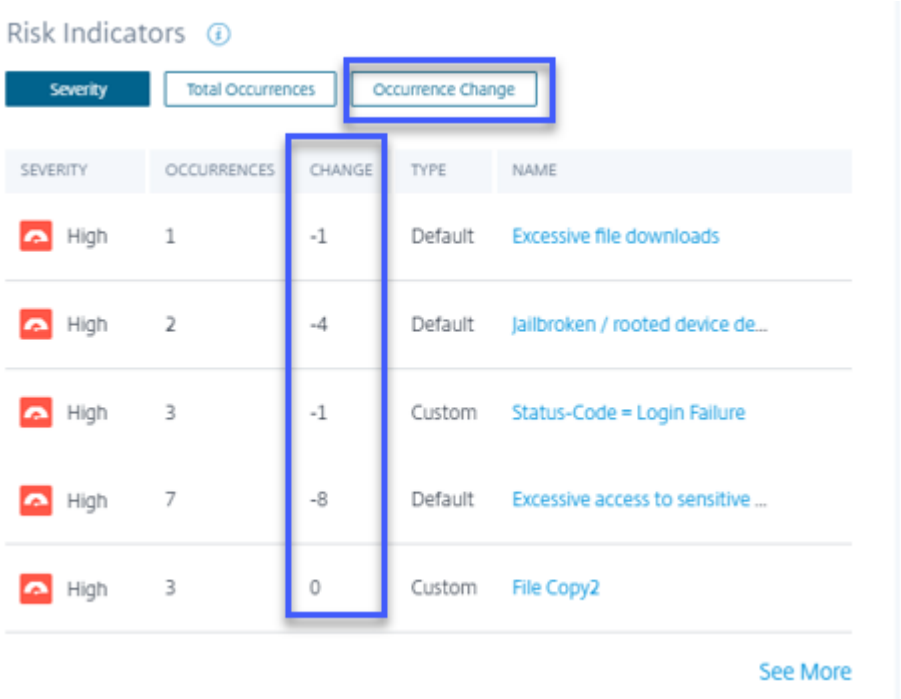


Volet Utilisateurs risqués Les onglets **Changement du score le plus élevé** et **Changement de l'indicateur de risque** sont supprimés du volet **Utilisateurs risqués** .



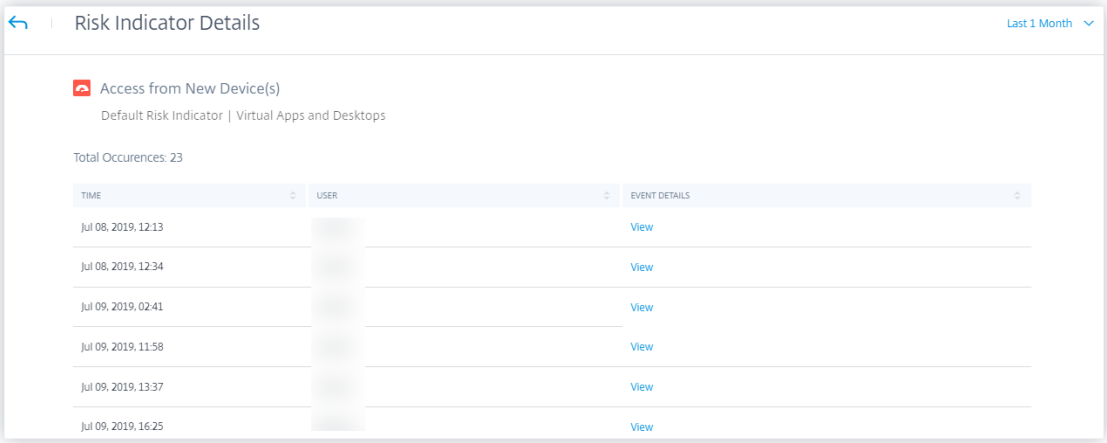
Volet Indicateur de risque

- L'onglet **Changement d'occurrence** et la colonne **CHANGE** sont supprimés.

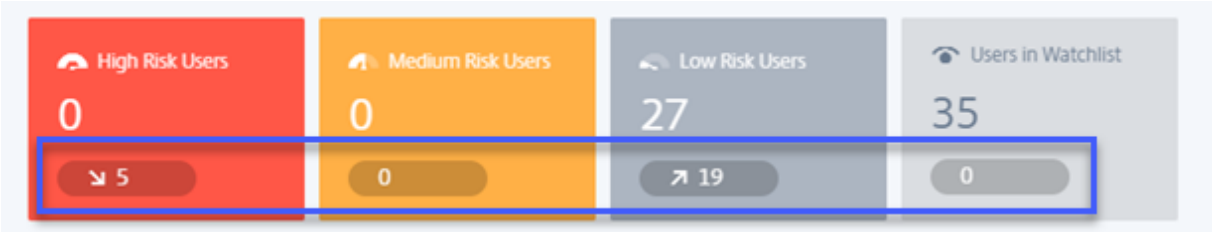


- La page **Détails de l'indicateur de risque** est obsolète. Auparavant, cette page était affichée lorsqu'un indicateur de risque était sélectionné dans le volet **Indicateurs de risque** ou sur la

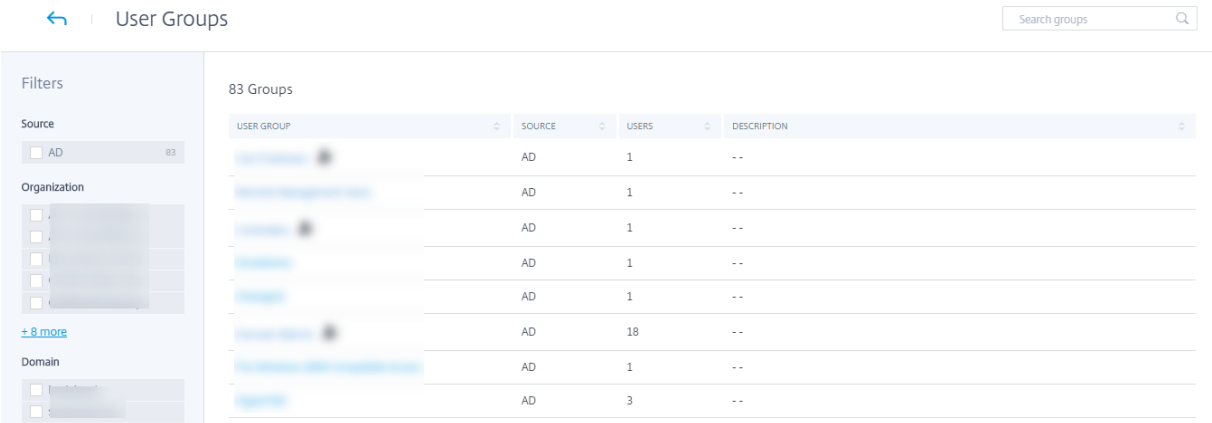
page **Aperçu de l'indicateur de risque** .



Vue des tendances Dans le tableau de bord **Utilisateurs**, la vue des tendances du nombre d'utilisateurs est supprimée des fiches **Utilisateurs à risque élevé**, **Utilisateurs à risque moyen**, **Utilisateurs à faible risque**et **Utilisateurs de la liste de surveillance**.



Page Groupes d'utilisateurs La page **Groupes d'utilisateurs** sous l'option **Paramètres** est obsolète. Vous ne pouvez plus ajouter ou supprimer un groupe d'utilisateurs en tant que groupe privilégié. Toutefois, vous pouvez ajouter ou supprimer des utilisateurs individuels en tant qu'utilisateurs privilégiés. Pour plus de détails, consultez la section Utilisateurs privilégiés.



26 juin 2020

Fonctionnalités obsolètes

Indicateurs de risque liés au temps inhabituel d'accès aux applications (virtuel/SaaS) dépréciés
Les indicateurs de risque Citrix Virtual Apps and Desktops - **Heure inhabituelle d'accès aux applications (virtuel)** et **Heure inhabituelle d'accès aux applications (SaaS)** ont été déconseillés. Vous ne pouvez consulter que les données historiques liées à ces indicateurs.

Les modifications suivantes sont applicables dans le cadre de cette dépréciation :

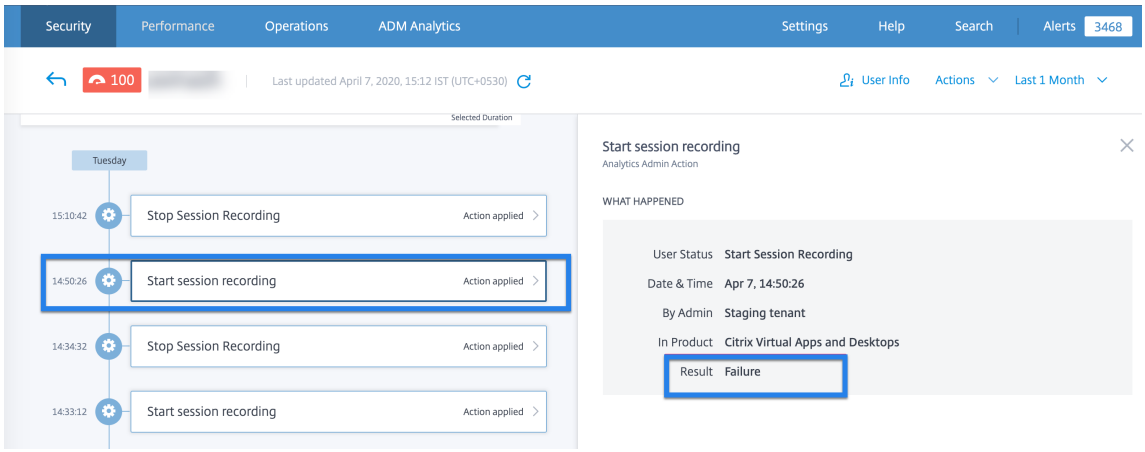
- Analytics ne génère plus ces indicateurs de risque.
- Analytics ne génère plus de stratégies avec ces indicateurs de risque comme conditions.
- Stratégies par défaut avec ces indicateurs de risque, car les conditions ne prennent plus effet.

Pour plus d'informations, consultez les sections Indicateurs de risque Citrix Virtual Apps and Desktops et Citrix DaaS.

02 juin 2020

Problèmes résolus

- Dans la chronologie des risques utilisateur, l'état des actions Virtual Apps and Desktops (basées sur une stratégie ou appliquées manuellement) apparaît comme « Échec », même si les actions ont été appliquées avec succès sur le compte d'utilisateur. Par exemple, l'action **Démarrer l'enregistrement de session** est appliquée avec succès sur le compte d'utilisateur, mais le résultat est affiché comme « Échec ». [CAS-32773]



11 mai 2020

Problèmes résolus

- Pour certains utilisateurs, les actions basées sur des stratégies ne sont pas déclenchées et le mode d'application de la stratégie ne peut pas être appliqué. Ce problème se produit lorsque les identifiants des clients ne sont pas en minuscules.

  [CAS-34209], [CAS-34141]

- Impossible de créer des indicateurs de risque personnalisés pour certains utilisateurs. Ce problème se produit lorsque les identifiants des clients ne sont pas en minuscules.

  [CAS-34139]

29 avril 2020

Problèmes résolus

- Les actions appliquées aux indicateurs de risque Citrix Virtual Apps and Desktops ne prennent pas effet, bien qu'Analytics affiche un message indiquant que les actions ont été correctement appliquées. Ce problème est observé dans la version Citrix Virtual Apps and Desktops 7 1912.

  [CAS-31544]

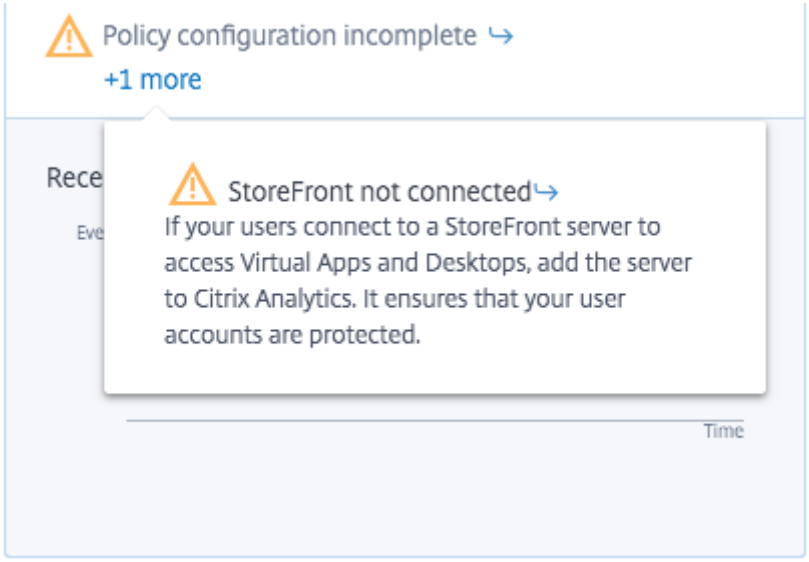
02 avril 2020

Nouvelles fonctionnalités

Désactiver le traitement des données lorsque StoreFront n'est pas ajouté Sur la fiche de site de la source de données **Paramètres** > **Sources de données** > **Sécurité** > **Virtual Apps and Desktops**, le bouton **Activer le traitement des données** n'est pas activé si vous n'avez pas intégré StoreFront. Le message d'avertissement **StoreFront non connecté** s'affiche sur la fiche de site. Si vous avez un site local actif à partir duquel vous souhaitez qu'Analytics reçoive des données, vous devez vérifier que vous avez intégré StoreFront à Citrix Analytics. Il garantit la protection de vos comptes d'utilisateurs.

Sur la fiche de site **Virtual Apps and Desktops**, sélectionnez les points de suspension verticaux () et cliquez sur **Connecter le déploiement StoreFront**. Sur l'écran qui s'affiche, suivez les instructions et terminez la configuration de StoreFront.

Pour plus d'informations, consultez Sites locaux Citrix Virtual Apps and Desktops intégrés à l'aide de StoreFront.



Problèmes résolus

- Pour les utilisateurs de Citrix Content Collaboration, les actions basées sur des stratégies ne prennent pas effet dans les conditions suivantes :
  - Lorsque les conditions de l'indicateur de risque personnalisé sont définies
  - Jusqu'à ce qu'un indicateur de risque soit généré pour un utilisateur

  [CAS-29226]

04 mars 2020

Problèmes résolus

- Lorsque les utilisateurs de passerelle sont connectés à Analytics pour la première fois, ils voient l'erreur **Citrix ADC ne répond pas ou les informations d'identification sont incorrectes**. Lors d'une nouvelle tentative, ils voient l'erreur L'**appareil avec cette adresse IP existe déjà**.

[CAS-31180]

20 février 2020

Nouvelles fonctionnalités

Offre Citrix Analytics for Security Citrix Analytics for Security est désormais disponible pour un abonnement individuel.

Vous pouvez vous abonner à Citrix Analytics for Security et obtenir des informations spécifiques à cette offre. Pour plus d'informations, reportez-vous à la section Mise en route.

Tableau de bord des catégories de risques Citrix Analytics introduit la catégorisation des indicateurs de risque en fonction des risques ayant un impact similaire sur l'aspect sécurité de l'entreprise. Ce tableau de bord fournit une vue complète des expositions aux risques et des risques critiques qui nécessitent une attention immédiate. Pour les indicateurs de risque par défaut, Analytics attribue automatiquement une catégorie de risque en fonction de l'exposition au risque. Pour les indicateurs de risque personnalisés, vous devez sélectionner une catégorie de risque appropriée en fonction de l'exposition au risque.

Analytics prend en charge les catégories de risques suivantes :

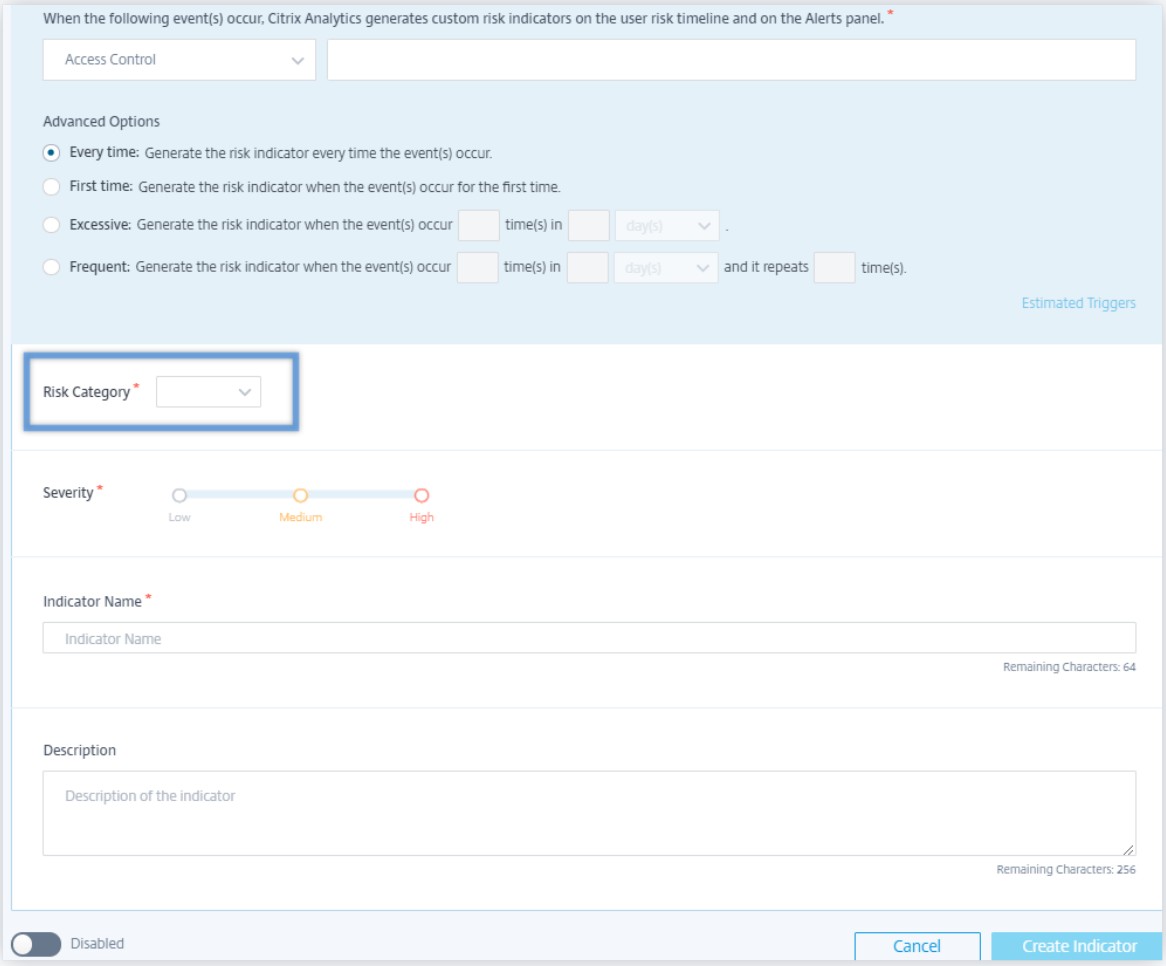
- Exfiltration de données
- Menaces internes
- Utilisateurs compromis
- Points de terminaison compromis

Pour plus d'informations, consultez Catégories de risques.

Colonne Catégorie de risque de la page Indicateurs personnalisés La colonne **Catégorie de risque** est introduite sur la page Indicateur de risque personnalisé. En fonction du type d'exposition au risque, vous pouvez sélectionner une catégorie de risque pour votre indicateur de risque personnalisé. Les indicateurs de risque personnalisés créés précédemment sont affichés dans le tableau de

bord Catégories de risques si vous les modifiez en sélectionnant une catégorie de risque.

Pour plus d'informations, consultez la section Indicateurs de risque personnalisés.



Changement de nom des indicateurs de risque Les noms des indicateurs de risque suivants ont été modifiés :

Source de données	Ancien nom	Nouveau nom
Citrix Virtual Apps and Desktops et Citrix DaaS	Utilisation inhabituelle des applications (Virtual)	Heure inhabituelle d'accès à l'application (Virtuel)
Citrix Virtual Apps and Desktops et Citrix DaaS	Utilisation inhabituelle des applications (SaaS)	Délai d'accès aux applications (SaaS) inhabituel
Citrix Content Collaboration	Échecs d'ouverture de session excessifs	Échec excessif de l'authentification

Source de données	Ancien nom	Nouveau nom
Citrix Content Collaboration	Accès inhabituel à l'ouverture de session	Accès pour la première fois depuis un nouvel emplacement
Citrix Access Control	Volume de téléchargement inhabituel	Téléchargement excessif de données
Citrix Gateway	Échecs d'ouverture de session	Échec excessif de l'authentification
Citrix Gateway	Échecs d'autorisation	Échecs excessifs d'autorisation
Citrix Gateway	Accès inhabituel à l'ouverture de session	Accès pour la première fois depuis un nouvel emplacement

Pour plus d'informations, consultez la section Indicateurs de risque.

Problèmes résolus

- Pour certains utilisateurs, Citrix Analytics ne peut pas recevoir de données de Virtual Apps and Desktops, même si la source de données est correctement intégrée et que StoreFront est activé. [CAS-24134]
- Citrix Analytics n'est pas en mesure de recevoir les événements de téléchargement de Citrix Content Collaboration. Par conséquent, les indicateurs de risque suivants ne sont pas déclenchés :
  - Téléchargement anonyme de partage sensible
  - Téléchargements de liens de partage excessifs
  - Accès excessif aux fichiers sensibles
  - Téléchargements excessifs de fichiers

  [CAS-29207]
- Pour les nouveaux utilisateurs intégrés, les actions manuelles et basées sur des stratégies appliquées aux indicateurs de risque Citrix Gateway n'ont aucun effet. [CAS-29029]
- Certains utilisateurs ne peuvent pas afficher les fiches de site sur la page Sources de données. Ce problème est résolu en remplissant à nouveau le cache. [CAS-28781]

09 janvier 2020

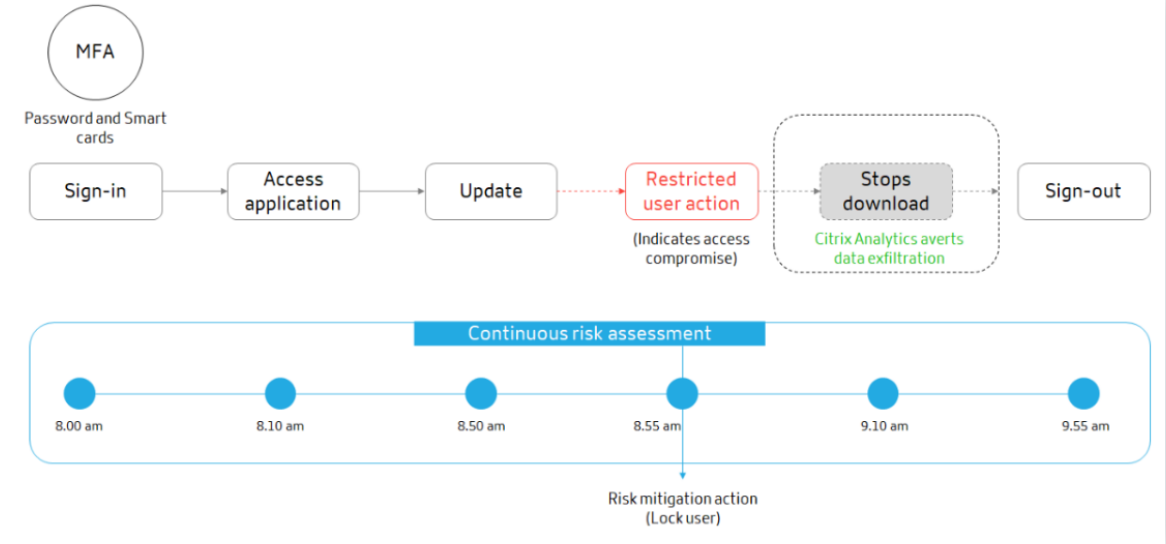
Nouvelles fonctionnalités

Évaluation continue des risques Parmi les défis auxquels les utilisateurs de Citrix Workspace sont confrontés, l'accès à distance expose les données sensibles à des risques de sécurité par le biais d'activités cybercriminelles telles que l'exfiltration de données, le vol, le vandalisme et les interruptions de service. Les employés au sein des organisations sont également susceptibles de contribuer à ces dommages.

Certains moyens de remédier à ces risques sont la mise en œuvre de l'authentification multifacteur, l'application de délais de connexion courts, etc. Bien que ces méthodes d'évaluation des risques garantissent un niveau de sécurité plus élevé, elles ne fournissent pas une sécurité complète après la validation initiale.

Pour améliorer l'aspect sécurité et garantir une meilleure expérience utilisateur, Citrix Analytics introduit la solution d'évaluation continue des risques. Cette solution vous aide à surveiller en permanence les profils des utilisateurs et à prendre diverses mesures lorsque des événements risqués sont détectés.

Pour plus d'informations, consultez la section Évaluation continue des risques.

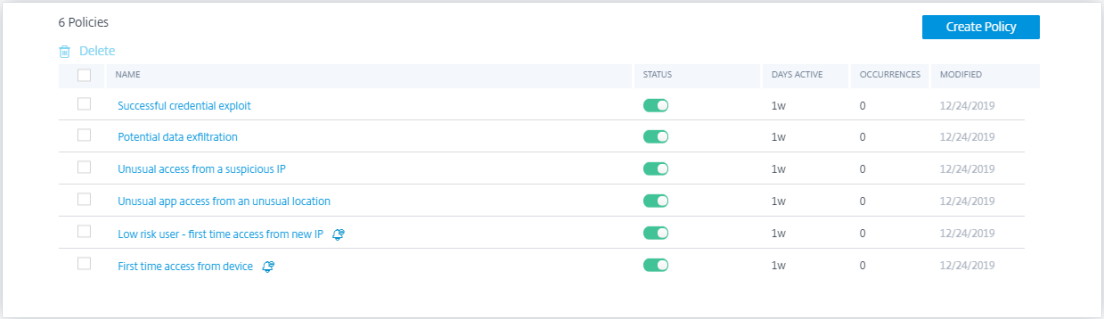


Configuration de la stratégie Citrix Analytics vous aide à gérer les configurations de stratégie plus efficacement. Vous pouvez protéger les comptes d'utilisateurs contre les attaques malveillantes à l'aide des fonctionnalités suivantes :

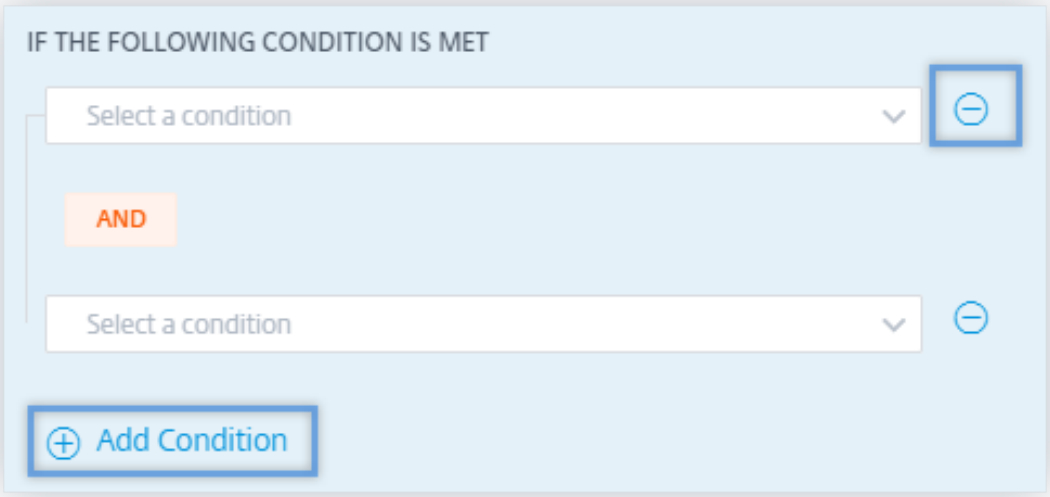
- **Stratégies par défaut** : Citrix Analytics prend en charge les stratégies par défaut suivantes :

- Exploitation réussie des informations d'identification
- Exfiltration potentielle des données
- Accès inhabituel à partir d'une adresse IP suspecte
- Accès inhabituel aux applications à partir d'un emplacement inhabituel
- Utilisateur à faible risque : premier accès à partir d'une nouvelle adresse IP
- Premier accès à partir de l'appareil

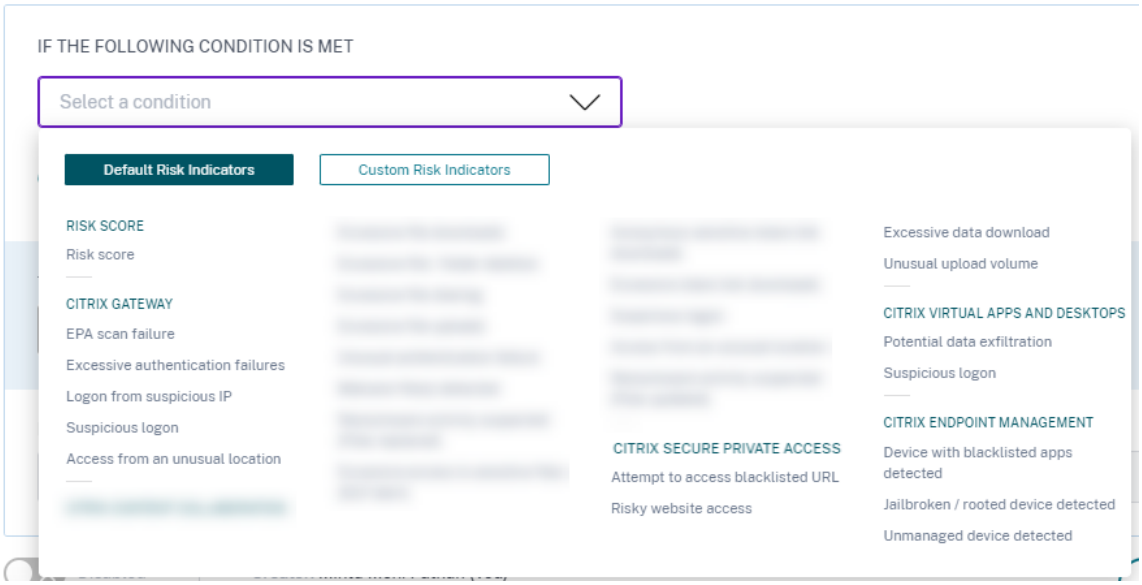
Vous pouvez modifier les stratégies par défaut en fonction de vos besoins.



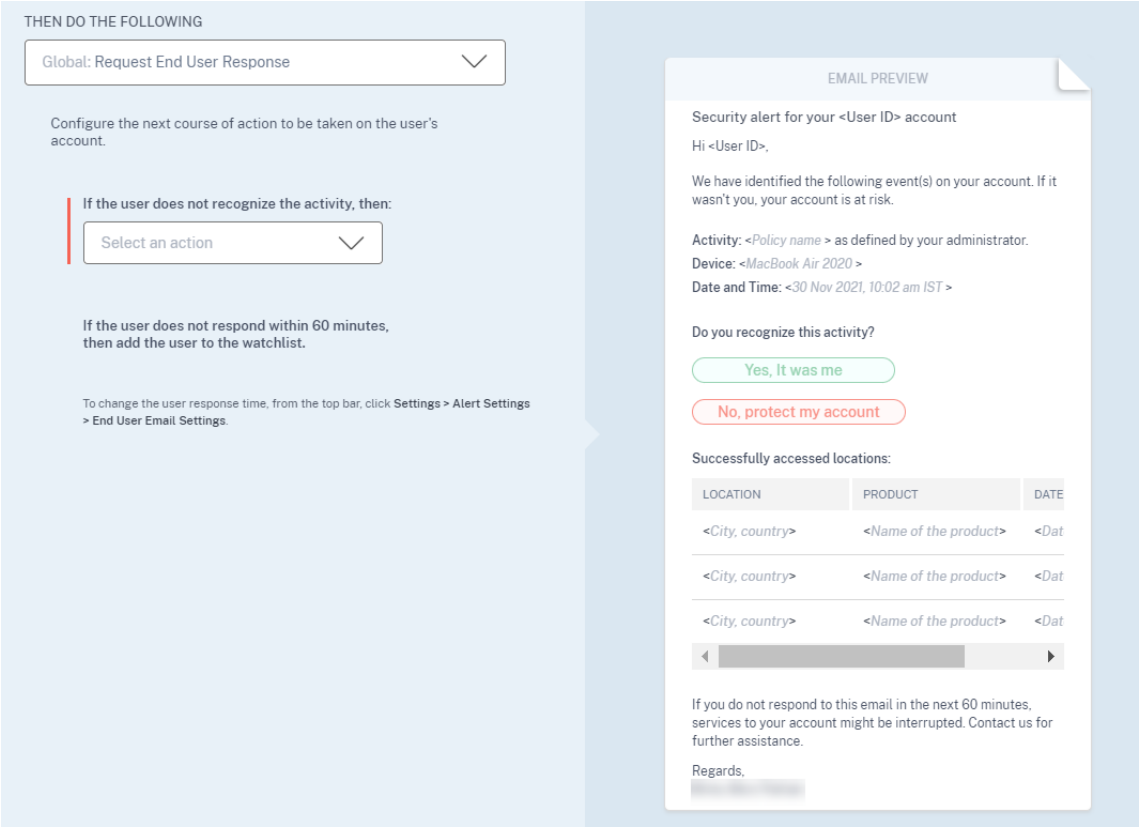
- **Conditions multiples** : une stratégie peut contenir jusqu'à quatre conditions. Les conditions peuvent être définies avec des combinaisons de scores de risque et d'indicateurs de risque, ou les deux.



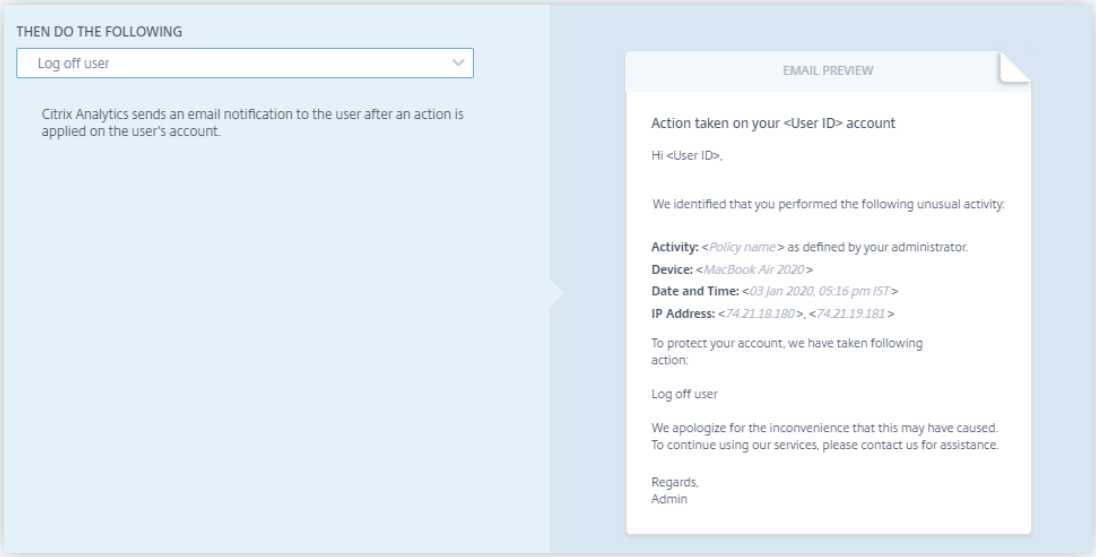
- **Indicateurs de risque par défaut et personnalisés** : Le menu des conditions de la page **Créer une stratégie** est désormais séparé en fonction des indicateurs de risque par défaut et personnalisés. Lorsque vous créez une stratégie, vous pouvez basculer entre les onglets des indicateurs de risque par défaut et personnalisés, et définir les conditions de l'indicateur de risque.



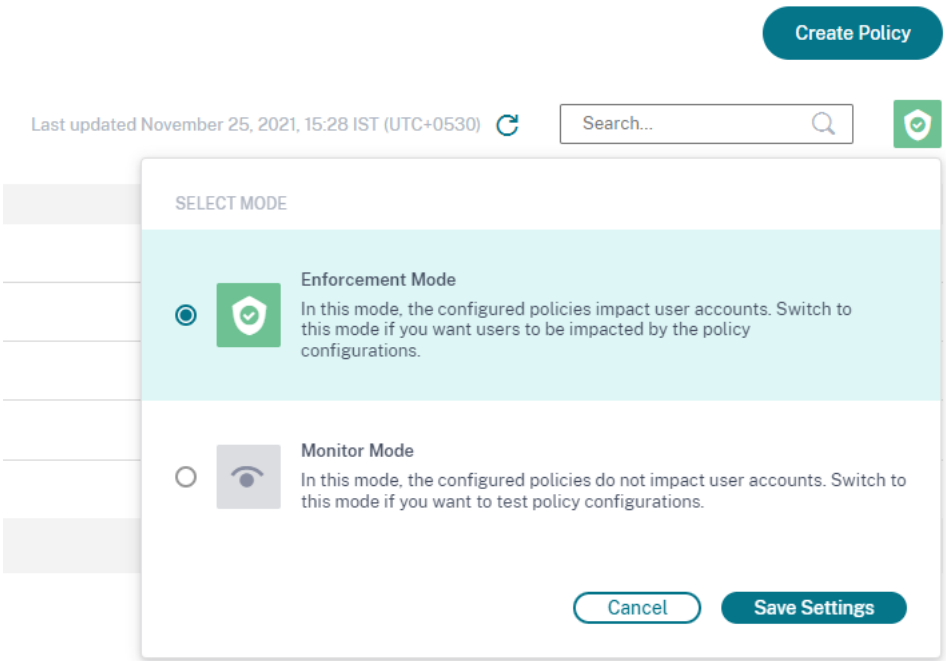
- **Demander une réponse de l'utilisateur final** : Citrix Analytics introduit l'action **Demander une réponse de l'utilisateur final** . Cette action vous permet d'envoyer une notification par e-mail à l'utilisateur concernant l'activité à risque détectée. Une fois que l'utilisateur répond à l'activité, vous pouvez déterminer le prochain plan d'action à prendre sur son compte. Vous pouvez également définir le temps de réponse de l'utilisateur. Si aucune réponse n'est reçue, Citrix Analytics considère **Aucune réponse** comme état.



- **Appliquer des actions perturbatrices** : Vous pouvez avertir les utilisateurs lorsqu'une action perturbatrice, telle que Fermer la **session de l'utilisateur** ou **Verrouiller l'utilisateur**, est appliquée. Une notification est envoyée à l'utilisateur avec les détails de l'activité et de l'action appliquée. Cette action interrompt temporairement les services du compte de l'utilisateur afin d'éviter toute autre utilisation abusive. Pour continuer à accéder au compte, l'utilisateur doit contacter l'administrateur pour obtenir de l'aide.



- **Modes d'application et de surveillance** : vous pouvez définir des modes d'application ou de surveillance pour vos stratégies.



Pour plus d'informations sur les améliorations apportées aux stratégies, consultez la section Stratégies et actions.

Verrouiller l'utilisateur et Déverrouiller les actions utilisateur Citrix Analytics introduit les actions de passerelle suivantes :

- Verrouiller l'utilisateur
- Déverrouiller l'utilisateur

Vous pouvez appliquer ces actions manuellement ou lorsque vous configurez des stratégies.

Pour plus d'informations, consultez la section Que sont les actions ?

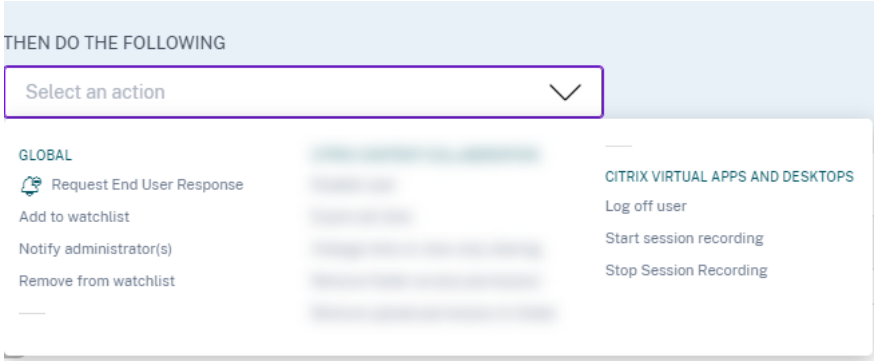
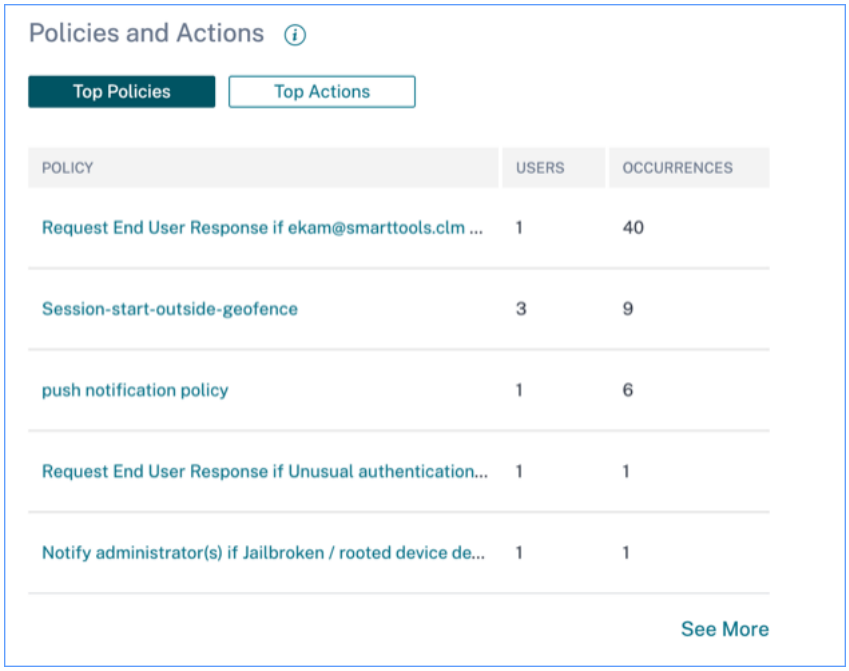


Tableau de bord de résumé des accès Citrix Analytics introduit le panneau **Résumé des accès** dans le tableau de bord **Utilisateurs** . Il récapitule le nombre total de tentatives effectuées par les utilisateurs pour accéder aux ressources au sein d'une organisation.

Pour plus d'informations, consultez la section Résumé des accès.

Tableau de bord Stratégies et actions Citrix Analytics introduit le panneau **Stratégies et actions** du tableau de bord **Utilisateurs** . Il affiche les cinq principales stratégies et actions appliquées aux profils utilisateur. Vous pouvez trier les données en fonction des principales stratégies et des principales actions pour une période sélectionnée.

Pour plus d'informations, consultez la section Stratégies et actions.



Recherche de stratégies en libre-service Utilisez la recherche en libre-service pour afficher les événements utilisateur qui respectent vos stratégies définies. Vous pouvez également afficher les actions qu'Analytics a appliquées pour ces événements anormaux. Utilisez les facettes et la zone de recherche pour rechercher les événements requis.

Pour afficher les événements, dans la zone de recherche, sélectionnez **Stratégies** dans la liste, sélectionnez la période, puis cliquez sur **Rechercher**.

Pour plus d'informations, consultez la section Recherche en libre-service de stratégies.

Fonctionnalités obsolètes

Condition basée sur la stratégie de changement de score de risque supprimée Lorsque vous configurez des stratégies, vous ne pouvez plus utiliser la condition basée sur la stratégie de **changement de score de risque** . Citrix Analytics ne prend pas en charge cette condition.

Pour plus d'informations, consultez la section Stratégies et actions.

Suppression de plusieurs actions basées sur des stratégies Lorsque vous configurez des stratégies, vous ne pouvez plus appliquer plusieurs actions. Citrix Analytics ne prend en charge qu'une seule action pour chaque stratégie.

Pour plus d'informations, consultez la section Stratégies et actions.

Problèmes résolus

- Les administrateurs délégués en lecture seule rencontrent une erreur lors de l'accès aux tableaux de bord **Accès utilisateur** et **Accès aux applications** . [CAS-16297]

12 décembre 2019

Nouvelles fonctionnalités

Prise en charge des versions Splunk Citrix Analytics prend en charge les versions suivantes de Splunk :

- **Splunk 8.0 64 bits**
- **Splunk 7.3 64 bits**

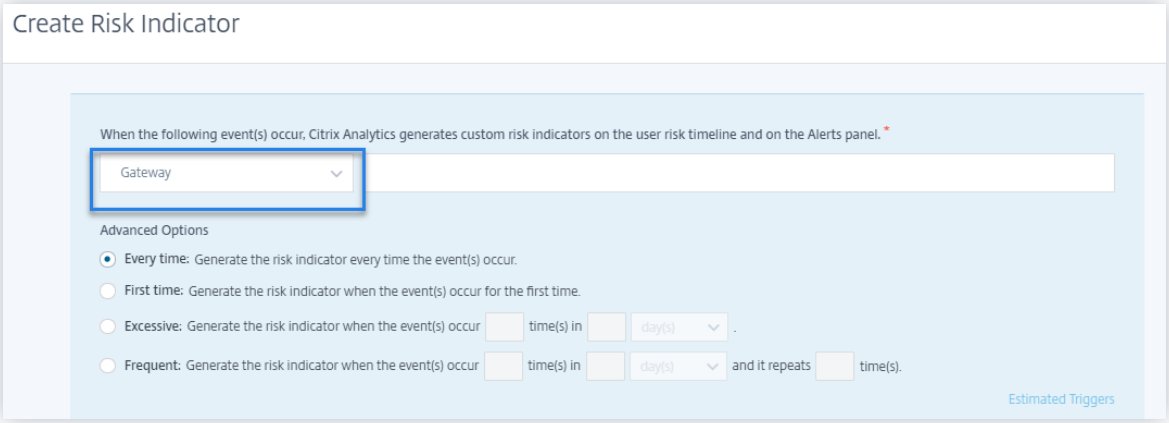
Pour bénéficier des avantages de sécurité maximaux de l'intégration de Splunk, effectuez une mise à niveau vers la dernière version de l'application complémentaire Splunk à partir de la page de téléchargement .

Pour plus d'informations sur les versions Splunk prises en charge, consultez Versions prises en charge.

04 décembre 2019

Nouvelles fonctionnalités

Indicateur de risque personnalisé pour Citrix Gateway À l'aide d'indicateurs de risque personnalisés, vous pouvez désormais définir les conditions et la fréquence de déclenchement des indicateurs de risque pour les événements Citrix Gateway. Lorsqu'un événement utilisateur remplit les conditions, Analytics déclenche les indicateurs de risque. Pour plus d'informations sur la création d'indicateurs de risque personnalisés, voir Indicateurs de risque personnalisés.

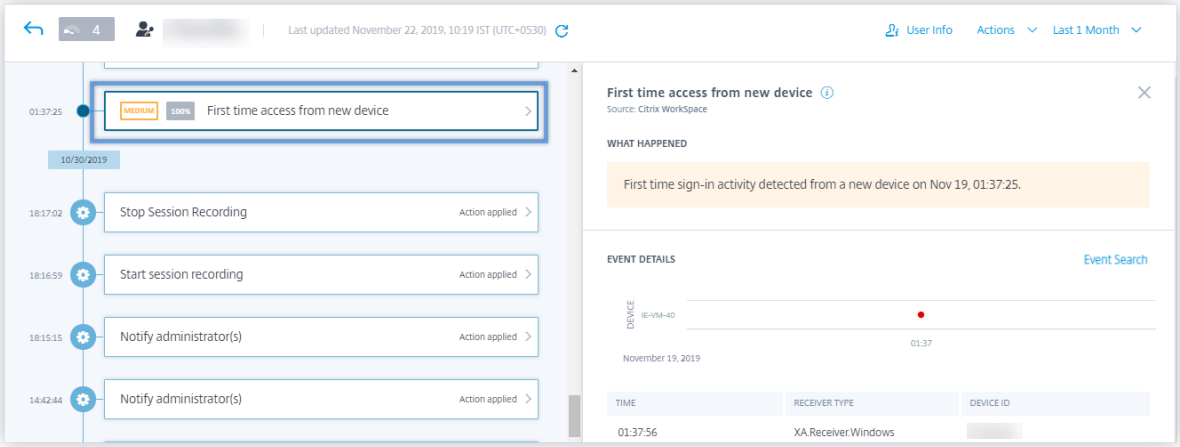


22 novembre 2019

Nouvelles fonctionnalités

Premier accès depuis un nouvel appareil : indicateur de risque Citrix Virtual Apps and Desktops Citrix Analytics détecte les menaces d'accès en fonction de l'accès à partir d'un nouvel appareil et déclenche l'indicateur de risque correspondant.

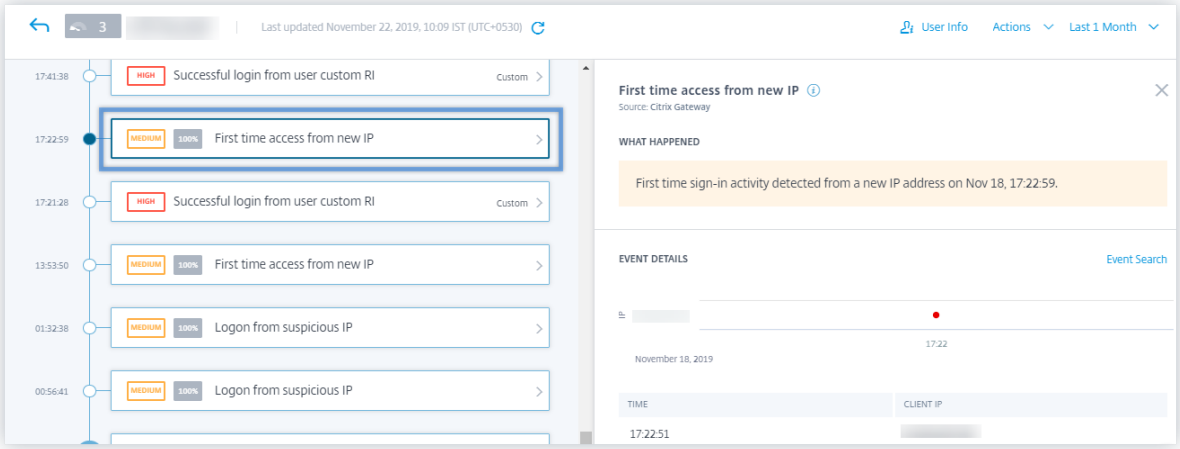
L'indicateur **de risque Premier accès à partir d'un nouvel appareil** est déclenché lorsqu'un utilisateur se connecte à partir d'un appareil après 90 jours. Cet événement est déclenché car Citrix Receiver n'a pas d'enregistrement de connexion à partir de cet appareil nouveau ou inconnu au cours des 90 derniers jours. Pour plus d'informations, consultez les sections Indicateurs de risque Citrix Virtual Apps and Desktops et Citrix DaaS.



Premier accès à partir d'une nouvelle adresse IP - indicateur de risque Citrix Gateway Citrix Analytics détecte les menaces d'accès en fonction de l'accès à partir d'une nouvelle adresse IP et déclenche l'indicateur de risque correspondant.

Le **premier accès à partir d'un nouvel indicateur de risque IP** est déclenché lorsqu'un utilisateur se connecte à partir d'une adresse IP après 90 jours. Cet événement est déclenché car Citrix Receiver n'a pas d'enregistrement de connexion à partir de la nouvelle adresse IP ou de l'adresse IP inconnue au cours des 90 derniers jours.

Pour plus d'informations, consultez la section Indicateurs de risque Citrix Gateway.



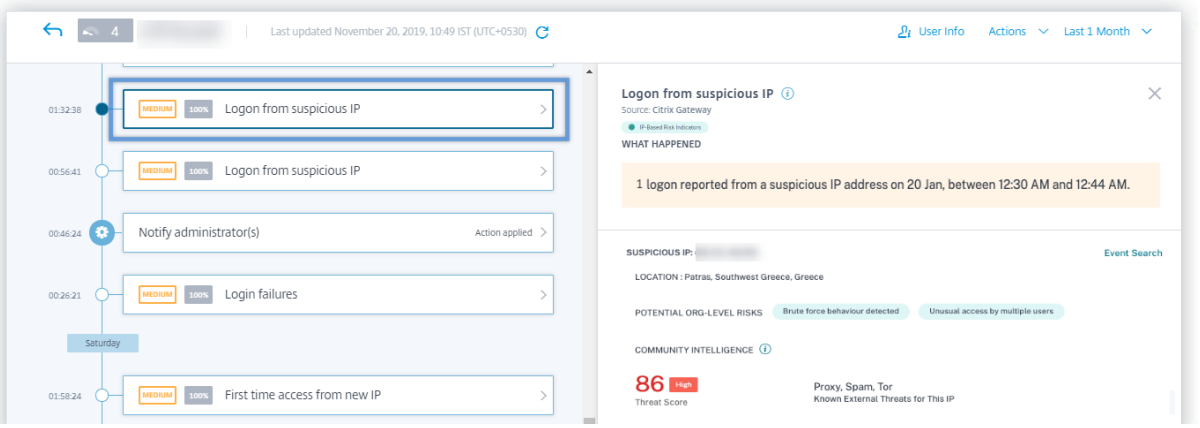
Ouverture de session à partir d'une adresse IP suspecte - indicateur de risque Citrix Gateway Citrix Analytics détecte les menaces d'accès des utilisateurs en fonction de l'activité de connexion IP suspecte et déclenche l'indicateur de risque d'ouverture de **session à partir d'adresses IP suspectes** .

Cet indicateur de risque est déclenché lorsqu'un utilisateur tente d'accéder au réseau à partir d'une

adresse IP suspecte. Analytics considère qu'une adresse IP est suspecte en fonction de l'une des conditions suivantes :

- Est répertorié dans le flux externe sur la détection des menaces IP
- A plusieurs enregistrements de connexion utilisateur à partir d'un emplacement inhabituel
- Contient des tentatives de connexion excessives qui peuvent indiquer une attaque par force brute

Pour plus d'informations, consultez la section Indicateurs de risque Citrix Gateway.



Recherche en libre-service des événements Citrix Gateway Utilisez la fonctionnalité de recherche en libre-service pour obtenir un aperçu des événements utilisateur reçus de la source de données Citrix Gateway. Citrix Analytics reçoit des événements tels que l'étape d'authentification, le type d'autorisation, le code de session VPN et l'état de la session VPN pour les utilisateurs de Citrix Gateway. Utilisez les facettes et la zone de recherche pour rechercher les événements requis et explorer les données sous-jacentes.

Pour afficher les événements, dans la zone de recherche, sélectionnez **Passerelle** dans la liste, sélectionnez la période, puis cliquez sur **Rechercher**.

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

Recherche en libre-service pour les événements Citrix Remote Browser Isolation Utilisez la fonction de recherche en libre-service pour obtenir un aperçu des événements de navigation reçus du service Citrix Remote Browser Isolation. Citrix Analytics reçoit des événements tels que la connexion de session, le lancement de session, les applications publiées, les applications supprimées pour chaque connexion utilisateur. Utilisez la zone de recherche pour rechercher les événements requis et explorer les données sous-jacentes.

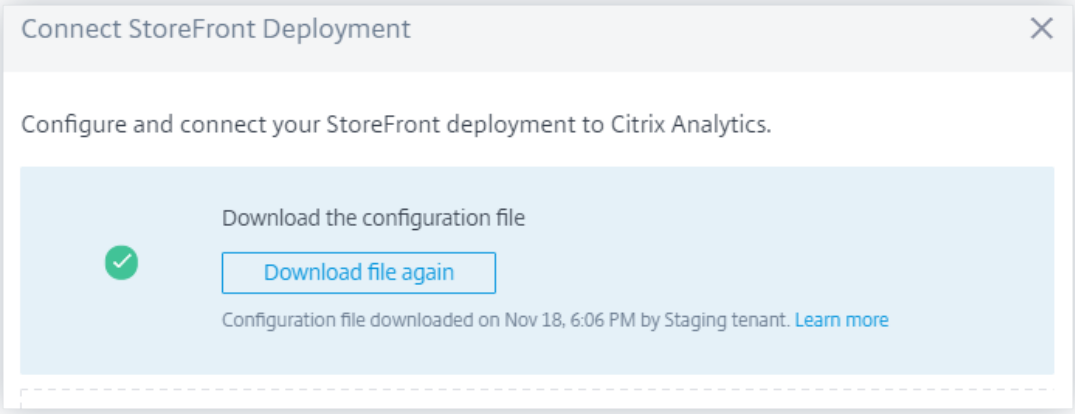
Pour afficher les événements, dans la zone de recherche, sélectionnez **Remote Browser Isolation** dans la liste, sélectionnez la période, puis cliquez sur **Rechercher**.

Pour plus d'informations, voir Recherche en libre-service pour Remote Browser Isolation.

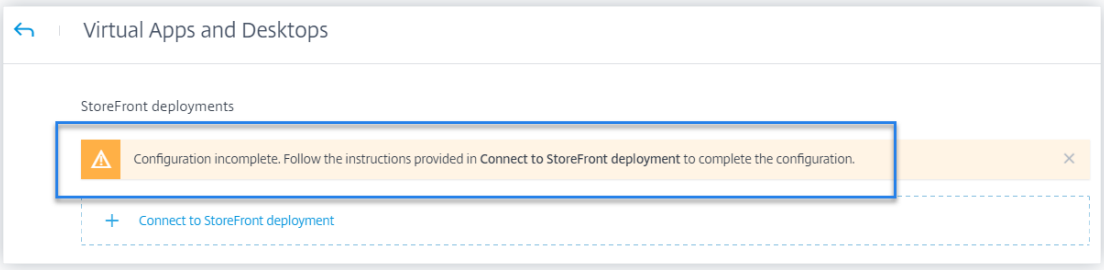
Action Supprimer de la liste de surveillance Vous pouvez supprimer un utilisateur de la liste de suivi en appliquant la méthode manuelle ou en appliquant une méthode basée sur des stratégies. Pour plus d'informations, consultez la section Liste de suivi.

Messages d'intégration améliorés lors de la configuration d'un déploiement StoreFront Citrix Analytics fournit désormais les messages suivants pour vous aider à configurer vos déploiements StoreFront :

- Après avoir téléchargé le fichier de configuration, vous pouvez voir un message indiquant la date et l'heure du téléchargement et le nom d'utilisateur. Lorsque vous actualisez cette page, le bouton **Télécharger le fichier** se transforme à **nouveau en Télécharger le fichier**.



- Si votre configuration StoreFront est incomplète, un message d'avertissement s'affiche pour vous demander de suivre les étapes de configuration et de connecter votre déploiement StoreFront à Analytics.



Pour plus d'informations sur la façon de configurer votre déploiement StoreFront, consultez Sites locaux Citrix Virtual Apps and Desktops intégrés à l'aide de StoreFront.

Fonctionnalités obsolètes

Indicateur de risque - Suppression de l'accès depuis un nouvel appareil Citrix Analytics ne déclenche plus l'indicateur de risque **Access from new device** . Toutefois, sur le tableau de bord utilisateur, la chronologie utilisateur et le tableau de bord des stratégies, vous pouvez afficher les données historiques liées à cet indicateur de risque.

Pour les stratégies créées précédemment en fonction de l'**accès à partir d'un nouvel appareil**, vous devez modifier la stratégie ou créer une stratégie avec le nouvel indicateur de risque **Premier accès depuis un nouvel appareil**.

Problèmes résolus

- La recherche d'authentification en libre-service ne parvient pas à afficher les événements. [CAS-24959]

08 novembre 2019

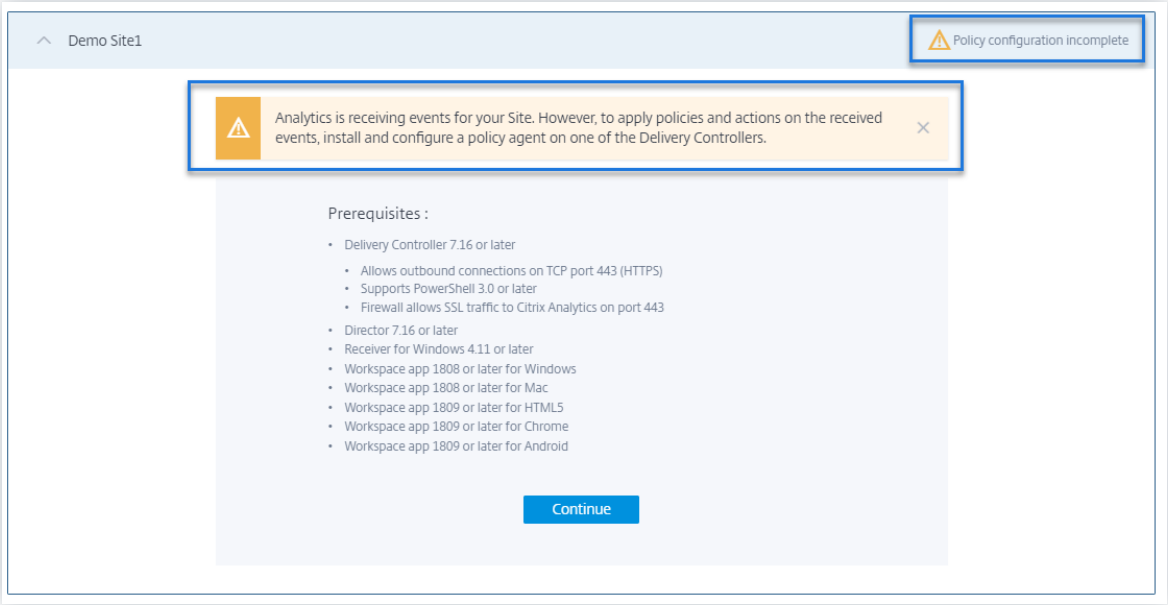
Problèmes résolus

- Pour les indicateurs de risque Citrix Content Collaboration, les utilisateurs ne peuvent pas appliquer d'actions sur la chronologie des risques. [CAS-24844]
- L'application Citrix Workspace pour Chrome antérieure à la version 1911 ne parvient pas à envoyer les détails de l'événement à Citrix Analytics. [CAS-24938]

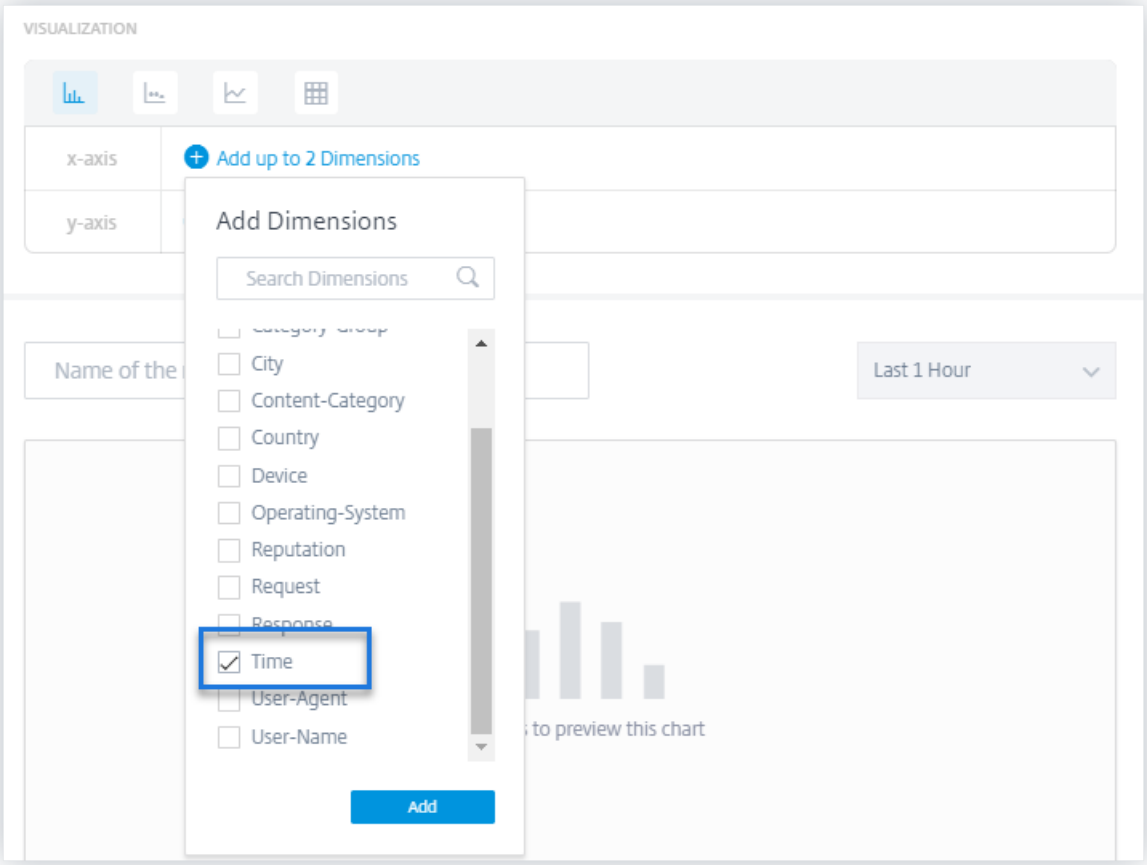
21 octobre 2019

Nouvelles fonctionnalités

Nom modifié de l'agent analytique Le nom de l'agent est désormais mentionné en tant qu'**agent de stratégie Analytics** sur les interfaces utilisateur pour indiquer son rôle. Lors de l'intégration des sources de données Citrix Virtual Apps and Desktops locales, Citrix Analytics indique clairement qu'un agent de stratégie est nécessaire uniquement pour configurer des stratégies et des actions pour votre site. Cet agent n'a aucun rôle dans la transmission des données depuis la source de données. Pour plus d'informations, consultez Citrix Virtual Apps and Desktops et Source de données Citrix DaaS.



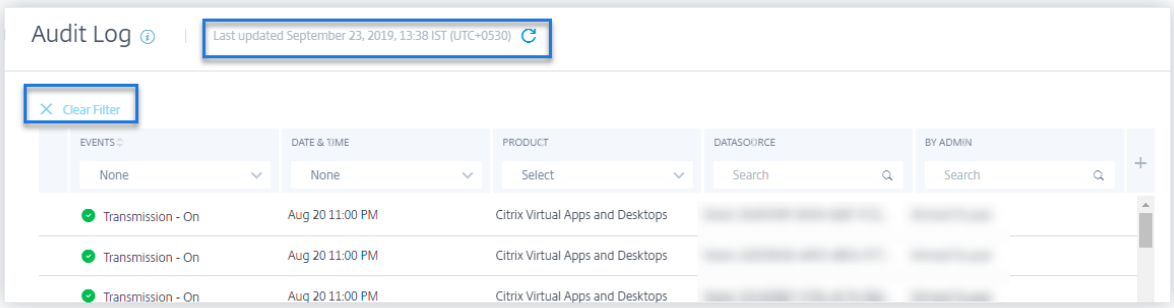
Prise en charge de la dimension temporelle pour le rapport personnalisé Vous pouvez désormais regrouper les événements en fonction du temps en sélectionnant la dimension **Temps** de l'axe X. Le rapport affiche le nombre total d'événements reçus en fonction des intervalles de temps pour la période sélectionnée. Pour plus d'informations sur la création de rapports, consultez la section Rapports personnalisés.



Améliorations apportées aux journaux d'audit L'expérience utilisateur de la page **Journal d'audit** est améliorée.

- Vous pouvez afficher les détails de la date et de l'heure de la dernière mise à jour de la page **Journal d'audit** et actualiser la page pour afficher les derniers journaux d'audit.
- Vous pouvez effacer tous les filtres appliqués aux journaux d'audit.

Pour plus d'informations sur les données d'audit, consultez Journaux d'audit.



Problèmes résolus

- Citrix Analytics n'est pas en mesure de générer l'indicateur de risque d'**adresse IP anonyme** même si Microsoft Graph Security est correctement intégré. [CAS-21329]
- L'application Citrix Workspace pour HTML5 antérieure à la version 1910 ne parvient pas à envoyer les détails de l'événement à Citrix Analytics. [CAS-24938]

23 septembre 2019

Problèmes résolus

- Sur les fiches de site des sources de données, le champ **Dernier événement** affiche des informations de date et d'heure incorrectes. [CAS-24087]

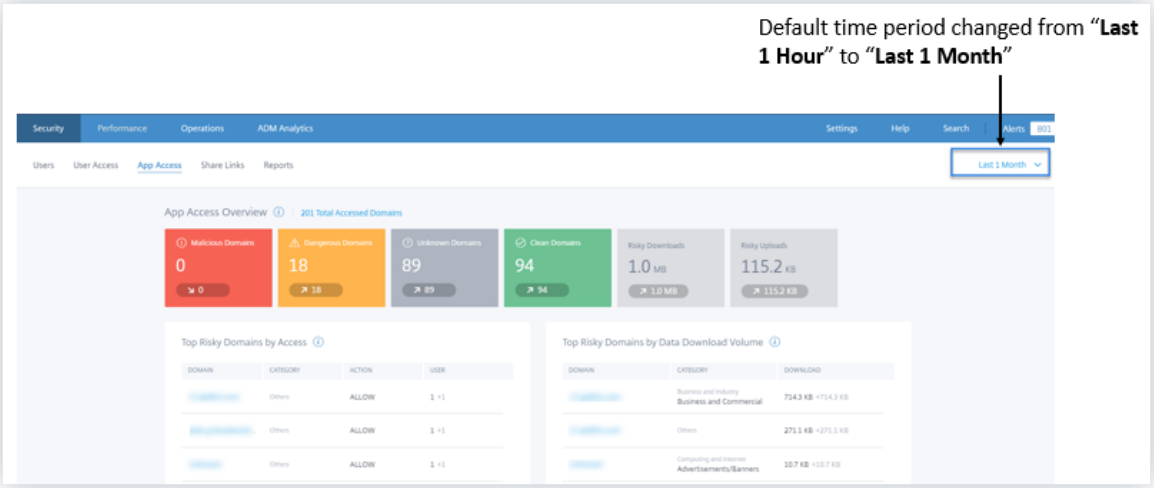
30 août 2019

Nouvelles fonctionnalités

Modification de la période par défaut dans les tableaux de bord La période par défaut des tableaux de bord suivants passe de la **dernière heure** au **dernier mois** :

- Utilisateurs
- Chronologie des risques
- Accès utilisateur
- Accès aux applications
- Partager des liens
- Historique des alertes

Les tableaux de bord affichent désormais les événements du dernier mois par défaut. Vous bénéficiez d'une expérience plus attrayante en utilisant ces tableaux de bord. Par exemple, lorsque vous ouvrez le tableau de bord **App Access**, le tableau de bord affiche par défaut les événements d'accès aux applications du dernier mois.



Problèmes résolus

- Pour les indicateurs de risque de Content Collaboration, l'action **Désactiver la stratégie utilisateur** ne peut pas être appliquée correctement. [CAS-17304]
- Citrix Analytics ne peut pas traiter les événements de Citrix Gateway 13.0. Ce problème se produit car Citrix Gateway 13.0 ne parvient pas à fournir les noms d'utilisateur dans les événements d'ouverture de session envoyés à Citrix Analytics. [CAS-21339]

20 août 2019

Nouvelles fonctionnalités

Améliorations de la recherche en libre-service

- L'expérience utilisateur de la page en libre-service est améliorée. Vous pouvez désormais basculer en toute transparence entre la chronologie des risques utilisateur et la page de recherche en libre-service.
- Vous pouvez désormais trier vos événements par heure. Par défaut, les derniers événements apparaissent en premier dans le tableau des événements. Cliquez sur l'icône de tri dans la colonne **TIME** pour trier les événements en fonction de l'heure la plus récente ou de la première heure.

Pour plus d'informations sur l'utilisation de la recherche en libre-service, consultez la rubrique Recherche en libre-service.

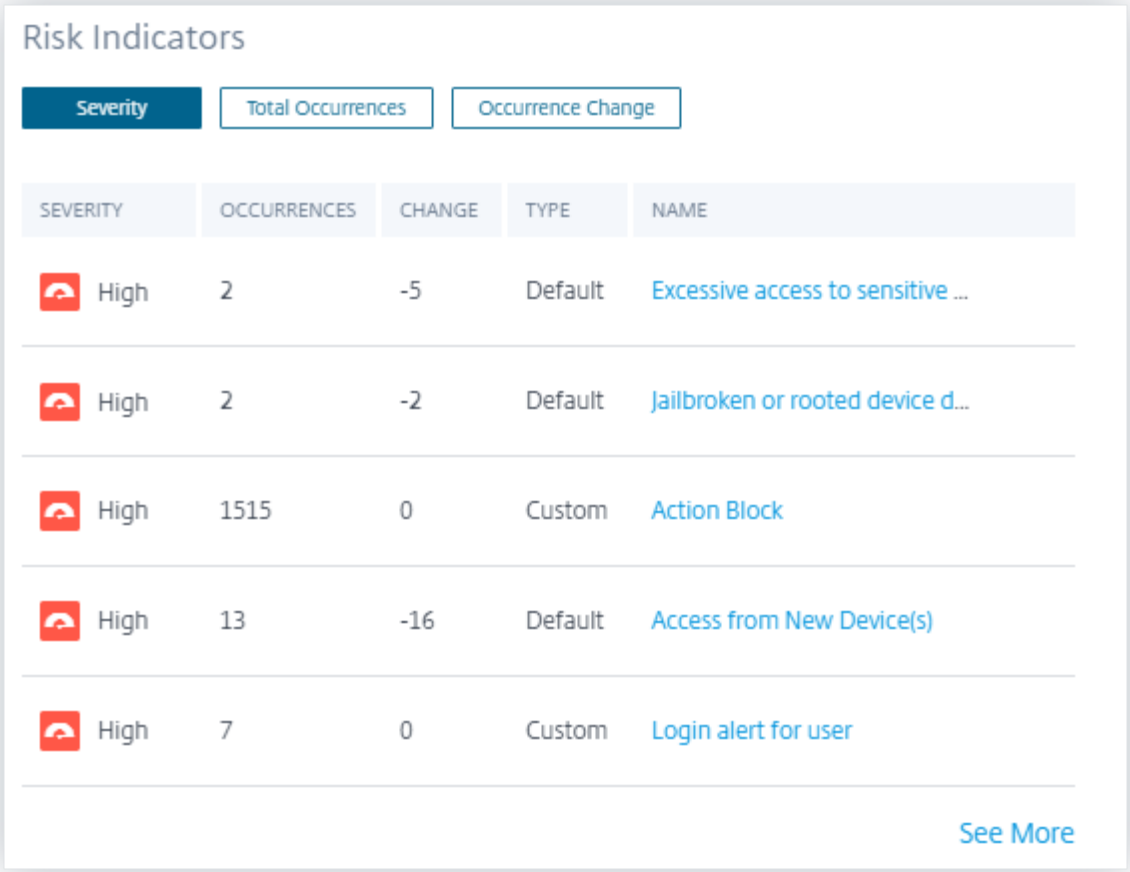
Améliorations des rapports personnalisés

- De nouvelles dimensions sont ajoutées pour les sources de données Contrôle d'accès, Content Collaboration et Apps and Desktops. Vous pouvez choisir ces dimensions pour créer des rapports. Les dimensions suivantes sont ajoutées pour les sources de données :
  - **Contrôle d'accès** : agent utilisateur, nom d'utilisateur
  - **Content Collaboration contenu** : e-mail de l'utilisateur, nom d'utilisateur, créé par, ID de compte, ID client OAuth, ID d'événement, ID de dossier, nom de dossier, ID de ressource, ID de formulaire, adresse IP du client
  - **Applications et postes de travail** : nom d'utilisateur, adresse IP, identifiant de l'appareil, prison interrompue, type de lancement de session, nom du serveur de session, nom d'utilisateur de la session, nom du fichier de téléchargement, chemin du fichier de téléchargement, nom de l'imprimante d'impression, nom du fichier des détails de la tâche d'impression, URL de lancement de l'application SaaS, opération du presse-papiers, résultat des détails
- L'interface utilisateur du rapport personnalisé est améliorée avec la prise en charge de la pagination et une option **Effacer tout** pour les filtres.

Pour plus d'informations sur la création d'un rapport personnalisé à l'aide de ces dimensions, consultez la section Rapports personnalisés.

Tableau de bord des indicateurs de risque Le tableau de bord **des indicateurs de risque** est présenté sur la page **Utilisateurs** . Il résume les cinq principaux indicateurs de risque par défaut et personnalisés pour un utilisateur. Un lien Voir plus vous redirige vers la page **Aperçu de l'indicateur de risque** . Cette page fournit des informations détaillées sur les indicateurs de risque générés pour une période sélectionnée.

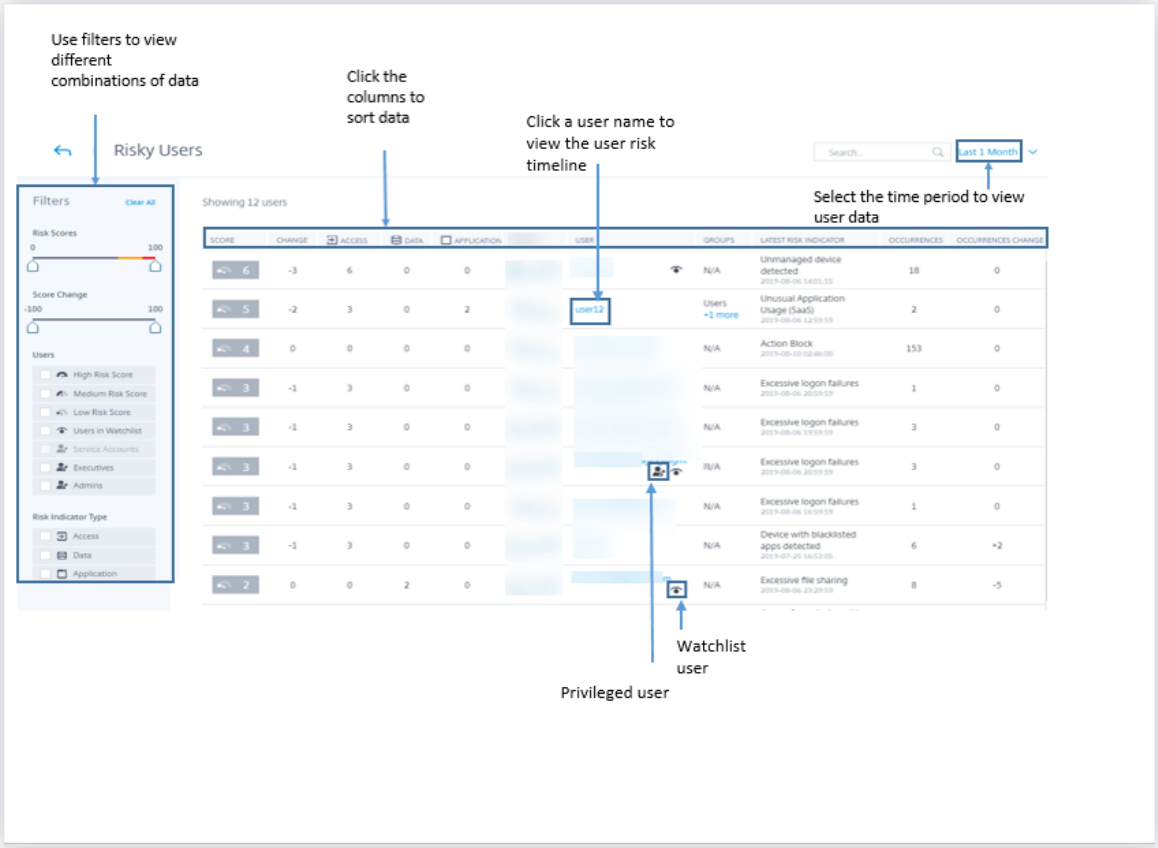
Pour plus d'informations, consultez Tableau de bord des utilisateurs.



Améliorations du tableau de bord des utilisateurs risqués Citrix Analytics introduit les onglets **Indicateurs** de **risque et Changement des indicateurs** de risque dans le tableau de bord **Utilisateurs risqués** . Vous pouvez consulter les cinq principaux utilisateurs à risque en fonction de ces onglets. Le tableau de bord présente également la colonne **Indicateurs de risque** . Il indique le nombre d'indicateurs de risque pour un utilisateur.

La page **Utilisateurs risqués** présente les colonnes **Occurrences** et **Occurrences Change** . Ces colonnes résument le nombre total d'occurrences et la modification des occurrences des indicateurs de risque personnalisés et par défaut.

Pour plus d'informations, consultez Tableau de bord des utilisateurs.



Indicateur de risque de lien de partage - Téléchargements excessifs Citrix Analytics détecte les menaces d'accès en fonction des téléchargements excessifs sur un lien de partage et déclenche l'indicateur de risque de **téléchargements excessifs** . En identifiant les liens de partage présentant des téléchargements excessifs, en fonction du comportement précédent, vous pouvez surveiller le lien de partage pour détecter les attaques potentielles. Cet indicateur de risque vous aide à identifier une activité excessive de téléchargement de fichiers.

Pour plus d'informations, consultez la section Téléchargements excessifs.

Recherche en libre-service des données d'authentification Utilisez la recherche en libre-service pour obtenir des informations sur les événements d'authentification. Citrix Analytics reçoit les événements d'authentification tels que la connexion utilisateur, la fermeture de session utilisateur et la mise à jour du client à partir du service Identity and Access Management de Citrix Cloud. La recherche fournit un rapport détaillé sur les événements d'authentification, vous aide à identifier les problèmes d'authentification et à les résoudre. Vous pouvez également définir une requête de recherche pour récupérer les événements qui correspondent à vos critères définis.

Pour afficher les événements, sélectionnez **Authentification** dans la liste, sélectionnez la période,

puis cliquez sur **Rechercher**.

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

11 Juillet 2019

Nouvelles fonctionnalités

Indicateurs de risque personnalisés Les indicateurs de risque par défaut générés par Citrix Analytics sont basés sur des algorithmes de machine learning. Citrix Analytics vous permet désormais de créer des indicateurs de risque personnalisés. En fonction des événements utilisateur, vous pouvez définir les conditions et créer des indicateurs de risque personnalisés.

Lorsque les conditions définies sont remplies, Citrix Analytics génère des indicateurs de risque personnalisés similaires aux indicateurs de risque par défaut, et les affiche sur la chronologie des risques de l'utilisateur. Les indicateurs de risque personnalisés sont désignés par une étiquette sur la chronologie des risques de l'utilisateur.

Pour plus d'informations, consultez la section Indicateurs de risque personnalisés.

Statut privilégié sur la chronologie des risques

La chronologie des risques utilisateur affiche les événements suivants chaque fois qu'il y a un changement dans le statut du privilège Admin ou Executive d'un utilisateur :

- Ajouté au groupe Executive
- Supprimé du groupe Exécutif
- Privilège élevé au rang d'administrateur
- Privilège d'administrateur supprimé

Lorsqu'un indicateur de risque est déclenché pour un utilisateur, vous pouvez le mettre en corrélation avec l'événement de changement de statut de privilège spécifié. Si nécessaire, vous pouvez appliquer les actions appropriées sur le profil utilisateur.

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

Action d'expiration du lien de partage

Citrix Analytics vous permet d'appliquer des actions sur les indicateurs de risque de lien de partage. Actuellement, l'action prise en charge est **Expire le lien de partage**.

Pour plus d'informations, consultez la section Indicateurs de risque de lien de partage Citrix.

Améliorations de la recherche en libre-service

- **Prise en charge du caractère joker * dans la requête de recherche** : Utilisez l'astérisque (*) dans votre requête de recherche pour correspondre à n'importe quel caractère zéro ou plusieurs fois. Par exemple, la requête de recherche User-Name = « John* » affiche les événements pour tous les noms d'utilisateurs commençant par John.
- **Ajout de l'option Effacer tout pour les facettes** : cliquez sur **Effacer**tout pour supprimer toutes les facettes sélectionnées à la fois.
- **Afficher les données de colonne masquées dans la liste des événements** : après avoir supprimé une colonne de la table des événements, vous pouvez afficher les données correspondantes dans la liste des événements utilisateur. Développez la ligne d'événement d'un utilisateur et affichez les données.

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

État des erreurs de données sur les fiches de site

Les fiches de site affichent l'étiquette **Aucune donnée reçue** en rouge lorsque Citrix Analytics ne reçoit pas d'événements de la dernière heure de la source de données. Il affiche également le nombre d'événements reçus et est lié à la page de recherche en libre-service correspondante. Cette fonctionnalité vous permet d'afficher les événements correspondants sur la page de recherche en libre-service et de rechercher tout problème de transmission de données.

> **Remarque**
>
> Actuellement, la recherche en libre-service n'est disponible que pour les sources de données Access, Content Collaboration et Apps and Desktop.

Pour plus d'informations, consultez la section Activer Analytics sur les sources de données Citrix.

Problèmes résolus

- Pour la source de données Access Control, le nombre d'événements sur la fiche de site ne correspond pas aux résultats de la recherche en libre-service. [CAS-18286]

19 juin 2019

Problèmes résolus

- La page **Journal d'audit** affiche l'état Activé ou désactivé de la transmission de données chaque fois que la source de données Active Directory est découverte. [CAS-17575]

- Le menu de période du tableau de bord **Utilisateurs** ne se charge pas correctement. Il affiche un message d'erreur de délai d'expiration. [CAS-19467]
- Les utilisateurs reçoivent un message d'erreur sur Citrix Analytics lorsqu'ils se connectent à un client depuis Splunk. Il arrive parfois que l'intégration de nouvelles sources de données échoue. [CAS-19429]

17 juin 2019

Nouvelles fonctionnalités

Configuration du StoreFront

Si votre organisation utilise StoreFront local, vous pouvez désormais configurer StoreFront pour qu'il se connecte à Citrix Analytics. La configuration est effectuée à l'aide d'un fichier de configuration importé depuis Citrix Analytics. Une fois la configuration terminée, l'application Citrix Workspace envoie des événements utilisateur à Citrix Analytics pour générer des informations exploitables sur les comportements des utilisateurs. Les informations vous aident à détecter tout comportement anormal des utilisateurs et à gérer de manière proactive les menaces de sécurité au sein de votre organisation. Pour plus d'informations, consultez Sites locaux Citrix Virtual Apps and Desktops intégrés à l'aide de StoreFront.

30 mai 2019

Nouvelles fonctionnalités

Échecs d'ouverture de session excessifs

Citrix Analytics détecte les menaces d'accès en fonction d'une activité d'ouverture de session excessive et déclenche l'indicateur de risque d'échecs de connexion excessifs. Cet indicateur de risque est déclenché lorsqu'un utilisateur rencontre plusieurs tentatives d'ouverture de session échouées pour accéder à Content Collaboration. En identifiant les utilisateurs présentant des échecs de connexion excessifs, en fonction du comportement précédent, les administrateurs peuvent surveiller le compte de l'utilisateur pour détecter les attaques par force brute.

> **Remarque**
>
> **Les échecs d'ouverture de session excessifs** sont désormais renommés en tant qu'**échecs d'authentification excessifs**.

Problèmes résolus

- Pour certains événements utilisateur transmis par les applications Citrix Workspace, la source de données est incorrectement identifiée comme Endpoint Management au lieu de Citrix Virtual Apps and Desktops.

  [CAS-17323]

- Le chargement du tableau de bord **Utilisateurs** est long pour la période du **dernier mois** . Ce problème se produit lorsque le nombre d'utilisateurs est élevé. Dans certains cas, vous pouvez même rencontrer des erreurs 601.

  [CAS-16300]

- Citrix Content Collaboration n'est pas découvert en tant que source de données, bien que certains utilisateurs s'abonnent au service sur Citrix Cloud.

  [CAS-16299]

09 mai 2019

Nouvelles fonctionnalités

Création de rapports personnalisés

Vous pouvez désormais créer des rapports personnalisés en fonction de vos besoins opérationnels. Citrix Analytics fournit une liste de dimensions et de mesures en fonction de la source de données sélectionnée. Choisissez les paramètres requis et les types de visualisation tels que le graphique à barres, le graphique d'événements, le graphique en courbes ou le tableau pour créer vos rapports. La création de rapports vous aide à organiser et à analyser graphiquement vos données.

Pour créer un rapport personnalisé, dans l'onglet **Sécurité**, cliquez sur **Rapports** > **Créer un rapport**. Pour afficher les rapports que vous avez créés précédemment, dans l'onglet **Sécurité**, cliquez sur **Rapports**. Pour plus d'informations, consultez la section Rapports personnalisés.

Surveillance des utilisateurs privilégiés

Citrix Analytics vous permet de surveiller de près les anomalies de comportement des utilisateurs privilégiés d'une organisation. Les utilisateurs privilégiés étant très vulnérables aux menaces de sécurité, il devient difficile de distinguer leurs activités quotidiennes des activités malveillantes. Par conséquent, les activités malveillantes des utilisateurs privilégiés restent longtemps inaperçues. Cette fonctionnalité vous permet de surveiller de manière proactive ces activités et de prendre les mesures appropriées sur les comptes d'utilisateurs appropriés. Les utilisateurs privilégiés sont représentés par une icône dans le tableau de bord **Utilisateurs** .

Citrix Analytics prend en charge la surveillance des types d'utilisateurs privilégiés suivants :

- **Admins** : utilisateurs auxquels des privilèges d'administrateur sont attribués par le service Citrix respectif. Actuellement, Citrix Analytics prend en charge la surveillance des utilisateurs privilégiés pour les utilisateurs disposant de privilèges d'administrateur dans le service Content Collaboration.
- **Executives** : sur Citrix Analytics, vous pouvez marquer un groupe AD en tant que groupe Executives. Le fait de marquer un groupe AD en tant que groupe exécutif fait de tous les utilisateurs du groupe des utilisateurs privilégiés. S'il n'est pas nécessaire de prendre en charge davantage les anomalies de comportement des utilisateurs d'un groupe AD, vous pouvez supprimer le groupe en tant que groupe exécutif.

Pour plus d'informations, consultez la section Utilisateurs privilégiés.

Récapitulatif hebdomadaire des courriels

Citrix Analytics envoie un e-mail hebdomadaire aux administrateurs pour résumer les risques de sécurité dans l'environnement informatique de leur entreprise. La notification par e-mail est envoyée tous les mardis aux administrateurs et elle met en évidence les événements de sécurité survenus la semaine précédente. Cet e-mail garantit que les administrateurs sont informés des risques de sécurité sans se connecter à Citrix Analytics. Pour plus d'informations, consultez la section Résumé hebdomadaire des e-mails.

26 avril 2019

Nouvelles fonctionnalités

Administrateurs délégués

Citrix Analytics prend désormais en charge les rôles d'administrateur délégué. Cette fonctionnalité vous permet d'inviter d'autres administrateurs sur votre compte Citrix Cloud afin de gérer Citrix Analytics pour votre organisation. Si vous êtes un administrateur Citrix Analytics avec une autorisation d'accès complet, vous pouvez ajouter d'autres administrateurs à votre compte Citrix Cloud. Ces administrateurs supplémentaires sont appelés administrateurs délégués. Vous pouvez actuellement attribuer un accès en lecture seule aux administrateurs délégués. Pour plus d'informations, consultez la section Administrateurs délégués.

Problèmes résolus

Peu d'indicateurs de risque pour les sources de données qui utilisent le flux de données ne génèrent pas d'alertes. Vous ne recevez aucune notification d'alerte et les actions basées sur des stratégies ne sont pas appliquées automatiquement si l'un des indicateurs de risque suivants est déclenché :

- **Indicateurs de risque Citrix Endpoint Management** : appareil non géré, appareil jailbreaké ou rooté et appareil avec des applications sur liste noire.
- **Indicateur de risque Citrix Virtual Apps and Desktops** : accès à partir d'un appareil doté d'un système d'exploitation (SE) non pris en charge.
- **Indicateur de risque Citrix Content Collaboration** : accès excessif aux fichiers sensibles.

[CAS-14590]

19 février 2019

Nouvelles fonctionnalités

Intégration de Splunk

Citrix Analytics s'intègre à Splunk pour améliorer vos expériences de surveillance des incidents de sécurité et de dépannage. Cette intégration augmente vos sources de données existantes avec les fonctionnalités d'analyse des risques et l'intelligence de Citrix Analytics for Security, telles que les indicateurs de risque, les scores de risque et les profils utilisateur. Citrix Analytics exporte les informations d'analyse des risques vers un canal. Splunk tire la même chose de cette chaîne.

L'intégration de Splunk implique la configuration sur Citrix Analytics, l'installation du **module complémentaire Citrix Analytics pour l'application Splunk** et la configuration de l'application. Assurez-vous d'activer le traitement des données pour au moins une source de données. Il aide Citrix Analytics à démarrer le processus d'intégration de Splunk.

Pour plus d'informations, consultez la section Intégration de Splunk.

Enregistrement de session dynamique Citrix Analytics offre la possibilité de déclencher l'enregistrement de session de manière dynamique sur les sessions Virtual Apps and Desktops actuelles des utilisateurs. Il permet de saisir les preuves requises pour l'analyse des risques et de prendre les mesures appropriées de réponse aux incidents, telles que les sessions de déconnexion et l'utilisateur de blocage.

Pour plus d'informations, consultez la section Stratégies et actions.

Tableau de bord Share Links et indicateur de risque Citrix Analytics introduit la visibilité des risques pour Share Links en fonction des données collectées à partir de Citrix Content Collaboration. Il vous aide à comprendre l'exposition au risque des liens de partage grâce aux indicateurs de risque déclenchés par ces liens.

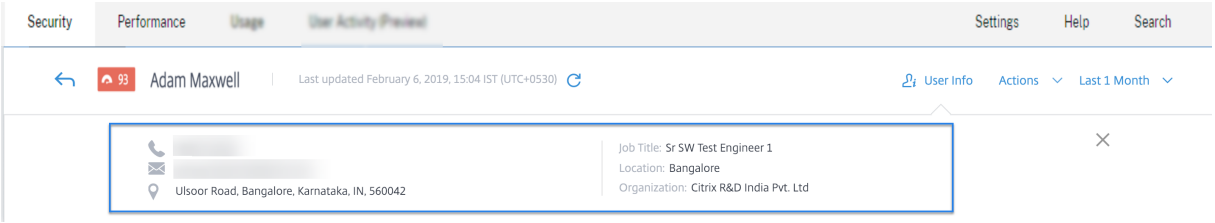
Pour plus d'informations, consultez la section Tableau de bord Partager des liens.

Actuellement, l'indicateur de risque de téléchargement de partage sensible anonyme est déclenché pour un lien de partage. Lorsque Content Collaboration détecte ce comportement risqué, Citrix Analytics reçoit les événements. Vous êtes averti dans le panneau **Alertes** et l'indicateur de risque de téléchargement de partage sensible anonyme est ajouté à la chronologie des risques du lien de partage.

Pour plus d'informations, consultez la chronologie des risques de Share Link et les indicateurs de risque Citrix Share Link.

Intégration de Microsoft Active Directory Vous pouvez désormais intégrer Microsoft Active Directory à Citrix Analytics. Cette intégration améliore le contexte des utilisateurs à risque avec des informations supplémentaires telles que l'intitulé du poste, l'organisation, l'emplacement du bureau, l'e-mail et les coordonnées. Vous pouvez obtenir une meilleure visibilité d'un utilisateur sur la page de profil utilisateur de Citrix Analytics.

Pour plus d'informations, voir Intégrer Analytics à Microsoft Active Directory.



04 janvier 2019

Nouvelles fonctionnalités

Ajout de la colonne SOURCE pour les indicateurs de risque existants La colonne **SOURCE** a été introduite dans la section **DÉTAILS DE L'ÉVÉNEMENT** pour les indicateurs de risque suivants :

- Chargements excessifs de fichiers
- Téléchargements excessifs de fichiers
- Partage excessif de fichiers
- Suppression excessive de fichiers ou de dossiers

Pour plus d'informations, consultez la section Indicateurs de risque Citrix Content Collaboration.

Profil utilisateur avancé La vue **Informations utilisateur** sur le profil utilisateur a été améliorée. Le lien **Trend View** a été introduit dans le coin supérieur droit des sections **Application**, **Devices**et **Data Usage** . Le lien **Vue sur la carte** a été introduit dans le coin supérieur droit de la section **Emplacements** . Ces liens fournissent une représentation graphique du comportement historique de l'utilisateur au cours d'une période spécifique. Vous pouvez accéder aux **informations utilisateur** à partir de la chronologie des risques de l'utilisateur ou à partir de la page **Sources de données** .

> **Remarque**
>
> Les données **d'authentification** et de **domaines** ne sont actuellement pas disponibles dans le profil Informations utilisateur.

Pour plus d'informations, consultez la section Chronologie et profil des risques utilisateur.

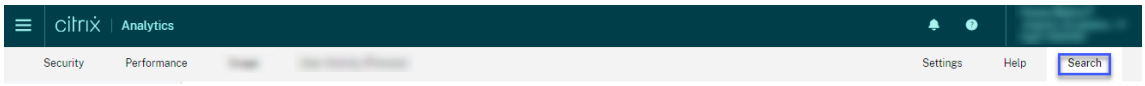
Indicateurs de risque Microsoft Graph Security Microsoft Graph Security intégré peut recevoir les détails des indicateurs de risque de l'un des fournisseurs de sécurité suivants, et les transmet à Citrix Analytics :

- Protection des identités Azure AD
- Microsoft Defender pour Endpoint

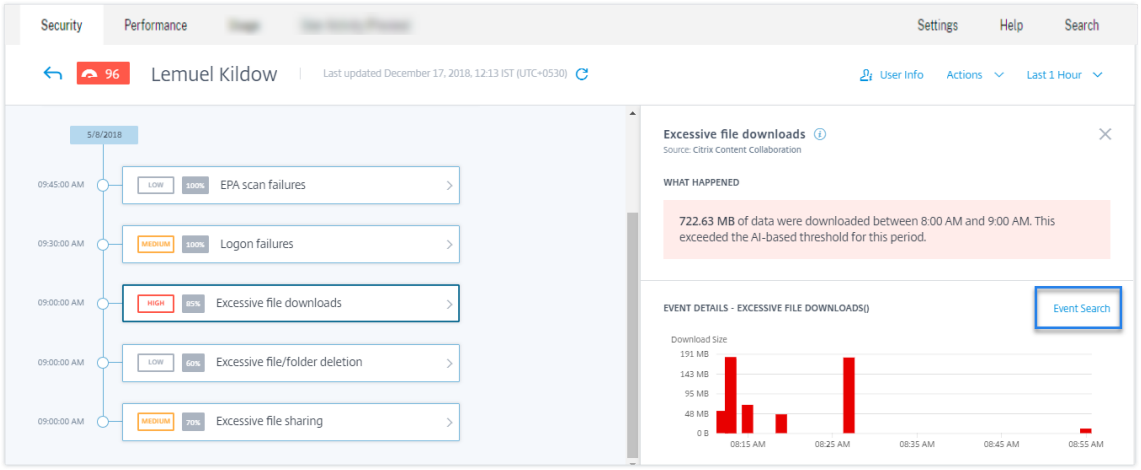
Pour plus d'informations, consultez la section Indicateurs de risque de sécurité Microsoft Graph.

Comment accéder à la page de recherche en libre-service Vous pouvez désormais accéder à la page de recherche en libre-service à l'aide des options suivantes :

- **Barre supérieure** : cliquez sur **Rechercher** dans la barre supérieure pour accéder directement à la page de recherche.



- **Chronologie des risques sur la page de profil utilisateur** : cliquez sur **Recherche d'événements** pour accéder à la page de recherche et afficher les événements correspondant à l'indicateur de risque d'un utilisateur spécifique et à la source de données. Pour plus d'informations, consultez la rubrique Recherche en libre-service.



Recherche en libre-service pour Content Collaboration Utilisez la recherche en libre-service pour obtenir des informations sur les événements associés à la source de données Content Collaboration. Pour afficher les événements, sélectionnez **Content Collaboration** dans la liste, sélectionnez la période, puis cliquez sur **Rechercher**.
Pour plus d'informations, voir Recherche en libre-service pour Content Collaboration.

Recherche en libre-service d'applications et de bureaux Utilisez la recherche en libre-service pour obtenir des informations sur les événements associés à la source de données Apps and Desktops. Pour afficher les événements, sélectionnez **Applications et bureaux** dans la liste, sélectionnez la période, puis cliquez sur **Rechercher**. Pour plus d'informations, consultez la section Recherche en libre-service d'applications et de bureaux.

Exporter les événements de recherche en libre-service dans un fichier CSV Vous pouvez désormais exporter les événements de recherche en libre-service dans un fichier CSV et télécharger le fichier pour une utilisation ultérieure. Pour plus d'informations, consultez la rubrique Recherche en libre-service.

Intégration améliorée pour Citrix Virtual Apps and Desktops Le processus d'intégration de la source de données Citrix Virtual Apps and Desktops est désormais amélioré afin d'offrir une meilleure expérience utilisateur. Les cartes de site et les étapes d'embarquement ont été modifiées. Pour plus d'informations, consultez Citrix Virtual Apps and Desktops et Source de données Citrix DaaS.

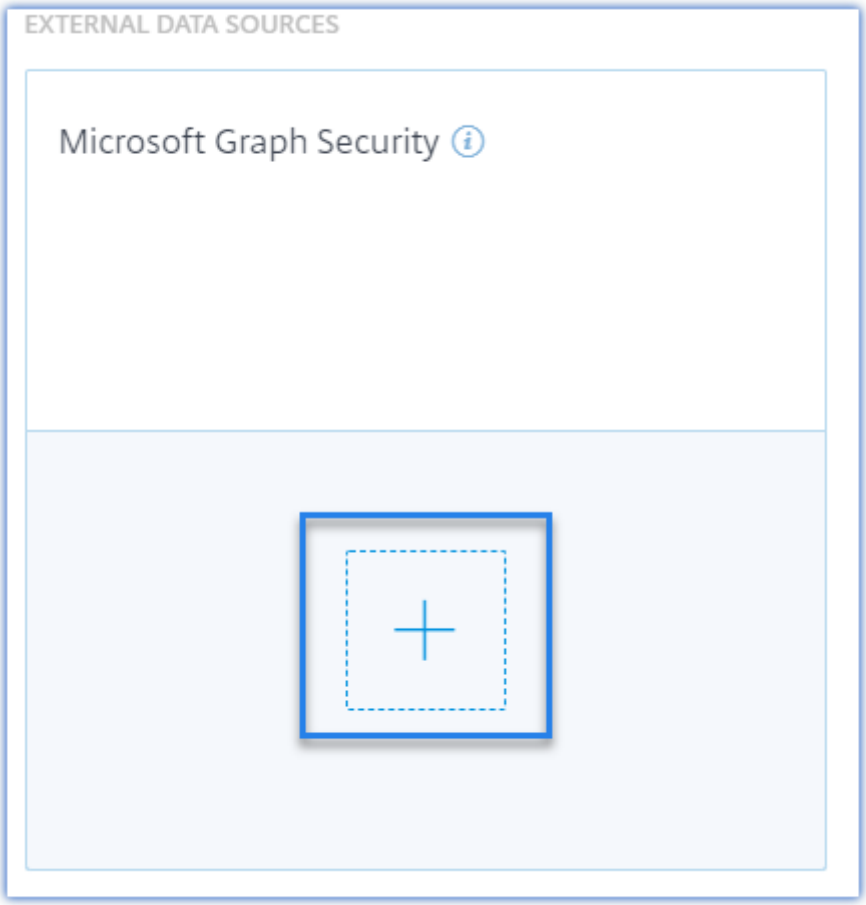
29 novembre 2018

Nouvelles fonctionnalités

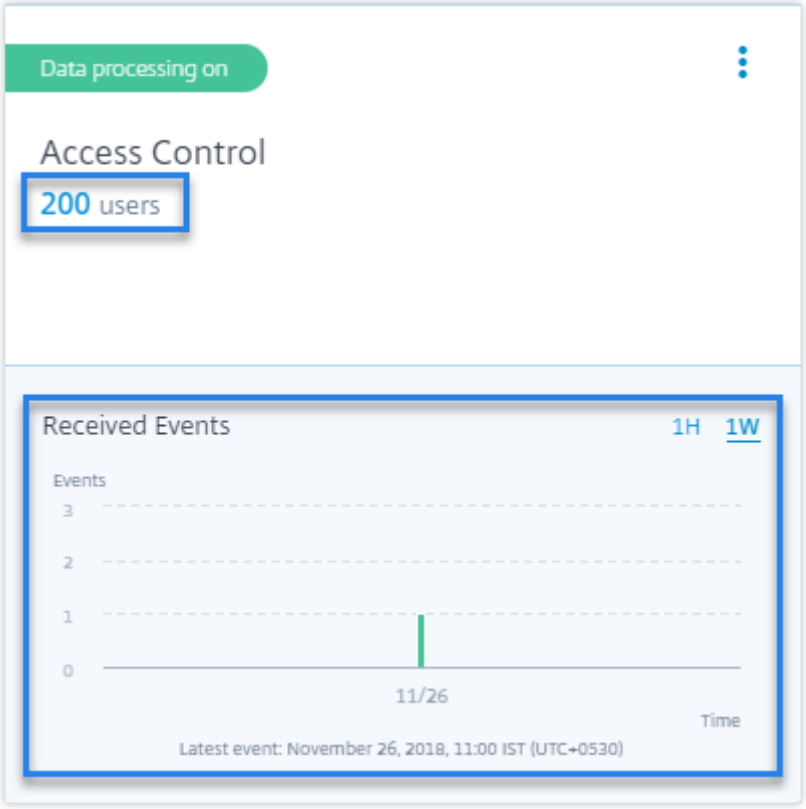
Source de données Microsoft Security Graph Microsoft Graph Security est une source de données externe qui regroupe les données de plusieurs fournisseurs de sécurité. Il permet également d'accéder aux données d'inventaire des utilisateurs.

Citrix Analytics prend actuellement en charge la **protection d'identité Azure AD** et les fournisseurs de sécurité **Microsoft Defender for Endpoint** associés à cette source de données.

Pour pouvoir utiliser cette source de données, vous devez obtenir des autorisations de la plateforme d'identité Microsoft. Pour plus d'informations, consultez la section Microsoft Graph Security.



Afficher les détails des événements et les utilisateurs découverts sur les fiches de site pour les sources de données Les fiches de site des sources de données affichent désormais les détails des événements et le nombre d'utilisateurs. Par exemple, vous pouvez afficher les détails de l'événement et les utilisateurs du contrôle d'accès sur la fiche de site. Pour plus d'informations, consultez la section Activer Analytics sur les sources de données.



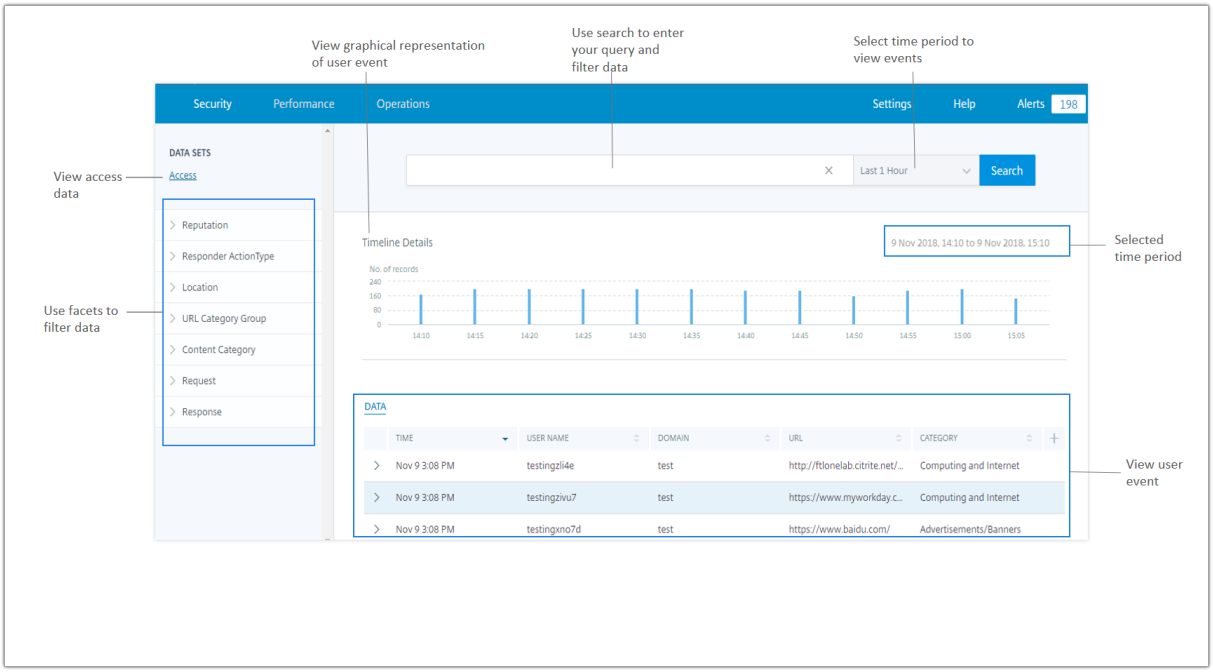
16 novembre 2018

Nouvelles fonctionnalités

Recherche en libre-service des données d'accès Vous pouvez utiliser la recherche en libre-service pour obtenir un aperçu des détails d'accès pour les utilisateurs de votre entreprise. Citrix Analytics collecte les détails d'accès des utilisateurs à partir du service Citrix Access Control. Utilisez les facettes et la requête de recherche pour affiner vos résultats de recherche.

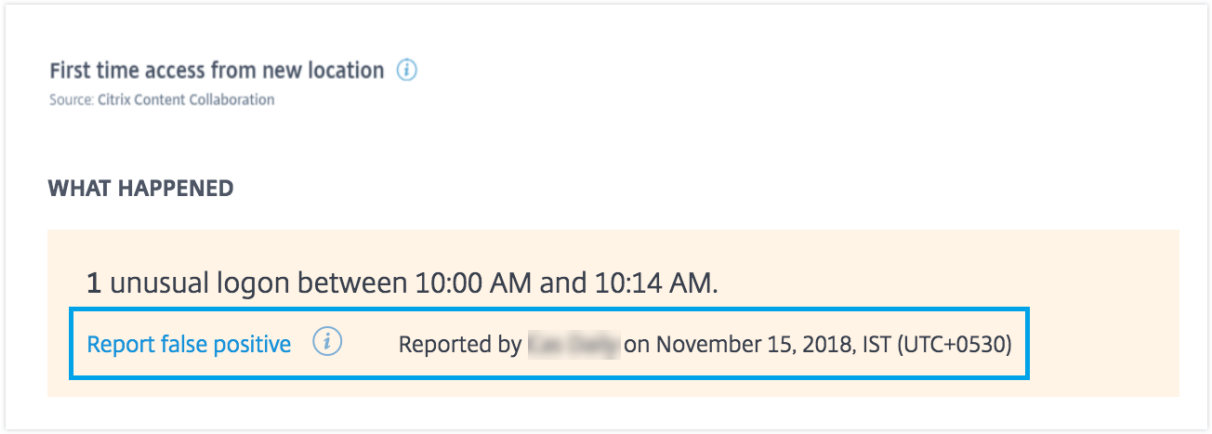
Pour utiliser la page de recherche en libre-service, dans l'onglet **Sécurité**, cliquez sur **Recherche d'événements**.

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



Feedback sur les indicateurs de risque À l'aide de la fonctionnalité de retour d'information sur les indicateurs de risque de Citrix Analytics, vous pouvez fournir des commentaires concernant un indicateur de risque. Vos commentaires permettent de confirmer si l'incident de sécurité signalé est exact ou non.

Actuellement, cette fonctionnalité est prise en charge sur l'indicateur de risque **d'accès de connexion inhabituel** déclenché par la source de données Content Collaboration. Si cet indicateur de risque déclenché est incorrect, vous pouvez le signaler comme un faux positif et fournir des commentaires. Vous pouvez également modifier les commentaires que vous avez déjà envoyés. Citrix Analytics capture vos commentaires et valide les informations prédites afin d'optimiser la détection des comportements anormaux.



Problèmes résolus

- Vous ne pouvez pas modifier et enregistrer une stratégie si vous accédez à Citrix Analytics à l'aide d'Internet Explorer 11.0.

Problèmes connus

December 7, 2023

Citrix Analytics for Security présente les problèmes connus suivants :

- L'application Citrix Workspace pour Linux ne parvient pas à envoyer des événements d'impression à Citrix Analytics lorsque les applications et les bureaux sont ouverts via un navigateur Web et lancés depuis ICA sur le client natif. [CAS-36238]

  > **Remarque**
  >
  > Pour plus d'informations sur les dates du cycle de vie et les phases du cycle de vie (disponibilité générale, fin de maintenance et fin de vie) de l'application Citrix Workspace et de Citrix Receiver sur toutes les plates-formes, consultez Étapes clés du cycle de vie pour l'application Citrix Workspace et Citrix Receiver.

Offres Citrix Analytics

December 7, 2023

Citrix Analytics for Security

Rassemble et fournit une visibilité sur le comportement des utilisateurs et des applications, collecté à partir des sources de données connectées des clients, telles que Secure Private Access, Citrix Virtual Apps and Desktops, Citrix DaaS Site ou NetScaler Gateway. Vous pouvez suivre tous les aspects du comportement et, en utilisant des algorithmes d'apprentissage automatique avancés, vous pouvez faire la distinction entre un comportement normal et un attaquant malveillant. Cela vous permet d'identifier et de gérer de manière proactive les menaces internes et externes.

En savoir plus : Citrix Analytics pour la sécurité

Citrix Analytics for Performance

Fournit une visibilité globale de bout en bout sur les déploiements hybrides de Citrix Virtual Apps and Desktops et de sites Citrix DaaS. Les performances sont indiquées par le score d'expérience utilisateur qui quantifie les facteurs historiques et les indicateurs qui définissent l'expérience d'un utilisateur lorsqu'il utilise une application publiée fournie par Citrix, un ordinateur de bureau publié ou un Remote PC.

En savoir plus : Citrix Analytics pour les performances

Citrix Analytics : utilisation (fin de vie)

> **Remarque**
>
> **Attention**: Citrix Usage Analytics a atteint sa fin de vie et n'est plus disponible pour les utilisateurs.

Sources de données

April 12, 2024

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

Sources de données Citrix

Le tableau suivant répertorie les différentes sources de données Citrix prises en charge par Citrix Analytics for Security. Pour plus d'informations, reportez-vous à la section Mise en route.

Source de données	Type de déploiement	Agents requis	Composant et version du produit
Citrix Endpoint Management	Service	S/O	Citrix Endpoint Management
Gateway	Local	Agent de gestion de la livraison des applications	Citrix Gateway 12.0.56.16 ou version ultérieure
Fournisseur d'identité Citrix	Service	S/O	Gestion des identités et des accès Citrix

Source de données	Type de déploiement	Agents requis	Composant et version du produit
Citrix Secure Private Access	Service	(Non applicable) S.O.	Citrix Secure Private Access
Citrix Remote Browser Isolation	Service	S/O	Citrix Remote Browser Isolation
Citrix DaaS (anciennement Virtual Apps and Desktops Service)	Service	S/O	application Citrix Workspace pour Windows 1907 ou version ultérieure, application Citrix Workspace pour Mac 1910.2 ou version ultérieure, application Citrix Workspace pour HTML5 2007 ou version ultérieure, application Citrix Workspace pour Chrome - Dernière version disponible dans Chrome Web Store, application Citrix Workspace pour Android - Dernière version disponible sur Google Play, application Citrix Workspace pour Android pour iOS - Dernière version disponible dans l'App Store d'Apple, l' application Citrix Workspace pour Linux 2006 ou version ultérieure

Source de données	Type de déploiement	Agents requis	Composant et version du produit
Citrix Virtual Apps and Desktops	Local	Agent Virtual Apps and Desktops L'agent est requis pour les fonctionnalités avancées telles que Actions.	Citrix Virtual Apps and Desktops 7 1808, Citrix XenApp et XenDesktop 7.16 et versions ultérieures application Citrix Workspace pour Windows 1907 ou version ultérieure, application Citrix Workspace pour Mac 1910.2 ou version ultérieure, application Citrix Workspace pour HTML5 2007 ou version ultérieure, application Citrix Workspace pour Chrome - Dernière version disponible dans Chrome Web Store, application Citrix Workspace pour Android - Dernière version disponible sur Google Play, application Citrix Workspace pour Android pour iOS - Dernière version disponible dans l'App Store d'Apple, l' application Citrix Workspace pour Linux 2006 ou version ultérieure Citrix Director 7.16 ou version ultérieure

Source de données	Type de déploiement	Agents requis	Composant et version du produit
			Pour les utilisateurs de Workspace : **Les**sites locaux Virtual Apps and Desktops doivent être ajoutés à Workspace à l'aide de l'agrégation de sites. **Pour les utilisateurs StoreFront** : la version de déploiement StoreFront doit être StoreFront 1906 ou ultérieure. StoreFront doit être accessible via l'un des clients suivants : sites Citrix Receiver pour Web dans des navigateurs compatibles 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. **Prise en charge de LTSR** : Pour Citrix Virtual Apps and Desktops 7 1912 LTSR, la version StoreFront prise en charge est 1912.

> **Remarque**
>
> Reportez-vous à la section Services Citrix Cloud pour en savoir plus sur les produits Citrix et leurs abonnements.

Sources de données externes

Le tableau suivant répertorie les sources de données externes (produits tiers) prises en charge par Citrix Analytics for Security.

Source de données	Type de déploiement	Agents requis
Microsoft Graph Security	Service	S/O
Microsoft Active Directory	Local	Citrix Cloud Connector

Régions d'origine prises

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.

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 où 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

Source de données	Supporté dans la région des États-Unis	Soutenu dans la région UE	Supporté dans la région APS
Citrix Secure Private Access	Oui	Oui	Oui
Citrix Remote Browser Isolation	Oui	Oui	Oui
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

Matrice des versions de l'application Citrix Workspace

Cette section affiche les versions prises en charge de l'application Citrix Workspace qui envoie toutes les données de télémétrie et contient toutes les corrections de bogues critiques nécessaires.

Le tableau suivant répertorie les versions prises en charge et non prises en charge pour l'application Citrix Workspace.

Plateforme	Version prise en charge
Windows	Toutes les versions de LTSR 2203 après CU3 23.0.3.0 ou supérieur
HTML5	21.5.0.0 ou supérieur
Macintosh	21.0.4.0 ou supérieur
Linux	21.4.0.0 ou supérieur
Chrome	21.5.0.0 ou supérieur
iOS	21.4.0.0 ou supérieur
Android	21.5.0.0 ou supérieur

Le tableau suivant répertorie la version minimale de l'application Citrix Workspace requise pour que

le système d'exploitation reçoive les attributs d'événements utilisateur suivants dans Citrix Analytics for Security.

Attributs d'événement	Caractéristiques associées	Windows	Mac	Linux	HTML5	Chrome	iOS	Android
Ville, pays	Emplacement d'assurance d'accès, recherche en libre-service - Applications et ordinateurs de bureau	2008 ou plus	2006 ou plus	2104 ou plus	2007 ou plus	Dernière version disponible dans le Chrome Web Store	Dernière version disponible dans l'App Store d'Apple	Dernière version disponible sur Google Play
IP du client	Recherche en libre-service : applications et ordinateurs de bureau	2008 ou plus	2006 ou plus	2104 ou plus	2007 ou plus	Dernière version disponible dans le Chrome Web Store	Dernière version disponible dans l'App Store d'Apple	Dernière version disponible sur Google Play

Attributs d'événement	Caractéristiques associées	Windows	Mac	Linux	HTML5	Chrome	iOS	Android
Nom du système d'exploitation, version du système d'exploitation, informations supplémentaires	Recherche en libre-service : applications et ordinateurs de bureau	2109 ou plus	2108 ou plus	2104 ou plus	2007 ou plus	Dernière version disponible dans le Chrome Web Store	Dernière version disponible dans l'App Store d'Apple	Dernière version disponible sur Google Play
Nom de l'imprimante	Recherche en libre-service : applications et ordinateurs de bureau	2106 ou version ultérieure	1809 ou version ultérieure	2006 ou version ultérieure	1911 ou version ultérieure	Dernière version disponible dans le Chrome Web Store	Dernière version disponible dans l'App Store d'Apple	Dernière version disponible sur Google Play
Tous les événements utilisateur pour le lancement Web	Recherche en libre-service : applications et ordinateurs de bureau	2008 ou version ultérieure	2006 ou version ultérieure	2006 ou version ultérieure	Non applicable	Non pris en charge	Dernière version disponible dans l'App Store d'Apple	Dernière version disponible sur Google Play

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, Cat-

egory 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

Configuration système requise

April 12, 2024

Avant de commencer à utiliser Citrix Analytics pour la sécurité, passez en revue les exigences suivantes.

Abonnement à Citrix Analytics pour la sécurité

Ce produit Analytics est une offre basée sur un abonnement. Vous devez disposer d'un abonnement valide pour utiliser Security Analytics. Pour plus d'informations, consultez la page de présentation du produit .

Exigences en matière de sources

Citrix Analytics for Security reçoit des événements provenant de différentes sources de données. Pour qu'Analytics fonctionne correctement, vous devez disposer d'un abonnement valide pour utiliser au moins l'un des produits suivants, qui agissent en tant que sources de données pour Analytics :

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

Navigateurs pris en charge

Pour accéder à 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 Security Analytics

December 7, 2023

En tant qu'administrateur Citrix Cloud disposant d'autorisations d'accès complet, vous pouvez inviter d'autres administrateurs à gérer l'offre Security Analytics et leur attribuer l'un des rôles personnalisés suivants :

- **Security Analytics - Administrateur complet**
- **Security Analytics - Administrateur en lecture seule**

Vous pouvez ajouter de nouveaux administrateurs de deux manières : individuellement en tant qu'utilisateurs ou à l'aide de groupes Azure Active Directory. Pour plus d'informations sur l'ajout de nouveaux administrateurs, consultez la section Gérer les rôles d'administrateur.

> **Remarque**
> 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.

Autorisations pour les rôles personnalisés

Les administrateurs ayant le rôle **Security Analytics- Administrateur complet** peuvent accéder à toutes les fonctionnalités et fonctionnalités de l'offre Security Analytics. Ils peuvent utiliser et modifier les fonctionnalités en fonction de leurs besoins organisationnels. Par exemple, un administrateur complet peut créer des indicateurs de risque personnalisés, activer le géorepérage et créer des stratégies.

Les administrateurs dotés du rôle d'**administrateur en lecture seule de Security Analytics** peuvent uniquement accéder aux tableaux de bord de sécurité et les consulter : utilisateurs, accès utilisateur,

accès aux applications, assurance d'accès et rapports. Ils peuvent surveiller le comportement des utilisateurs et consulter les événements des utilisateurs sur ces tableaux de bord. Cependant, ils ne sont pas autorisés à effectuer des tâches critiques telles que :

- Activer ou désactiver le traitement des données pour les sources de données
- Création ou suppression de stratégies et d'actions
- Appliquez des actions manuellement sur les indicateurs de risque affichés sur la chronologie du risque utilisateur
- Créer, modifier ou supprimer des indicateurs de risque personnalisés
- Créer des rapports personnalisés
- Ajouter, modifier ou supprimer un autre utilisateur administrateur
- Ajouter ou modifier une barrière géographique pour la localisation de l'assurance d'accès

Notifications d'alerte de sécurité pour les administrateurs

Tout comme les administrateurs Citrix Cloud disposant d'autorisations d'accès complet, les administrateurs dotés des rôles personnalisés (accès complet et accès en lecture seule) reçoivent des notifications par e-mail de Security Analytics.

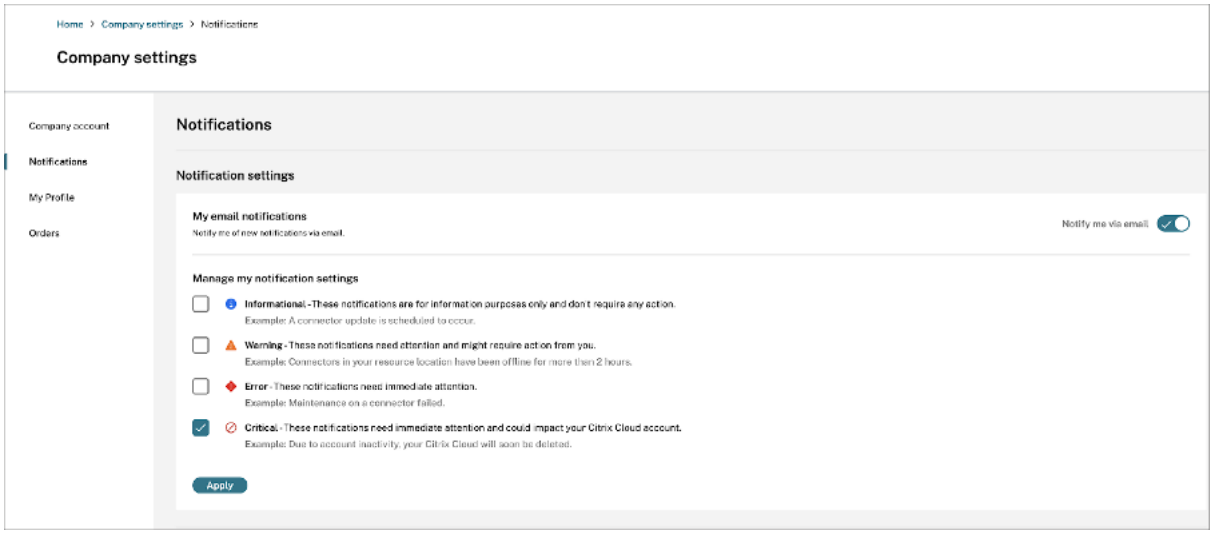
Les administrateurs reçoivent deux types de notifications par e-mail :

- Notification hebdomadaire concernant les informations de sécurité au sein de leur organisation. Pour plus d'informations, voir Notification hebdomadaire par e-mail.
- Notifications basées sur l'action Notifier les administrateurs. Pour plus d'informations, consultez la section Stratégies et actions.

Si vous êtes administrateur Citrix Cloud et que vous disposez d'une autorisation d'accès complète ou personnalisée, les notifications par e-mail sont désactivées par défaut sur votre compte Citrix Cloud. Pour recevoir des notifications par e-mail de la part de tout service Citrix Cloud tel que Citrix Analytics, activez l'option de notification dans votre Citrix Cloud. Pour plus d'informations, consultez Notifications par e-mail reçues. Les préférences de notification ne sont pas disponibles pour les administrateurs ajoutés via Active Directory/Azure AD Groups.

La préférence de notification est exploitée lors de l'envoi de notifications telles que des e-mails hebdomadaires, des e-mails d'action Notifier les administrateurs et des alertes pour les exportations de données. En ce qui concerne les notifications par e-mail, si vous ne souhaitez plus recevoir d'e-mails, un administrateur disposant d'un accès complet à Security Analytics doit vous retirer de la liste de distribution. Pour plus d'informations sur la liste de distribution, consultez la section Liste de distribution des e-mails.

> **Remarque**
>
> Les administrateurs Citrix Cloud (dotés d'une autorisation d'accès complète ou personnalisée) ne reçoivent aucune notification de la part d'autres services Citrix Cloud qui exploitent les **préférences de notification**.



Pour plus d'informations, consultez Gérer les administrateurs pour Citrix Analytics.

Mise en route

December 7, 2023

Ce document explique comment démarrer avec Citrix Analytics for Security pour la première fois.

Étape 1 : Se connecter à Citrix Cloud

Pour utiliser Citrix Analytics pour la sécurité, 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 Security Analytics

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

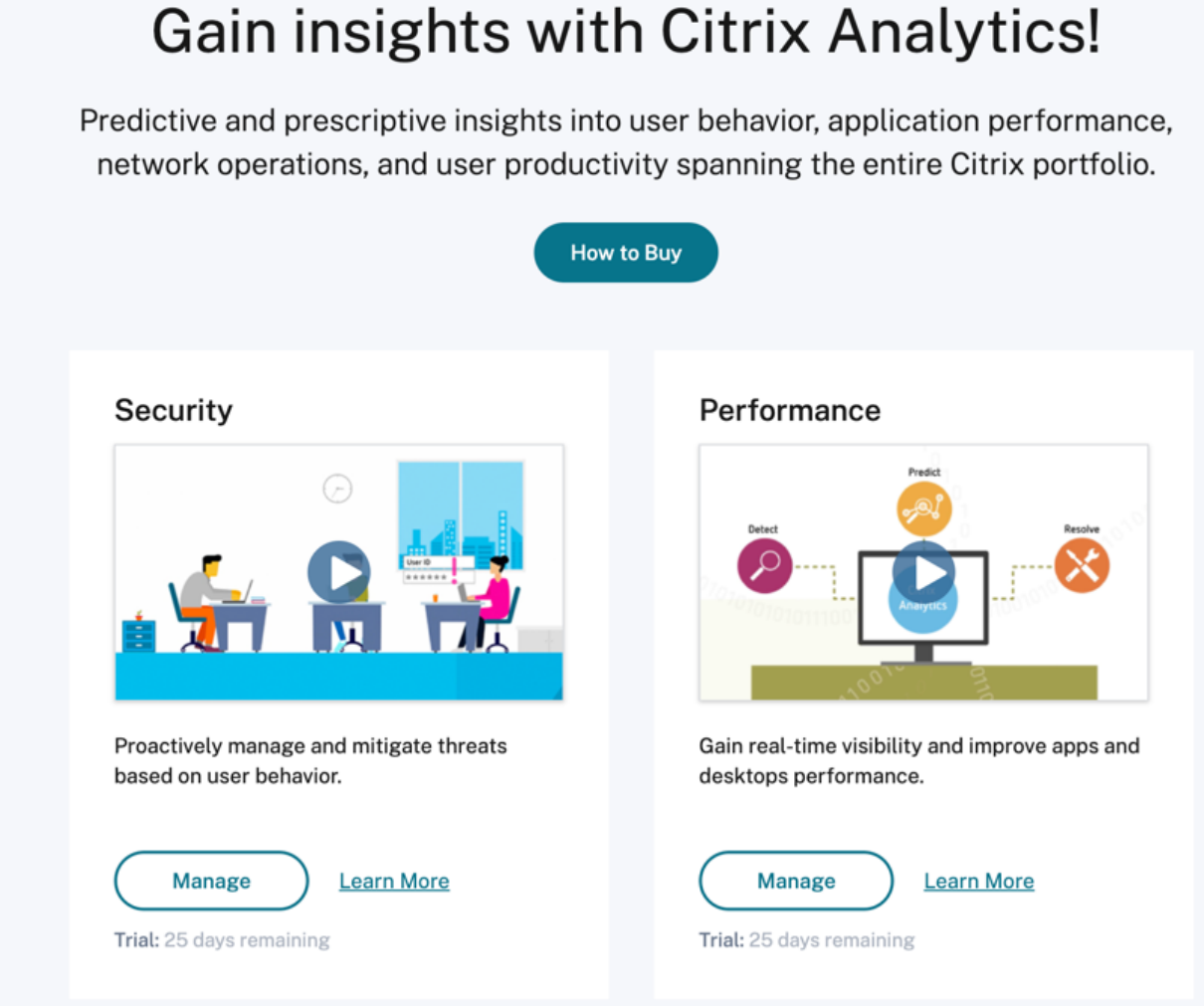
- **Demandez un essai de Citrix Analytics for Security**. Après vous être connecté à Citrix Cloud, procédez comme suit :
  1. Dans la section **Services disponibles**, cliquez sur **Gérer** dans la vignette **Analytics** . Vous êtes redirigé vers la page de présentation d'Analytics.
  2. Sur la vignette **Sécurité**, cliquez sur **Demander un essai** ou contactez directement votre compte Citrix ou Citrix Partner.
- **Abonnez-vous à Citrix Analytics pour la sécurité**. Pour acheter un abonnement à Citrix Analytics for Security, rendez-vous sur https://www.citrix.com/en-in/products/citrix-analytics/form/inquiry/ et contactez un expert Citrix Analytics qui pourra vous aider.

> **Remarque**
>
> - À compter du 8 mars 2023, Citrix Analytics for Security ne sera plus disponible à l'achat en tant qu'offre autonome avec ShareFile/Citrix Content Collaboration. Nous annonçons la fin des ventes (EOS) et la fin des renouvellements (EOR) du module complémentaire autonome Citrix Analytics Service pour ShareFile/Citrix Content Collaboration. Les droits existants des clients à Citrix Analytics for Security restent valables jusqu'à l'expiration de leur abonnement. Toutefois, les essais, les renouvellements et les nouveaux achats ne seront pas pris en charge pour les intégrations Sharefile/Citrix Content Collaboration. Les intégrations de Citrix Analytics Service à d'autres produits Citrix continuent d'être proposées sous forme d'offres autonomes ou groupées dans le cadre des plans Citrix DaaS existants, des déploiements Citrix Virtual Apps and Desktops et des déploiements Citrix Workspace.
> - À compter du 3 février 2020, Citrix Analytics pour la sécurité n'est plus inclus dans les abonnements Workspace Premium et Workspace Premium Plus. Les clients qui ont acheté l'abonnement Workspace Premium ou Workspace Premium Plus avant le 3 février 2020 peuvent accéder à Citrix Analytics for Security dans le cadre de l'abonnement Workspace jusqu'

> à l'expiration de leur abonnement. Citrix Analytics for Security est désormais proposé 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 les analyses de sécurité

Une fois que vous avez l'abonnement nécessaire ou que vous êtes autorisé à accéder à la version d'évaluation, sur la page de présentation d'Analytics, le bouton **Demander un essai** pour l'offre de sécurité change en **Gérer**. Cliquez sur **Gérer** pour afficher le tableau de bord utilisateur.



Analytics prend en charge les sources de données Citrix et les sources de données externes. Il découvre automatiquement les sources de données Citrix associées à votre compte Citrix Cloud. Pour recevoir des données provenant de sources de données externes, vous devez intégrer les sources de données externes à Analytics. Pour afficher vos sources de données découvertes, cliquez sur **Paramètres > Sources de données > Sécurité**.

Prochaine étape

- Le traitement des données est activé pour les services cloud suivants lorsque leur autorisation Citrix Analytics for Security est approuvée :
  - Sources de données Citrix
    - Citrix Secure Private Access
    - Citrix Virtual Apps and Desktops et Citrix DaaS
- Pour vérifier l'état du traitement des données ou savoir comment l'activer manuellement, consultez les articles suivants :
  - Sources de données Citrix :
    - Citrix Endpoint Management
    - Citrix Gateway
  - Sources de données externes :
    - Microsoft Graph Security
    - Microsoft Active Directory
- Exportez les données traitées depuis Analytics vers les produits suivants :
  - Splunk
  - Sentinelle Microsoft Azure
  - Elasticsearch
  - Autres SIEM utilisant un connecteur de données basé sur Kafka ou Logstash
- Utilisez le tableau de bord Utilisateurs pour afficher les utilisateurs découverts et leurs profils de risque de sécurité. Le tableau de bord des **utilisateurs** est le point de départ de l'analyse du comportement des utilisateurs et de la prévention des menaces.

  > **Remarque**
  >
  > Si vous utilisez Analytics pour la première fois, les profils de risque utilisateur prennent un certain temps avant d'apparaître sur le tableau de bord. Analytics utilise l'apprentissage automatique pour déterminer le modèle ou les anomalies à risque dans les événements utilisateur et identifie les profils utilisateur comme présentant un risque élevé, un risque moyen et un risque faible en fonction de la gravité des risques.

- Utilisez la fonction de recherche en libre-service pour afficher et filtrer les événements utilisateur (données brutes) reçus des sources de données.

Source de données de Citrix Endpoint Management

December 6, 2021

La source **de données Endpoint Management** représente le service Citrix Endpoint Management associé à votre compte Citrix Cloud. Lorsque les utilisateurs utilisent ce service, Citrix Analytics reçoit les événements utilisateur liés aux points de terminaison des utilisateurs et à leurs activités en temps réel. Les événements utilisateur sont traités pour détecter les éventuelles menaces à la sécurité.

Conditions préalables

- Abonnez-vous à Citrix Endpoint Management proposé sur Citrix Cloud. Pour savoir comment configurer votre service Endpoint Management, consultez la section Intégration et configuration des ressources.
- **Configuration du site cloud et de l'annuaire d'entreprise**. Assurez-vous que vous disposez de deux machines exécutant un serveur Windows 2012 R2 ou Windows 2016 pour installer le Cloud Connector.
- **Cloud Connector installé**. Téléchargez et installez le Cloud Connector sur une machine virtuelle qui fait partie d'Active Directory.
- Passez en revue la configuration système requise et assurez-vous que votre environnement répond aux exigences.

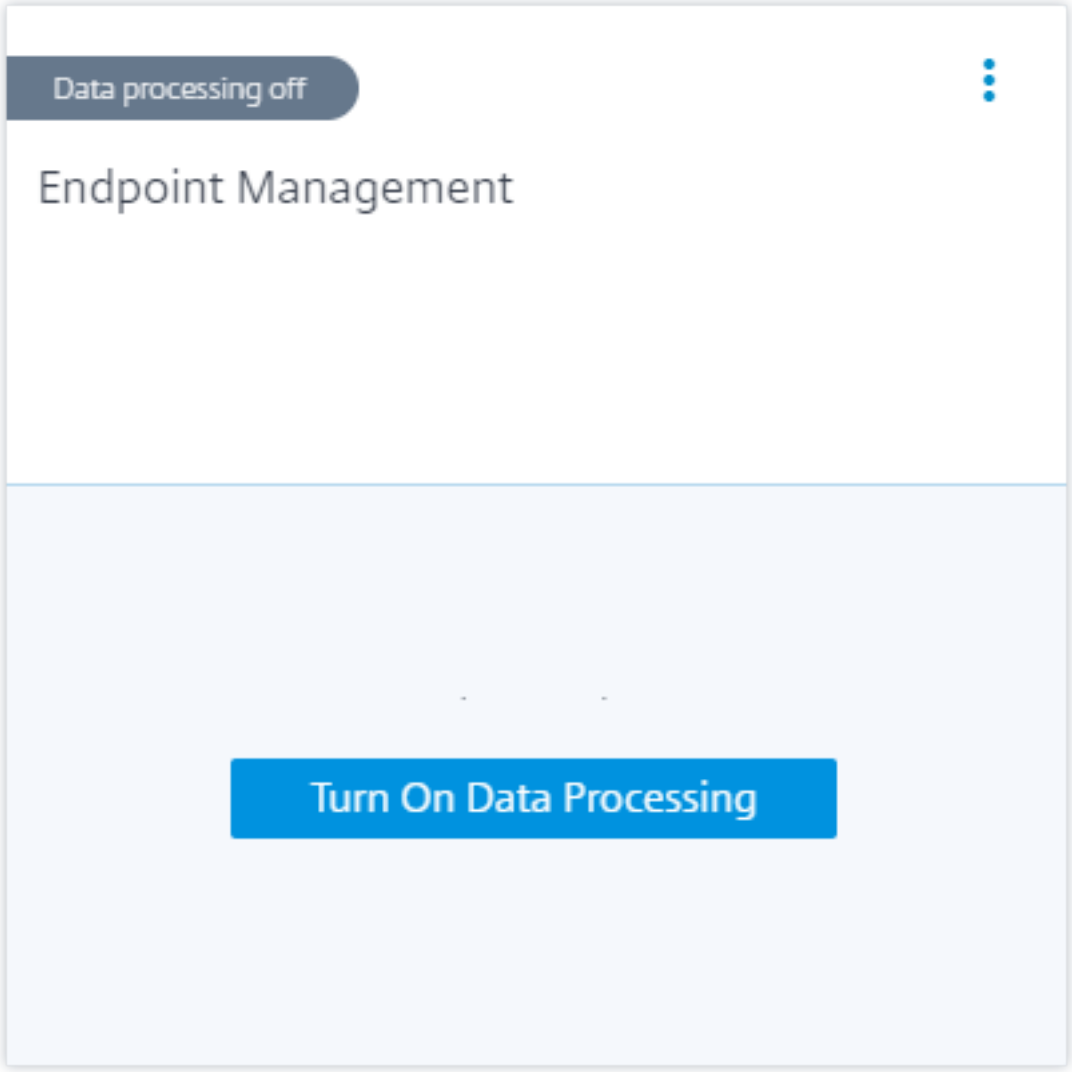
Afficher la source de données et activer le traitement des données

Citrix Analytics découvre automatiquement toutes les sources de données Endpoint Management associées à votre compte Citrix Cloud.

Pour afficher la source de données :

Dans la barre supérieure, cliquez sur **Paramètres** > **Sources de données** > **Sécurité**.

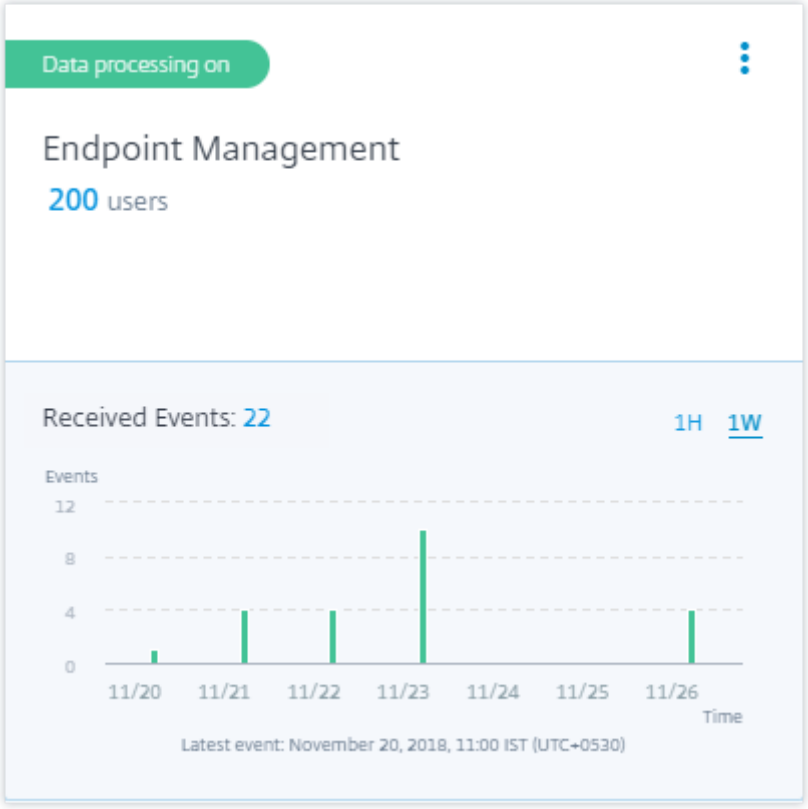
Une fiche de site pour la source de données Endpoint Management s'affiche sur la page **Sources de données** . Cliquez **sur Activer le traitement des données** pour permettre à Citrix Analytics de commencer à traiter les données de cette source de données.



Afficher les utilisateurs et les événements reçus

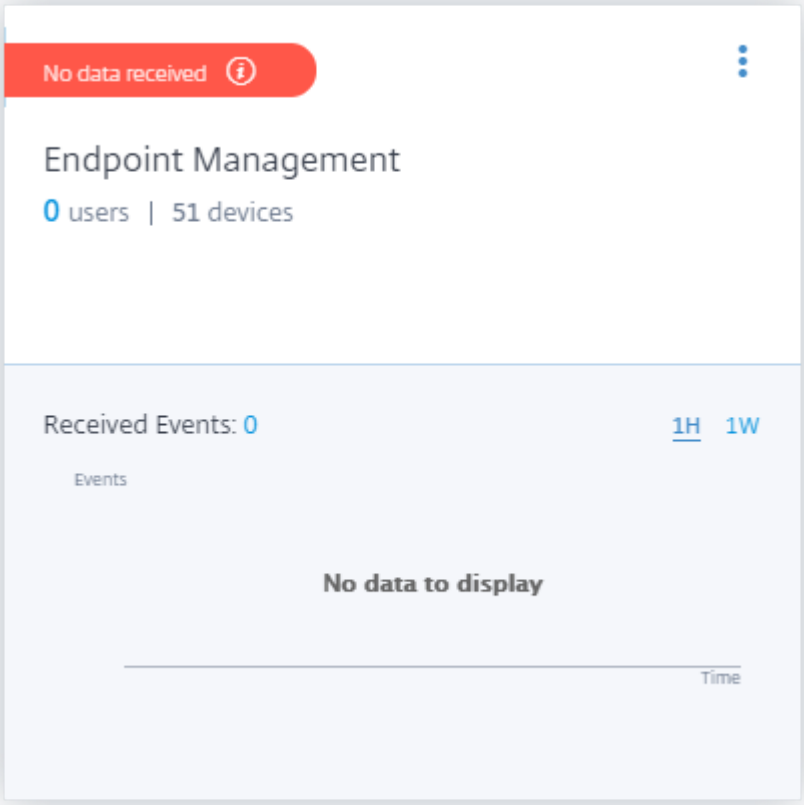
La fiche de site affiche le nombre d'utilisateurs et d'appareils Endpoint Management et les événements reçus au cours de la dernière heure, qui est la sélection de l'heure par défaut. Vous pouvez également sélectionner 1 semaine (**1 W**) et afficher les données.

Cliquez sur le nombre d'utilisateurs pour afficher les détails de l'utilisateur sur la page **Utilisateurs** .



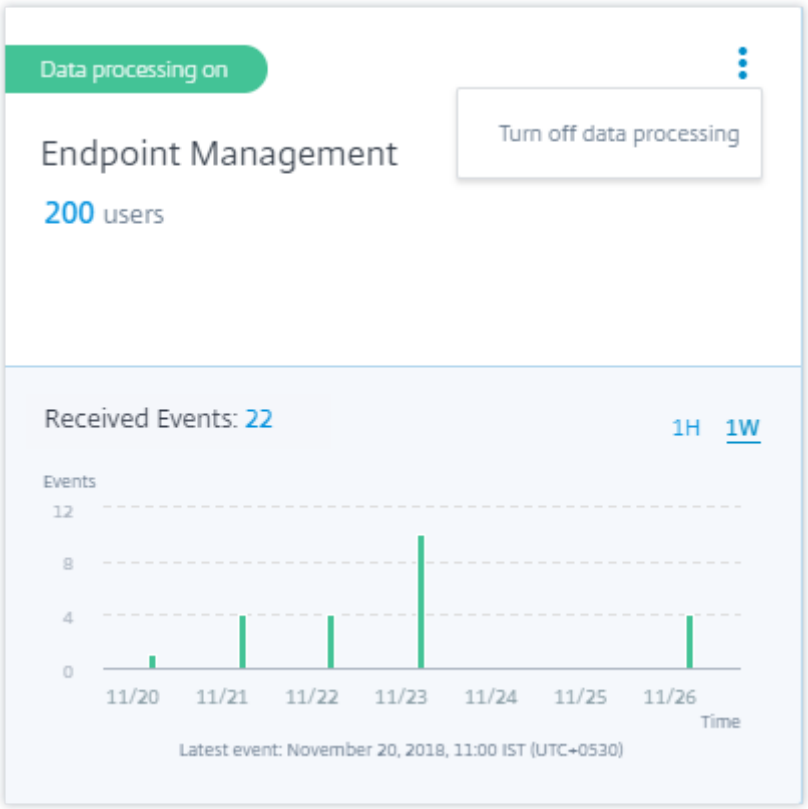
Une fois le traitement des données activé, la fiche de site peut afficher l'état **Aucune donnée reçue** . Ce statut apparaît pour deux raisons :

1. Si vous avez activé le traitement des données pour la première fois, les événements prennent un certain temps avant d'atteindre le hub d'événements dans Citrix Analytics. Lorsque Citrix Analytics reçoit les événements, l'état passe à **Traitement des données sur**. 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.

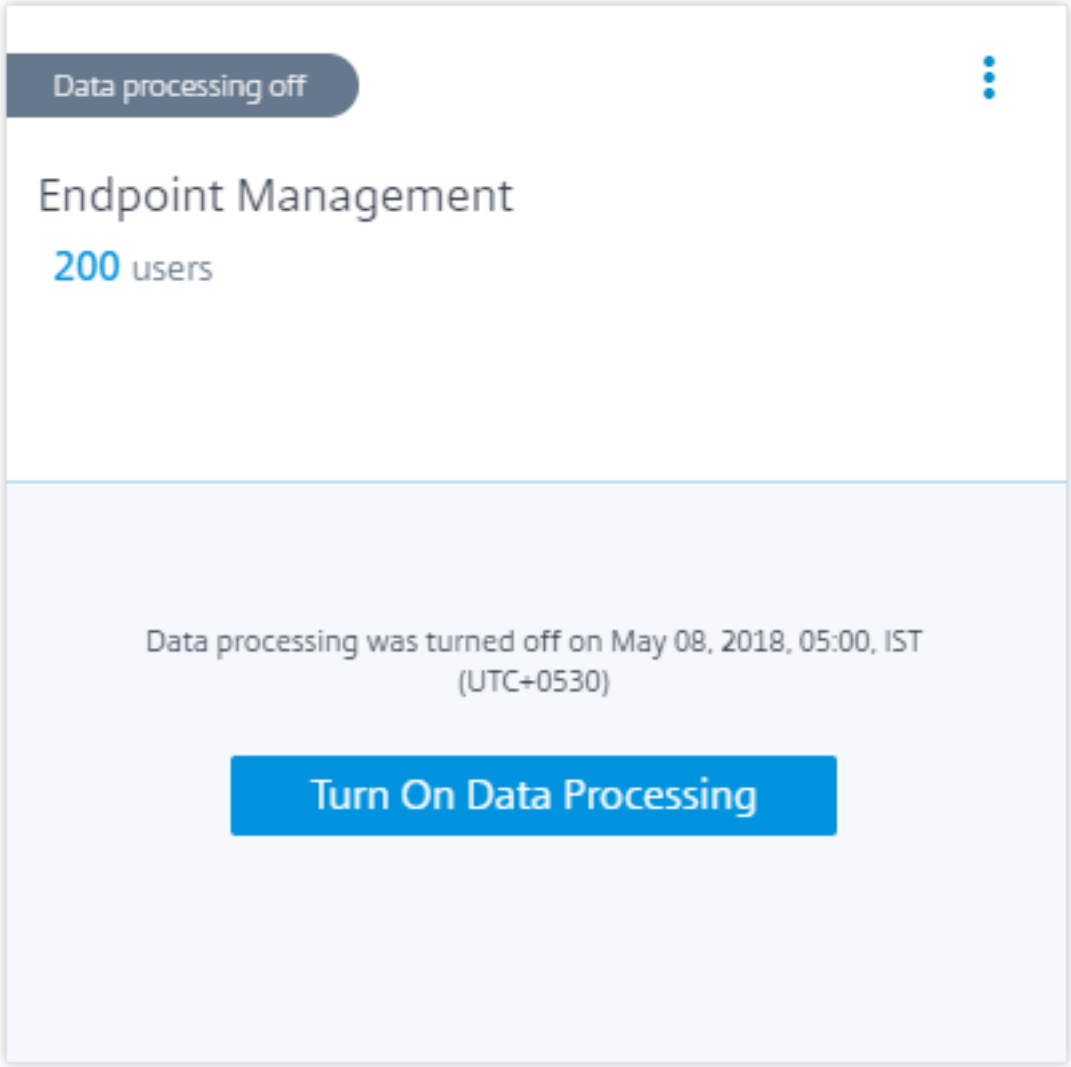


Activer ou désactiver le traitement des données

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**.



Source de données Citrix Gateway (sur site)

April 12, 2024

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

Pour plus d'informations sur les prérequis et les étapes d'intégration, consultez l'article sur la source

de données Citrix Gateway dans la documentation de la plate-forme Citrix Analytics.

Source de données de Citrix Remote Browser Isolation

March 22, 2023

Le Citrix Remote Browser Isolation Service isole la navigation Web afin de protéger le réseau de l'entreprise contre les attaques basées sur le navigateur. Ce service fournit un accès distant sécurisé et cohérent aux applications Web hébergées sur Internet sans configuration du terminal.

Dans Citrix Analytics for Security, vous pouvez consulter les événements utilisateur d'une session d'isolation du navigateur à distance publiée. Pour plus d'informations sur les événements utilisateur, voir Recherche en libre-service pour Remote Browser Isolation.

Pour recevoir les événements utilisateur issus d'une session d'isolation du navigateur à distance publiée, activez la politique de **suivi des noms d'hôtes** dans l'isolation du navigateur à distance. Par défaut, la stratégie est désactivée.

L'activation de la politique de **suivi des noms d'hôtes** permet à Remote Browser Isolation d'envoyer les noms d'hôtes utilisés pendant la session utilisateur à Citrix Analytics for Security.
Pour plus d'informations, voir Gérer les isolations de navigateurs distants publiées.

Source de données Citrix Secure Private Access

April 12, 2024

La source de données **Secure Private Access** représente le Citrix Secure Private Access service associé à votre compte Citrix Cloud. Lorsque les utilisateurs utilisent ce service, Citrix Analytics reçoit les événements d'accès utilisateur (journaux) en temps réel. Les événements utilisateur sont traités pour détecter les éventuelles menaces à la sécurité.

Conditions préalables

- Abonnez-vous au Citrix Secure Private Access service proposé sur Citrix Cloud. Pour savoir comment démarrer, consultez la section Service d'accès privé sécurisé.
- Passez en revue la configuration système requise et assurez-vous que votre environnement répond aux exigences.

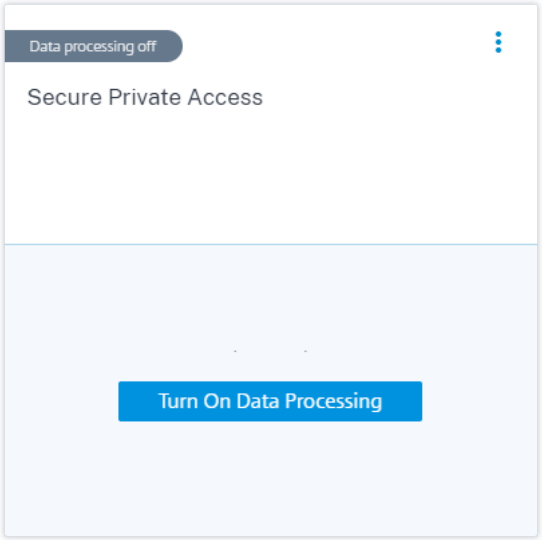
Afficher la source de données et activer le traitement des données

Citrix Analytics découvre automatiquement la source de données Secure Private Access associée à votre compte Citrix Cloud.

Pour afficher la source de données :

Dans la barre supérieure, cliquez sur **Paramètres** > **Sources de données** > **Sécurité**.

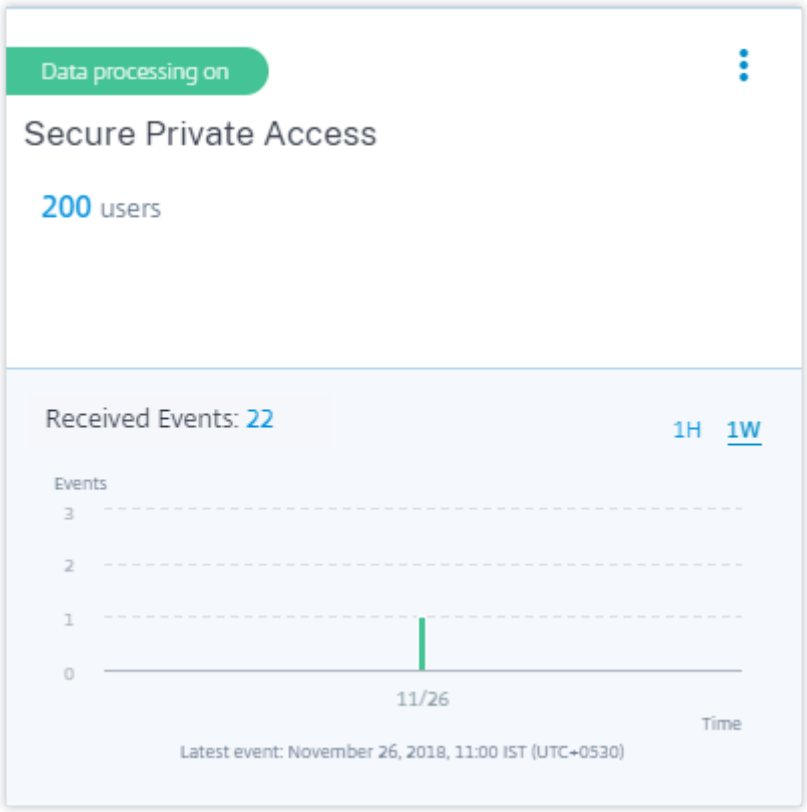
Une carte de site pour la source de données **Secure Private Access** apparaît sur la page **Sources de données** . Cliquez **sur Activer le traitement des données** pour permettre à Citrix Analytics de commencer à traiter les données de cette source de données.



Afficher les utilisateurs et les événements reçus

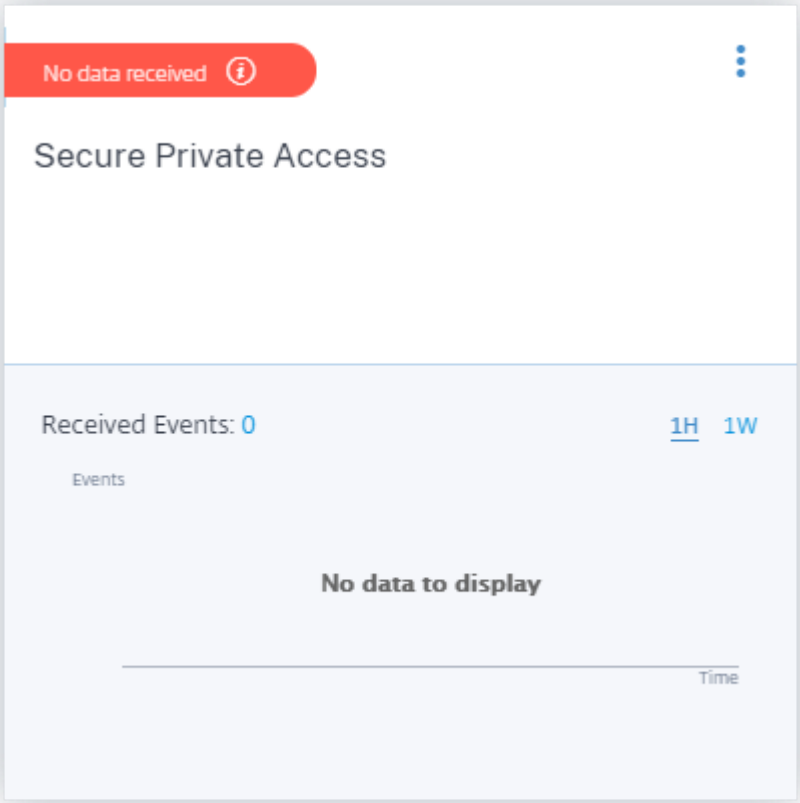
La fiche de site affiche le nombre d'utilisateurs actifs et les événements reçus de la source de données au cours de la dernière heure, qui est la sélection de l'heure par défaut. Vous pouvez également sélectionner 1 semaine (1 W) et afficher les données.

Cliquez sur le nombre d'utilisateurs pour afficher les détails de l'utilisateur sur la page **Utilisateurs** . Cliquez sur le nombre d'événements reçus pour afficher les détails de l'événement sur la page de recherche en libre-service .



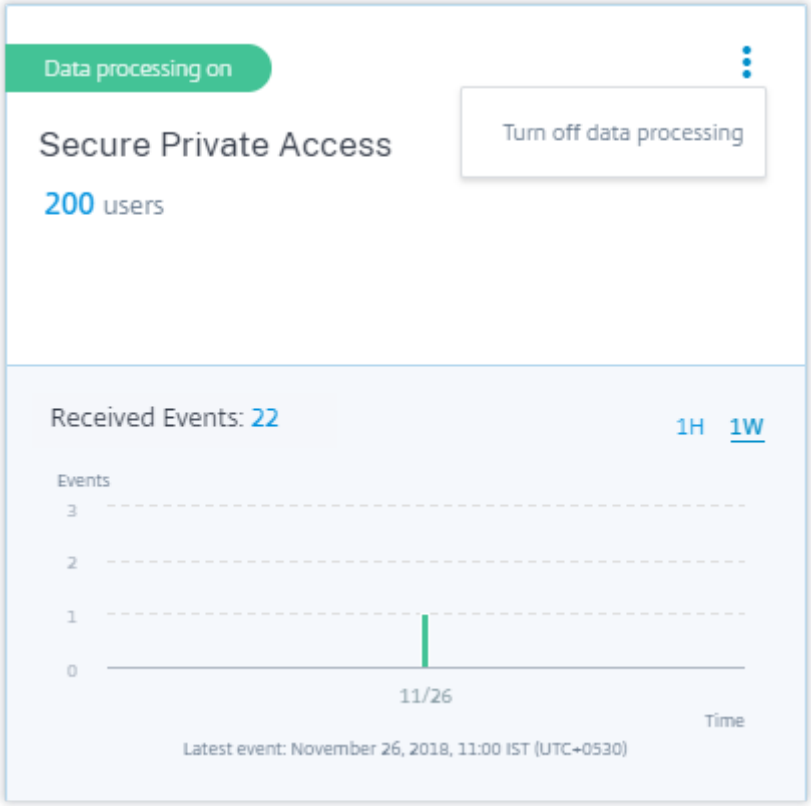
Une fois le traitement des données activé, la fiche de site peut afficher l'état **Aucune donnée reçue** . Cet état apparaît pour deux raisons :

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.

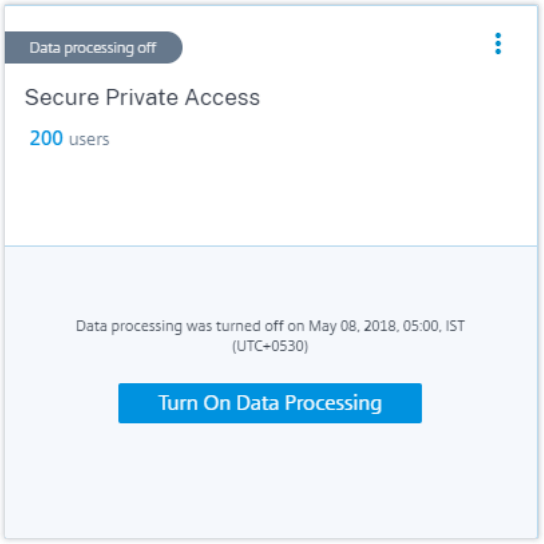


Activer ou désactiver le traitement des données

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**.



Source de données Citrix Virtual Apps and Desktops et Citrix DaaS

April 12, 2024

La source de données **Apps and Desktops** représente Citrix Virtual Apps and Desktops et Citrix DaaS (anciennement le Citrix Virtual Apps and Desktops Service) locaux au sein de votre organisation.

Citrix Analytics for Security prend en charge à la fois les offres et reçoit des événements utilisateur de la source de données. Cet article décrit les prérequis et les procédures permettant d'activer Analytics sur les deux offres.

Citrix Analytics for Security reçoit les événements utilisateur des composants suivants de la source de données Citrix Virtual Apps and Desktops et Citrix DaaS :

- Application Citrix Workspace installée sur les machines utilisateur
- Citrix Director pour le déploiement sur site
- Service Citrix Monitor
- serveurs d'enregistrement de session

Les événements utilisateur sont reçus en temps réel dans Citrix Analytics for Security lorsque les utilisateurs utilisent des applications virtuelles ou des bureaux virtuels.

Versions client prises en charge

Citrix Analytics reçoit des événements utilisateur lorsqu'une version client prise en charge est utilisée sur les points de terminaison utilisateur. Si les utilisateurs utilisent des versions de client non prises en charge, ils doivent mettre à niveau leurs clients vers l'une des versions suivantes :

- Application Citrix Workspace pour Windows 1907 ou version ultérieure
- Application Citrix Workspace pour Mac 1910.2 ou version ultérieure
- Application Citrix Workspace pour HTML5 2007 ou version ultérieure
- Application Citrix Workspace pour Chrome - Dernière version disponible dans le Chrome Web Store
- Application Citrix Workspace pour Android - Dernière version disponible dans Google Play
- Application Citrix Workspace pour iOS : dernière version disponible dans l'App Store d'Apple
- Application Citrix Workspace pour Linux 2006 ou version ultérieure

Activer Analytics sur Citrix DaaS

Conditions préalables

- Abonnez-vous aux Citrix DaaS proposés sur Citrix Cloud. Pour savoir comment démarrer avec Citrix DaaS, consultez la section Installer et configurer.

- Consultez la section **Configuration système requise** et vérifiez que vous répondez à la configuration requise.

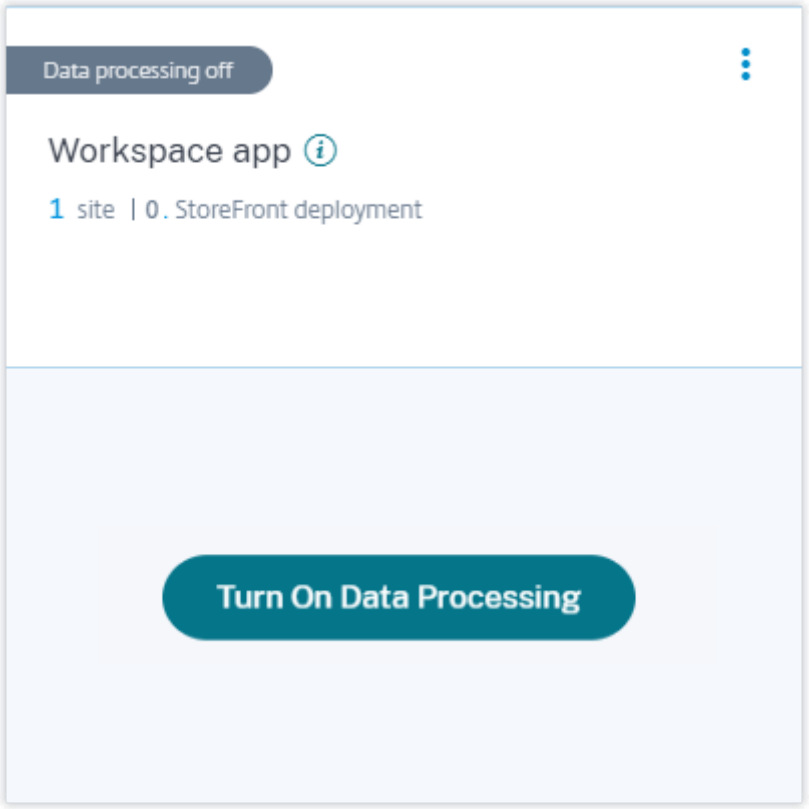
Afficher la source de données et activer le traitement des données

Citrix Analytics découvre automatiquement les Citrix DaaS associés à votre compte Citrix Cloud.

Pour consulter la source de données :

Dans la barre supérieure, cliquez sur **Paramètres** > **Sources de données** > **Sécurité**.

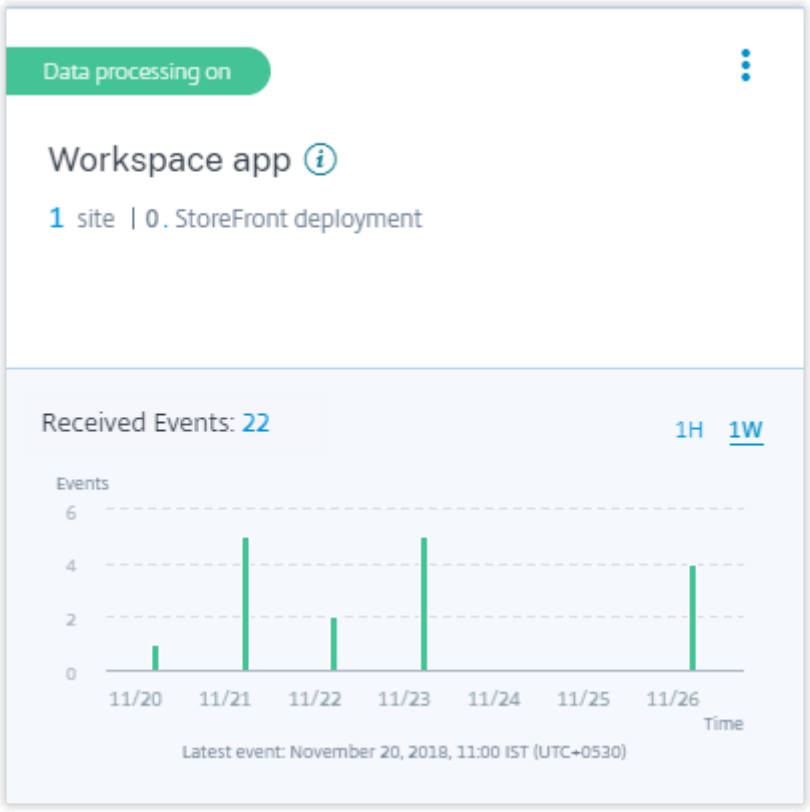
La fiche de site de l'**application Apps and Desktops- Workspace** apparaît sur la page **Sources de données** . Cliquez **sur Activer le traitement des données** pour permettre à Citrix Analytics de commencer à traiter les données de cette source de données.



Afficher le site cloud, les utilisateurs et les événements reçus

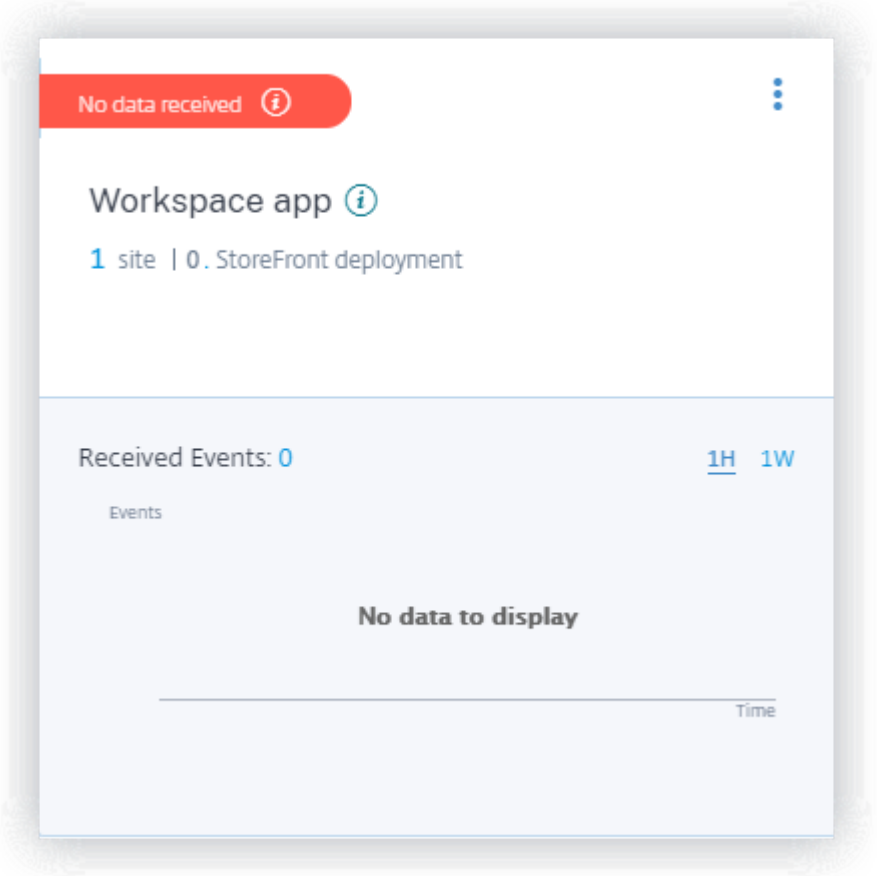
La fiche de site affiche le nombre d'utilisateurs Apps and Desktops, le site cloud découvert et les événements reçus au cours de la dernière heure, qui correspond à la sélection de l'heure par défaut. Vous pouvez également sélectionner 1 semaine (1 W) et afficher les données.

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. Analytics n'a reçu aucun événement de la source de données au cours de la dernière heure.



Activer Analytics sur Citrix Virtual Apps and Desktops sur site

Citrix Analytics reçoit des événements utilisateur provenant de sites locaux ajoutés à Workspace et de sites accessibles via des déploiements StoreFront.

Si votre organisation utilise des sites locaux, vous devez utiliser l'une des méthodes suivantes pour intégrer vos sites afin qu'Analytics découvre les sites :

- Intégrez vos sites locaux à l'aide de StoreFront
- Intégration de vos sites locaux à l'aide de Workspace

Conditions préalables

- Vous devez disposer d'une licence pour utiliser la solution locale Citrix Virtual Apps and Desktops. Pour savoir comment démarrer avec Citrix Virtual Apps and Desktops sur site, consultez la section Installer et configurer.
- Consultez la section **Configuration système requise** et vérifiez que vous répondez à la configuration requise.

- Votre Director utilise la version 1912 CU2 ou ultérieure. Pour de plus amples informations, consultez la section Tableau de compatibilité des fonctionnalités.
- **Abonnement à Citrix Workspace**. Si vous souhaitez ajouter vos sites à Citrix Workspace, vous devez disposer d'un abonnement Workspace.

  Pour acheter un abonnement Citrix Workspace, rendez-vous sur https://www.citrix.com/products/citrix-workspace/get-started.html et contactez un expert Citrix Workspace qui pourra vous aider.
- **Sites ajoutés à Workspace**. Citrix Analytics détecte automatiquement les sites ajoutés à Citrix Workspace. Ajoutez vos sites à Citrix Workspace avant de procéder à l'intégration sur Citrix Analytics. Ce processus est appelé **Agrégation de sites**.

  L'agrégation de sites nécessite l'installation de Cloud Connector, la configuration des serveurs STA NetScaler Gateway Gateway pour la connectivité interne et externe aux ressources Workspace, puis l'ajout des sites à Workspace. Pour obtenir des instructions détaillées sur l'agrégation de sites, consultez Agrégation d'applications et de bureaux virtuels locaux dans des espaces de travail.
- **Version StoreFront**. Si vous utilisez un déploiement StoreFront pour vos sites, assurez-vous que la version StoreFront est 1906 ou ultérieure.

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

Pour plus d'informations sur les prérequis et les étapes d'intégration, consultez l'article sur la source de données Citrix Virtual Apps and Desktops dans la documentation de la plate-forme Citrix Analytics.

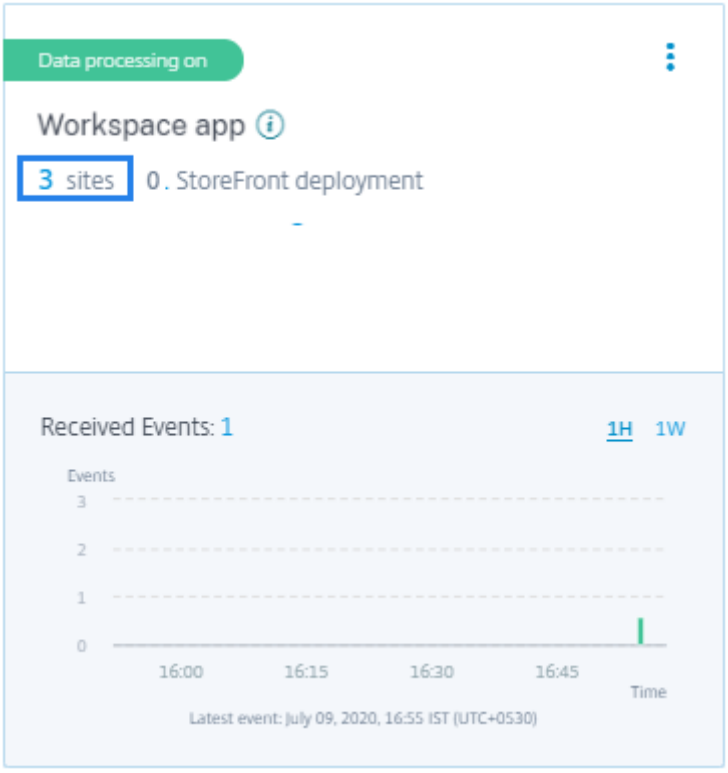
Sites locaux Citrix Virtual Apps and Desktops intégrés à l'aide de Workspace

Sites déjà ajoutés à Citrix Workspace Citrix Analytics détecte automatiquement les sites locaux déjà ajoutés à Citrix Workspace et les affiche sur la fiche de site de la source de données.

Pour consulter la source de données :

Dans la barre supérieure, cliquez sur **Paramètres** > **Sources de données** > **Sécurité**.

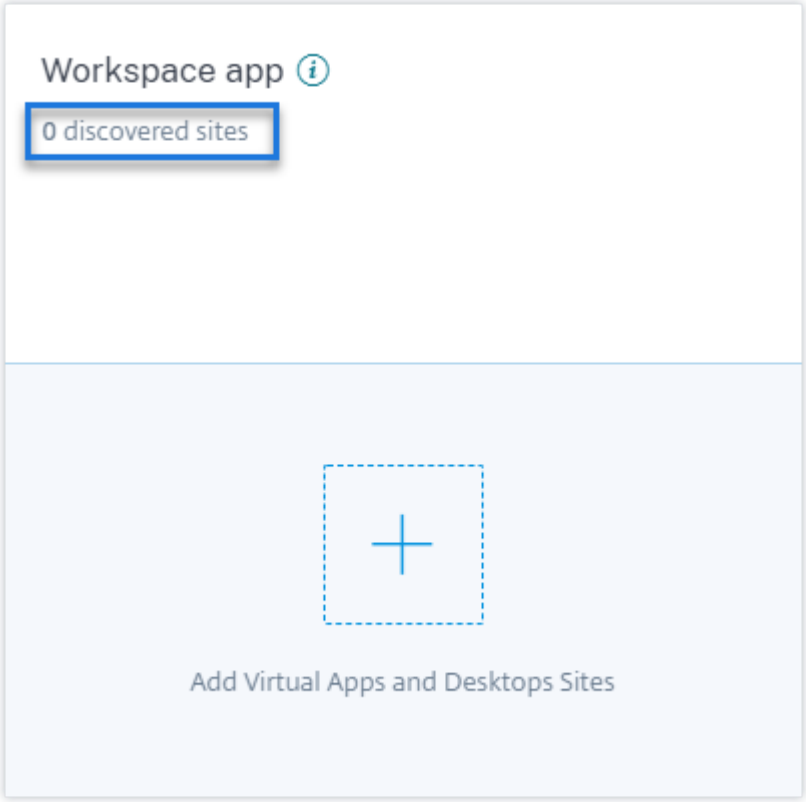
La carte de site **Apps and Desktops** affiche le nombre de sites ajoutés à Workspace et les utilisateurs connectés à ces sites. Cliquez sur le nombre de sites pour afficher les sites découverts. Cliquez sur le nombre d'utilisateurs pour afficher les utilisateurs découverts sur la page **Utilisateurs** .



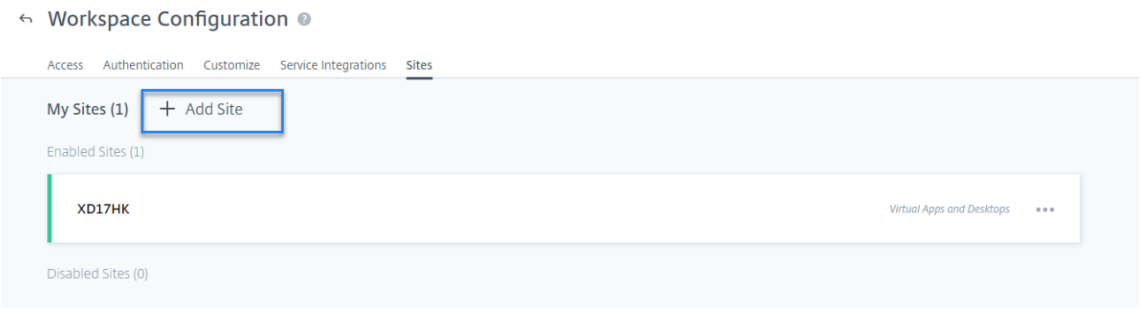
Sites non ajoutés à Citrix Workspace Si vous n'avez pas encore ajouté vos sites locaux à Workspace, Analytics ne peut pas détecter vos sites. La fiche de site affiche **0 sites découverts**.

Pour ajouter un site à Workspace :

1. Cliquez sur + sur la fiche de site.



2. Sur la page **Configuration de l'espace de travail**, cliquez sur **+Ajouter un site**.

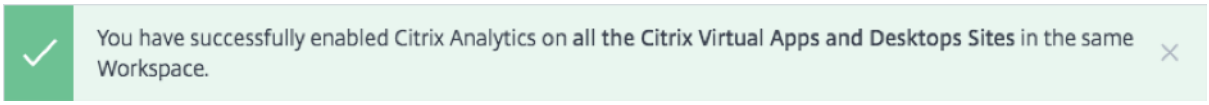


3. Suivez les instructions à l'écran pour ajouter un site. Pour plus d'informations, consultez la rubrique Agréger des applications et bureaux virtuels locaux dans des espaces de travail.
4. Après avoir ajouté le site, reconnectez-vous à Citrix Analytics et actualisez la page **Sources de données** pour afficher le site récemment ajouté sur la fiche de site.

Activer le traitement des données et afficher les événements reçus Pour permettre à Analytics de commencer à traiter les données des sites découverts, cliquez **sur Activer le traitement des données** sur la fiche de site et suivez les instructions à l'écran.

Si plusieurs sites sont ajoutés au même espace de travail, Analytics traite et stocke les données de tous les sites de l'espace de travail. Un message de réussite s'affiche lorsque Analytics est correctement

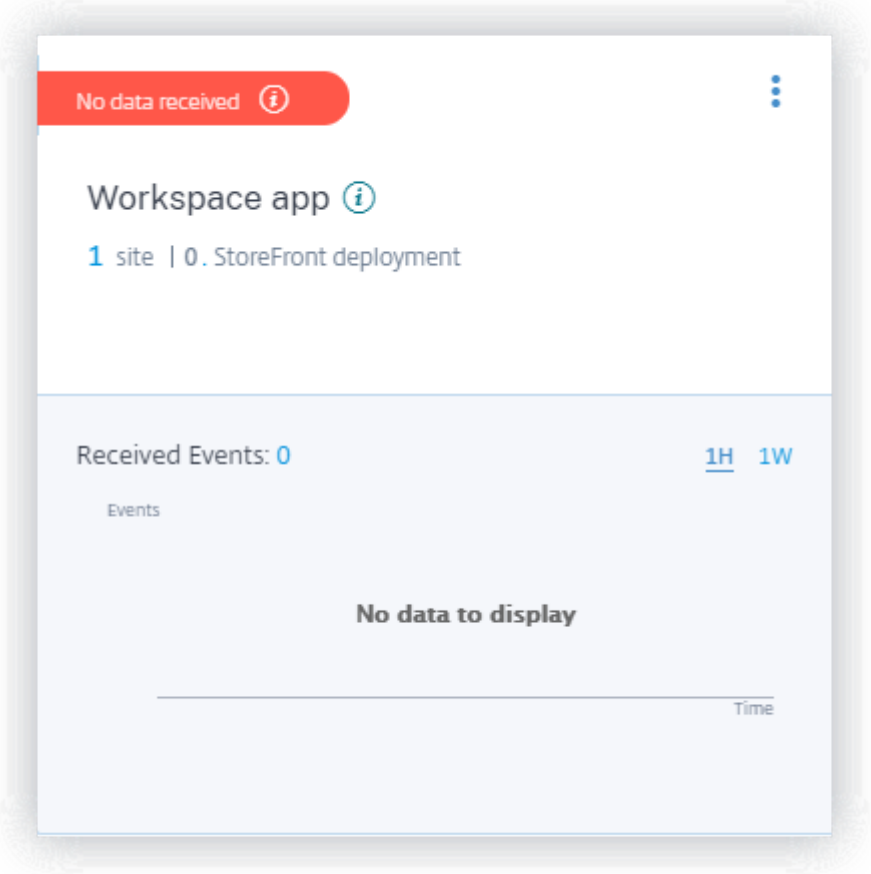
activé sur tous vos sites.



La fiche de site affiche les événements reçus au cours de la dernière heure, qui est la sélection d'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 correspondante.

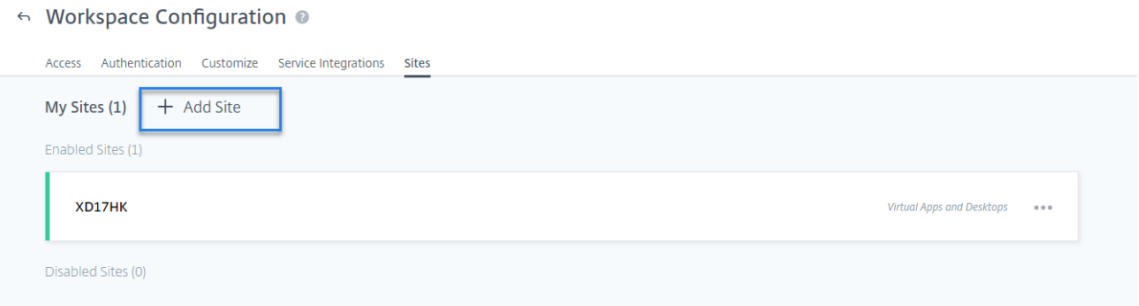
Une fois que vous avez activé le traitement des données, la carte de site peut afficher l'état **No data received** (Aucune donnée reçue). Cet état apparaît pour deux raisons :

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.



Ajouter un site Si vous souhaitez ajouter un autre site local à Workspace, vous pouvez l'ajouter à partir d'Analytics :

1. Sur la page Configuration de l'espace de travail, cliquez sur **+Ajouter un site.**



2. Suivez les instructions à l'écran pour ajouter un site. Pour plus d'informations, consultez la rubrique Agréger des applications et bureaux virtuels locaux dans des espaces de travail.
3. Après avoir ajouté le site, accédez à Citrix Analytics et actualisez la page **Sources de données** pour afficher le site récemment ajouté sur la fiche de site.

Connexion à Citrix Director pour les sites locaux

Citrix Director est une console de surveillance et de dépannage pour Citrix Virtual Apps and Desktops. Vous pouvez utiliser Director pour configurer vos sites locaux pour Citrix Analytics for Security (Security Analytics). Une fois les sites configurés, Director envoie les événements de surveillance à Security Analytics.

Si vous utilisez Citrix DaaS, le service Citrix Monitor envoie les événements de votre site cloud à Security Analytics.

Dans un environnement hybride où vous avez des déploiements dans le cloud et sur site, Security Analytics reçoit des événements du service Citrix Monitor et des sites intégrés sur Citrix Director.

Prérequis et étapes de configuration

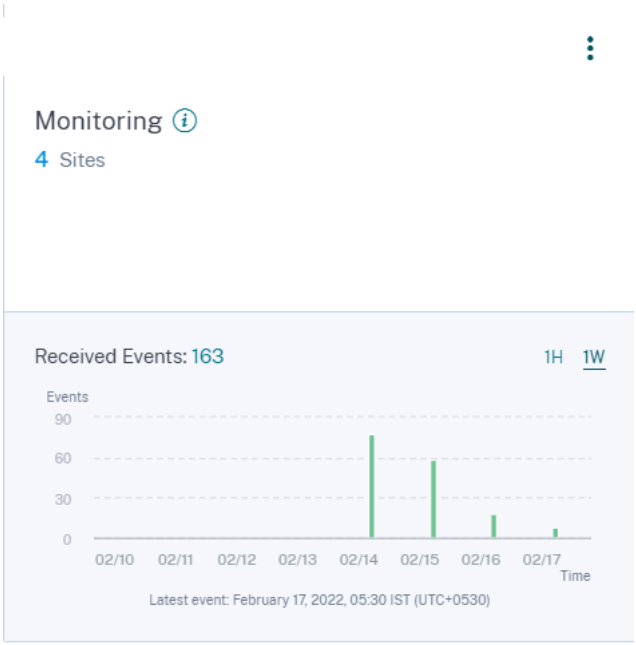
> **Remarques**
>
> - Actuellement, l'interface utilisateur de Director affiche les étapes de configuration liées à Citrix Analytics for Performance (Performance Analytics). Ces étapes de configuration s'appliquent également à Citrix Analytics for Security (Security Analytics). Si vous disposez d'un droit Citrix Cloud actif pour Security Analytics, vous pouvez vous connecter à Citrix Director en suivant ces étapes.
> - Si votre compte Citrix Cloud possède des droits actifs pour Security Analytics et Perfor-

> mance Analytics et que vous avez déjà configuré votre site pour Performance Analytics, vous n'avez pas besoin de configurer à nouveau Director pour Security Analytics.

Pour plus d'informations sur les conditions préalables et les étapes de configuration, consultez la documentation Citrix Analytics for Performance.

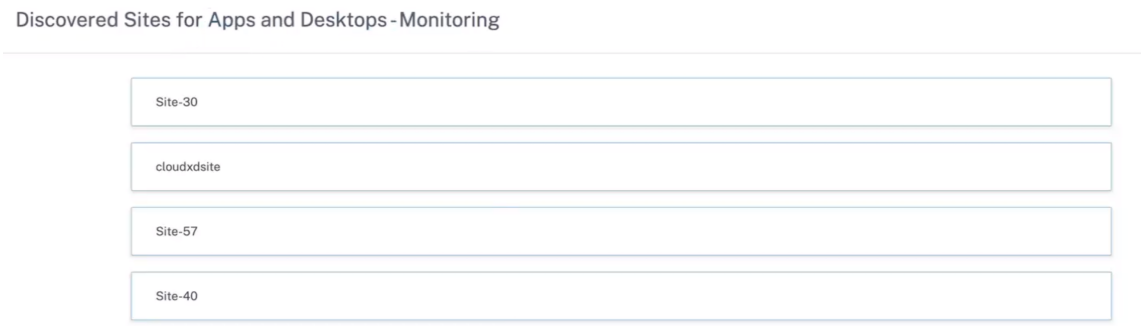
Afficher vos sites connectés et les événements reçus

1. Dans Citrix Analytics, accédez à la page **Sources de données** .
2. Cliquez sur l'onglet **Sécurité**.
3. Sur la carte de site **Apps and Desktops- Monitoring**, vous pouvez afficher vos sites locaux ou le site cloud (selon le cas). Vous pouvez également consulter les événements reçus des sites.



> **Remarques**
>
> - La première fois que vous configurez un site local sur Director, le traitement des événements du site peut prendre un certain temps (environ une heure), ce qui entraîne un retard dans l'affichage du site connecté sur la carte de site **Surveillance des applications et des bureaux** .
> - Sur la carte de site Monitoring, le traitement des données pour le service Monitor ou la source de données Director est activé par défaut. Vous pouvez également désactiver le traitement des données en fonction de vos besoins. Cependant, il est recommandé de poursuivre le traitement des données afin de tirer le meilleur parti de Security Analytics.

4. Cliquez sur le site pour afficher les détails.



Déploiement Connexion à l'enregistrement de session

L'enregistrement de session vous permet d' enregistrer l'activité à l'écran de n'importe quelle session utilisateur dans Citrix Virtual Apps and Desktops et Citrix DaaS. Vous pouvez configurer les serveurs d'enregistrement de session pour envoyer les événements utilisateur à Citrix Analytics for Security. Les événements utilisateur sont traités pour fournir des informations exploitables sur les comportements à risque des utilisateurs.

Conditions préalables

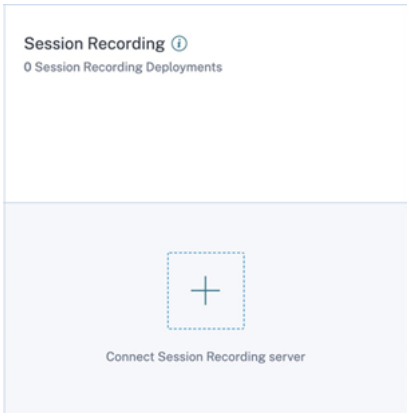
Avant de commencer, vérifiez les points suivants :

- Votre serveur d'enregistrement de session et l'agent VDA doivent être 2103 ou version ultérieure.
- Le serveur d'enregistrement de session doit pouvoir se connecter aux adresses requises. Pour plus d'informations sur les URL, consultez la section Configuration réseau requise.
- Le port 443 du déploiement d'enregistrement de session doit être ouvert pour les connexions Internet sortantes. Tous les serveurs proxy du réseau doivent autoriser cette communication avec Citrix Analytics for Security.
- Si vous utilisez Citrix Virtual Apps and Desktops 7 1912 LTSR, la version d'enregistrement de session prise en charge est 2103 ou ultérieure.

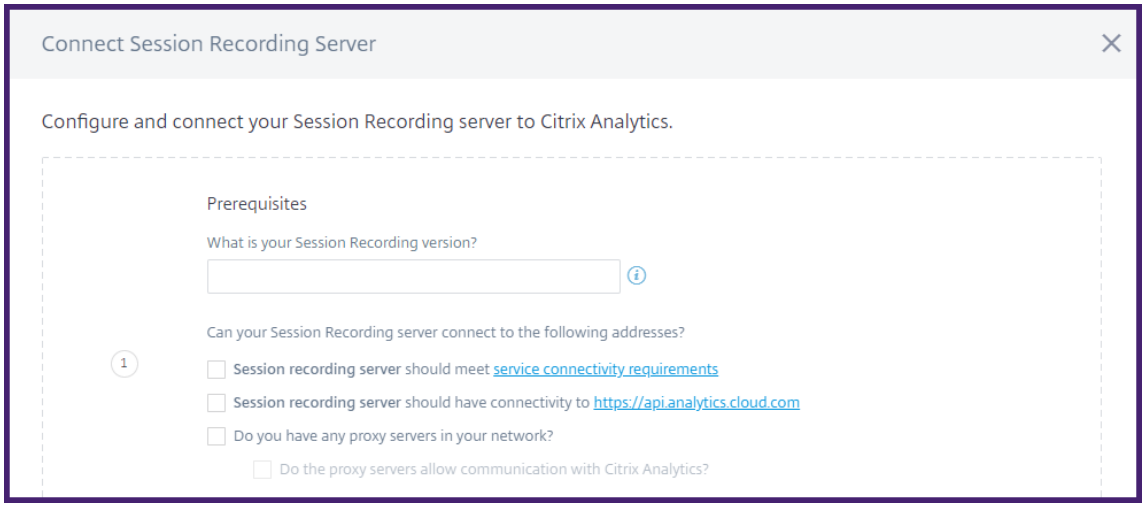
> **Remarque**
>
> Assurez-vous de vérifier les exigences de connectivité supplémentaires lors de l'utilisation du service **d'enregistrement de session** .

Configurez votre serveur d'enregistrement de session

1. Sur la carte de site **Apps and Desktops - Enregistrement de session**, cliquez sur **Connecter le serveur d'enregistrement de session**.



2. Sur la page **Connecter Serveur d'enregistrement de session**, consultez la liste de contrôle et sélectionnez toutes les conditions obligatoires. Si vous ne sélectionnez aucune condition obligatoire, l'option Télécharger le fichier est désactivée.



3. Si vous avez des serveurs proxy sur votre réseau, saisissez l'adresse proxy dans le fichier *SSREC-StorageManager.exe.config* de votre serveur d'enregistrement de session.

   Le fichier de configuration se trouve sous `<Session Recording Server installation path>\bin\SsRecStorageManager.exe.config`

   Pa exemple : `C:\Program Files\Citrix\SessionRecording\Server\Bin\SsRecStorageManager.exe.config`

4. Cliquez sur **Télécharger le fichier** pour télécharger le fichier *SessionRecordingConfigurationFile.json* .

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

5. Copiez le fichier sur le serveur d'enregistrement de session que vous souhaitez connecter à Citrix Analytics for Security.
6. Si votre déploiement comporte plusieurs serveurs d'enregistrement de session, vous devez copier le fichier sur chaque serveur auquel vous souhaitez vous connecter et suivre les étapes de configuration pour chaque serveur.
7. Sur le serveur d'enregistrement de session, exécutez la commande suivante pour importer les paramètres :

   ```
   <Session Recording Server installation path>\bin\SsRecUtils.exe -
       Import_SRCasConfigurations <configuration file path>
   ```

   Par exemple :

   ```
   C:\Program Files\Citrix\SessionRecording\Server\bin\ SsRecUtils.
   exe -Import_SRCasConfigurations C:\Users\administrator \Downloads
   \SessionRecordingConfigurationFile.json
   ```

8. Redémarrez les services suivants :

   - Service d'analyse de l'enregistrement de session Citrix
   - Gestionnaire de stockage d'enregistrement de session Citrix

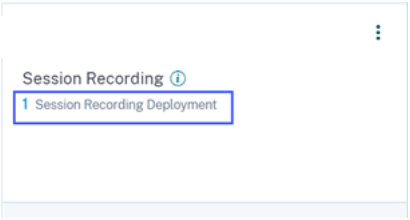
9. Une fois la configuration terminée, accédez à Citrix Analytics for Security pour afficher le serveur d'enregistrement de session connecté. Cliquez **sur Activer le traitement des données** pour permettre à Citrix Analytics for Security de traiter les données.

> **Remarque**
>
> Si vous utilisez le serveur d'enregistrement de session version 2103 ou 2104, vous devez d'abord lancer une session Apps and Desktops pour afficher le serveur d'enregistrement de session connecté sur Citrix Analytics pour la sécurité. Sinon, le serveur d'enregistrement de session connecté ne s'affiche pas. Cette exigence ne s'applique pas aux versions 2106 et ultérieures du serveur d'enregistrement de session.

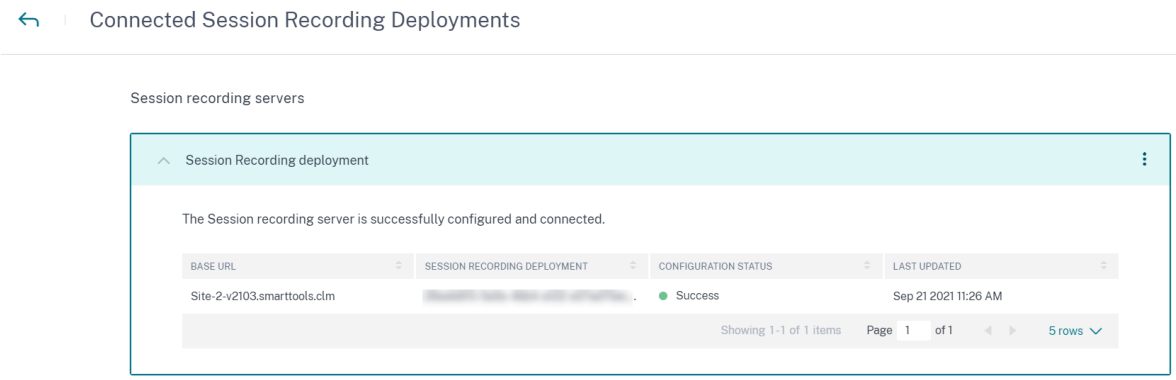
Afficher les déploiements connectés

Les déploiements de serveurs apparaissent sur la carte de site Enregistrement de session uniquement si la configuration est réussie. La fiche de site indique le nombre de serveurs configurés qui ont établi des connexions avec Citrix Analytics for Security.

Si vous ne voyez pas vos serveurs d'enregistrement de session même après la réussite de la configuration, reportez-vous à l'article Dépannage.



Sur la fiche de site, cliquez sur le nombre de déploiements pour afficher les groupes de serveurs connectés avec Citrix Analytics for Security. Par exemple, cliquez sur **1 déploiement d'enregistrement de session** pour afficher le ou les groupes de serveurs connectés. Chaque serveur d'enregistrement de session est représenté par une URL de base et un ServerGroupID.



Afficher les événements reçus

La carte de site affiche les déploiements d'enregistrement de session connectés et les événements reçus de ces déploiements au cours de la dernière heure, qui est la période sélectionnée 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.

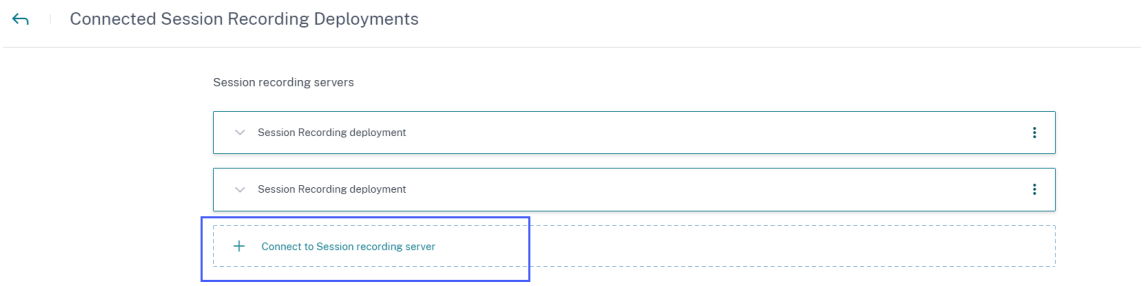
Une fois que vous avez activé le traitement des données, la carte de site peut afficher l'état **No data received** (Aucune donnée reçue). Cet état apparaît pour deux raisons :

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 des sources de données.
2. Citrix Analytics n'a reçu aucun événement de la source de données au cours de la dernière heure.

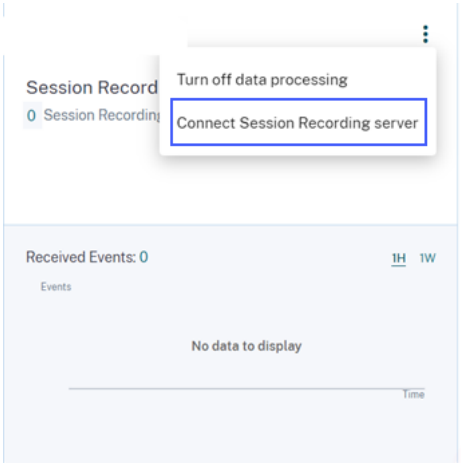
Ajouter des serveurs d'enregistrement de session

Pour ajouter un serveur d'enregistrement de session, effectuez l'une des opérations suivantes :

- Sur la page des **déploiements d'enregistrement de session connectés**, cliquez sur **Connecter Serveur d'enregistrement de session**.



- Sur la fiche de site **Apps and Desktops - Enregistrement de session**, cliquez sur les points de suspension verticaux (), puis sélectionnez **Connecter le serveur d'enregistrement de session**.

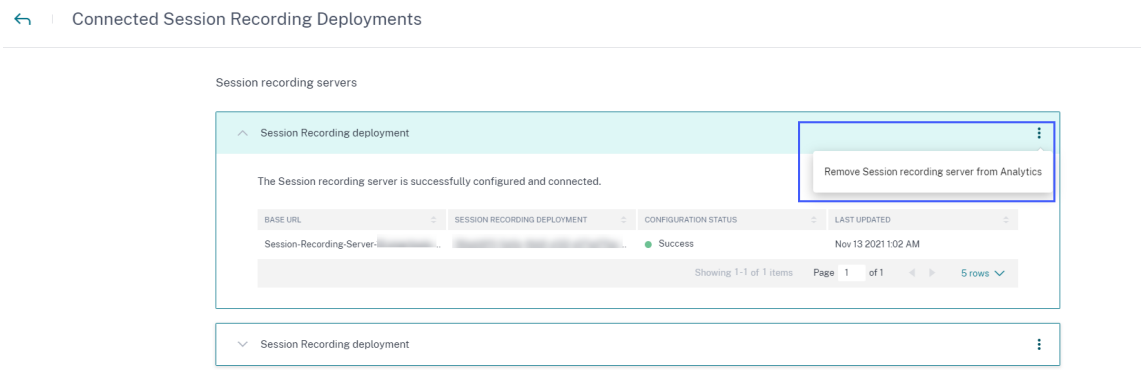


Suivez les étapes pour télécharger le fichier de configuration et configurer un serveur d'enregistrement de session.

Supprimer les serveurs d'enregistrement de session

Pour supprimer un serveur d'enregistrement de session :

1. Sur Citrix Analytics for Security, accédez à la page des **déploiements d'enregistrement de session connectés** et sélectionnez le déploiement de serveur que vous souhaitez supprimer.
2. Cliquez sur les points de suspension verticaux (⋮) et sélectionnez **Remove Session Recording server from Analytics**.



3. Sur le serveur d'enregistrement de session que vous avez supprimé de Citrix Analytics, exécutez la commande suivante :

```
<Session Recording Server installation path>\bin\SsRecUtils.exe -
    Remove_SRCasConfigurations
```

Par exemple :

```
C:\Program Files\Citrix\SessionRecording\Server\bin\ SsRecUtils.
exe -Remove_SRCasConfigurations
```


Activation de la télémétrie d'impression pour Citrix DaaS

Lorsque les utilisateurs effectuent des tâches d'impression dans Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service), vous pouvez afficher les journaux associés à ces tâches d'impression dans Citrix Analytics for Security. Ces journaux d'impression fournissent des informations vitales sur les activités d'impression telles que les noms des imprimantes, les noms des fichiers d'impression et le nombre total de copies imprimées.

> **Remarque**
>
> Cette fonctionnalité n'est prise en charge que pour Citrix DaaS.

Dans Citrix Analytics for Security, sur la page **de recherche**, vous pouvez sélectionner la source de données **Apps and Desktops** pour afficher les journaux d'impression. En tant qu'administrateur de la sécurité, vous pouvez utiliser ces journaux pour analyser les risques et enquêter sur vos utilisateurs.

Par défaut, la fonction de télémétrie d'impression, qui est la collecte et la transmission de ces journaux d'impression, est désactivée sur les Virtual Delivery Agents (VDA).

Pour activer la télémétrie d'impression et la transmission des journaux d'impression à Citrix Analytics for Security, vous devez créer des clés de registre et configurer votre VDA.

> **Important**
>
> Cette configuration ne s'applique qu'aux VDA Windows.

Conditions préalables

- La version de votre VDA doit être identique à la version de référence pour Citrix Virtual Apps and Desktops 7 2203 LTSR ou version ultérieure. Pour plus d'informations, consultez Composants de base de Citrix Virtual Apps and Desktops 7 2203.
- Vous devez disposer d'autorisations d'accès complètes pour effectuer les mises à jour de la clé de registre.

Activer la télémétrie d'impression sur les machines gérées par l'alimentation

Les machines gérées par l'alimentation incluent des machines virtuelles ou des PC lames avec les scénarios suivants :

- Image principale existante
- Nouvelle image principale

Activer la télémétrie d'impression pour une image principale existante dont la version du VDA est inférieure à celle de Citrix Virtual Apps and Desktops 7 2203 LTSR

1. Connectez-vous à la machine VDA principale et créez un instantané de l'état actuel.
2. Activez les journaux du service d'impression en ajoutant les clés de registre suivantes :

   - Microsoft-Windows-PrintService/Operational
   - ShowJobTitleInEventLogs

   Pour plus d'informations sur les clés de registre, voir Créer des clés de registre.
3. Mettez à niveau le VDA vers une version de base pour Citrix Virtual Apps and Desktops 7 2203 LTSR ou version ultérieure. Pour plus d'informations, consultez Composants de base de Citrix Virtual Apps and Desktops 7 2203.
4. Mettez la machine hors tension et prenez un instantané de l'état le plus récent.
5. Connectez-vous à Citrix Cloud. Sélectionnez le catalogue de machines, cliquez sur **Mettre à jour les machines**et suivez les instructions à l'écran. Pour de plus amples informations, consultez l'article Créer des catalogues de machines.
6. Attendez 24 heures. La configuration est automatiquement poussée dans les 24 heures. Si la configuration est déjà terminée, vous n'avez pas besoin d'attendre.
7. Démarrez une session de bureau avec l'application Citrix Workspace. Tous les événements d'impression déclenchés à l'aide de l'imprimante cliente sont visibles sur la page de **recherche** de Citrix Analytics for Security.

Activer la télémétrie d'impression pour une image principale existante dont la version du VDA est identique à celle de Citrix Virtual Apps and Desktops 7 2203 LTSR ou version ultérieure Option 1 : ajoutez les clés de registre d'impression dans le VDA maître et mettez à jour les bureaux virtuels.

1. Connectez-vous à la machine VDA principale et créez un instantané de l'état actuel.
2. Activez les journaux du service d'impression en ajoutant les clés de registre suivantes :

   - Microsoft-Windows-PrintService/Operational
   - ShowJobTitleInEventLogs

   Pour plus d'informations sur les clés de registre, voir Créer des clés de registre.
3. Mettez la machine VDA hors tension et prenez un instantané de l'état le plus récent.
4. Connectez-vous à Citrix Cloud, sélectionnez le catalogue de machines, cliquez sur **Mettre à jour les machines**et suivez les instructions qui s'affichent à l'écran.

5. Démarrez une session de bureau avec l'application Citrix Workspace. Tous les événements d'impression déclenchés à l'aide de l'imprimante cliente sont visibles sur la page de **recherche** de Citrix Analytics for Security.

Option 2 : déplacer le bureau virtuel vers l'unité d'organisation (OU) et créer des clés de registre à l'aide de l'objet de stratégie de groupe

> **Remarque La**
>
> méthode de l'option 2 ne fonctionne que pour les machines statiques. Pour les machines aléatoires, vous devez suivre la méthode de l'option 1 (comme mentionné ci-dessus).

1. Connectez-vous à la machine du contrôleur de domaine.
2. Activez les journaux du service d'impression en ajoutant les clés de registre suivantes :

   - Microsoft-Windows-PrintService/Operational
   - ShowJobTitleInEventLogs

   Pour plus d'informations sur les clés de registre, voir Créer des clés de registre.

> **Remarque**
>
> Dans tout contrôleur de domaine, la création des clés de registre est une tâche ponctuelle.

1. Redémarrez la machine VDA à partir de Citrix Cloud.
2. Démarrez une session de bureau avec l'application Citrix Workspace. Tous les événements d'impression déclenchés à l'aide de l'imprimante cliente sont visibles sur la page de **recherche** de Citrix Analytics for Security.

Activer la télémétrie d'impression dans une nouvelle image principale

1. Créez une machine virtuelle (VM) à l'aide de l'outil de gestion de l'hyperviseur. Cette machine virtuelle est traitée comme un VDA principal.
2. Assurez-vous que le VDA maître est ajouté au domaine requis.
3. Connectez-vous au VDA maître et activez les journaux du service d'impression en ajoutant les clés de registre suivantes :

   - Microsoft-Windows-PrintService/Operational
   - ShowJobTitleInEventLogs

   Pour plus d'informations, consultez la section Créer des clés de registre.
4. Installez la version du VDA pour Citrix Virtual Apps and Desktops 7 2203 LTSR ou version ultérieure. Lors de l'installation du VDA, sélectionnez l'option **Master Image** . Pour plus d'informations, consultez Composants de base de Citrix Virtual Apps and Desktops 7 2203.

5. Assurez-vous que la connexion d'hébergement est ajoutée à Citrix Cloud. Pour de plus amples informations, consultez l'article Créer des catalogues de machines.
6. Créez un catalogue de machines à l'aide de l'image principale. Pour de plus amples informations, consultez l'article Créer des catalogues de machines.
7. Créez un groupe de mise à disposition et ajoutez le catalogue de machines. Pour plus d'informations, consultez la section Créer des groupes de mise à disposition.
8. Attendez 24 heures. La configuration est automatiquement poussée dans les 24 heures par le moteur de stratégie de groupe.
9. Démarrez une session de bureau avec l'application Citrix Workspace. Tous les événements d'impression déclenchés à l'aide de l'imprimante cliente sont visibles sur la page de **recherche** de Citrix Analytics for Security.

Activer la télémétrie d'impression sur les machines qui ne sont pas gérées par l'alimentation

Les machines non gérées par l'alimentation incluent les ordinateurs physiques avec les scénarios suivants :

- VDA physique existant
- Nouveau VDA physique

Activer la télémétrie d'impression pour un VDA physique existant dont la version du VDA est inférieure à celle de Citrix Virtual Apps and Desktops 7 2203 LTSR

1. Activez les journaux du service d'impression en ajoutant les clés de registre suivantes :

   - Microsoft-Windows-PrintService/Operational
   - ShowJobTitleInEventLogs

   Pour plus d'informations, consultez la section Créer des clés de registre.
2. Mettez à niveau le VDA vers une version de base pour Citrix Virtual Apps and Desktops 7 2203 LTSR ou version ultérieure. Pour plus d'informations, consultez Composants de base de Citrix Virtual Apps and Desktops 7 2203.
3. Attendez 24 heures. La configuration est automatiquement poussée dans les 24 heures. Si la configuration est déjà terminée, vous n'avez pas besoin d'attendre.
4. Démarrez une session de bureau avec l'application Citrix Workspace. Tous les événements d'impression déclenchés à l'aide de l'imprimante cliente sont visibles sur la page de **recherche** de Citrix Analytics for Security.

Activer la télémétrie d'impression pour un nouveau VDA physique

1. Créez une machine virtuelle physique et remplacez le domaine par le nom de domaine requis.
2. Connectez-vous à la machine virtuelle et activez les journaux du service d'impression en ajoutant les clés de registre suivantes :

   - Microsoft-Windows-PrintService/Operational
   - ShowJobTitleInEventLogs

   Pour plus d'informations, consultez la section Créer des clés de registre.
3. Installez la version VDA pour Citrix Virtual Apps and Desktops 7 2203 LTSR ou version ultérieure. Lors de l'installation du VDA, sélectionnez l'option Remote PC Access.
4. Créez un catalogue de machines. Pour de plus amples informations, consultez l'article Créer des catalogues de machines.

   > **Remarque La**
   >
   > gestion des machines doit être sélectionnée en tant **que machines qui ne sont pas gérées par l'alimentation (par exemple, des machines physiques)**.

5. Créez un groupe de mise à disposition et ajoutez le catalogue de machines. Pour plus d'informations, consultez la section Créer des groupes de mise à disposition.
6. Attendez 24 heures. La configuration est automatiquement poussée dans les 24 heures par le moteur de stratégie de groupe.
7. Démarrez une session de bureau avec l'application Citrix Workspace. Tous les événements d'impression déclenchés à l'aide de l'imprimante cliente sont visibles sur la page de **recherche** de Citrix Analytics for Security.

Création de clés de registre

Dans votre VDA, utilisez l'une des options suivantes :

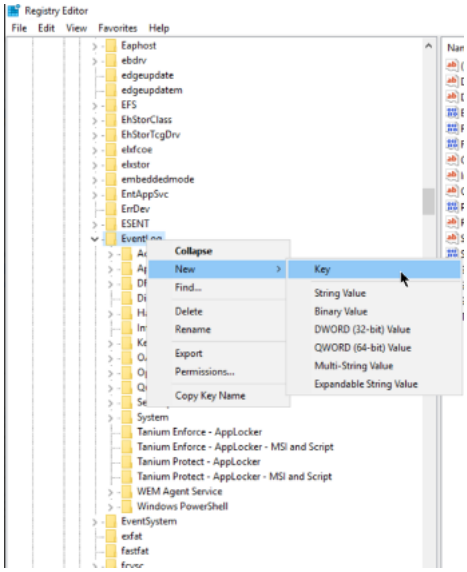
- Créez des clés de registre manuellement. Utilisez cette méthode pour les VDA maîtres et pour avoir un plus petit nombre de VDA physiques dans votre déploiement.
- Créez des clés de registre à l'aide d'un objet de stratégie de groupe (GPO). Utilisez cette méthode lorsque votre déploiement comporte un plus grand nombre de machines VDA physiques et que vous devez activer la télémétrie d'impression sur chacune d'entre elles.

Détails des clés de registre

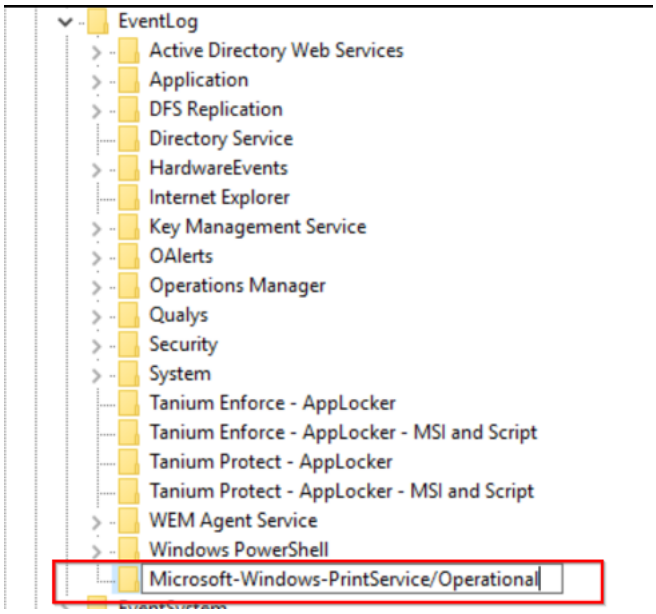
SL	Nom de clé de registre	Objectif de la clé	Détails du registre
1	Microsoft-Windows-PrintService/Operational	Permet d'imprimer les journaux de service dans l'observateur d'événements.	**Chemin d'accès au registre** : HKLM:\SYSTEM\CurrentControlSet\
2	ShowJobTitleInEventLogs	Contrôle si le nom de la tâche d'impression est inclus dans les journaux d'événements d'impression, sinon considère le nom générique de la tâche « Imprimer le document ».	**Ruche de registre** : HKEY_LOCAL_MACHINE **Chemin d'accès au registre** : Software \ Policies \ Microsoft \ Windows NT \ Printers **Nom de la valeur** : ShowJobTitleInEvent-Logs **Type de valeur** : REG_DWORD **Valeur** : 1

Création manuelle de clés de registre sur une machine VDA Utilisez cette approche pour créer la clé de registre dans l'image principale du VDA. L'ajout de clés à l'image principale permet de conserver les clés persistantes pour tous les types de VDA créés à l'aide de l'image principale.

1. Connectez-vous à la machine principale du VDA.
2. Ouvrez Exécuter et tapez Regedit pour ouvrir le registre Windows.
3. Accédez à l'emplacement HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ EventLog
4. Cliquez avec le bouton droit sur **EventLog** et sélectionnez **Nouveau > Clé**.

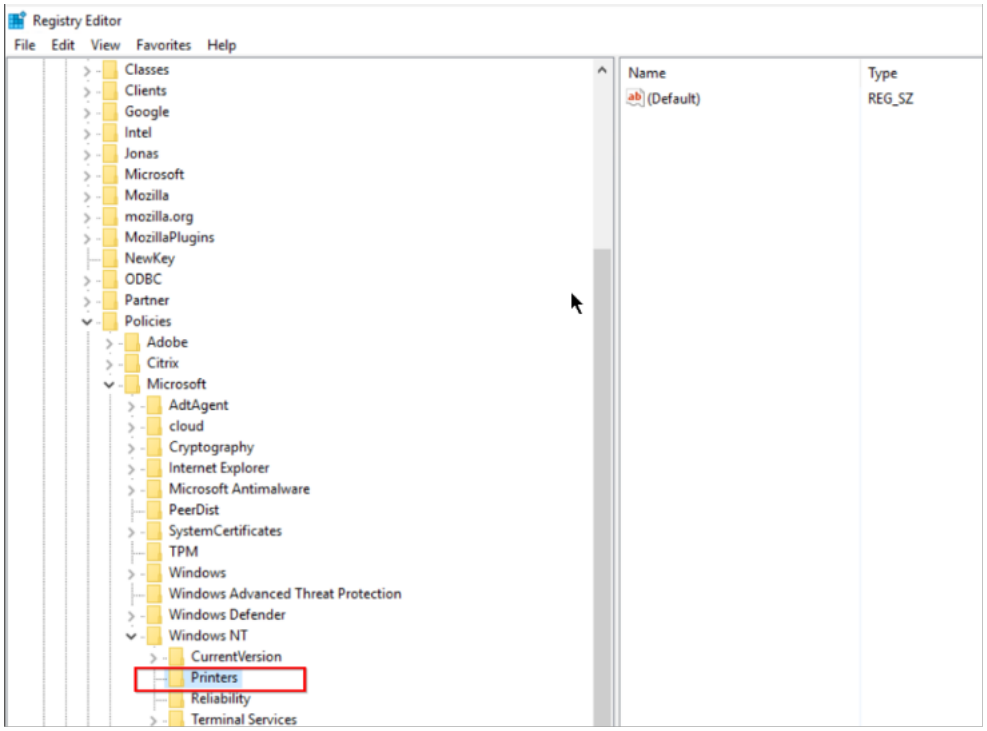


5. Créez une clé portant le nom **Microsoft-Windows-PrintService/Operational**. Cette clé active les journaux du service d'impression.

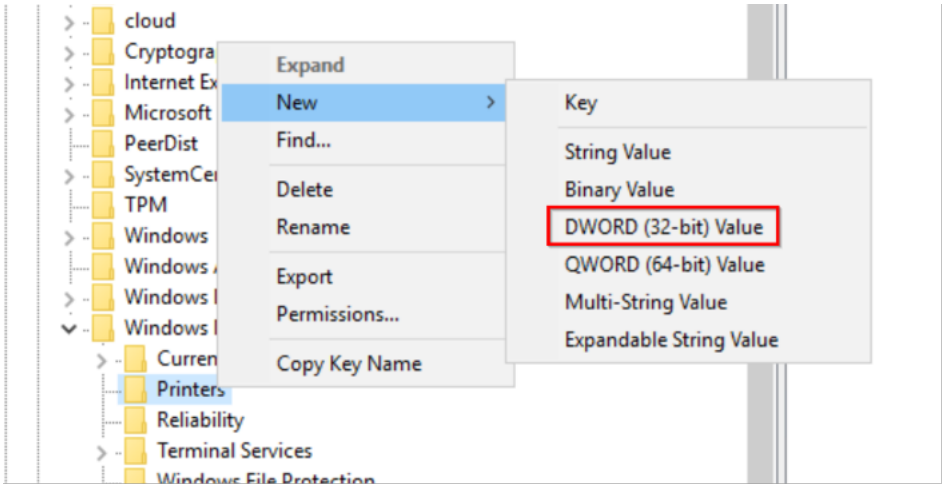


6. Accédez à l'emplacement **HKEY_LOCAL_MACHINE \ Software \ Policies \ Microsoft \ Windows NT \ Printers**.

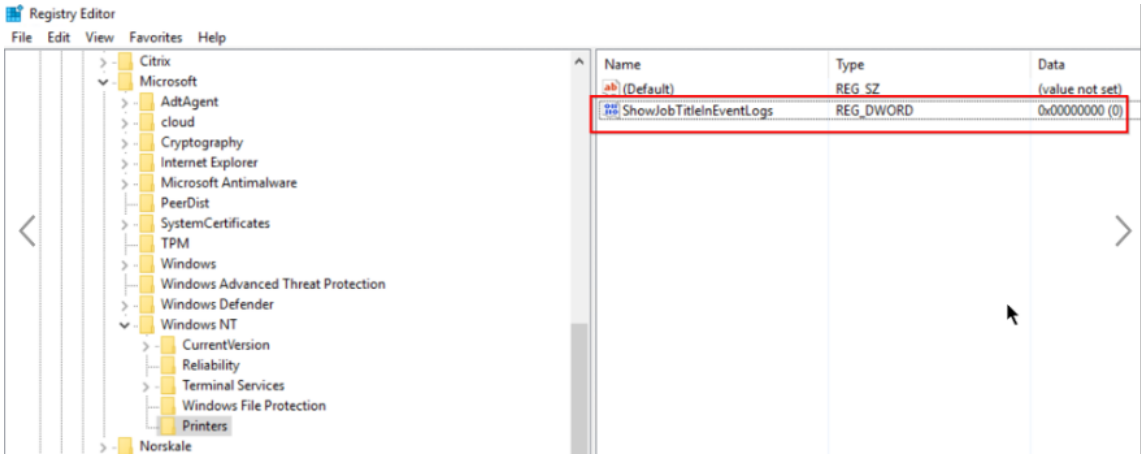
> **Remarque**
>
> Si le dossier Imprimantes n'est pas disponible, créez une clé portant le nom Printers dans le dossier Windows NT.



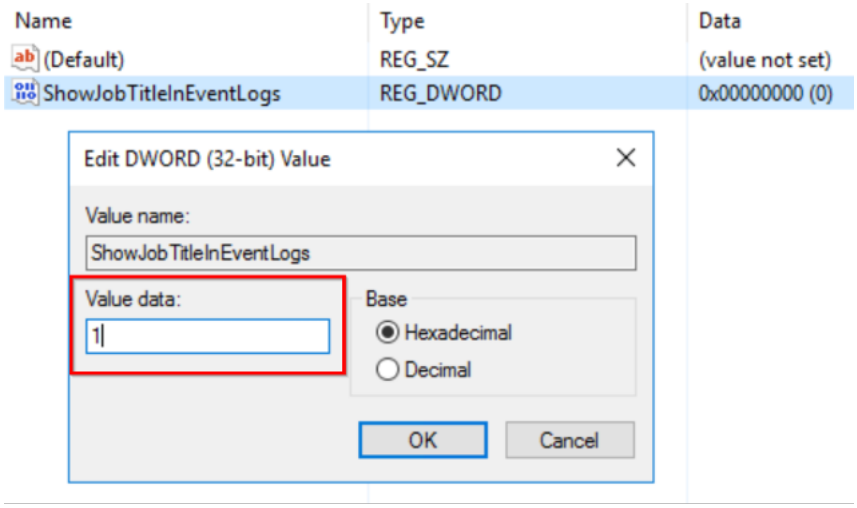
7. Cliquez avec le bouton droit sur le dossier **Imprimantes** et sélectionnez **Nouveau > Valeur DWORD (32 bits)**.



8. Créez une valeur nommée **ShowJobTitleInEventLogs**.



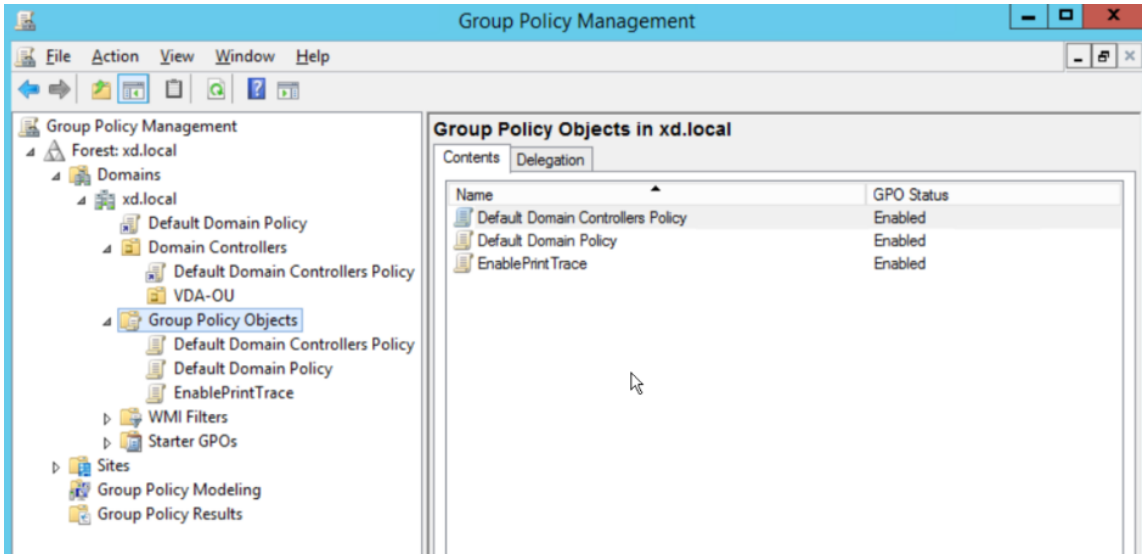
9. Faites un clic droit sur **ShowJobTitleInEventLogs** et sélectionnez **Modifier**. Entrez les **données de valeur** sous la forme 1 et cliquez sur **OK**.



Créer des clés de registre dans plusieurs VDA à l'aide de GPO Cette approche fonctionne uniquement pour les VDA persistants et nécessite le redémarrage des VDA après la création des clés de registre. Un VDA persistant est une machine qui conserve son état après un redémarrage. Les données des utilisateurs ne sont pas perdues après le redémarrage.

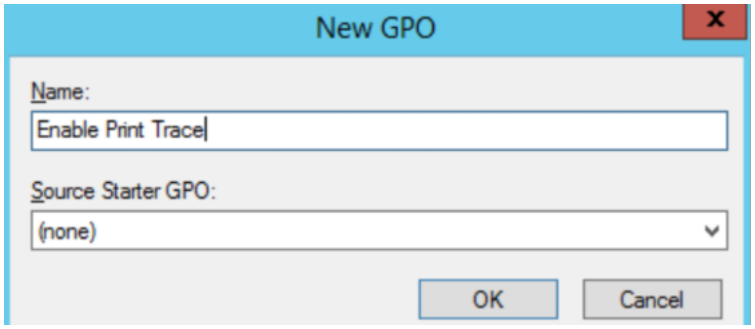
Création d'un objet de stratégie de groupe de registre avec les clés

1. Ouvrez Gestion des stratégies de groupe et cliquez avec le bouton droit sur **Objets de stratégie**

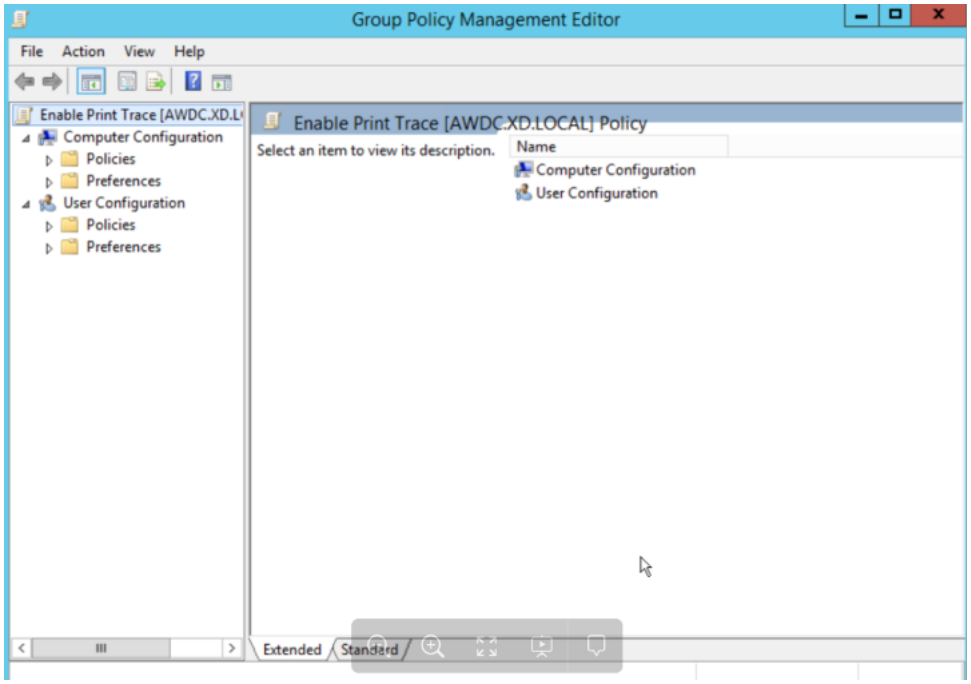


2. Dans la fenêtre **Nouveau GPO**, entrez les valeurs dans les champs suivants :

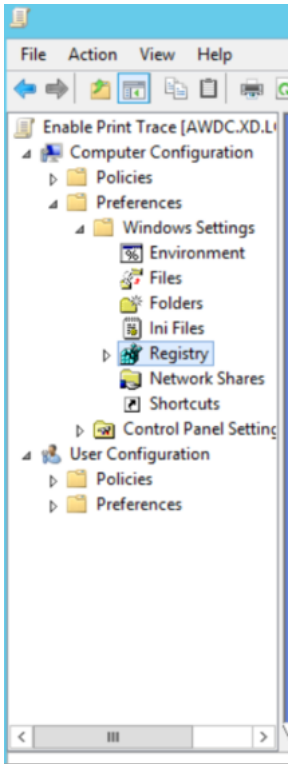
   - Nom : Enable Print Trace
   - GPO Source Starter : (aucun)



3. Sélectionnez **OK**.
4. Cliquez avec le bouton droit sur l'objet **Activer le suivi d'impression** que vous avez créé et sélectionnez **Modifier**



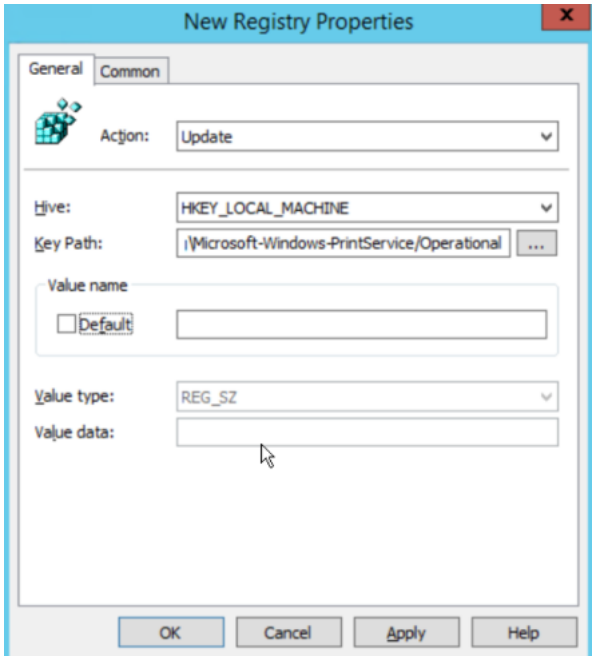
5. Dans la liste **Configuration de l'ordinateur**, sélectionnez **Préférences > Paramètres Windows**.



6. Cliquez avec **le bouton droit sur Registre**, sélectionnez **Nouveau > Élément de registre** Entrez les propriétés suivantes pour activer les journaux d'impression :

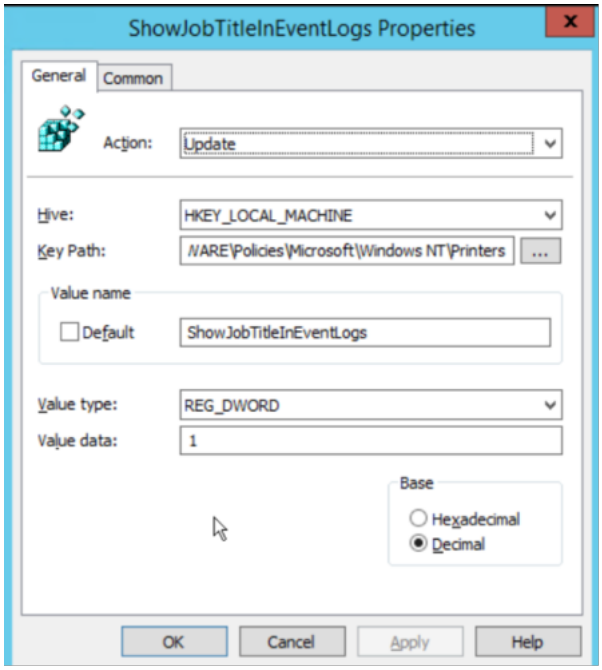
   - Action : Mettre à jour

- Ruche : HKEY_LOCAL_MACHINE
- Chemin d'accès clé : SYSTEM \ CurrentControlSet \ Services \ EventLog \ Microsoft-Windows-PrintService/Operational



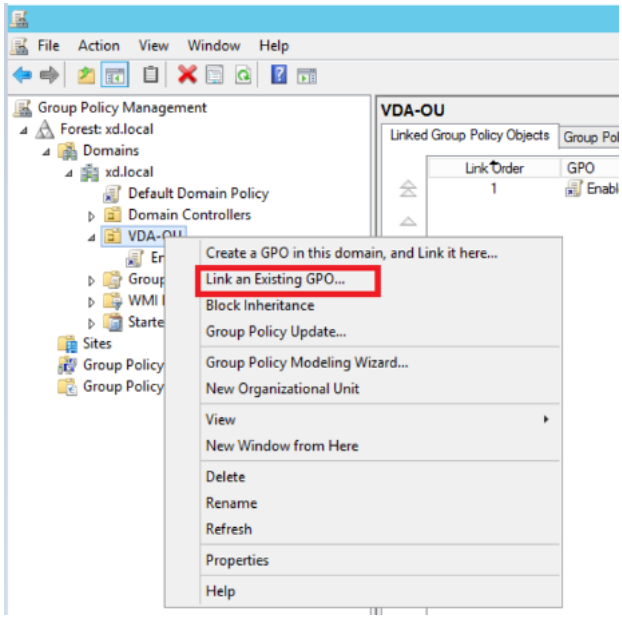
7. Sélectionnez **Appliquer**, puis **OK**.
8. Encore une fois, cliquez avec le bouton droit sur **Registre**, puis sélectionnez **Nouveau > Registre**. Entrez les propriétés suivantes pour activer les noms des tâches d'impression :

   - Action : Mettre à jour
   - Ruche : HKEY_LOCAL_MACHINE
   - Chemin d'accès clé : SOFTWARE \ Policies \ Microsoft \ Windows NT \ Printers
   - Nom de la valeur : ShowJobTitleInEventLogs
   - Type de valeur : REG_DWORD
   - Données de valeur : 1
   - Base : décimale

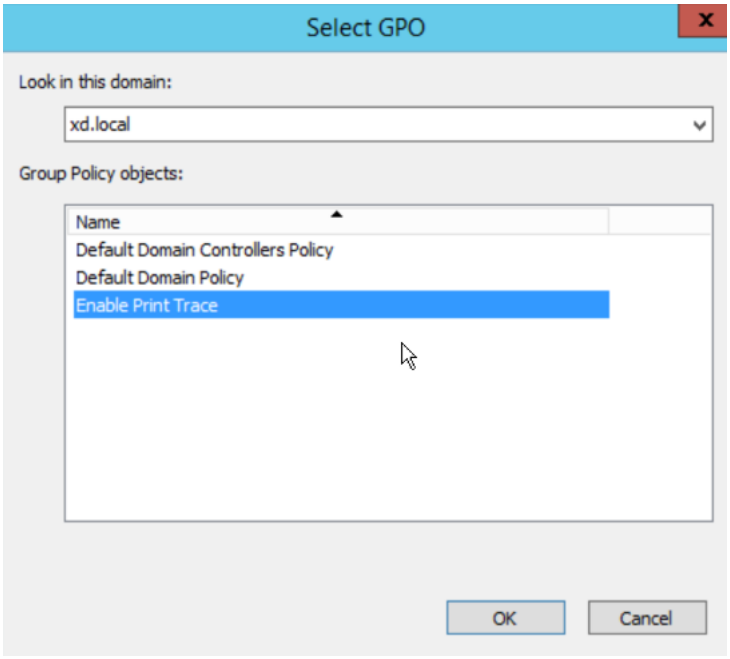


Activer le suivi d'impression pour l'unité organisationnelle

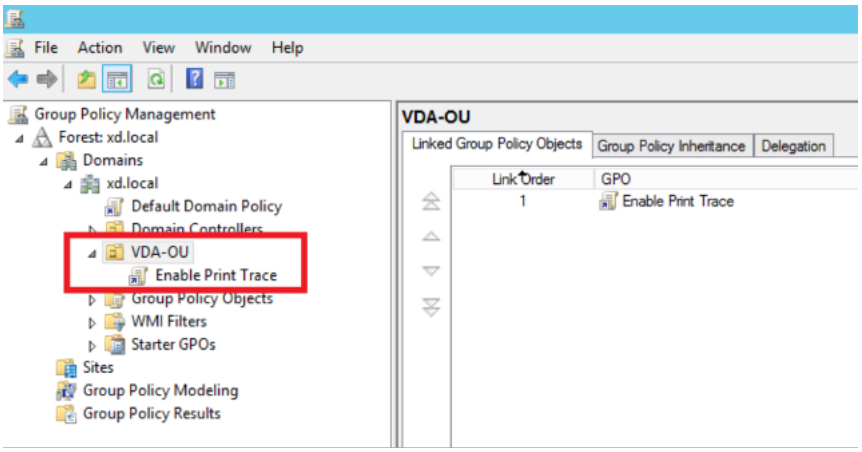
1. Ouvrez **Group Policy Management** et sélectionnez le domaine (par exemple, xd.local) ou l'UO si des VDA en font partie (par exemple, VDA-OU).
2. Cliquez avec le bouton droit sur le domaine (xd.local) ou l'UO (VDA-OU) et sélectionnez **Lier un objet de stratégie de groupe existant**.



3. Dans la boîte de dialogue **Sélectionner un objet de stratégie** de groupe, sélectionnez Activer le suivi d'impression, puis **OK**.



4. Vérifiez que l'objet de **stratégie de groupe Activer le suivi de l'impression** est lié à l'unité d'organisation.



Remarque

- Lorsque vous redémarrez un VDA, tous les événements de la file d'attente sont perdus et ne sont pas disponibles dans Citrix Analytics.
- Ce redémarrage a un faible impact sur un VDA à session unique, car une seule session peut être active à la fois, ce qui réduit le nombre d'événements.
- Ce redémarrage a un impact important sur un VDA multi-session, car toutes les sessions actives sont interrompues pendant le redémarrage et les événements qui se trouvent dans la file d'attente sont perdus.

Activation de la télémétrie du presse-papiers pour Citrix DaaS

Citrix DaaS (anciennement connu sous le nom de Citrix Virtual Apps and Desktops Service) permet aux utilisateurs d'effectuer des opérations sur le presse-papiers, et les journaux associés peuvent être consultés dans Citrix Analytics for Security. Ces journaux du presse-papiers fournissent des informations précieuses telles que le nom du VDA, la taille du presse-papiers, le type de format du presse-papiers, l'adresse IP du client, le fonctionnement du presse-papiers, la direction du fonctionnement du presse-papiers et si l'opération du presse-papiers était autorisée.

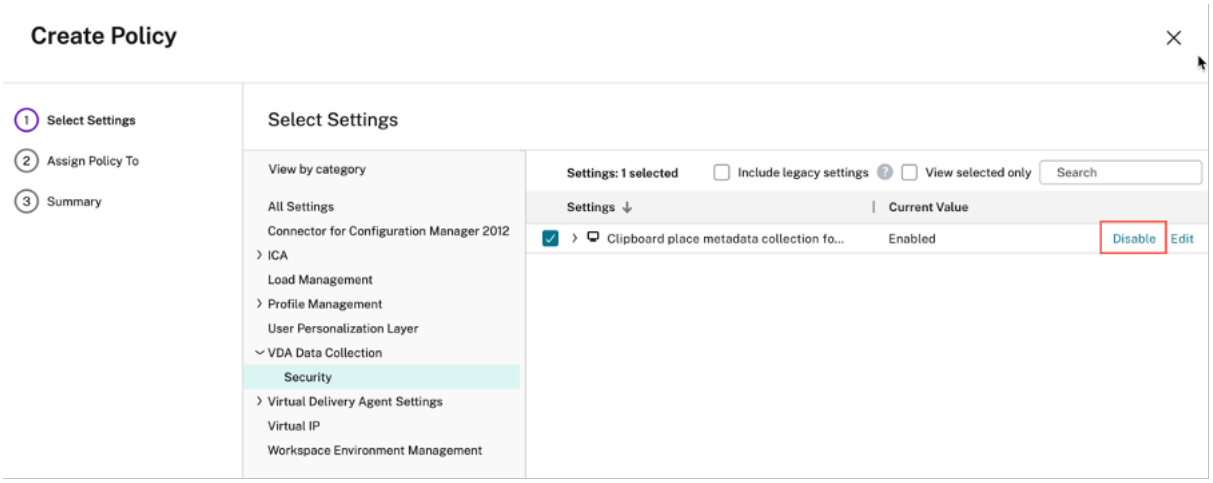
En tant qu'administrateur de sécurité, vous pouvez utiliser ces journaux à des fins d'analyse des risques et d'investigation en sélectionnant la source de données **Apps and Desktops** sur la page de **recherche** de Citrix Analytics for Security.

> **Remarque**
>
> - Par défaut, la collecte et la transmission de ces journaux du presse-papiers sont activées sur les Virtual Delivery Agents (VDA).
> - Cette configuration s'applique uniquement aux VDA Windows.

Conditions préalables

- La version de votre VDA doit être identique à la version de référence pour Citrix Virtual Apps and Desktops 7 2305 ou version ultérieure. Pour plus d'informations, consultez Citrix Virtual Apps and Desktops 7 2305.
- Assurez-vous que le paramètre de **redirection du presse-papiers client** sur la page **Web Studio Policies** n'est pas configuré sur un état interdit. Pour plus d'informations, consultez la section Redirection du presse-papiers du client.

Vous pouvez utiliser la **collection de métadonnées Clipboard Place pour la stratégie de surveillance de la sécurité** afin d'activer ou de désactiver la télémétrie du presse-papiers. Cette stratégie est activée par défaut. Pour désactiver, vous devez vous rendre sur la page des **stratégies** > sélectionner **Sécurité** dans la section **Collecte de données du VDA** > vérifier la stratégie > cliquer sur **Désactiver**.



Pour plus d'informations, consultez la section Collecte de métadonnées Clipboard Place pour la surveillance de la sécurité.

Activer ou désactiver le traitement des données sur la source de données

Vous pouvez arrêter le traitement des données à tout moment pour une source de données particulière : Director et l'application Workspace. Sur la fiche de site de la source de données, cliquez sur les points de **suspension verticaux () > Désactiver le traitement des données**. Citrix Analytics arrête de traiter les données de cette source de données. Vous pouvez également arrêter le traitement des données à partir de la carte de site Apps and Desktops. Cette option s'applique à la fois aux sources de données de Director et de l'application Workspace.

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

Intégration de Microsoft Active Directory et Azure Active Directory

May 6, 2022

Connectez votre Active Directory ou votre Azure Active Directory et importez les détails des utilisateurs et les groupes d'utilisateurs du domaine de votre organisation vers Citrix Analytics for Security.

Cette intégration améliore les profils utilisateur dans Citrix Analytics for Security avec des informations d'identité utilisateur telles que le titre du poste, l'organisation, l'emplacement du bureau, l'adresse e-mail et les coordonnées. Sur la page Profil utilisateur, vous pouvez consulter ces informations utilisateur, qui vous aident lors de l'enquête et de l'analyse des risques.

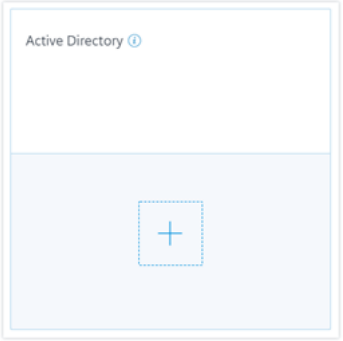
Conditions préalables

- Si vous souhaitez connecter Active Directory à Citrix Analytics pour la sécurité, assurez-vous que votre Active Directory est d'abord connecté à votre compte Citrix Cloud. Pour plus d'informations, consultez Connecter Active Directory à Citrix Cloud.
- Si vous souhaitez connecter Azure Active Directory à Citrix Analytics pour la sécurité, assurez-vous que votre Azure Active Directory est d'abord connecté à votre compte Citrix Cloud. Pour de plus amples informations, consultez la section Connecter Azure Active Directory à Citrix Cloud.

Connexion à Microsoft Active Directory

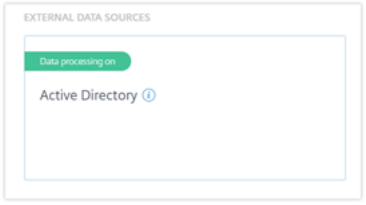
Pour connecter votre Active Directory à Citrix Analytics for Security, procédez comme suit :

1. Accédez à **Paramètres** > **Sources de données** > **Sécurité**, puis accédez à la section **SOURCES DE DONNÉES EXTERNES** .
2. Sur la fiche **de site Active Directory**, cliquez sur le signe plus **+** .



3. Citrix Analytics vous invite à connecter Active Directory à votre compte Citrix Cloud. Pour plus d'informations, consultez la section Prérequis.

Une fois que vous avez connecté votre Active Directory à votre compte Citrix Cloud, Citrix Analytics découvre automatiquement cette nouvelle source de données. Sur la page **Sources de données**, la fiche de site Active Directory affiche **Traitement des données activé**.

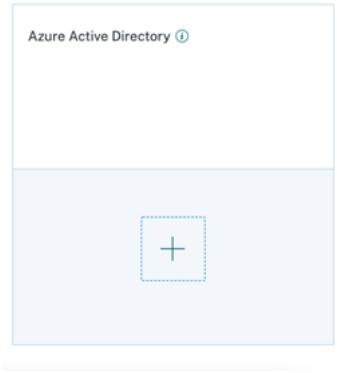


L'état **Traitement des données activé** indique qu'Active Directory est découvert et que les informations utilisateur sont extraites de votre Active Directory.

Connectez Microsoft Azure Active Directory

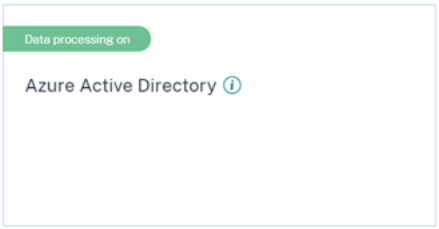
Pour connecter votre Azure Active Directory à Citrix Analytics, procédez comme suit :

1. Accédez à **Paramètres > Sources de données > Sécurité**, puis accédez à la section **SOURCES DE DONNÉES EXTERNES** .
2. Sur la carte de site **Azure Active Directory**, cliquez sur le signe plus +.



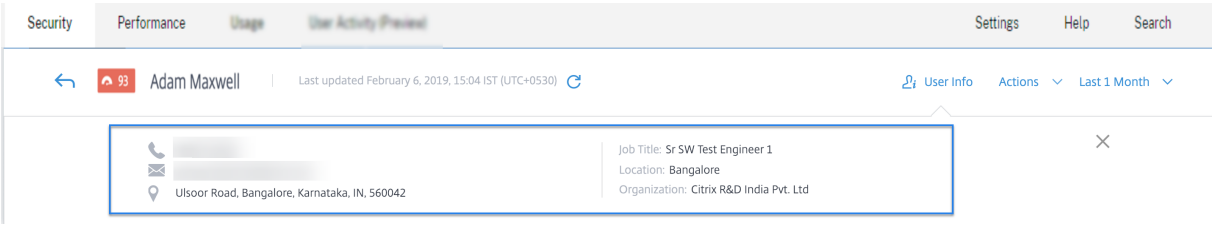
3. Citrix Analytics vous invite à connecter Azure Active Directory à votre compte Citrix Cloud. Pour de plus amples informations, consultez la section Connecter Azure Active Directory à Citrix Cloud.

Une fois que vous avez connecté votre Azure Active Directory à votre compte Citrix Cloud, Citrix Analytics découvre automatiquement cette nouvelle source de données. Sur la page **Sources de données**, la carte de site **Azure Active Directory** affiche **Traitement des données activé**. Cet état indique que Azure Active Directory est découvert et que les informations utilisateur sont récupérées à partir de votre Azure Active Directory.



Afficher les informations utilisateur

Dans l'onglet **Sécurité**, cliquez sur un utilisateur à risque pour afficher la page de profil utilisateur. Si l'utilisateur est disponible dans Active Directory ou Azure Active Directory, vous pouvez afficher son titre de poste, son organisation, son adresse e-mail et son numéro de contact sur la page de profil utilisateur.



Intégration de Microsoft Graph Security

June 17, 2021

Microsoft Graph Security est une source de données externe qui regroupe les données de plusieurs fournisseurs de sécurité. Il permet également d'accéder aux données d'inventaire des utilisateurs.

Citrix Analytics prend actuellement en charge les fournisseurs de sécurité suivants de Microsoft Graph Security :

- Azure AD identity protection
- Microsoft Defender pour Endpoint

Pour plus d'informations sur les fournisseurs de sécurité, consultez les liens suivants :

- Pour **Azure AD Identity Protection** :https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-risk-events
- Pour **Microsoft Defender pour Endpoint** : https://docs.microsoft.com/en-us/mem/configmgr/protect/deploy-use/defender-advanced-threat-protection

Pour accéder à la source de données Microsoft Graph Security, vous devez obtenir les autorisations requises au nom d'un locataire, à partir de la plate-forme d'identité Microsoft.

Conditions préalables

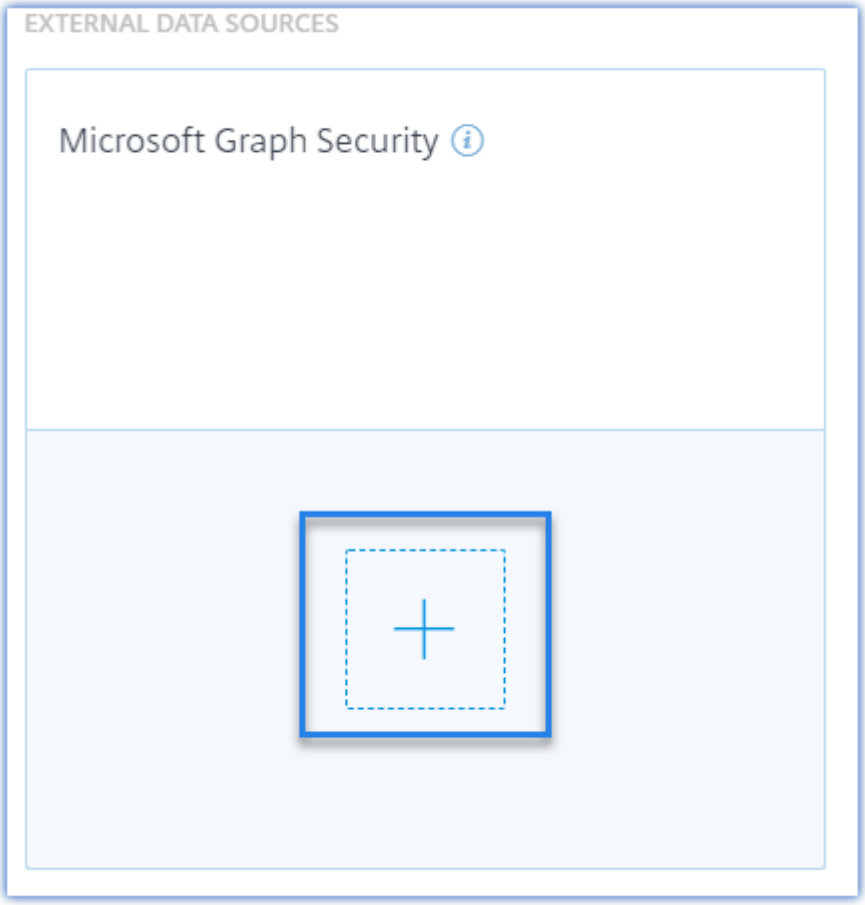
Avant de commencer à intégrer la source de données Microsoft Graph Security, assurez-vous que :

- L'administrateur utilise le fournisseur de sécurité Azure AD Identity Protection (faisant partie d'Azure AD Premium P2) fournisseur de sécurité.
- L'utilisateur final est connecté au Microsoft Store avec des comptes Travail ou École.

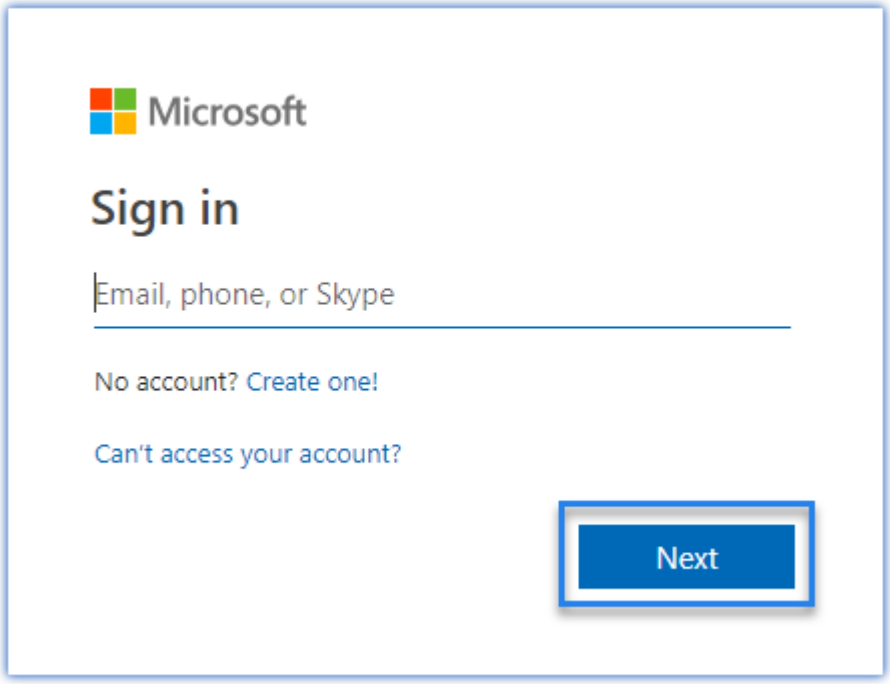
Intégration d'instances Microsoft Graph Security

1. Accédez à **Paramètres** > **Sources de données** > **Sécurité**, puis accédez à la section **SOURCES DE DONNÉES EXTERNES**.

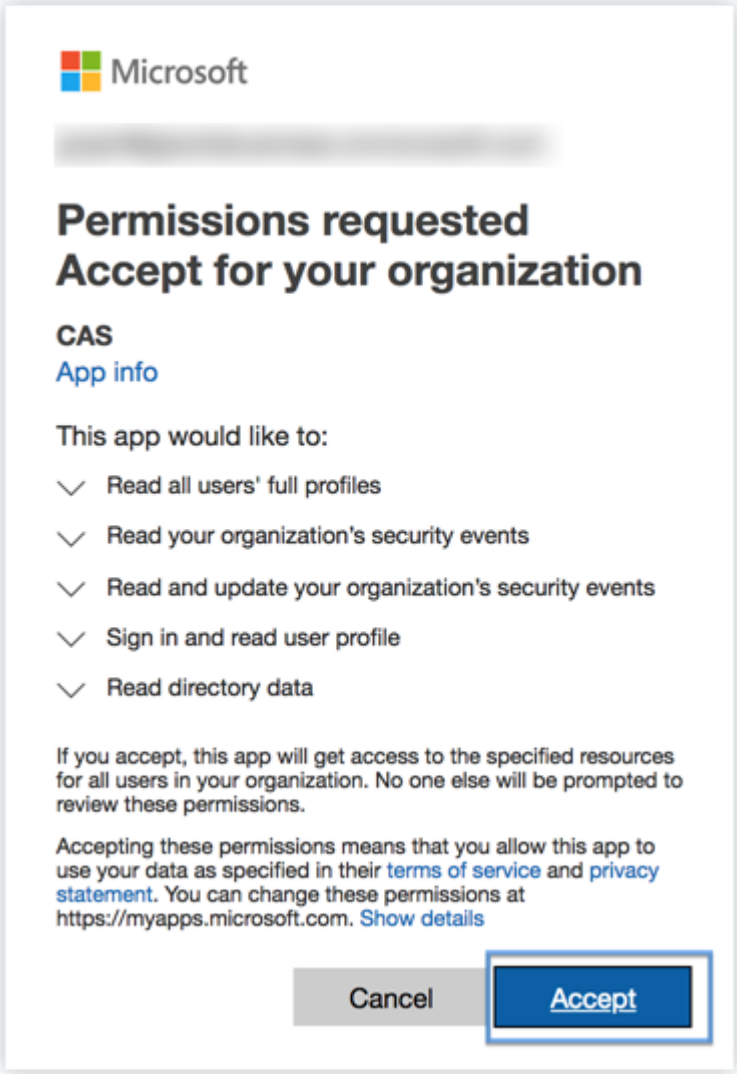
2. Cliquez sur le signe plus (**+**) sur la carte de site Microsoft Graph Security. Vous êtes redirigé vers le point de terminaison d'autorisation.



3. Dans la fenêtre **Microsoft**, connectez-vous à l'aide de vos informations d'identification d'ouverture de session Azure pour enregistrer un compte. Ou sélectionnez un compte existant.
4. Cliquez sur **Suivant**.



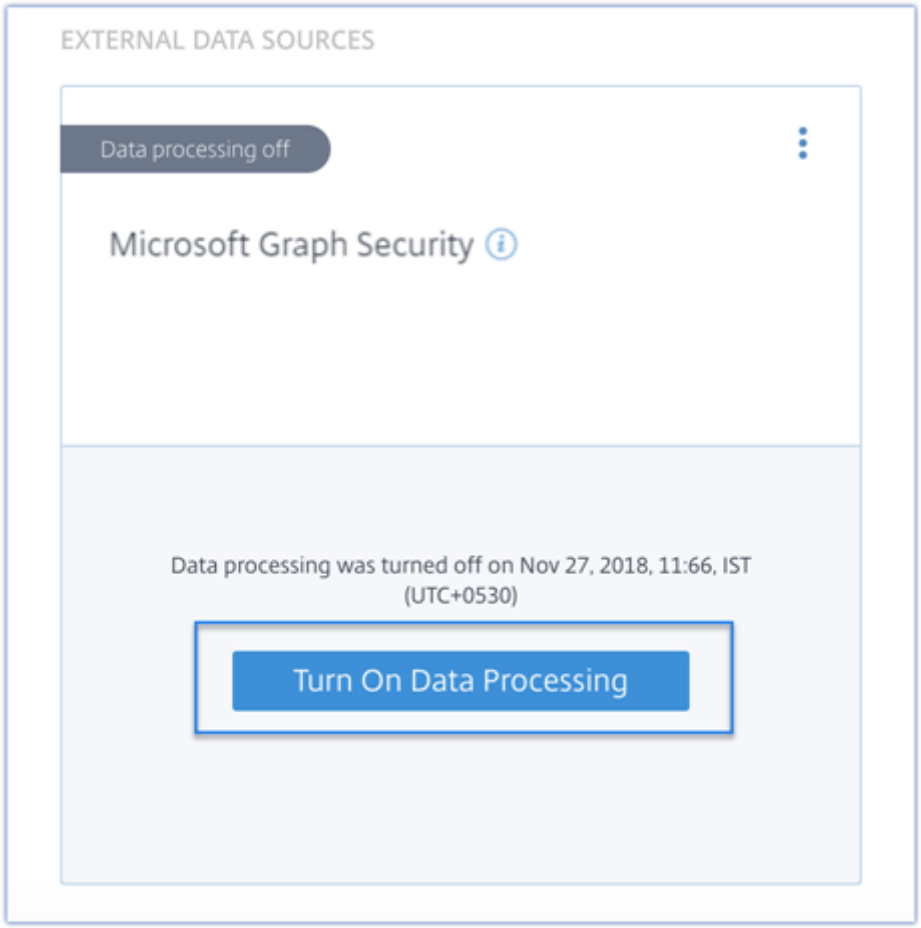
5. Cliquez sur **Accepter**. Vous êtes redirigé vers la page Sources de données. La source de données Microsoft Graph Security est désormais liée à votre compte Citrix Cloud.



Activer ou désactiver le traitement des données

Pour désactiver le traitement des données, cliquez sur les points de suspension verticaux () sur la fiche de site et sélectionnez **Désactiver le traitement des données**. Il empêche Citrix Analytics de traiter les données de cette source de données.

Vous pouvez réactiver le traitement des données en sélectionnant **Activer le traitement des données** sur la carte de site.



Pour plus d'informations sur les indicateurs de risque Microsoft Graph Security, reportez-vous à la section Indicateurs de risque Microsoft Graph Security.

Intégration de Security Information and Event Management (SIEM)

December 7, 2023

> **Remarque**
>
> Contactez CAS-PM-Ext@cloud.com pour demander de l'aide pour l'intégration du SIEM, l'exportation de données vers le SIEM et pour faire part de vos commentaires.

Intégrez Citrix Analytics for Security à vos services SIEM et exportez les données des utilisateurs de l'environnement informatique Citrix vers votre SIEM. Corrélez les données exportées avec les données disponibles dans votre SIEM pour obtenir des informations plus approfondies sur la position de sécurité de votre entreprise.

Cette intégration améliore la valeur de votre Citrix Analytics for Security et de votre SIEM.

Avantages

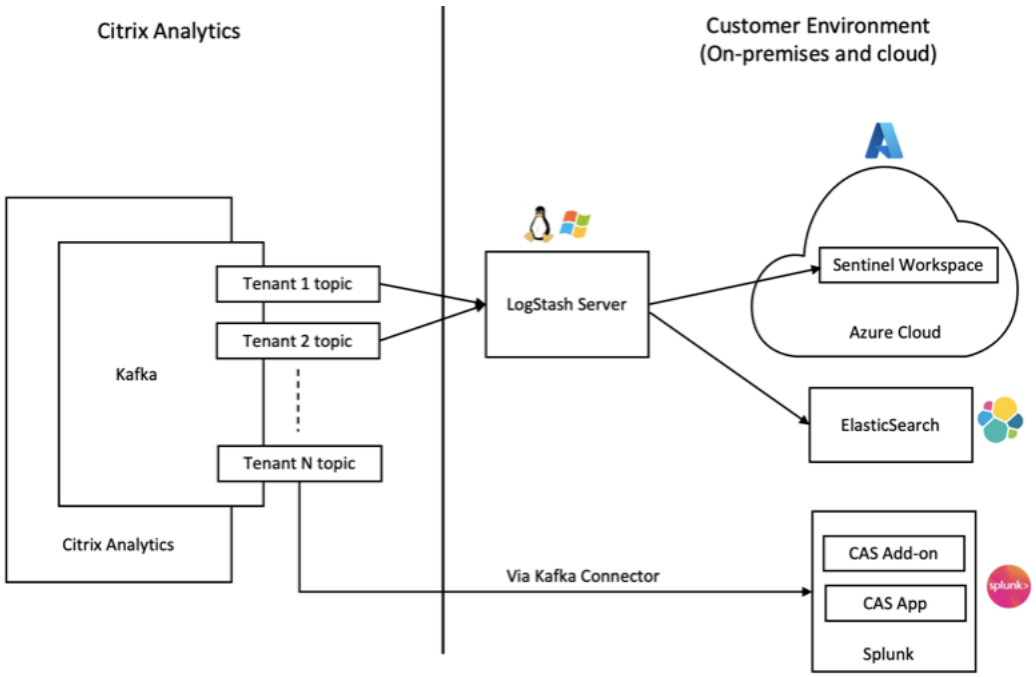
- Permet à vos équipes des opérations de sécurité de corréler, d'analyser et de rechercher des données à partir de journaux disparates.
- Aide vos équipes des opérations de sécurité à identifier et à corriger rapidement les risques de sécurité.
- Visibilité des alertes de sécurité dans un endroit centralisé.
- Approche centralisée pour détecter les menaces de sécurité potentielles pour les fonctionnalités d'analyse des risques organisationnels telles que les indicateurs de risque, les profils utilisateur et les scores de risque.
- Possibilité de combiner et de corréler les informations de veille sur les risques Citrix Analytics d'un compte utilisateur avec les sources de données externes connectées au sein de votre SIEM.

Architecture d'intégration SIEM

Votre intégration SIEM se connecte au Kafka en direction nord déployé sur le cloud Citrix Analytics for Security. Cela peut être réalisé de deux manières :

- **Points de terminaison Kafka** : si votre SIEM prend en charge les points de terminaison Kafka, utilisez les paramètres fournis dans le fichier de configuration Logstash et les détails du certificat dans le fichier JKS ou le fichier PEM pour intégrer votre SIEM à Citrix Analytics for Security. À l'aide des points de terminaison Kafka, vous pouvez vous connecter et extraire les données vers le SIEM de votre choix.
- **Moteur Logstash** : si votre SIEM ne prend pas en charge les terminaux Kafka, vous pouvez utiliser le moteur de collecte de données Logstash. Vous pouvez envoyer les données d'analyse des risques de Citrix Analytics for Security vers l'un des plug-ins de sortie pris en charge par Logstash.

Reportez-vous au schéma d'architecture de solution SIEM suivant pour comprendre comment les données circulent entre Citrix Analytics for Security et votre service SIEM :

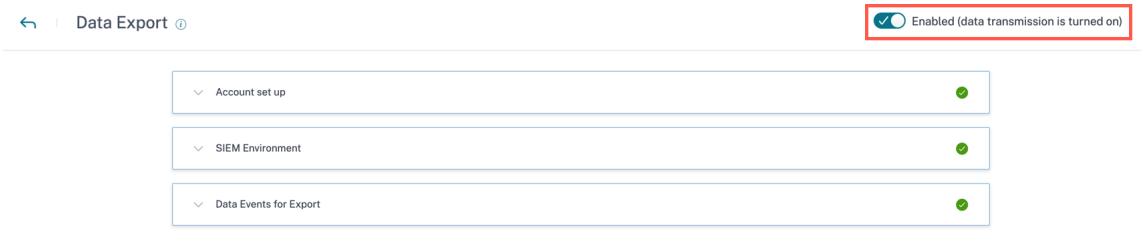


Activer ou désactiver la transmission des données

Pour arrêter de transmettre des données depuis Citrix Analytics for Security, procédez comme suit :

1. Accédez à **Réglages > Exportations de données**.
2. Désactivez le bouton pour désactiver la **transmission de données**.

> **Remarque**
> Par défaut, la transmission de données est toujours activée/activée pour le SIEM.



Pour réactiver la transmission de données, activez le bouton.

Configuration de l'environnement SIEM

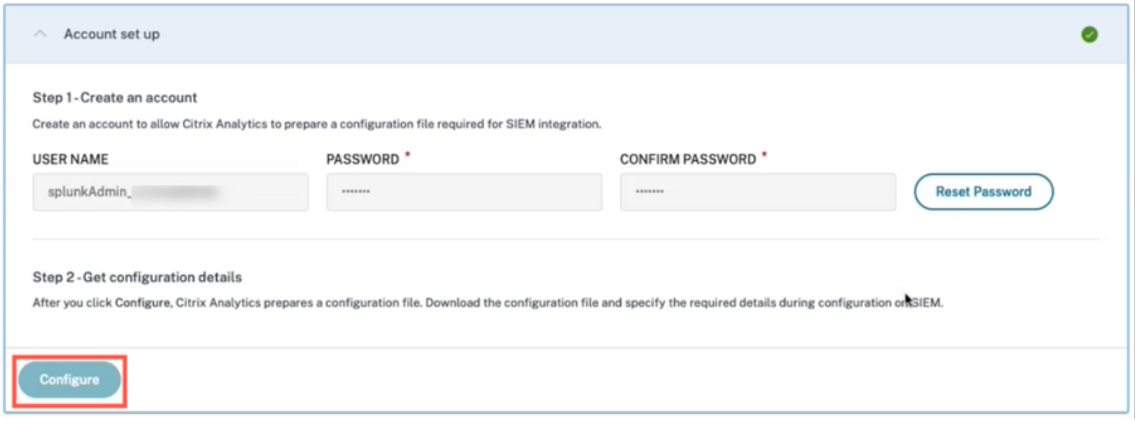
Pour exporter des données vers le SIEM, vous devez effectuer les actions suivantes :

- Configurez votre compte Kafka et vos informations d'authentification

- Téléchargez la configuration préremplie et configurez l'environnement SIEM
- Événements de données pour l'exportation

Configuration du compte d'exportation SIEM

1. Pour configurer votre compte, accédez à **Paramètres > Exportations de données > développer Configuration du compte**. Créez un compte en spécifiant le nom d'utilisateur et le mot de passe. Une fois que vous avez configuré votre compte, vos informations Kafka sont générées. Ces informations sont automatiquement intégrées lors de la génération du fichier de configuration.

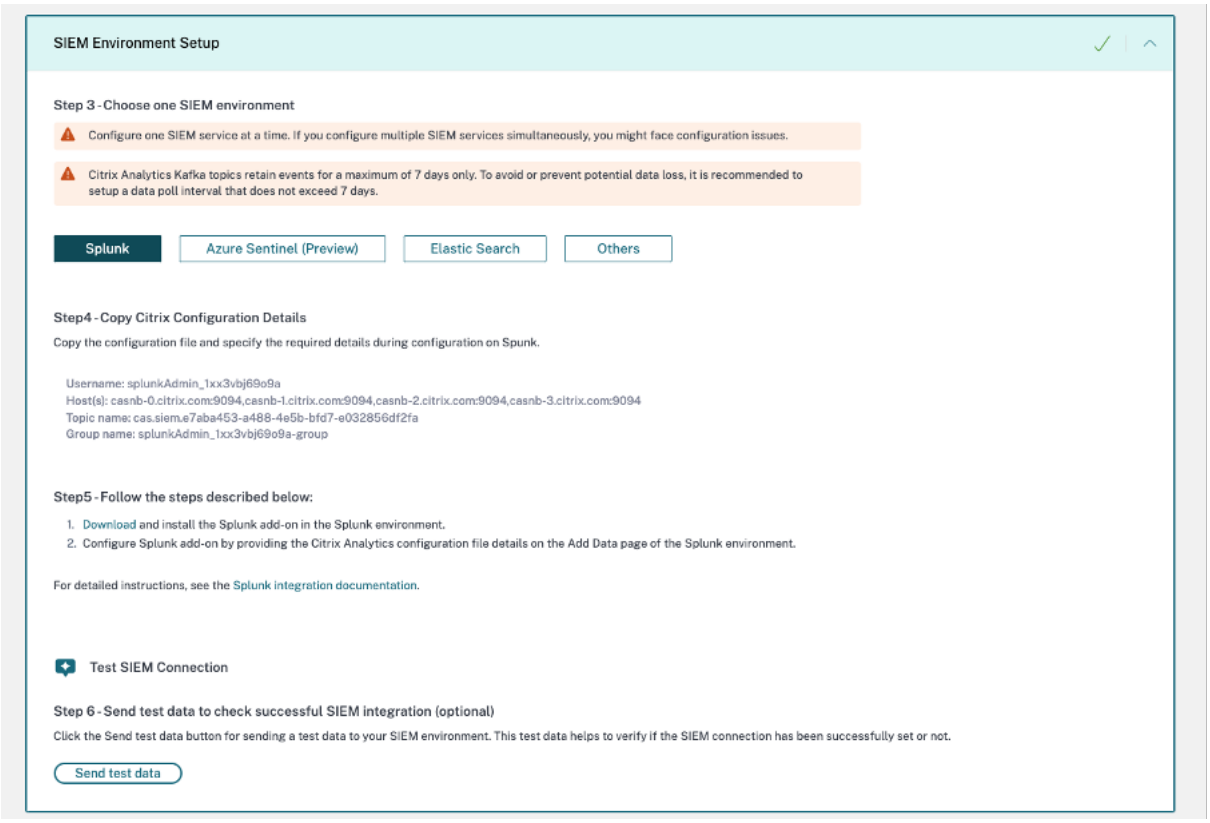


2. Cliquez sur **Configurer** pour générer le fichier de configuration. Le fichier de configuration contient des détails tels que les points de terminaison Kafka, les sujets spécifiques de votre abonnement et les identifiants de groupe. En outre, il préconfigure les attributs Kafka et SSL qui sont nécessaires pour terminer l'authentification et le flux de données.

Configuration SIEM et configuration de l'environnement

Choisissez l'environnement SIEM selon vos besoins. Vous pouvez intégrer Citrix Analytics for Security aux services suivants. Consultez les liens suivants pour obtenir des informations détaillées et des configurations spécifiques au SIEM :

- Splunk
- Sentinel
- Elasticsearch
- Autres SIEM utilisant un connecteur de données basé sur Kafka ou Logstash



Événements de données exportés depuis Citrix Analytics for Security vers votre service SIEM

Dans le cadre des exportations SIEM, il existe deux types d'ensembles de données :

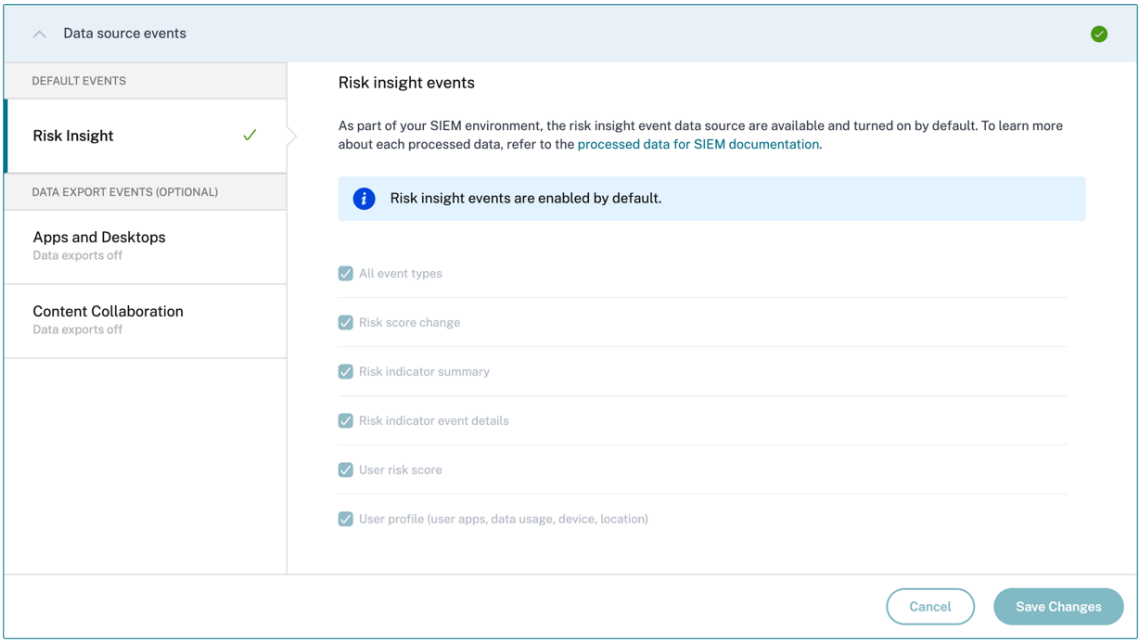
1. **Événements d'analyse des risques (exportations par défaut)** : une fois que vous avez terminé la configuration du compte et la configuration du SIEM, les données par défaut (événements liés aux informations sur les risques) commencent à être transférées vers votre déploiement SIEM. Les données d'analyse des risques contiennent le score de risque des utilisateurs, le profil utilisateur et les alertes relatives aux indicateurs de risque Ils sont générés par l'algorithme d'apprentissage automatique Citrix Analytics, l'analyse du comportement des utilisateurs et en fonction des événements des utilisateurs. Pour plus d'informations sur les types d'événements, les métadonnées et le schéma disponibles, voir Données d'analyse des risques pour le SIEM.
2. **Événements relatifs aux sources de données (exportations facultatives)** : vous pouvez également configurer la fonctionnalité d'exportation de données pour exporter les événements utilisateur à partir des sources de données de vos produits compatibles avec Citrix Analytics for Security. Lorsque vous effectuez une activité dans l'environnement Citrix, les événements de la source de données sont générés. Les événements exportés sont des données d'utilisation

des utilisateurs et des produits non traitées en temps réel, disponibles dans l'affichage en libre-service. Les métadonnées contenues dans ces événements peuvent également être utilisées pour une analyse plus approfondie des menaces, pour créer de nouveaux tableaux de bord et pour établir des liens avec d'autres événements liés à des sources de données autres que Citrix concernant votre infrastructure informatique et de sécurité.

Actuellement, Citrix Analytics for Security envoie les événements utilisateur à votre SIEM pour la source de données Citrix Virtual Apps and Desktops.

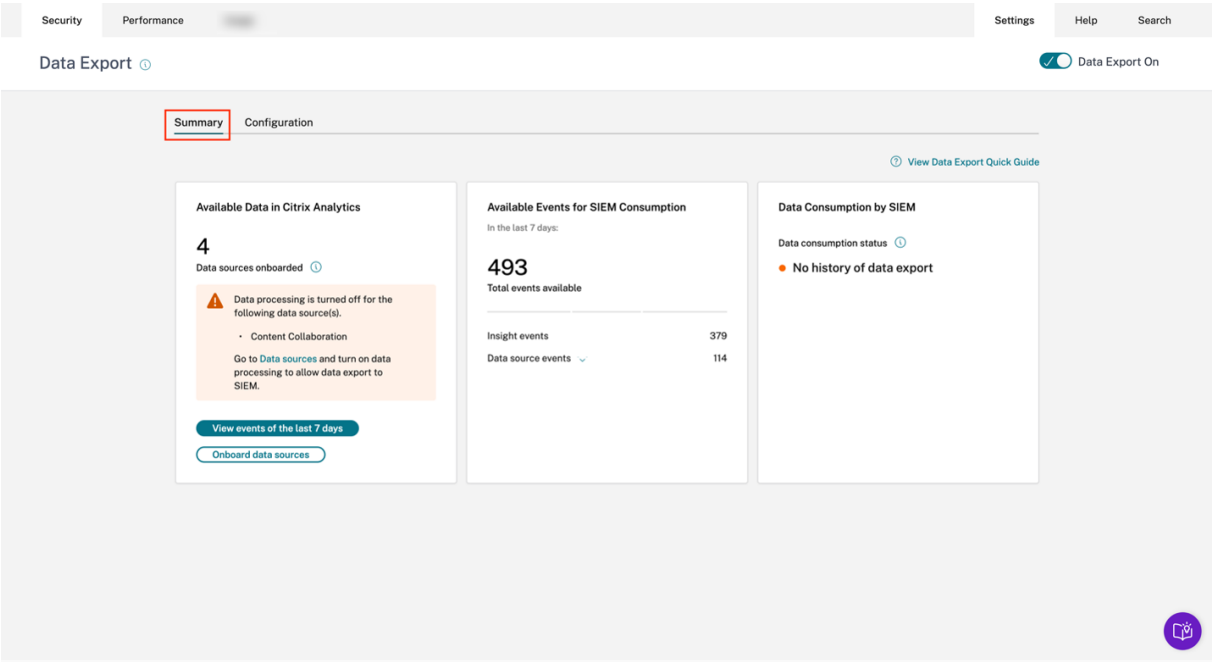
Pour plus d'informations sur les types d'événements, les métadonnées et le schéma disponibles, voir Événements de source de données.

> **Remarque**
>
> Pour les clients qui utilisent un broker de données Logstash, il est recommandé de télécharger le dernier fichier de configuration depuis le portail Citrix Analytics for Security et de le mettre à jour lors du déploiement du service Logstash. Cela garantit que les tables d'événements de source de données correctes sont créées et que les événements sont désormais disponibles dans les index SIEM.



Résolution des problèmes liés à l'intégration SIEM

La vue Exportations de données pour la sécurité inclut un onglet **Résumé** qui aide les administrateurs à résoudre les problèmes liés à leur intégration SIEM avec Citrix Analytics. Le tableau de bord **récapitulatif** fournit une visibilité sur l'état et le flux des données en les guidant vers les points de contrôle qui facilitent le processus de résolution des problèmes.



Pour en savoir plus sur cette fonctionnalité, consultez Résolution des problèmes liés à l'exportation de données.

Intégration de Splunk

November 16, 2023

Intégrez Citrix Analytics for Security à Splunk pour exporter et corréler les données des utilisateurs de votre environnement informatique Citrix vers Splunk et obtenir des informations plus détaillées sur la posture de sécurité de votre organisation.

Pour plus d'informations sur les avantages de l'intégration et le type de données traitées qui sont envoyées à votre SIEM, voir Intégration des informations de sécurité et de la gestion des événements.

Pour acquérir une compréhension complète de la méthodologie de déploiement Splunk et adopter les stratégies nécessaires à une planification efficace, reportez-vous à l'architecture Splunk avec les applications Citrix
Analytics hébergées dans la documentation Splunk.

Intégrez Citrix Analytics pour la sécurité à Splunk

Suivez les instructions mentionnées pour intégrer Citrix Analytics for Security à Splunk :

- Exportation de données. Citrix Analytics for Security crée un canal Kafka et exporte les informations sur les risques et les événements relatifs aux sources de données. Splunk récupère cette information sur les risques du canal.
- Obtenez la configuration sur Citrix Analytics. Créez un mot de passe pour votre compte prédéfini pour l'authentification. Citrix Analytics for Security prépare un fichier de configuration nécessaire à la configuration du module complémentaire Citrix Analytics pour Splunk.
- Téléchargez et installez le module complémentaire Citrix Analytics pour Splunk. Téléchargez le **module complémentaire Citrix Analytics pour Splunk** à l'aide de Slunkbase ou de Splunk Cloud pour terminer le processus d'installation.
- Configurez le module complémentaire Citrix Analytics pour Splunk. Configurez une entrée de données à l'aide des détails de configuration fournis par Citrix Analytics for Security et configurez le module complémentaire Citrix Analytics pour Splunk.

Une fois le fichier de configuration de Citrix Analytics préparé, consultez :

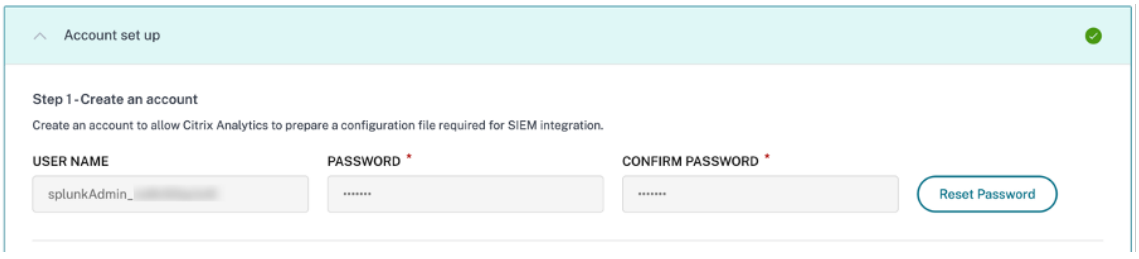
- Possibilité de réinitialiser le mot de passe
- Activer ou désactiver la transmission des données

Une fois que le module complémentaire Citrix Analytics pour Splunk est configuré, consultez :

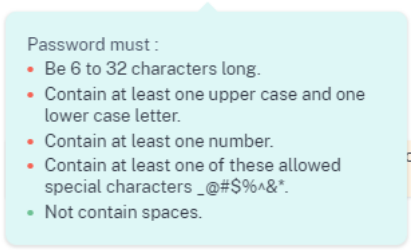
- Comment gérer les événements dans Splunk Environment
- Comment configurer l'application Citrix Analytics pour Splunk

Exportation de données

1. Accédez à **Réglages** > **Exportations de données**.
2. Dans la section **Configuration du compte**, créez un compte en spécifiant le nom d'utilisateur et le mot de passe. Ce compte est utilisé pour préparer un fichier de configuration, qui est nécessaire à l'intégration.

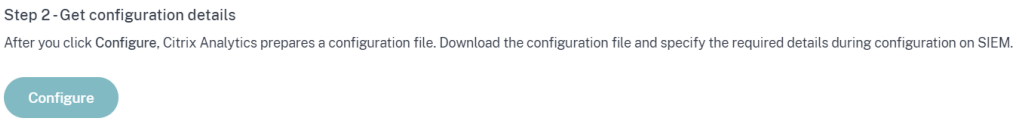


3. Assurez-vous que le mot de passe répond aux conditions suivantes :



4. Sélectionnez **Configurer**.

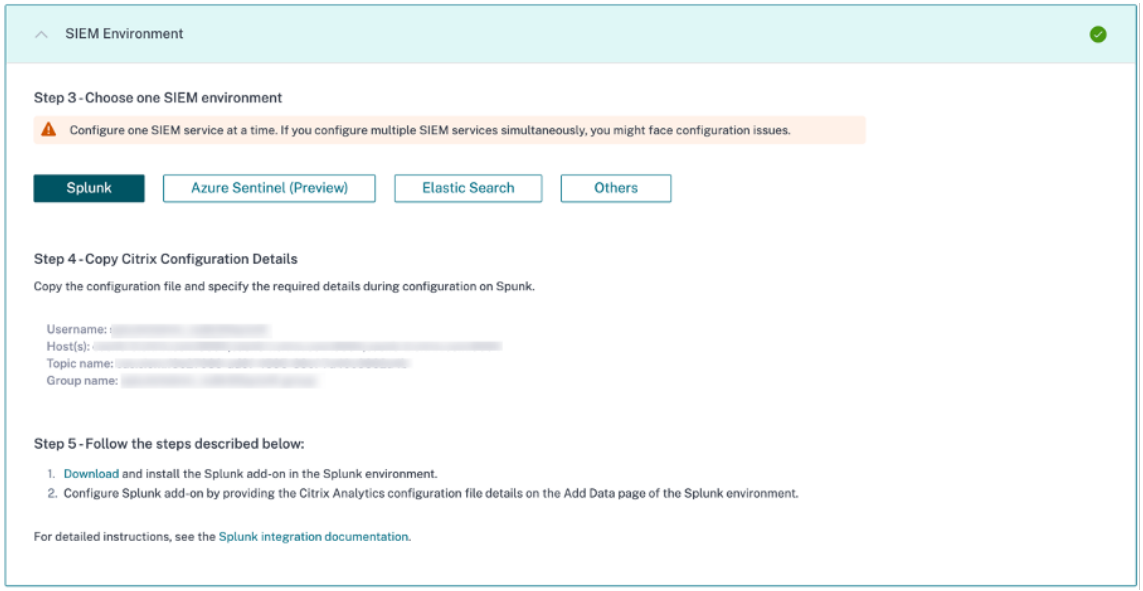
   Citrix Analytics for Security prépare les détails de configuration nécessaires à l'intégration de Splunk.



5. Sélectionnez **Splunk**.
6. Copiez les détails de configuration, qui incluent le nom d'utilisateur, les hôtes, le nom de la rubrique Kafka et le nom du groupe.

   Vous avez besoin de ces informations pour configurer le module complémentaire Citrix Analytics pour Splunk dans les étapes suivantes.

   > **IMPORTANT**
   >
   > Ces informations sont sensibles et vous devez les stocker dans un endroit sécurisé.



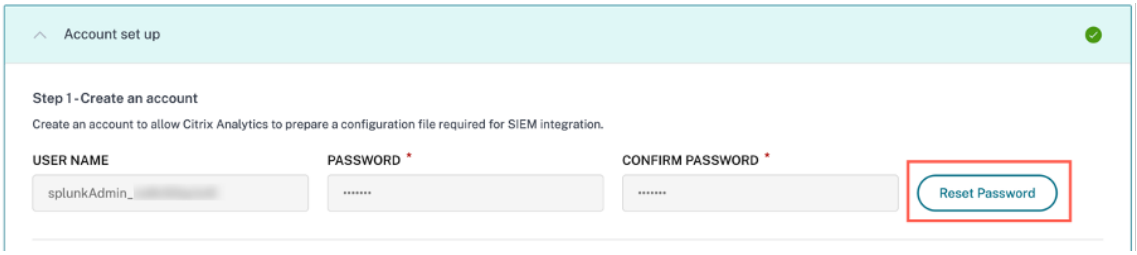
Pour générer des données candidates pour Splunk Integration, activez le traitement des données pour au moins une source de données ou utilisez la fonctionnalité de génération d'événements de test.

Cela aide Citrix Analytics
for Security à démarrer le processus d'intégration de Splunk.

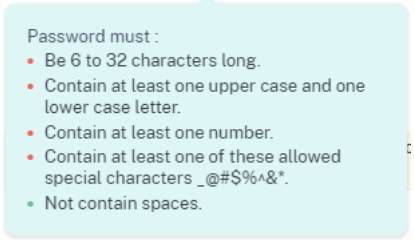
Possibilité de réinitialiser le mot de passe

Si vous souhaitez réinitialiser votre mot de passe de configuration sur Citrix Analytics for Security, procédez comme suit :

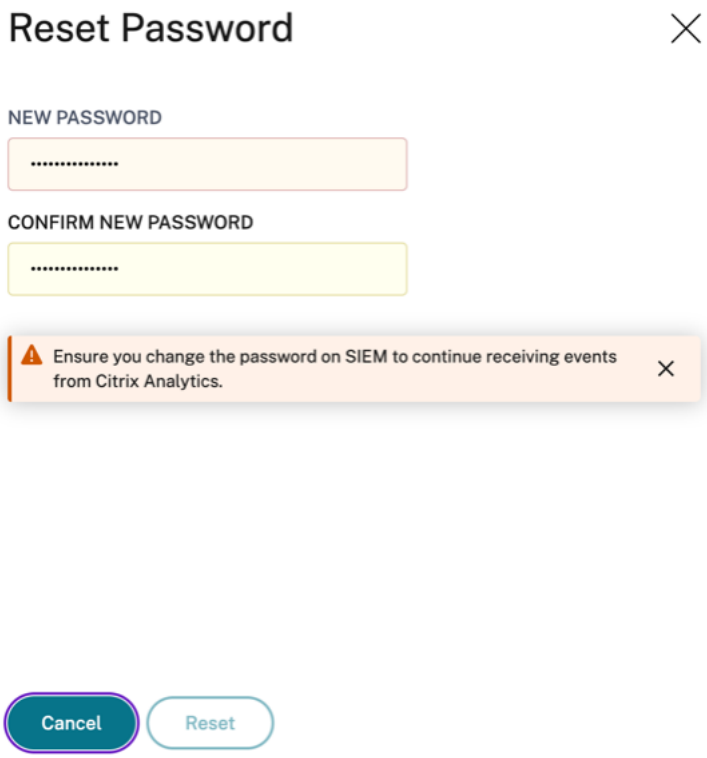
1. Sur la page de **configuration du compte**, cliquez sur **Réinitialiser le mot de passe**.



2. Dans la fenêtre de **réinitialisation du mot de passe**, spécifiez le mot de passe mis à jour dans les champs **NOUVEAU MOT** DE **PASSE et CONFIRMER LE NOUVEAU** MOT Suivez les règles de mot de passe qui s'affichent.



3. Cliquez sur **Réinitialiser**. La préparation du fichier de configuration est lancée.



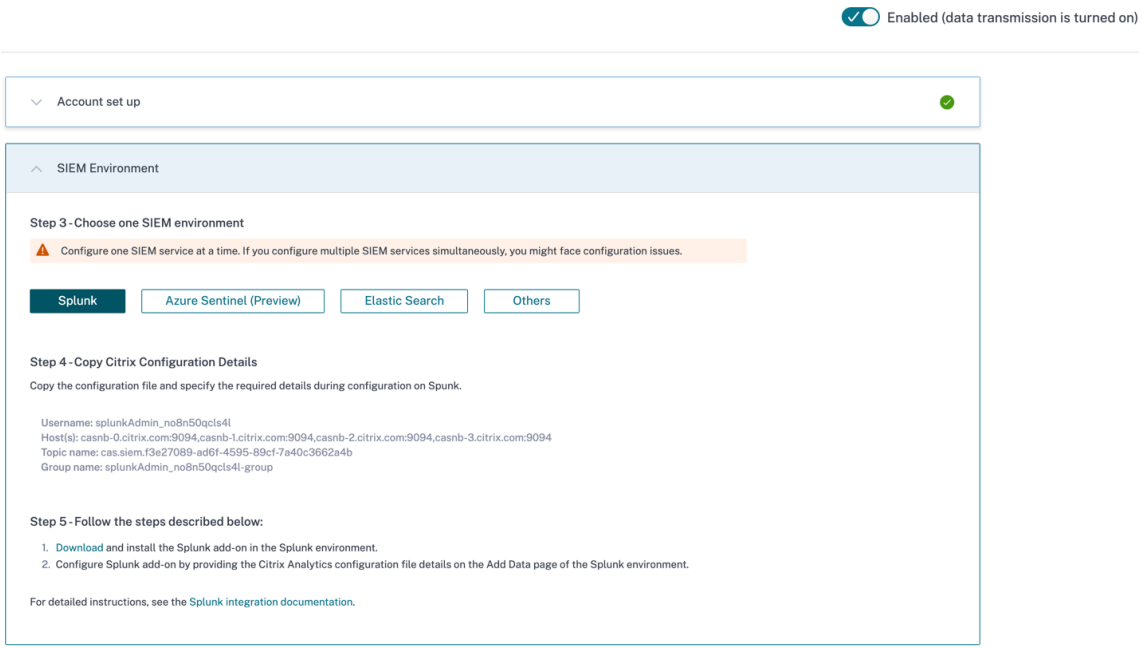
> **Remarque**
>
> Après avoir réinitialisé le mot de passe de configuration, veillez à mettre à jour le nouveau mot de passe lorsque vous configurez l'entrée de données sur la page **Ajouter des données**de votre environnement Splunk. Il permet à Citrix Analytics for Security de continuer à transmettre des données vers Splunk.

Activer ou désactiver la transmission des données

La transmission de données pour l'exportation de données Splunk depuis Citrix Analytics est activée par défaut.

Pour arrêter de transmettre des données depuis Citrix Analytics for Security, procédez comme suit :

1. Accédez à **Réglages > Exportations de données**.
2. Désactivez le bouton pour désactiver la **transmission de données**.



Pour réactiver la transmission de données, activez le bouton.

Module complémentaire Citrix Analytics pour Splunk

Vous pouvez choisir d'installer l'application complémentaire sur l'une des plateformes suivantes :

- Splunk Enterprise (Heavy Forwarder)
- Splunk Cloud

Module complémentaire Citrix Analytics pour Splunk (on-Prem/Enterprise)

Versions prises en charge

Citrix Analytics for Security prend en charge l'intégration de Splunk sur les systèmes d'exploitation suivants :

- CentOS Linux 7 et versions ultérieures
- Debian GNU/Linux 10.0 et versions ultérieures
- Red Hat Enterprise Linux Server 7.0 et versions ultérieures
- Ubuntu 18.04 LTS et versions ultérieures

> **Remarque**
>
> - Citrix recommande d'utiliser la dernière version des systèmes d'exploitation précédents ou

> les versions qui sont toujours prises en charge par les fournisseurs concernés.
>
> - Pour les systèmes d'exploitation du noyau Linux (64 bits), utilisez une version du noyau prise en charge par Splunk. Pour plus d'informations, consultez la documentation de Splunk.

Vous pouvez configurer notre intégration Splunk sur la version suivante de Splunk : Splunk 8.1 (64 bits) et versions ultérieures.

Conditions préalables

- Le **module complémentaire Citrix Analytics pour Splunk** se connecte aux points de terminaison suivants sur Citrix Analytics for Security. Assurez-vous que les points de terminaison figurent dans la liste d'autorisation 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`

> **Remarque**
>
> Essayez d'utiliser les noms des points de terminaison et non les adresses IP. Les adresses IP publiques des points de terminaison peuvent changer.

Téléchargez et installez le module complémentaire Citrix Analytics pour Splunk

Vous pouvez choisir d'installer le module complémentaire à l'aide de l'option **Installer l'application depuis un fichier** ou depuis l'environnement Splunk.

Installer l'application depuis un fichier

1. Allez sur Splunkbase.
2. Téléchargez le fichier du module complémentaire Citrix Analytics pour Splunk.
3. Sur la page d'accueil de Splunk Web, cliquez sur l'icône en forme de roue dentée en regard de **Applications**.
4. Cliquez sur **Installer l'application depuis un fichier**.
5. Recherchez le fichier téléchargé et cliquez sur **Charger**.

   > **Remarques**
   >
   > - Si vous disposez d'une ancienne version du module complémentaire, sélectionnez **Mettre à niveau l'application** pour la remplacer.
   > - Si vous mettez à niveau le **module complémentaire Citrix Analytics pour Splunk** à partir d'une version antérieure à 2.0.0, vous devez supprimer les fichiers et dossiers suivants situés dans le dossier */bin* du dossier d'installation du module complémentaire et redémarrer votre environnement Splunk Forwarder ou Splunk Standalone :
   >
   > ```
   > - 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
   > ```

6. Vérifiez que l'application apparaît dans la liste des **applications**.

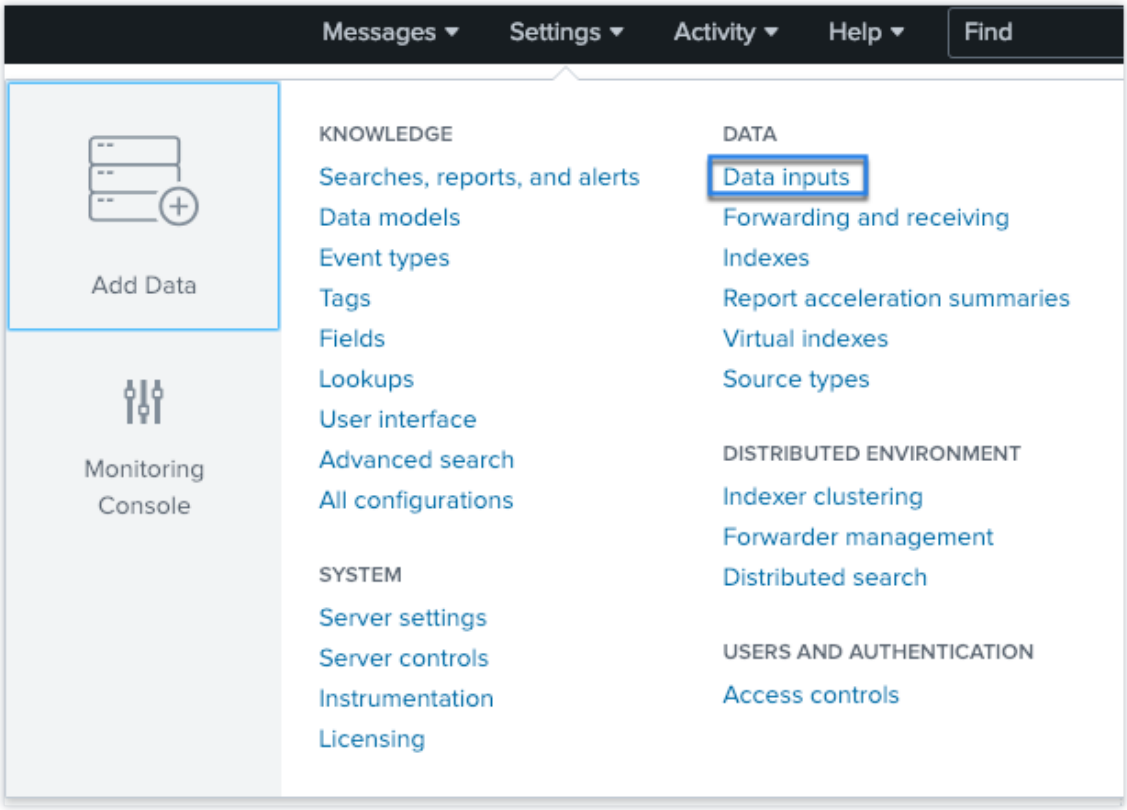
Installez l'application depuis Splunk

1. Sur la page d'accueil de Splunk Web, cliquez **sur+Trouver d'autres applications**.
2. Sur la page Parcourir d'autres applications, recherchez **Splunk dans le module complémentaire Citrix Analytics**.
3. Cliquez sur **Installer** en regard de l'application.
4. Vérifiez que l'application apparaît dans la liste des **applications**.

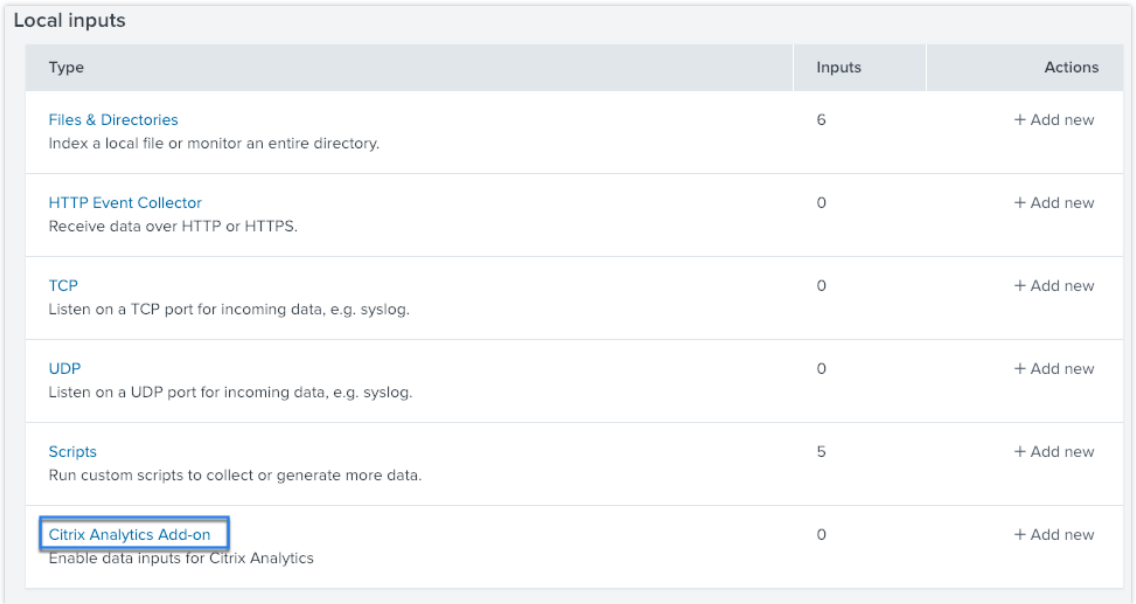
Configurer le module complémentaire Citrix Analytics pour Splunk

Configurez le module complémentaire Citrix Analytics pour Splunk à l'aide des détails de configuration fournis par Citrix Analytics for Security. Une fois le module complémentaire configuré, Splunk commence à consommer les événements de Citrix Analytics for Security.

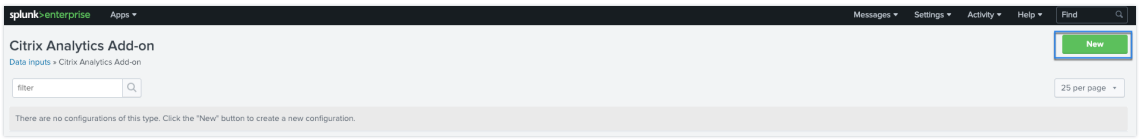
1. Sur la page d'accueil de Splunk, accédez à **Paramètres** > **Entrées de données**.



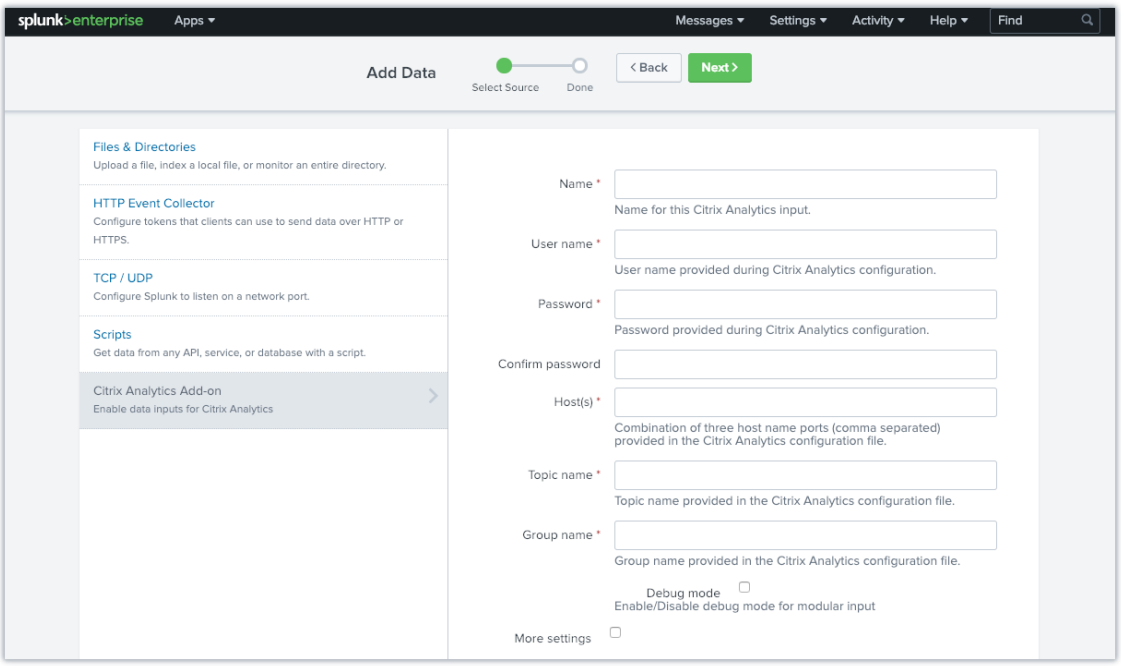
2. Dans la section **Entrées locales**, cliquez sur **Citrix Analytics Add-on**.



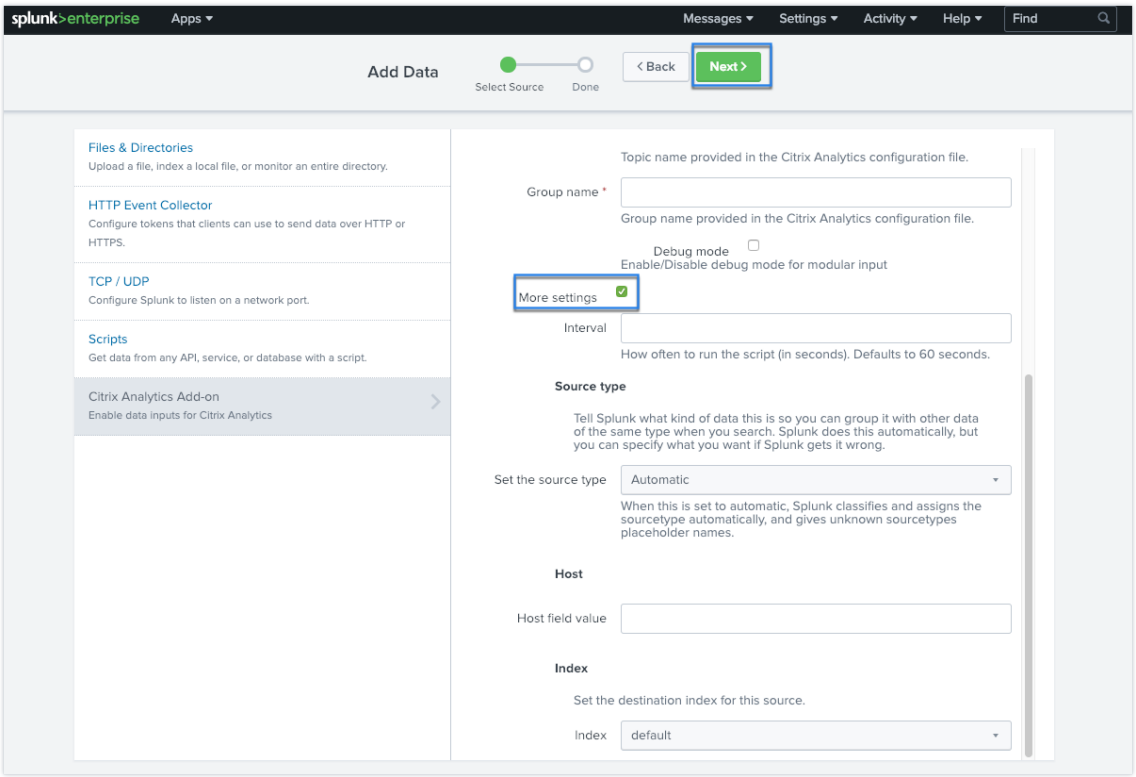
3. Cliquez sur **New**.



4. Sur la page **Ajouter des données**, entrez les détails fournis dans le fichier de configuration de Citrix Analytics.



5. Pour personnaliser vos paramètres par défaut, cliquez sur **Plus de paramètres** et configurez la saisie des données. Vous pouvez définir votre propre index Splunk, votre nom d'hôte et votre type de source.



6. Cliquez sur **Suivant**. Votre entrée de données Citrix Analytics est créée et le module complémentaire Citrix Analytics pour Splunk est correctement configuré.

Module complémentaire Citrix Analytics pour Splunk (Cloud)

Vous pouvez configurer notre intégration Splunk sur la version suivante de Splunk : Splunk 8.1 et versions ultérieures.

Conditions préalables

Le module complémentaire Citrix Analytics pour Splunk se connecte aux adresses IP et aux ports sortants suivants pour se connecter à Citrix Analytics for Security. Assurez-vous que les adresses IP et les ports sortants suivants (en fonction de votre région Citrix Cloud) figurent dans la liste autorisée de votre réseau. Pour configurer ces adresses IP et ces ports sortants, consultez la section **Ajouter les adresses IP et les ports sortants de Citrix Analytics à la liste d'autorisation de Splunk Cloud à l'aide du service de configuration d'administration (** ACS).

Région des États-Unis	Adresse IP	Port sortant	Région de l'Union eu-ropéenne	Adresse IP	Port sortant	Région Asie-Pacifique Sud	Adresse IP	Port sortant
casnb-0 cit-rix.com	20.242.21.89	9094	casnb-eu-0 cit-rix.com	20.229.150.91	9094	casnb-aps-0 cit-rix.com	20.211.0.219	9094
casnb-1.citrix.com	20.98.232.69	9094	casnb-eu-1.citrix.com	20.107.97.59	9094	casnb-aps-1 cit-rix.com	20.211.38.102	9094
casnb-2.citrix.com	20.242.21.198	9094	casnb-eu-2.citrix.com	51.124.223.162	9094	casnb-aps-2 cit-rix.com	20.211.36.180	9094
casnb-3.citrix.com	20.242.57.14	9094						

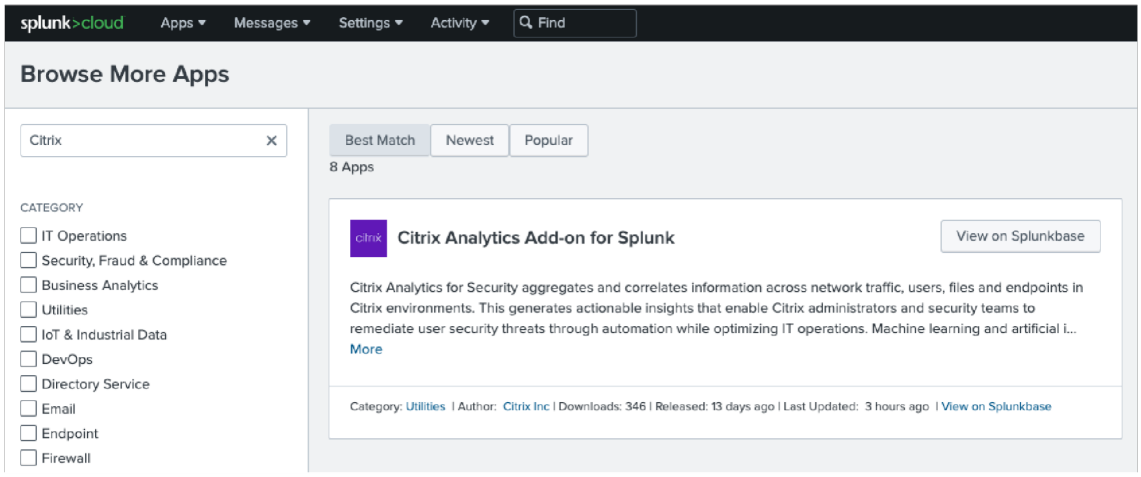
> **Remarque**
>
> Ces adresses IP peuvent faire l'objet d'une rotation. Assurez-vous de maintenir votre liste d'adresses IP autorisées à jour avec les adresses IP
> les plus récentes, comme indiqué ci-dessus.

Ajoutez les adresses IP et les ports sortants de Citrix Analytics à la liste d'autorisation de Splunk Cloud à l'aide du service de configuration d'administration (ACS)

1. En fonction de votre région Citrix Cloud, vous devez ajouter des adresses IP à la liste des adresses IP autorisées.
2. Activez le service de configuration d'administration (ACS) sur Splunk Cloud Platform.
3. Créez un jeton pour la liste d'autorisation à l'aide d'un compte local avec des privilèges d'administrateur.
4. Exécutez les commandes cURL GET et POST pour ajouter des sous-réseaux à la liste d'autorisation sur les ports respectifs et validez s'ils ont été ajoutés avec succès.
5. Exécutez les commandes cURL GET et POST pour ajouter des ports sortants à la liste des ports autorisés et vérifier s'ils ont été ajoutés avec succès.

Téléchargez et installez le module complémentaire Citrix Analytics pour Splunk

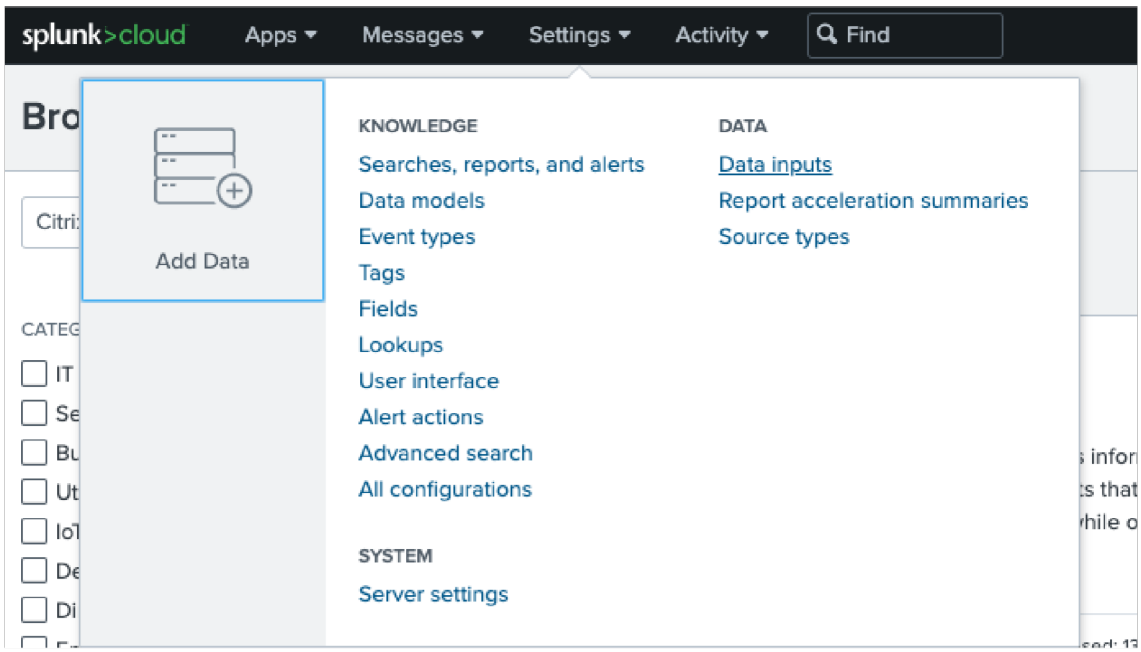
1. Accédez à **Applications > Trouver d'autres applications > Rechercher le module complémentaire Citrix Analytics pour Splunk**.



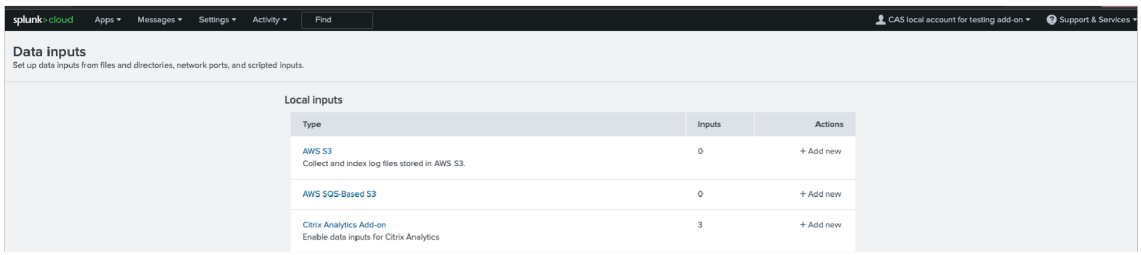
2. Installez l'application.
3. Vérifiez que l'application apparaît dans la liste des applications.

Configurer le module complémentaire Citrix Analytics pour Splunk

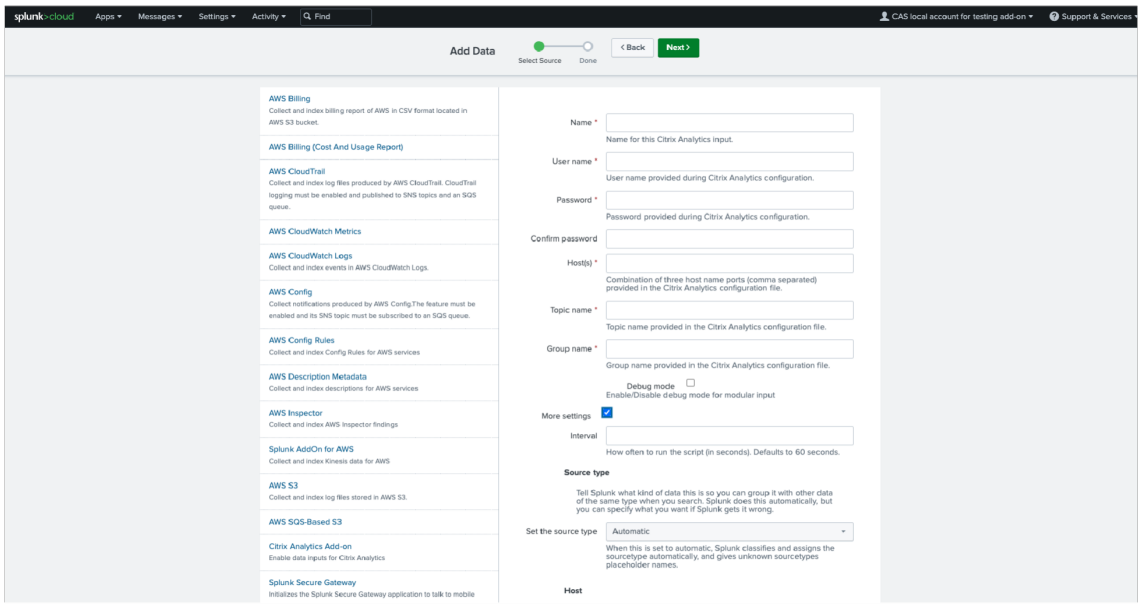
1. Accédez à **Paramètres > Entrées de données > Citrix Analytics Add-on**.



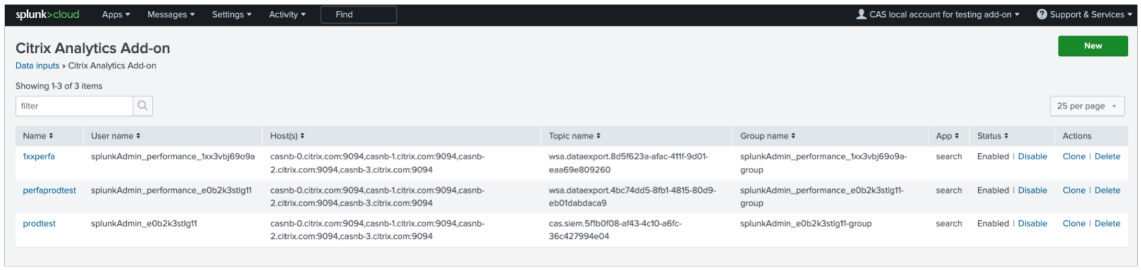
Ajoutez l'entrée : Intégration Splunk	Citrix Analytics pour la sécurité. Cliquez sur **Ajouter un nouveau**.

2. 

3. Configurez la saisie de données en saisissant les détails configurés sur la page **Citrix Analytics Data Exports** .



4. Vérifiez si votre saisie de données a bien été ajoutée.

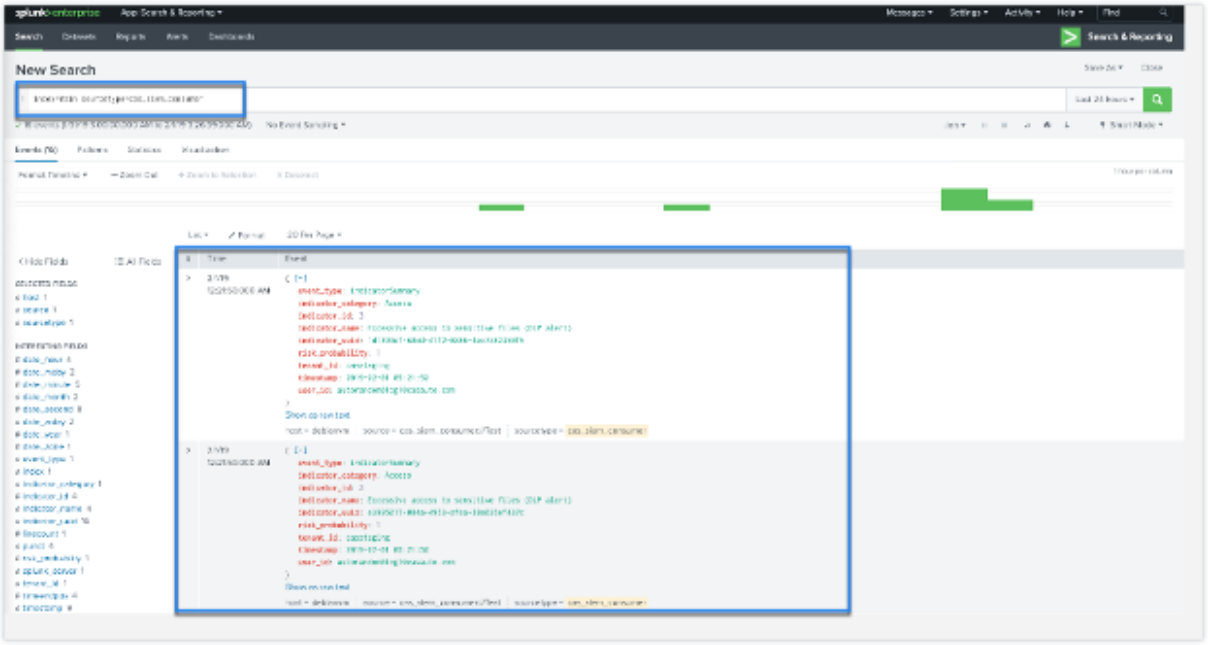


Comment gérer les événements dans votre environnement Splunk

Après avoir configuré le module complémentaire, Splunk commence à récupérer des renseignements sur les risques à partir de Citrix Analytics for Security. Vous pouvez commencer à rechercher les événe-

ments de votre organisation sur la tête de recherche Splunk en fonction de l'entrée de données configurée.

Les résultats de la recherche sont affichés dans le format suivant :



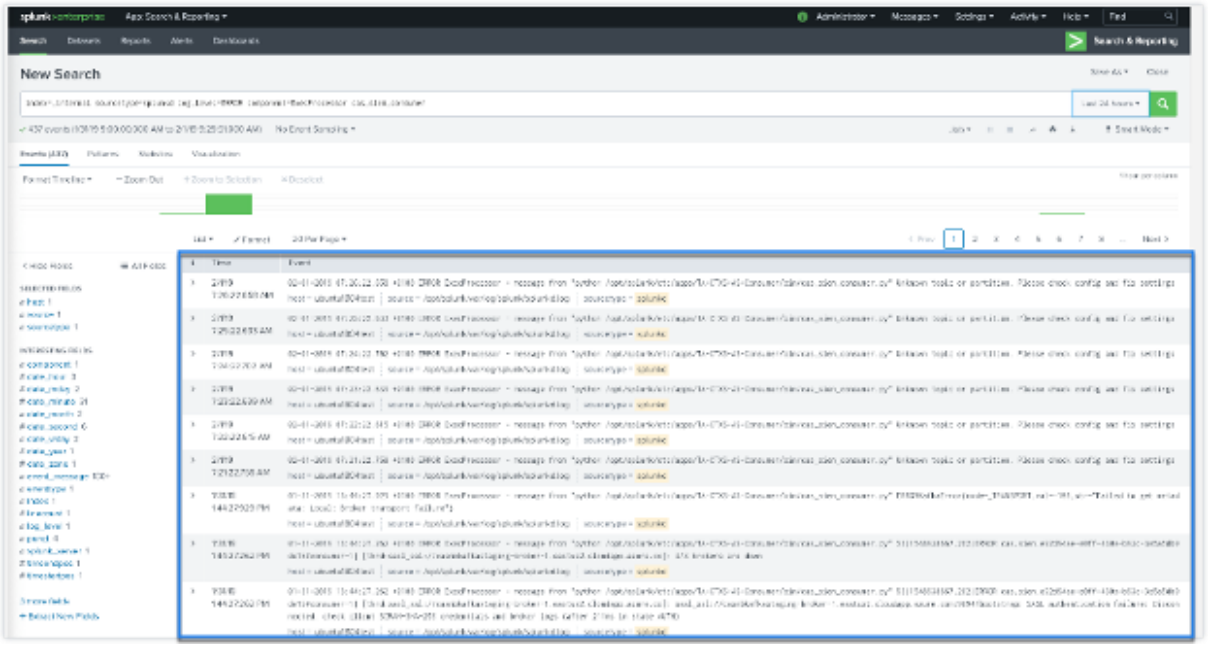
Un exemple de sortie :

```
{"event_type": "indicatorSummary", "indicator_category": "Access",
"indicator_id": 200, "indicator_name": "Jailbroken / Rooted Device
Detected", "indicator_uuid": "1b97c3be-0000-000-0000-0000000000",
"risk_probability": 1.0, "tenant_id": "notcloud", "timestamp": "2017-11-16
23:59:59", "user_id": "testuser00001"}
```

Pour rechercher et déboguer les problèmes liés au module complémentaire, utilisez la requête de recherche suivante :

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

Les résultats sont affichés dans le format suivant :



Pour plus d'informations sur le format des données, consultez la section Format de données Citrix Analytics pour SIEM.

Dépannage du module complémentaire Citrix Analytics pour Splunk

Si vous ne voyez aucune donnée dans vos tableaux de bord Splunk ou si vous rencontrez des problèmes lors de la configuration du module complémentaire Citrix Analytics pour Splunk, suivez les étapes de débogage pour résoudre le problème. Pour plus d'informations, consultez Problèmes de configuration liés au module complémentaire Citrix Analytics pour Splunk.

> **Remarque**
>
> Contactez CAS-PM-Ext@cloud.com pour demander de l'aide concernant l'intégration de Splunk, l'exportation de données vers Splunk ou pour nous faire part de vos commentaires.

Application Citrix Analytics pour Splunk

> **Remarque**
>
> Cette application est en avant-première.

L'application Citrix Analytics pour Splunk permet aux administrateurs de Splunk Enterprise d'afficher les données utilisateur collectées à partir de Citrix Analytics for Security sous la forme de tableaux de bord pertinents et exploitables sur Splunk. À l'aide de ces tableaux de bord, vous obtenez une vue détaillée des comportements à risque des utilisateurs au sein de votre organisation et vous pouvez prendre des mesures opportunes pour atténuer les menaces internes. Vous pouvez également mettre

en corrélation les données collectées à partir de Citrix Analytics for Security avec d'autres sources de données configurées sur votre Splunk. Cette corrélation vous donne une visibilité sur les activités risquées des utilisateurs à partir de plusieurs sources et permet de prendre des mesures pour protéger votre environnement informatique.

Version Splunk prise en charge

L'application Citrix Analytics pour Splunk s'exécute sur les versions Splunk suivantes :

- Splunk 9.0 64 bits
- Splunk 8.2 64 bits
- Splunk 8.1 64 bits

Conditions préalables à l'application Citrix Analytics pour Splunk

- Installez le module complémentaire Citrix Analytics pour Splunk.
- Assurez-vous que les conditions préalables mentionnées pour le module complémentaire Citrix Analytics pour Splunk sont déjà remplies.
- Assurez-vous que les données sont transférées de Citrix Analytics for Security vers Splunk.

Installation et configuration

Où installer l'application ? Tête de recherche Splunk

Comment installer et configurer l'application ? Vous pouvez installer l'application Citrix Analytics pour Splunk en la téléchargeant depuis Spunkbase ou en l'installant depuis Splunk.

Installer l'application depuis un fichier

1. Allez sur Splunkbase.
2. Téléchargez le fichier de l'application Citrix Analytics pour Splunk.
3. Sur la page d'accueil de Splunk Web, cliquez sur l'icône en forme de roue dentée en regard de **Applications**.
4. Cliquez sur **Installer l'application depuis un fichier**.
5. Recherchez le fichier téléchargé et cliquez sur **Charger**.

> **Remarque**
>
> Si vous disposez d'une ancienne version de l'application, sélectionnez **Mettre à niveau l'application** pour la remplacer.

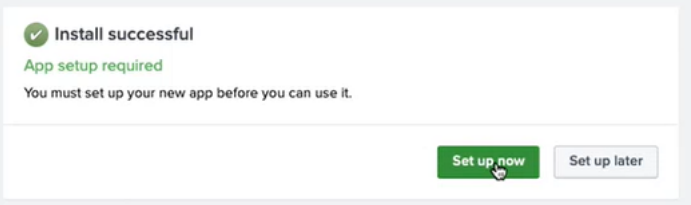
6. Vérifiez que l'application apparaît dans la liste des **applications**.

Installez l'application depuis Splunk

1. Sur la page d'accueil de Splunk Web, cliquez **sur+Trouver d'autres applications**.
2. Sur la page Parcourir plus d'applications, recherchez **Splunk dans l'application Citrix Analytics**.
3. Cliquez sur **Installer** en regard de l'application.

Configurez votre index et votre type de source pour corréler les données

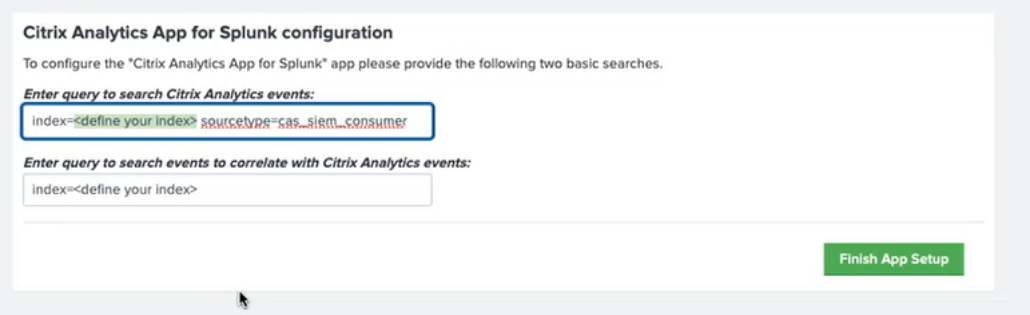
1. Après avoir installé l'application, cliquez sur **Configurer maintenant**.



2. Entrez les requêtes suivantes :
   - Index et type de source dans lesquels les données de Citrix Analytics for Security sont stockées.

     > **Remarque**
     >
     > Ces valeurs de requête doivent être identiques à celles spécifiées dans le module complémentaire Citrix Analytics pour Splunk. Pour plus d'informations, consultez la section Configurer le module complémentaire Citrix Analytics pour Splunk.

   - Index à partir duquel vous souhaitez mettre en corrélation vos données avec Citrix Analytics for Security.



3. Cliquez sur **Terminer la configuration de l'application** pour terminer la configuration.

Après avoir configuré et configuré l'application Citrix Analytics pour Splunk, utilisez les tableaux de bord Citrix Analytics pour afficher les événements utilisateur sur votre Splunk.

Pour plus d'informations sur l'intégration de Splunk, consultez les liens suivants :

- Intégration de Citrix Analytics à Splunk
- L'application Citrix Analytics pour Splunk, désormais disponible dans Splunkbase

Architecture Splunk avec application complémentaire Citrix Analytics

February 13, 2023

L'architecture de Splunk comprend les trois niveaux suivants :

- Collection
- Indexation
- Recherche

Splunk prend en charge un large éventail de mécanismes de collecte de données qui permettent d'intégrer facilement des données dans Splunk, afin qu'elles puissent être indexées et mises à disposition pour la recherche. Ce niveau n'est rien d'autre que votre transitaire lourd ou votre transitaire universel.

Vous devez installer l'application complémentaire sur la couche de redirection lourde plutôt que sur la couche de transfert universelle. En effet, à quelques exceptions près pour les données bien structurées (telles que json, csv, tsv), le redirecteur universel n'analyse pas les sources des journaux en événements. Il ne peut donc effectuer aucune action nécessitant une compréhension du format des journaux.

Il est également livré avec une version allégée de Python, ce qui le rend incompatible avec les applications d'entrée modulaires qui nécessitent une pile Splunk complète pour fonctionner. Le transitaire lourd n'est rien d'autre que votre niveau de collection.

La principale différence entre un redirecteur universel et un redirecteur lourd réside dans le fait que le redirecteur lourd contient le pipeline d'analyse complet, exécutant les mêmes fonctions qu'un indexeur sans réellement écrire et indexer les événements sur le disque. Cela permet au transitaire lourd de comprendre et d'agir sur des événements individuels, tels que le masquage des données, le filtrage et le routage en fonction des données d'événements. Comme l'application complémentaire dispose d'une installation complète de Splunk Enterprise, elle peut héberger des entrées modulaires qui nécessitent une pile Python complète pour collecter correctement les données, ou servir de point de terminaison pour le collecteur d'événements HTTP (HEC) de Splunk.

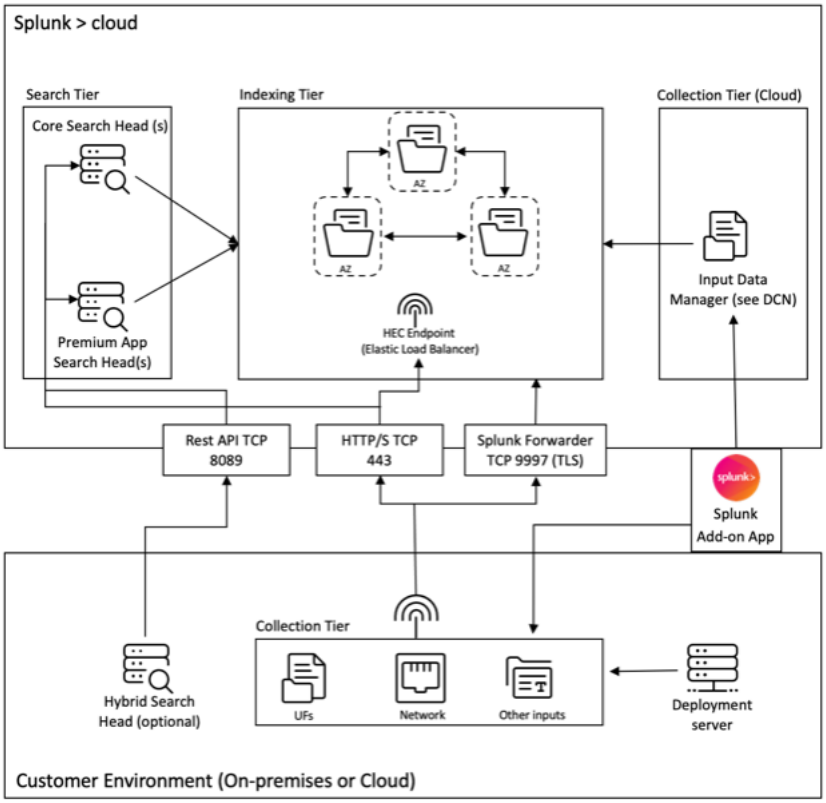
Une fois les données collectées, elles sont indexées ou traitées et stockées de manière à pouvoir être consultées.

La recherche est le principal moyen pour les clients d'explorer leurs données. Une recherche peut être enregistrée sous forme de rapport et utilisée pour alimenter les panneaux du tableau de bord. Les recherches sont des informations extraites de vos données.

En général, l'application complémentaire Splunk est déployée au niveau Collection (au niveau de l'entreprise Splunk), tandis que notre application de tableau de bord est déployée sur la couche de recherche (au niveau de Splunk Cloud). Dans le cadre d'une configuration sur site simple, vous pouvez disposer de ces trois niveaux sur un seul hôte Splunk (ce que l'on appelle le déploiement sur un seul serveur).

Le niveau de collecte est un bien meilleur moyen d'utiliser l'application complémentaire pour Splunk. Il existe deux manières d'installer l'application complémentaire. Vous pouvez l'installer au niveau de collecte dans l'environnement client ou vous pouvez l'installer dans le gestionnaire de données d'entrée de l'**instance Splunk Cloud**.

Reportez-vous au schéma suivant pour comprendre l'architecture de déploiement de Splunk avec notre application complémentaire :



Le gestionnaire de données d'entrée (IDM) illustré dans le schéma ci-dessus est l'implémentation gérée par Splunk Cloud d'un nœud de collecte de données (DCN) qui prend uniquement en charge les entrées scriptées et modulaires. Pour les besoins de collecte de données supplémentaires, vous pouvez déployer et gérer un DCN dans votre environnement à l'aide d'un Splunk Heavy Forwarder.

Splunk permet de collecter, d'indexer et de rechercher des données provenant de différentes sources. L'un des moyens de collecter des données consiste à utiliser des API, qui permettent à Splunk d'accéder aux données stockées dans d'autres systèmes ou applications. Ces API peuvent inclure REST, des services Web, JMS et/ou JDBC en tant que mécanisme de requête. Splunk et tous les développeurs tiers proposent une gamme d'applications qui permettent des interactions avec les API via le framework de saisie modulaire Splunk. Ces applications nécessitent généralement une installation complète du logiciel d'entreprise Splunk pour fonctionner correctement.

Pour faciliter la collecte de données via des API, il est courant de déployer un redirecteur lourd en tant que DCN. Les redirecteurs lourds sont des agents plus puissants que les redirecteurs universels, car ils contiennent l'intégralité du pipeline d'analyse et peuvent comprendre les événements individuels et agir en conséquence. Cela leur permet de collecter des données via des API et de les traiter avant de les transmettre à une instance Splunk à des fins d'indexation.

Pour en savoir plus sur l'architecture de haut niveau d'un déploiement de Splunk Cloud, consultez la section Architectures validées par Splunk.

Tableaux de bord Citrix Analytics pour Splunk

December 7, 2023

> **Remarque**
>
> **Attention** : Citrix Content Collaboration et ShareFile ont atteint leur fin de vie et ne sont plus disponibles pour les utilisateurs.
>
> Cette fonctionnalité est disponible dans la Tech Preview.

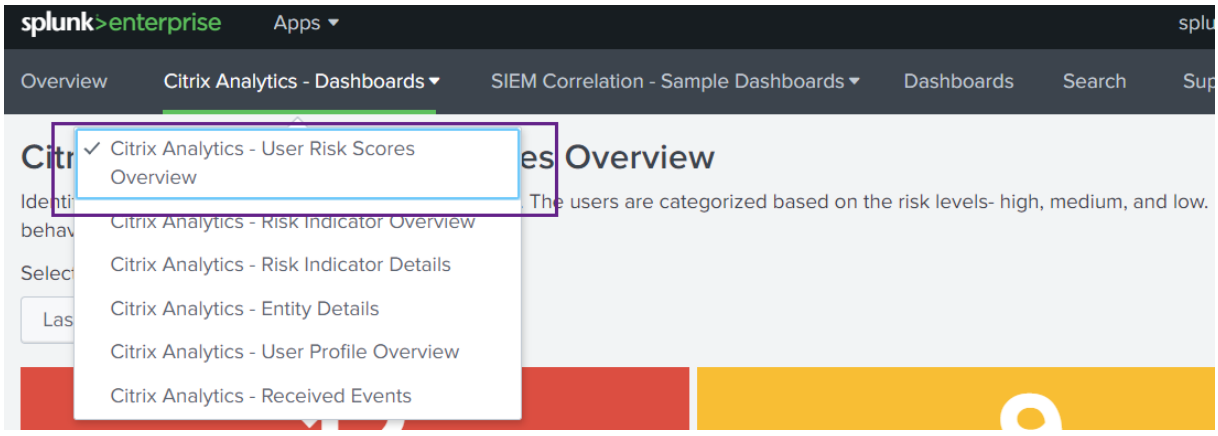
Conditions préalables

Pour utiliser les tableaux de bord Citrix Analytics suivants, vérifiez que vous avez déjà configuré et configuré l'application Citrix Analytics pour Splunk.

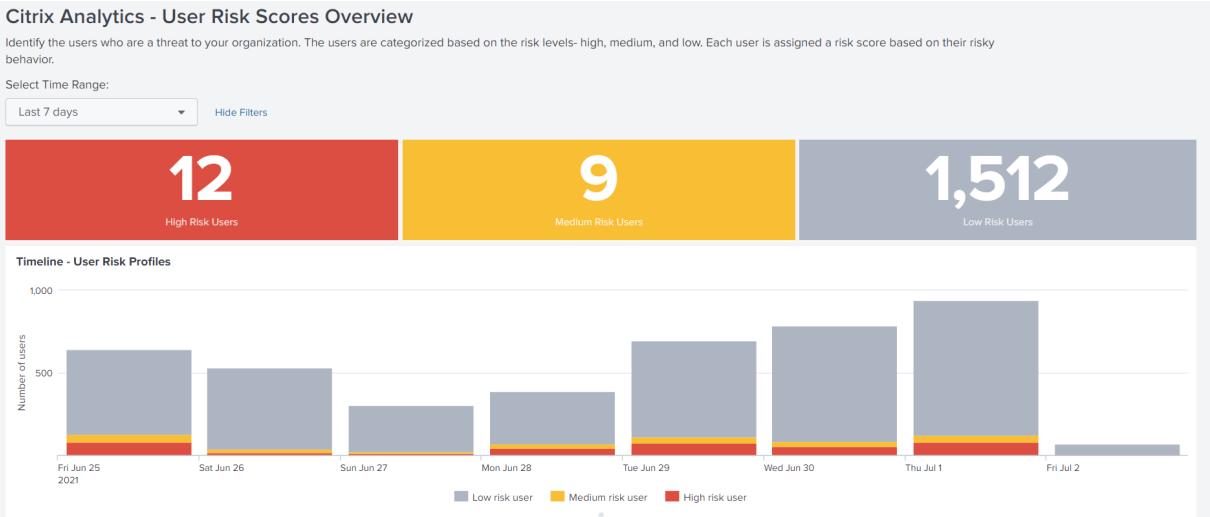
Aperçu du score de risque utilisateur

Ce tableau de bord fournit une vue consolidée des utilisateurs à risque de votre organisation. Les utilisateurs sont classés en fonction des niveaux de risque : élevé, moyen et faible. Les niveaux de risque sont basés sur les anomalies des activités de l'utilisateur et, par conséquent, un score de risque est attribué. Pour plus d'informations sur les types d'utilisateurs à risque, consultez le tableau de bord Utilisateurs.

Pour afficher ce tableau de bord, cliquez sur **Citrix Analytics- Tableaux de bord > Citrix Analytics- Aperçu des scores de risque utilisateur**.



Sélectionnez une plage de temps prédéfinie ou une plage de temps personnalisée pour afficher la chronologie des utilisateurs à risque et leurs détails.



Le tableau Utilisateurs risqués fournit les informations suivantes :

- **Utilisateur** : indique le nom d'utilisateur. Cliquez sur un nom d'utilisateur pour afficher les détails du comportement risqué de l'utilisateur dans le tableau de bord Citrix Analytics - Détails de l'entité.
- **Risques de points de terminaison compromis détectés** : indique le nombre d'indicateurs de risque déclenchés par l'utilisateur qui appartiennent à la catégorie de risque des points de terminaison compromis.
- **Risques détectés par les utilisateurs compromis** : indique le nombre d'indicateurs de risque déclenchés par l'utilisateur appartenant à la catégorie de risque des utilisateurs compromis.
- **Risques d'exfiltration de données détectés** : indique le nombre d'indicateurs de risque déclenchés par l'utilisateur qui appartiennent à la catégorie de risque d'exfiltration de données.
- **Risques de menaces internes détectés** : indique le nombre d'indicateurs de risque déclenchés par l'utilisateur qui appartiennent à la catégorie de risque de menaces internes.
- **Score de risque** : indique le score de risque de l'utilisateur.

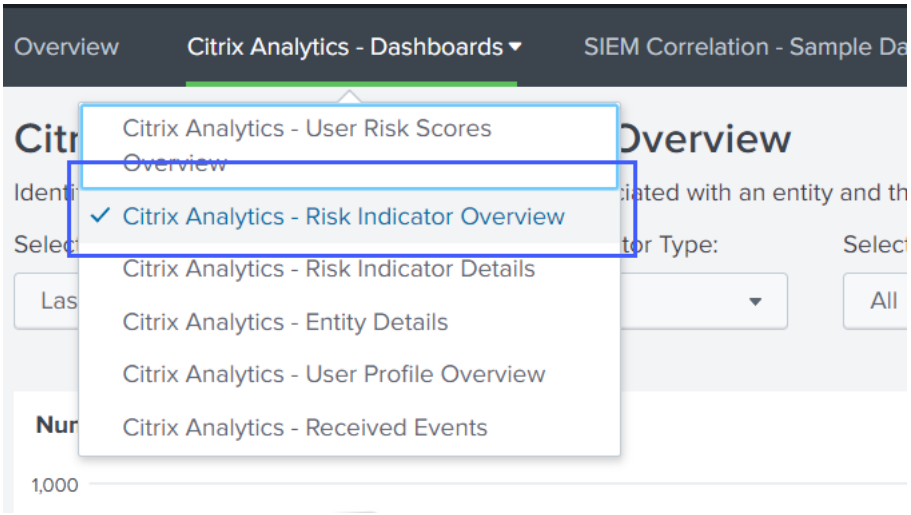
Vous pouvez également rechercher un utilisateur par son nom d'utilisateur et obtenir les informations requises.

Pour plus d'informations, consultez la section Catégories de risques.

Aperçu des indicateurs de risque

Le tableau de bord fournit une vue consolidée des indicateurs de risque déclenchés par les utilisateurs de votre organisation.

Pour afficher le tableau de bord, cliquez sur **Citrix Analytics - Tableaux de bord > Citrix Analytics - Vue d'ensemble des indicateurs de risque**.

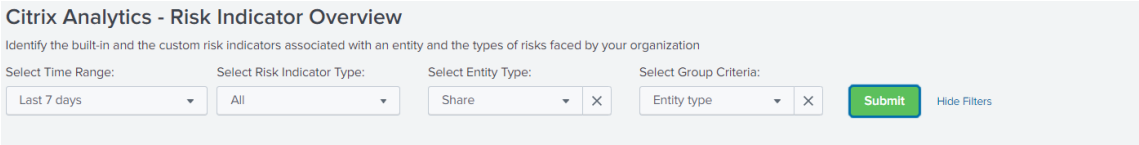


Sélectionnez une catégorie pour afficher le rapport

Recherchez les indicateurs de risque en sélectionnant une ou plusieurs catégories :

- Période : sélectionnez une**plage**de temps prédéfinie ou une plage de temps personnalisée pour afficher les indicateurs de risque déclenchés pour cette période.
- **Type d'indicateur de risque** : sélectionnez le type d'indicateur de risque : intégré ou personnalisé.
- **Type d'entité** : sélectionnez un utilisateur pour afficher les indicateurs de risque associés.

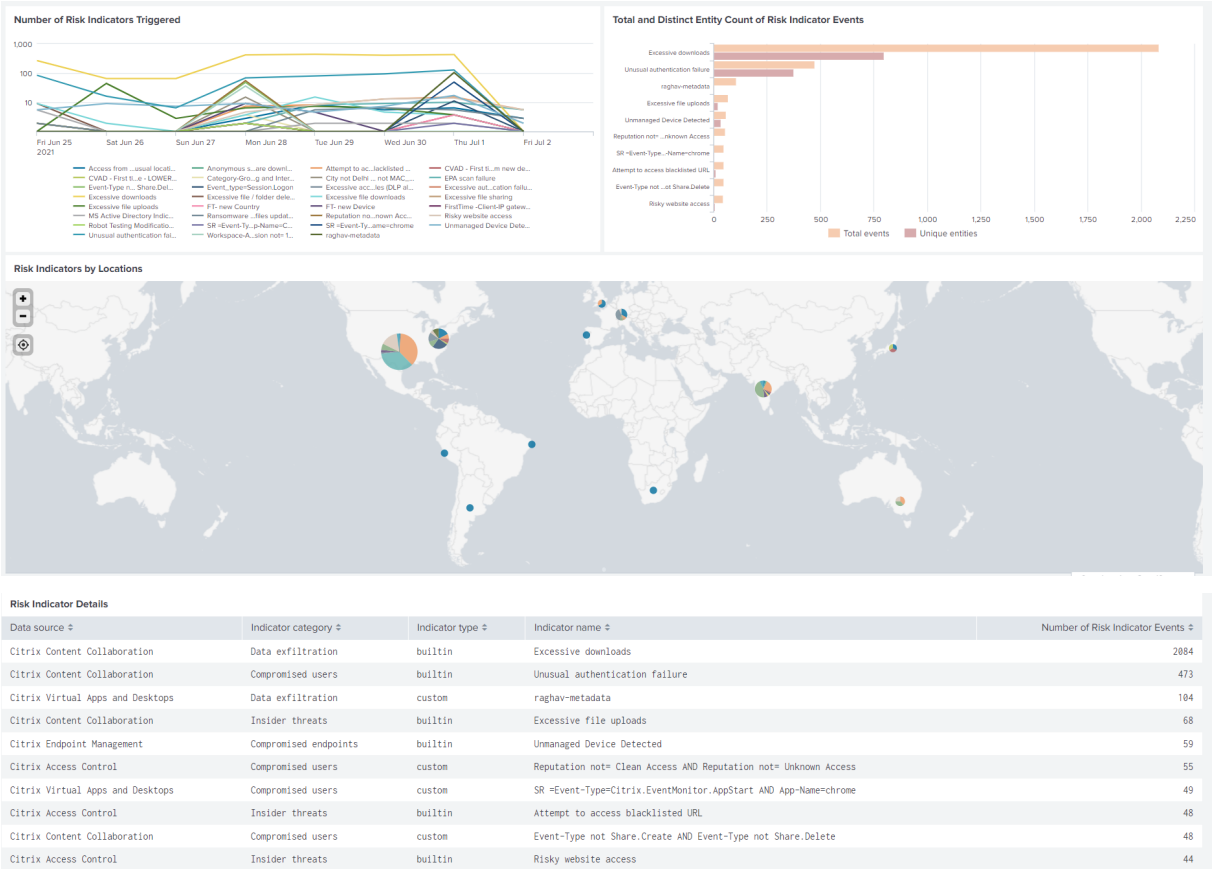
- **Groupe** : sélectionnez un critère pour regrouper les événements utilisateur par source de données, catégorie d'indicateur, nom d'indicateur, type d'indicateur ou type d'entité, et affichez les indicateurs de risque associés.



Afficher le rapport

Utilisez les rapports suivants pour afficher des détails sur les indicateurs de risque en sélectionnant une ou plusieurs catégories :

- **Nombre d'indicateurs de risque déclenchés** : affiche le nombre d'indicateurs de risque déclenchés pour la période sélectionnée. Utilisez ce rapport pour identifier le schéma et les domaines d'activités à risque. Identifiez également les activités les plus risquées de votre organisation.
- **Nombre total et distinct d'événements d'indicateurs de risque** : affiche le total des événements et les événements uniques correspondant à un indicateur de risque. Utilisez ce rapport pour identifier les occurrences de chaque indicateur de risque et les principaux indicateurs de risque de votre organisation. Vous pouvez également identifier le nombre d'utilisateurs uniques qui ont déclenché un indicateur de risque particulier et vérifier si l'indicateur de risque est déclenché par un groupe d'utilisateurs plus ou moins important.
- **Indicateurs de risque par emplacement** : affiche le nombre d'indicateurs de risque déclenchés par les utilisateurs sur tous les sites. Utilisez ce rapport pour identifier les sites qui présentent les activités les plus risquées et vérifier si les sites se trouvent en dehors de la zone d'opérations de votre organisation.
- **Détails de l'indicateur de risque** : affiche les détails de l'indicateur de risque, tels que la source de données associée, la catégorie d'indicateur, le type d'indicateur et le nombre d'occurrences.



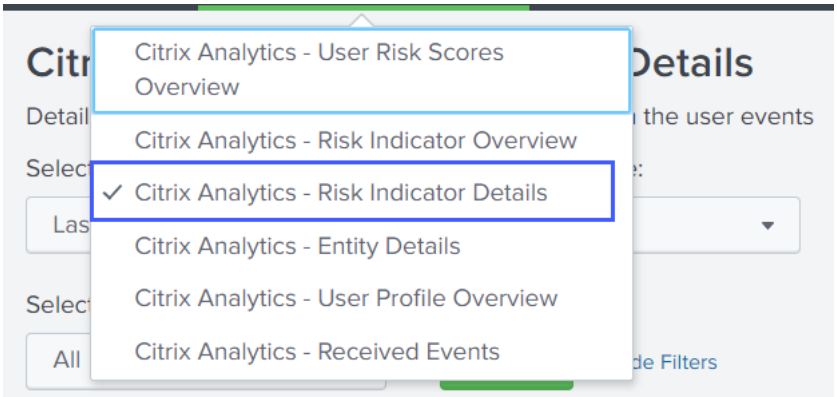
Risk Indicator Details

Data source	Indicator category	Indicator type	Indicator name	Number of Risk Indicator Events
Citrix Content Collaboration	Data exfiltration	builtin	Excessive downloads	2084
Citrix Content Collaboration	Compromised users	builtin	Unusual authentication failure	473
Citrix Virtual Apps and Desktops	Data exfiltration	custom	raghav-metadata	104
Citrix Content Collaboration	Insider threats	builtin	Excessive file uploads	68
Citrix Endpoint Management	Compromised endpoints	builtin	Unmanaged Device Detected	59
Citrix Access Control	Compromised users	custom	Reputation not= Clean Access AND Reputation not= Unknown Access	55
Citrix Virtual Apps and Desktops	Compromised users	custom	SR =Event-Type=Citrix.EventMonitor.AppStart AND App-Name=chrome	49
Citrix Access Control	Insider threats	builtin	Attempt to access blacklisted URL	48
Citrix Content Collaboration	Compromised users	custom	Event-Type not Share.Create AND Event-Type not Share.Delete	48
Citrix Access Control	Insider threats	builtin	Risky website access	44

Détails de l'indicateur de risque

Le tableau de bord fournit des informations détaillées sur les indicateurs de risque intégrés et personnalisés déclenchés par les utilisateurs. Pour plus d'informations, consultez les sections Indicateurs de risque utilisateur Citrix et Indicateursde risque personnalisés.

Pour afficher le tableau de bord, cliquez sur **Citrix Analytics - Tableaux de bord > Citrix Analytics - Détails de l'indicateur de risque**.



Sélectionnez une catégorie pour afficher les rapports

Affichez les détails des indicateurs de risque en sélectionnant une ou plusieurs catégories :

- **Période : sélectionnez une plage de temps prédéfinie ou une plage de temps personnalisée pour afficher les détails des indicateurs de risque déclenchés pour cette période.**
- **Type d'entité** : sélectionnez un utilisateur pour afficher les détails des indicateurs de risque associés.
- **Type d'indicateur de risque** : sélectionnez le type d'indicateur de risque intégré ou personnalisé pour afficher ses détails.
- **Source de données** : sélectionnez la source de données pour afficher les détails des indicateurs de risque associés.
- **Catégorie d'indicateurs de risque**- Sélectionnez la catégorie de risque pour afficher les détails des indicateurs de risque associés.
- **Indicateur de risque**- Sélectionnez l'indicateur de risque pour afficher ses détails.

Afficher les rapports

Par exemple, dans la liste Sélectionner un indicateur de risque, sélectionnez **Échec d'authentification inhabituel (Citrix Content Collaboration)**, cliquez sur **Soumettre**et affichez les informations suivantes :

- Les 10 principaux utilisateurs associés à l'indicateur de risque
- Des détails sur l'indicateur de risque, tels que
  - Date et heure du déclenchement
  - Source de données associée
  - Catégorie de risque associée
  - ID d'entité associé et type d'entité utilisateur
  - Gravité du risque élevée, moyenne ou faible
  - Probabilité de risque de l'événement utilisateur
  - Identité unique de l'indicateur de risque (UUID)

Dans **Top 10 des entités par indicateurs de risque**, cliquez sur une entité pour afficher ses détails dans le tableau de bord **Citrix Analytics - Détails de l'entité** .

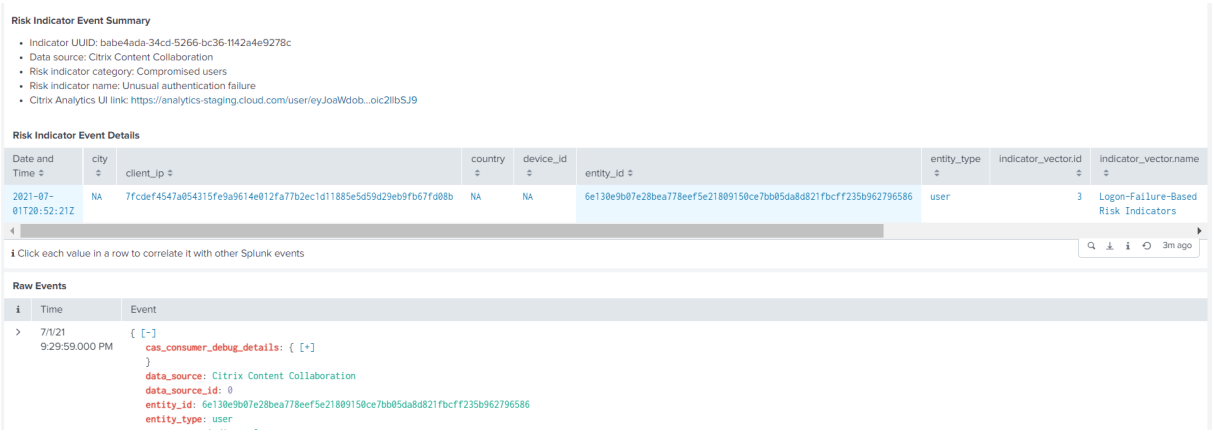
Risk Indicator Details

Date and Time	Data Source	Risk Indicator Category	Risk Indicator Name	Entity ID	Entity Type	Severity	Risk Probability	Risk Indicator UUID
2021-07-01T21:29:59Z	Citrix Content Collaboration	Compromised users	Unusual authentication failure	6e130e9b07e28bea778eef5e21809150ce7bb05da8d821fbcff235b962796586	user	medium	1.0	babe4ada-34cd-5266-bc36-1142a4e9278c
2021-07-01T21:29:59Z	Citrix Content Collaboration	Compromised users	Unusual authentication failure	102854bc92af241d303ab4c3cc62ec969a0c64c69985703293372 8b1d10a848	user	medium	1.0	f594a2bf-8121-5231-ab32-a2e3735ee6d5
2021-07-01T21:29:59Z	Citrix Content Collaboration	Compromised users	Unusual authentication failure	dc61f0b0a9218cb5f1925778069c112a4236d40e73f2dd8170e89eeabe717714	user	medium	1.0	6720f113-dc3e-5986-967e-26a748b0d00b

Cliquez sur chaque ligne du tableau des **détails de l'indicateur de risque** pour afficher le résumé de l'événement, les détails de l'événement et les événements bruts de l'indicateur de risque sélectionné.

Dans la section **Résumé des événements de l'indicateur de risque**, cliquez sur le **lien de l'interface utilisateur de Citrix Analytics** pour accéder directement à la chronologie utilisateur de Citrix Analytics for Security depuis votre Splunk. Sur la chronologie de l'utilisateur, affichez l'indicateur de risque, les événements associés et toutes les actions appliquées à l'utilisateur.

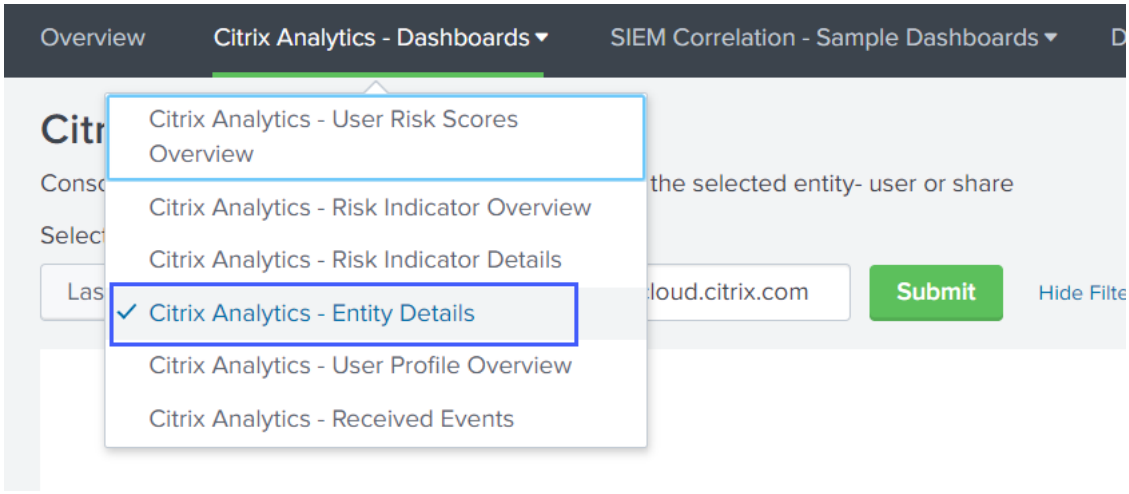
Pour plus d'informations sur le résumé des événements et les détails des événements, consultez la section Format de données Citrix Analytics pour SIEM.



Détails de l'entité

Utilisez le tableau de bord pour afficher les informations relatives à un utilisateur de l'entité utilisateur et à son comportement risqué.

Pour afficher le tableau de bord, cliquez sur **Citrix Analytics - Tableaux de bord > Citrix Analytics - Détails de l'entité**.

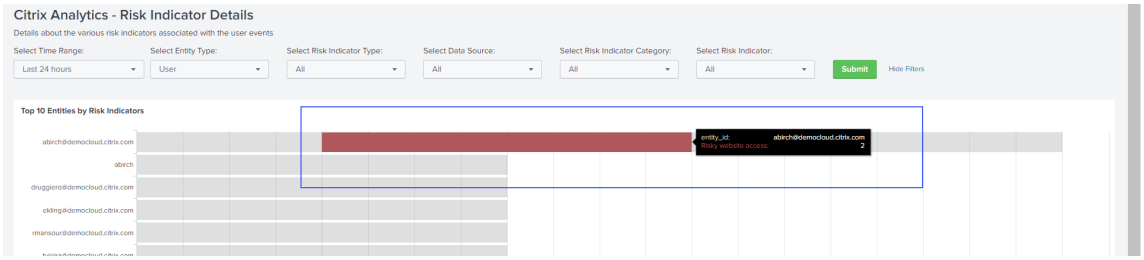


Afficher le rapport

Entrez une plage horaire et l'entité (nom d'utilisateur) et cliquez sur **Soumettre** pour afficher les informations détaillées.

Vous pouvez également afficher les informations détaillées sur une entité à partir des tableaux de bord suivants :

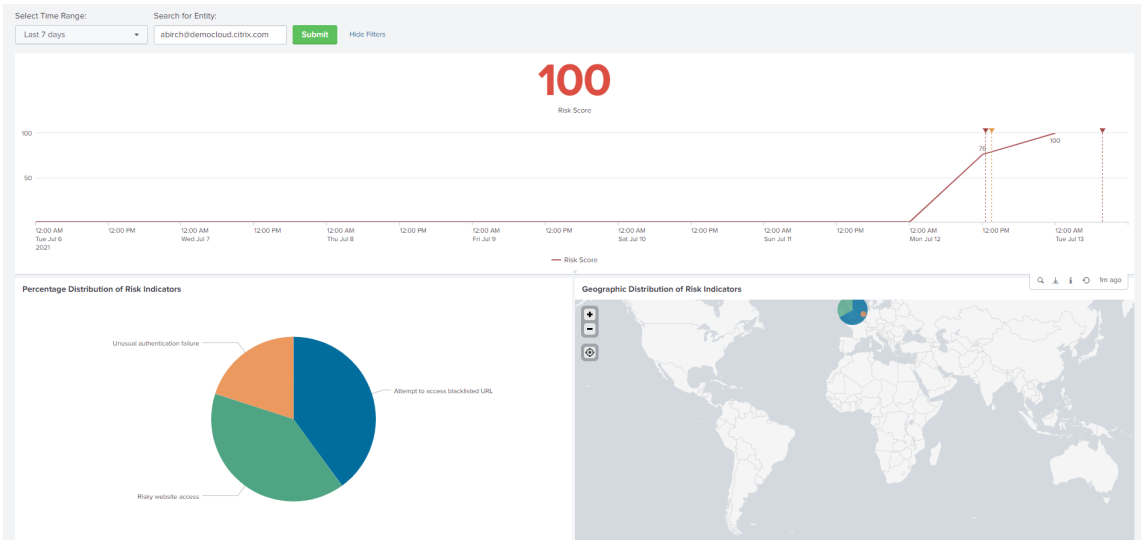
- Dans **Citrix Analytics - Détails des indicateurs de risque**, accédez à **Top 10 Entities by Risk Indicators**, puis cliquez sur une entité.

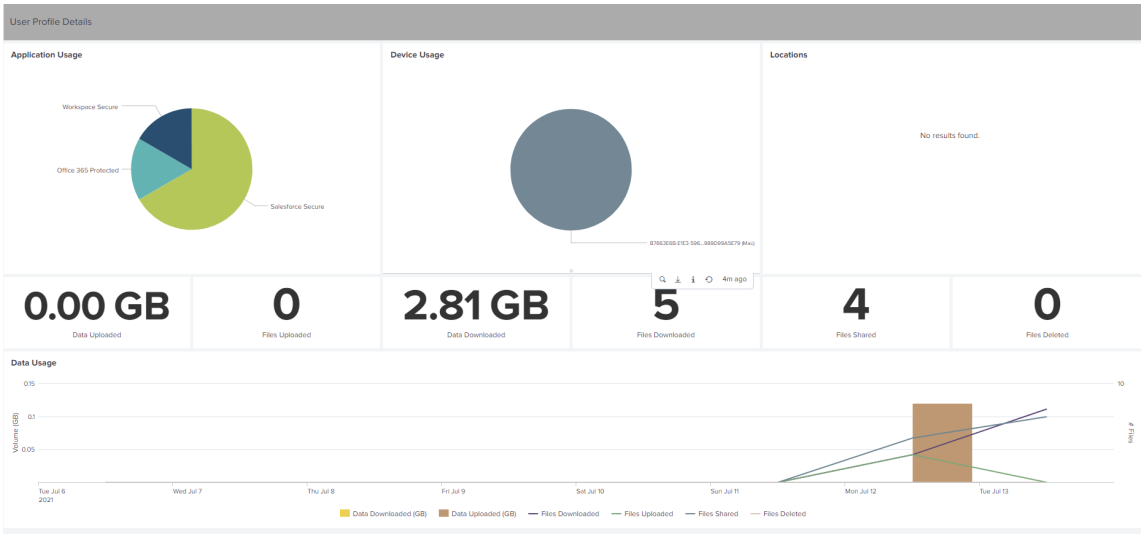


- Dans **Citrix Analytics - Vue d'ensemble du score de risque**, accédez à **Utilisateurs risqués**, puis cliquez sur un nom d'utilisateur.

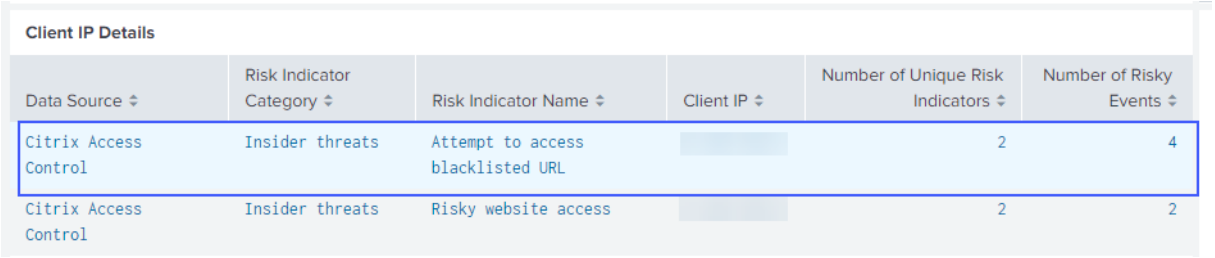
Les informations détaillées suivantes sont affichées :

- Score de risque actuel et chronologie du score de risque pour la période sélectionnée.
- Distribution en pourcentage des indicateurs de risque. Vous aide à analyser le schéma des activités à risque de l'entité.
- Distribution géographique des indicateurs de risque. Vous aide à identifier les lieux inhabituels et à haut risque.
- Détails de l'adresse IP du client associés aux activités à risque.
- Détails de l'appareil utilisateur associés aux activités à risque.
- Détails des indicateurs de risque tels que la source de données associée, la catégorie de risque, la gravité du risque, etc.





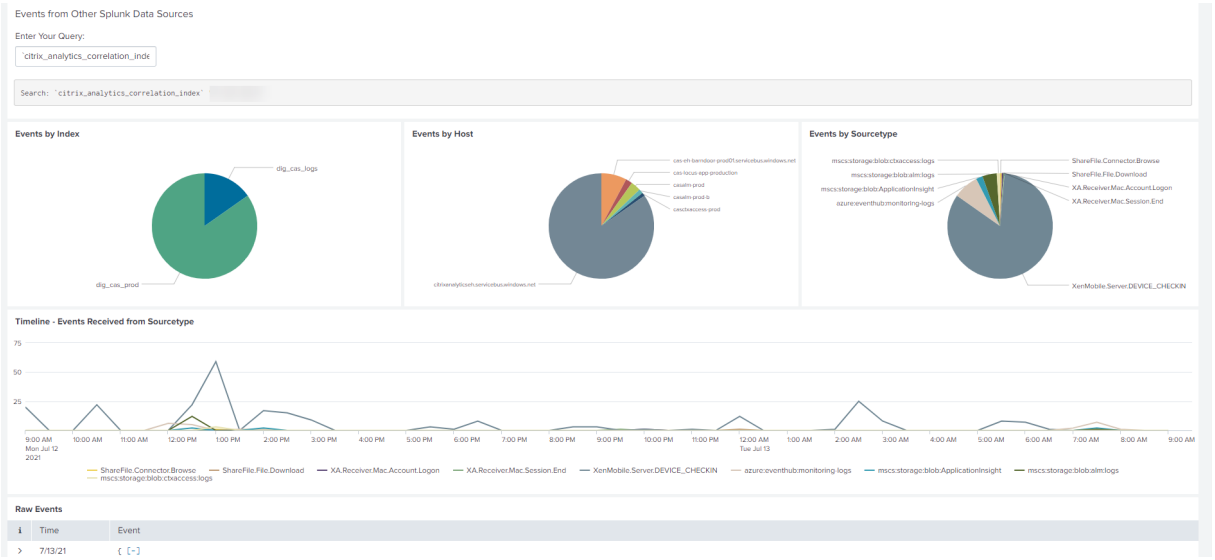
Corrélez les adresses IP des clients et les appareils des utilisateurs associés aux activités risquées avec les événements collectés auprès d'autres sources de sécurité connectées à votre Splunk. Par exemple, cliquez sur une ligne de la table **Client IP Details** .



Client IP Details

Data Source	Risk Indicator Category	Risk Indicator Name	Client IP	Number of Unique Risk Indicators	Number of Risky Events
Citrix Access Control	Insider threats	Attempt to access blacklisted URL		2	4
Citrix Access Control	Insider threats	Risky website access		2	2

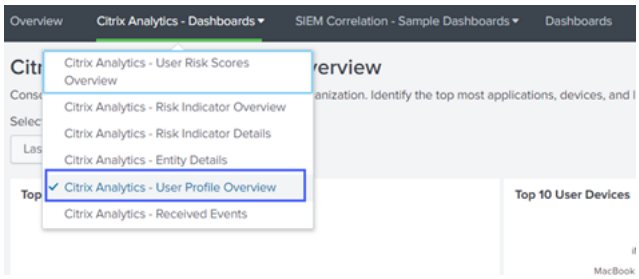
Dans le tableau de bord **Citrix Analytics Event Corrélation**, vous pouvez afficher les événements associés à l'adresse IP client sélectionnée qui sont corrélés à partir de vos autres sources de données de sécurité (en fonction de l'index et du type de source). Ces événements fournissent des informations plus approfondies sur les activités malveillantes associées à l'adresse IP du client.



Vue d'ensemble du profil utilisateur

Utilisez le tableau de bord pour afficher les mesures d'événements associées aux utilisateurs de votre organisation.

Pour afficher le tableau de bord, cliquez sur **Citrix Analytics - Tableaux de bord > Citrix Analytics - Vue d'ensemble du profil utilisateur**.



Afficher les événements

Sélectionnez une plage de temps et affichez les mesures suivantes :

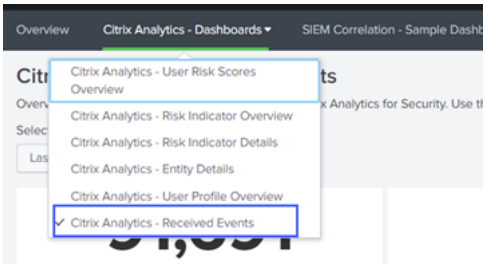
- 10 applications les plus utilisées par les utilisateurs
- Les 10 principaux appareils utilisés par les utilisateurs
- Top 10 des emplacements utilisés par les utilisateurs
- Nombre d'applications Web et SaaS utilisées
- Nombre d'appareils utilisés
- Nombre d'utilisateurs ayant accédé à différents emplacements
- Mesures d'utilisation des données telles que les fichiers téléchargés, téléchargés et partagés

Ces mesures vous fournissent des informations sur les activités des utilisateurs au sein de votre organisation. Vous pouvez identifier les principales applications et appareils, les modèles d'utilisation, les appareils et applications non conformes, les emplacements inhabituels, les accès à risque et les activités de fichiers inhabituelles.

Événements reçus

Utilisez le tableau de bord pour afficher les événements reçus de Citrix Analytics for Security. Un événement indique un type d'activité utilisateur.

Pour afficher le tableau de bord, cliquez sur **Citrix Analytics - Tableaux de bord > Citrix Analytics - Événements reçus**.

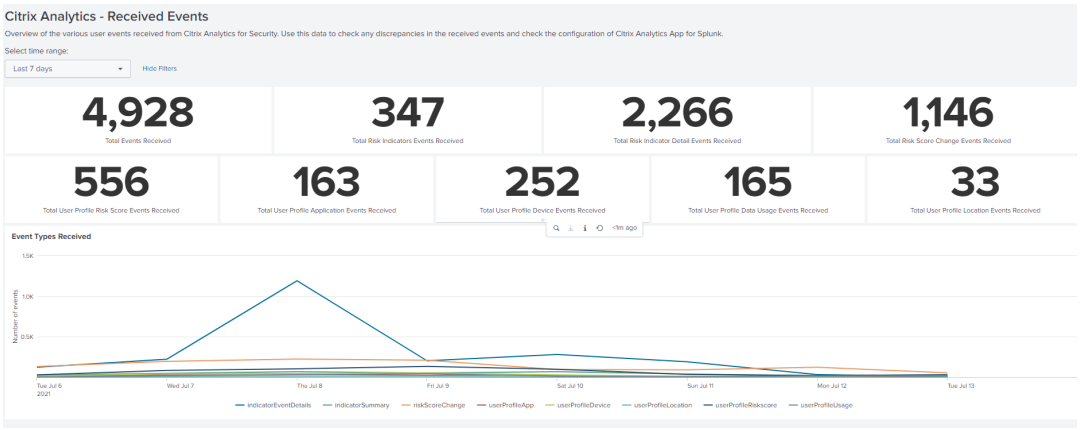


Afficher les rapports

Sélectionnez une plage horaire pour visualiser et comparer les différents types d'événements reçus. Le tableau de bord fournit les informations suivantes :

- Total des événements reçus : il s'agit de la somme de tous les événements reçus de Citrix Analytics for Security, y compris les suivants :
  - Événements d'indicateur de risque total : indique les événements associés aux indicateurs de risque déclenchés par les utilisateurs.
  - Événements détaillés de l'indicateur de risque total : indique les événements associés aux détails des indicateurs de risque déclenchés.

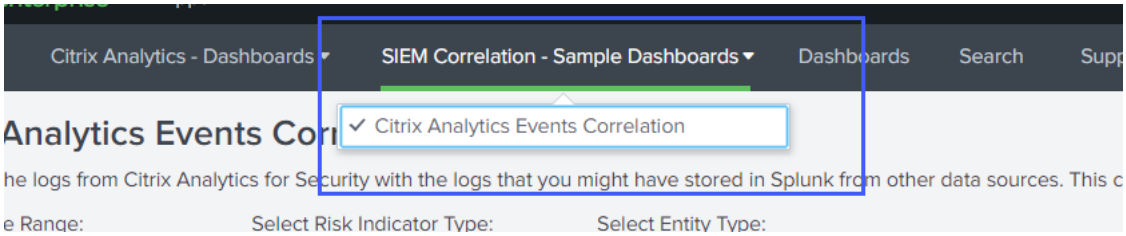
- Événements de modification du score de risque total : indique les événements associés à la modification du score de risque de l'utilisateur.
- Total des événements de score de risque du profil utilisateur : indique les événements associés aux scores de risque des utilisateurs.
- Nombre total d'événements d'application de profil utilisateur : indique les événements associés aux applications utilisées par les utilisateurs.
- Nombre total d'événements d'appareils de profil utilisateur : indique les événements associés aux terminaux utilisés par les utilisateurs.
- Nombre total d'événements d'utilisation des données de profil utilisateur : indique les événements associés à l'utilisation des données par les utilisateurs.
- Nombre total d'événements d'emplacement de profil utilisateur : indique les événements associés aux emplacements auxquels les utilisateurs ont accédé.



Exemple de corrélation d'événements

Utilisez le tableau de bord pour mettre en corrélation les événements reçus de Citrix Analytics for Security avec les événements collectés à partir d'autres sources de données de sécurité configurées dans votre Splunk. Vous obtenez des informations plus détaillées sur les activités risquées de l'utilisateur collectées à partir de plusieurs sources de données, vous trouvez des relations entre les événements et vous identifiez les menaces éventuelles.

Pour afficher le tableau de bord, cliquez sur **Corrélation SIEM - Exemples de tableaux de bord > Corrélation des événements Citrix Analytics**.



Conditions préalables

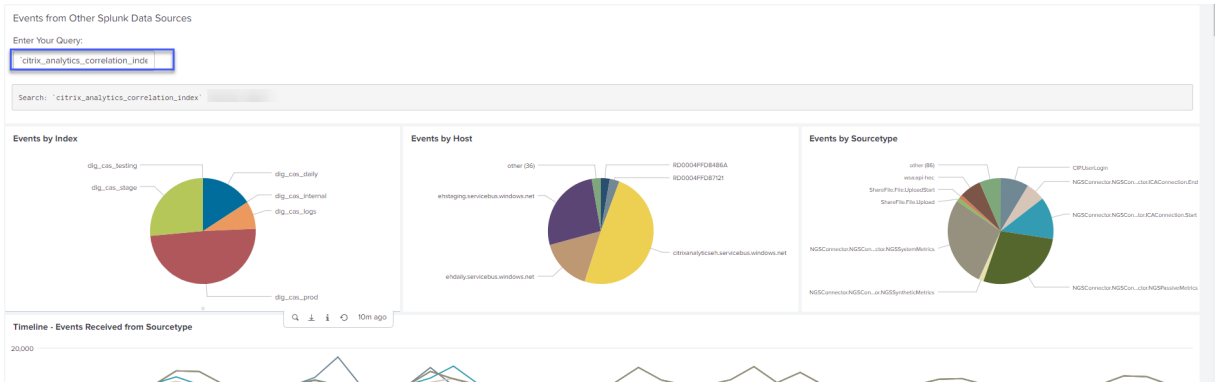
Pour effectuer une corrélation, vérifiez les points suivants :

- Vous devez disposer d'événements provenant de vos autres sources de données de sécurité pour pouvoir établir une corrélation. Par exemple, les événements associés aux utilisateurs, aux appareils et aux adresses IP des clients reçus d'autres sources de données configurées dans votre Splunk.
- Vous devez disposer d'un index de corrélation déjà défini lors de la configuration.

Corrélez les événements

Vous pouvez afficher les entités les plus risquées et les adresses IP les plus risquées détectées par Citrix Analytics for Security. Pour mettre en corrélation ces événements avec d'autres sources de données (définies dans l'index et le type de source), cliquez sur une entité ou une adresse IP dans les tables.

La valeur d'index affichée dans le champ de requête est définie lors de la configuration de l'application. Vous pouvez remplacer la valeur de l'index par une autre source de données de sécurité en fonction de vos besoins.

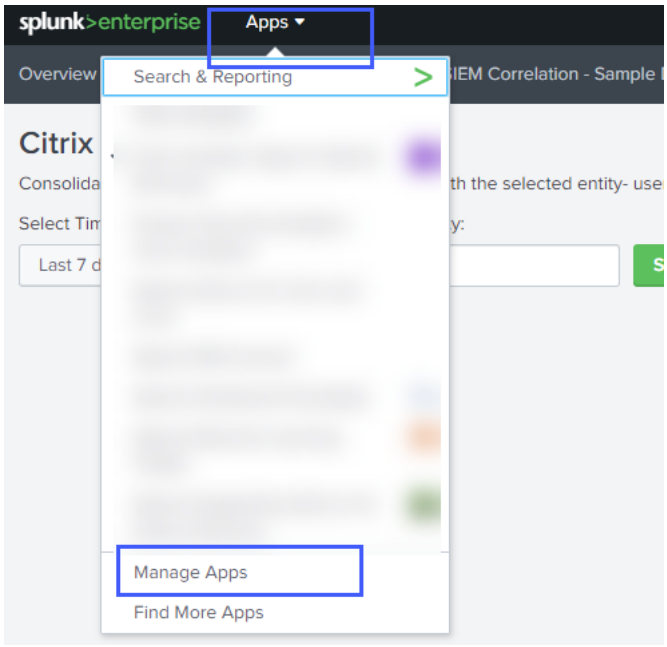


Dépannage en cas d'absence d'événements

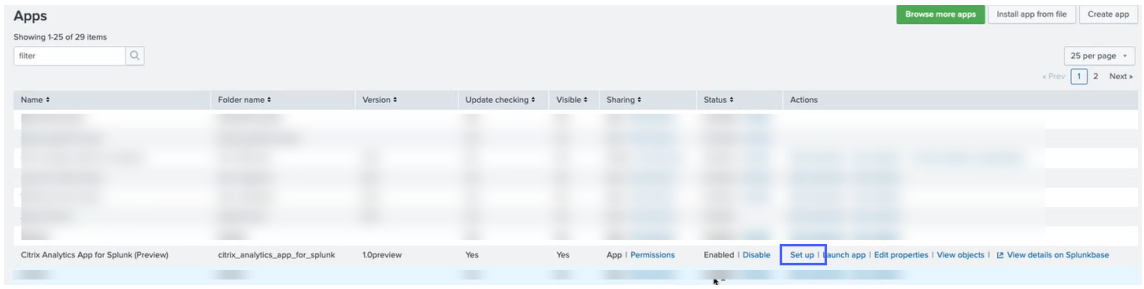
Si vous ne trouvez aucun événement sur tous les tableaux de bord, cela peut être dû aux problèmes de configuration de l'application Citrix Analytics pour Splunk et du module complémentaire Citrix Analytics pour Splunk. Dans un tel scénario, vérifiez la valeur de l'index et la valeur du type de source. Assurez-vous que les valeurs de l'index et du type de source sont identiques dans l'application et dans le module complémentaire.

Pour afficher les paramètres de configuration de l'application Citrix Analytics pour Splunk, procédez comme suit :

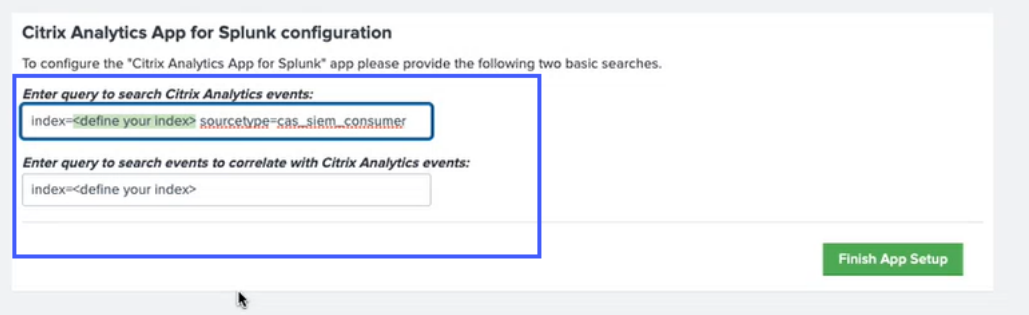
1. Cliquez sur **Applications > Gérer les applications**.



2. Recherchez l'application Citrix Analytics pour Splunk dans la liste. Cliquez sur **Configurer**.

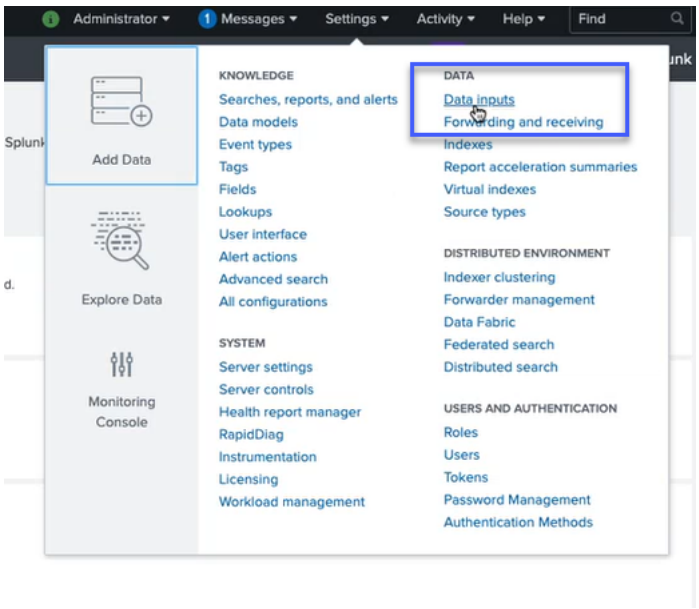


3. Vérifiez le type de source et l'index.

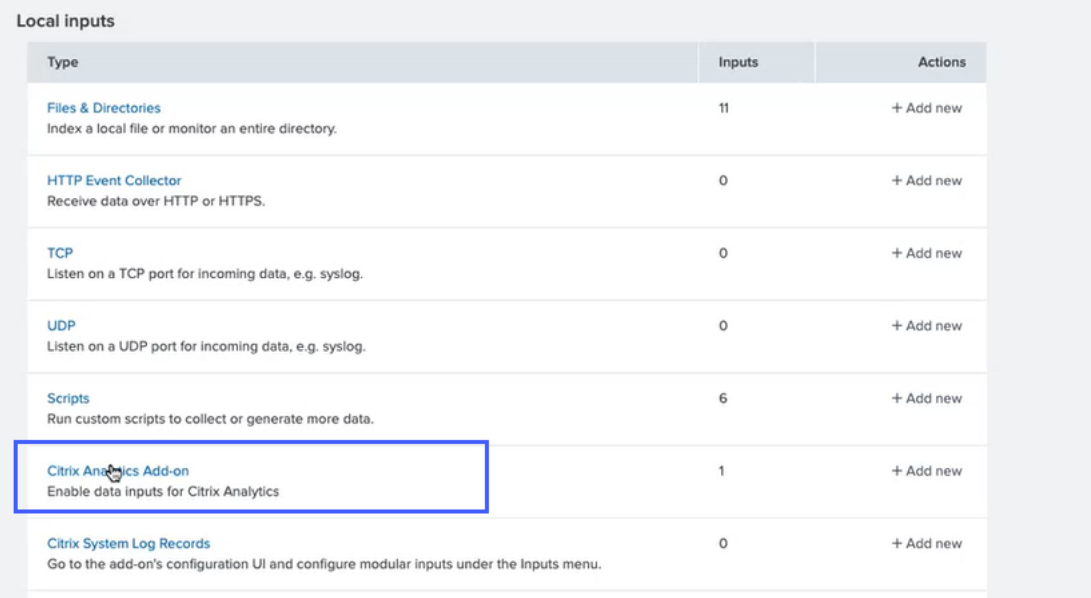


Pour afficher les paramètres de configuration du module complémentaire Citrix Analytics pour Splunk, procédez comme suit :

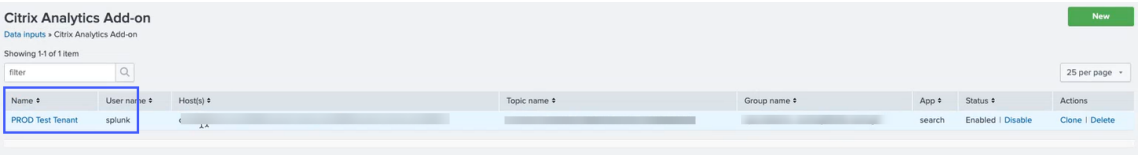
1. Cliquez sur **Paramètres > Entrées de données**.



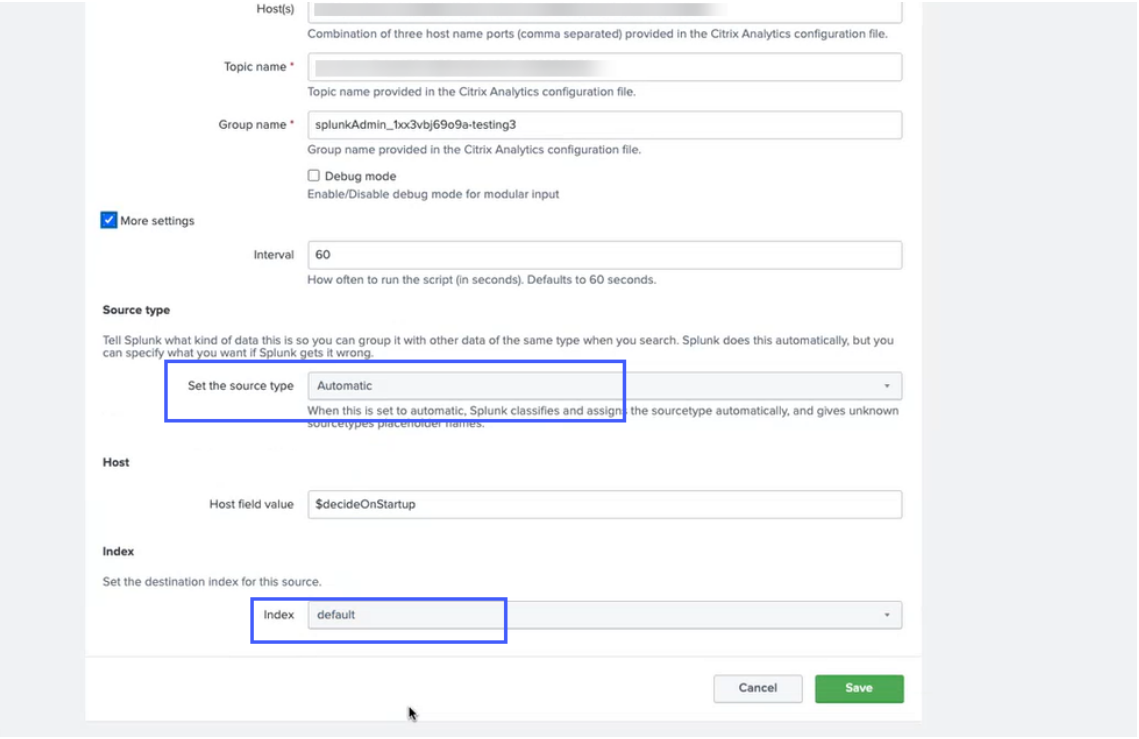
2. Cliquez sur **Citrix Analytics Add-on**.



3. Cliquez sur le locataire à partir duquel vous obtenez les événements.
4. Sélectionnez **Plus de paramètres**.



5. Vérifiez le type de source et l'index.



Pour plus d'informations sur la configuration, consultez Configurer le module complémentaire Citrix Analytics pour Splunk.

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.

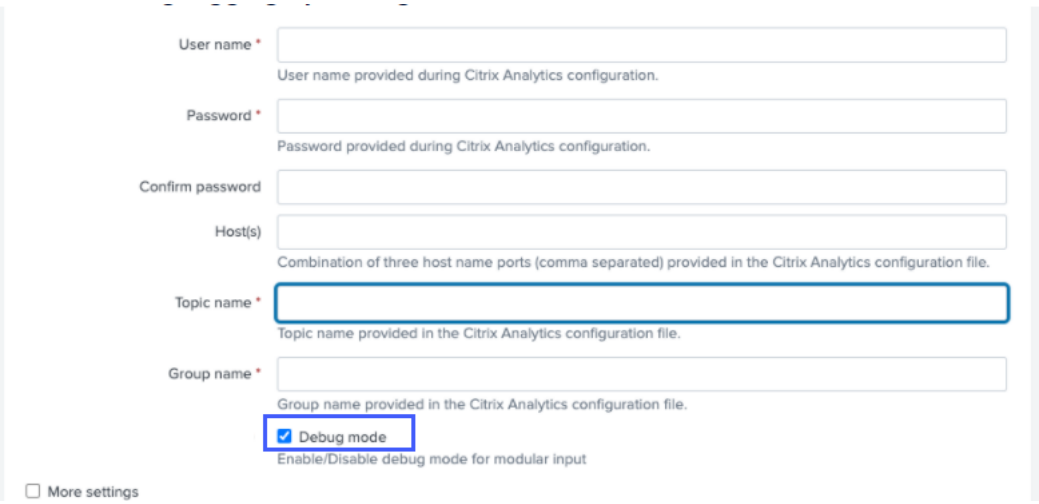
   - Détails de configuration incorrects dans **Paramètres > Entrées de données > Module complémentaire Citrix Analytics**.

     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.

Intégration Microsoft Sentinel

November 16, 2023

> **Remarques**
>
> - Contactez CAS-PM-Ext@cloud.com pour demander de l'aide concernant l'intégration de

> Microsoft Sentinel, l'exportation de données vers Microsoft Sentinel ou pour faire part de vos commentaires.
>
> - L'exportation des données vers Microsoft Sentinel à l'aide du moteur Logstash est en préversion. Cette fonctionnalité est fournie sans accord de niveau de service et n'est pas recommandée pour les charges de travail de production. Pour plus d'informations, consultez la documentation Microsoft Sentinel .

Intégrez Citrix Analytics for Security à votre Microsoft Sentinel à l'aide du moteur Logstash.

Cette intégration vous permet d'exporter et de corréler les données des utilisateurs de votre environnement informatique Citrix vers Microsoft Sentinel et d'obtenir des informations plus approfondies sur la posture de sécurité de votre organisation. Consultez les tableaux de bord pertinents propres à Citrix Analytics for Security dans votre environnement Splunk. Vous pouvez également créer des vues personnalisées en fonction de vos exigences de sécurité.

Pour plus d'informations sur les avantages de l'intégration et le type de données traitées qui sont envoyées à votre SIEM, voir Intégration des informations de sécurité et de la gestion des événements.

Conditions préalables

- Activez le traitement des données pour au moins une source de données. Il aide Citrix Analytics for Security à démarrer le processus d'intégration de Microsoft Sentinel.
- Assurez-vous que le point de terminaison suivant figure dans la liste d'autorisation de votre réseau.

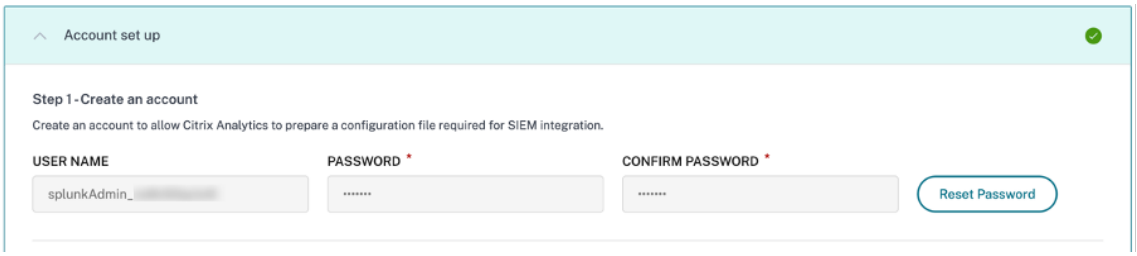
Point de terminaison	Région des États-Unis	Région de l'Union européenne	Région Asie-Pacifique Sud

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`

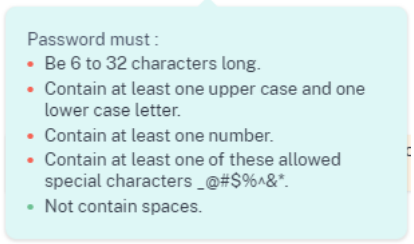
- Assurez-vous d'utiliser les versions 7.17.7 ou ultérieures de Logstash (versions testées pour la compatibilité avec Citrix Analytics for Security : v7.17.7 et v8.5.3) avec le plug-in de sortie Microsoft Sentinel pour Logstash.

Intégration à Microsoft Sentinel

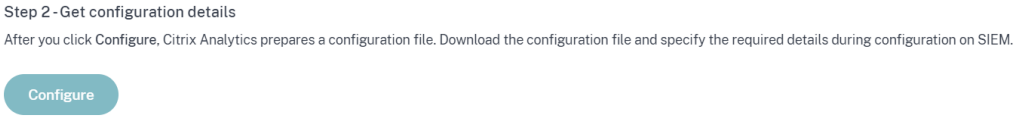
1. Accédez à **Réglages > Exportations de données**.
2. Dans la section **Configuration du compte**, créez un compte en spécifiant le nom d'utilisateur et le mot de passe. Ce compte est utilisé pour préparer un fichier de configuration, qui est nécessaire à l'intégration.



3. Assurez-vous que le mot de passe répond aux conditions suivantes :



4. Cliquez sur **Configurer** pour générer le fichier de configuration Logstash.



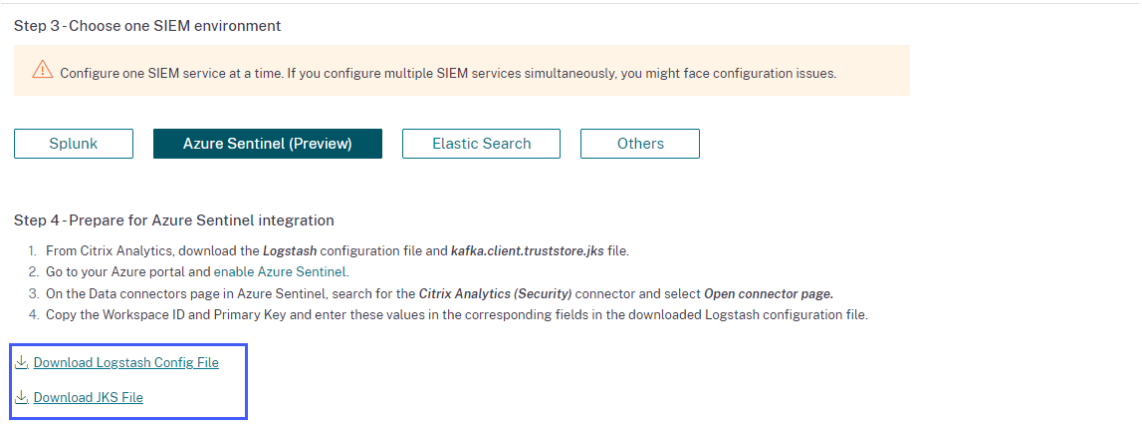
5. Sélectionnez l'onglet Azure Sentinel (version préliminaire) pour télécharger les fichiers de configuration :

   - **Fichier de configuration Logstash** : contient les données de configuration (sections d'entrée, de filtre et de sortie) pour l'envoi d'événements de Citrix Analytics for Security à Microsoft Sentinel à l'aide du moteur de collecte de données Logstash.

     Pour plus d'informations sur la structure du fichier de configuration Logstash, consultez la documentation Logstash .

   - **Fichier JKS** : contient les certificats nécessaires à la connexion SSL.

> **Remarque**
>
> Ces fichiers contiennent des informations sensibles. Conservez-les dans un endroit sûr et sécurisé.



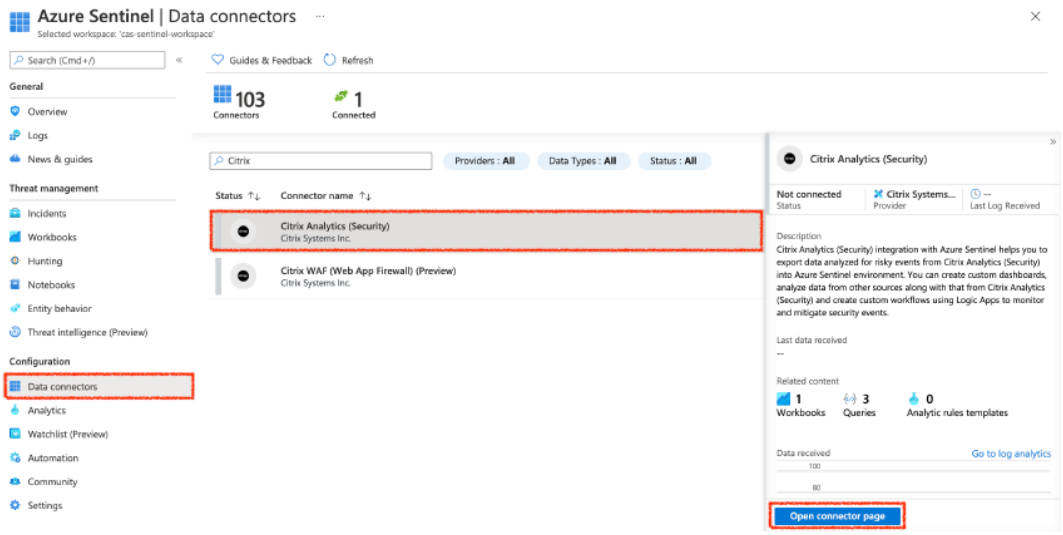
6. Préparez votre intégration Azure Sentinel :

   a) Sur votre portail Azure, activez Microsoft Sentinel. Vous pouvez créer un espace de travail ou utiliser votre espace de travail existant pour exécuter Microsoft Sentinel.

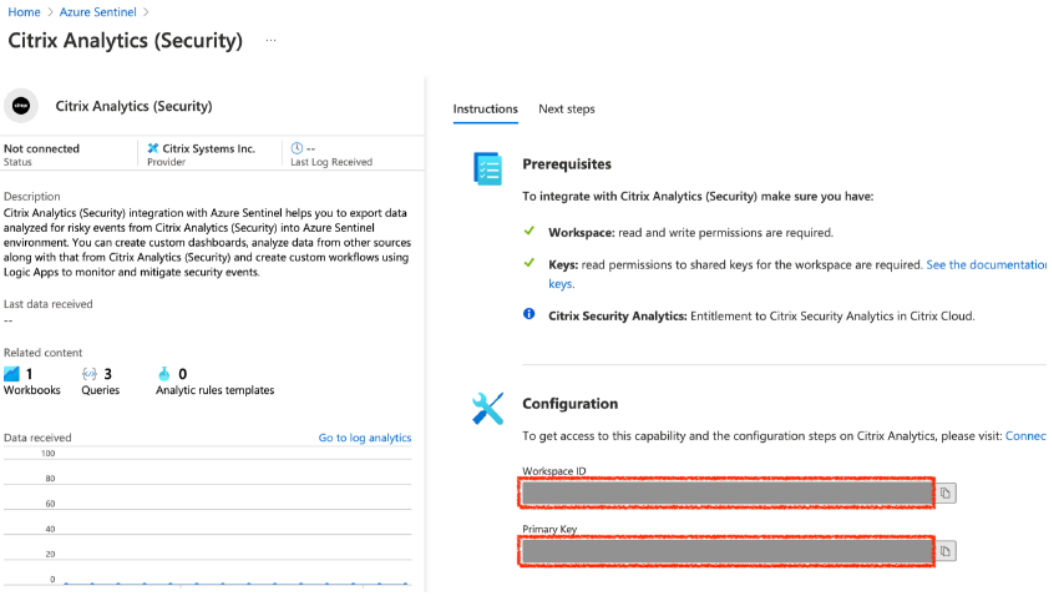
   b) Dans le menu principal, sélectionnez **Connecteurs de données** pour ouvrir la galerie de connecteurs de données.

   c) Recherchez **Citrix Analytics (sécurité)**.

   d) Sélectionnez **Citrix Analytics (sécurité)** et sélectionnez **Ouvrir la page du connecteur**.



   e) Sur la page **Citrix Analytics (sécurité)**, copiez l'**ID de l'espace** de travail et la **clé primaire**. Vous devez entrer ces informations dans le fichier de configuration Logstash lors des étapes suivantes.



f) Configurez Logstash sur votre machine hôte :

i. Sur votre machine hôte Linux ou Windows, installez Logstash et le plug-in de sortie Microsoft Sentinel pour Logstash.

ii. Sur la machine hôte sur laquelle vous avez installé Logstash, placez les fichiers suivants dans le répertoire spécifié :

Type de machine hôte	Nom du fichier	Chemin du répertoire
Linux	CAS_AzureSentinel_LogStash_Config.conf	Pour les paquets Debian et RPM : `/etc/logstash/conf.d/` Pour les archives .zip et .tar.gz : `{ extract.path } / config`
	kafka.client.truststore.jks	Pour les paquets Debian et RPM : `/etc/logstash/ssl/` Pour les archives .zip et .tar.gz : `{ extract.path } /ssl`
Windows	CAS_AzureSentinel_LogStash_Config.conf	`C:\Logstash-7.xx.x\ config`
	kafka.client.truststore.jks	

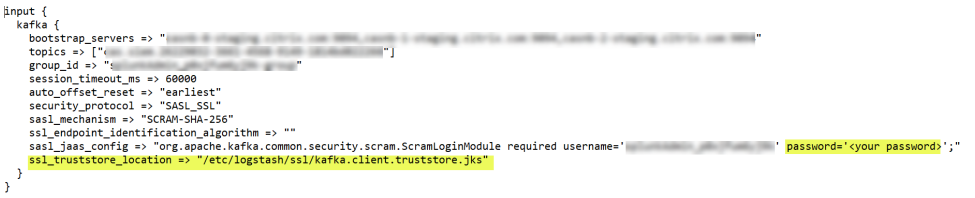
Pour plus d'informations sur la structure de répertoires par défaut des packages d'

installation de Logstash, consultez la documentation de Logstash.

iii. Ouvrez le fichier de configuration Logstash et procédez comme suit :

A. Dans la section de saisie du fichier, saisissez ce qui suit :

- **Mot**de passe : mot de passe du compte que vous avez créé dans Citrix Analytics for Security pour préparer le fichier de configuration.
- **Emplacement du truststore SSL** : emplacement de votre certificat client SSL. Il s'agit de l'emplacement du fichier kafka.client.truststore.jks sur votre machine hôte.



B. Dans la section de sortie du fichier, entrez l'**ID de l'espace** de travail et la **clé primaire** (que vous avez copiés à partir de Microsoft Sentinel) dans la section de sortie du fichier.

```
output {
  if [event_type] == "indicatorSummary" {
    microsoft-logstash-output-azure-loganalytics {
          workspace_id => "<your Azure Log analytics Workspace ID>"
          workspace_key => "<your Shared Key>"
          custom_log_table_name => "CitrixAnalytics_indicatorSummary"
          time_generated_field => "timestamp"
    }
  } else if [event_type] == "indicatorEventDetails" {
    microsoft-logstash-output-azure-loganalytics {
          workspace_id => "<your Azure Log analytics Workspace ID>"
          workspace_key => "<your Shared Key>"
          custom_log_table_name => "CitrixAnalytics_indicatorEventDetails"
          time_generated_field => "timestamp"
    }
  }else if [event_type] == "riskScoreChange" {
    microsoft-logstash-output-azure-loganalytics {
          workspace_id => "<your Azure Log analytics Workspace ID>"
          workspace_key => "<your Shared Key>"
          custom_log_table_name => "CitrixAnalytics_riskScoreChange"
          time_generated_field => "timestamp"
    }
  } else if [event_type] =~ "userProfile.+" {
    microsoft-logstash-output-azure-loganalytics {
          workspace_id => "<your Azure Log analytics Workspace ID>"
          workspace_key => "<your Shared Key>"
          custom_log_table_name => "CitrixAnalytics_userProfile"
          time_generated_field => "timestamp"
    }
  } else {
    microsoft-logstash-output-azure-loganalytics {
          workspace_id => "<your Azure Log analytics Workspace ID>"
          workspace_key => "<your Shared Key>"
          custom_log_table_name => "CitrixAnalytics_misc"
          time_generated_field => "timestamp"
    }
```

iv. Redémarrez la machine hôte Logstash pour envoyer les données traitées depuis Citrix Analytics for Security vers Microsoft Sentinel.

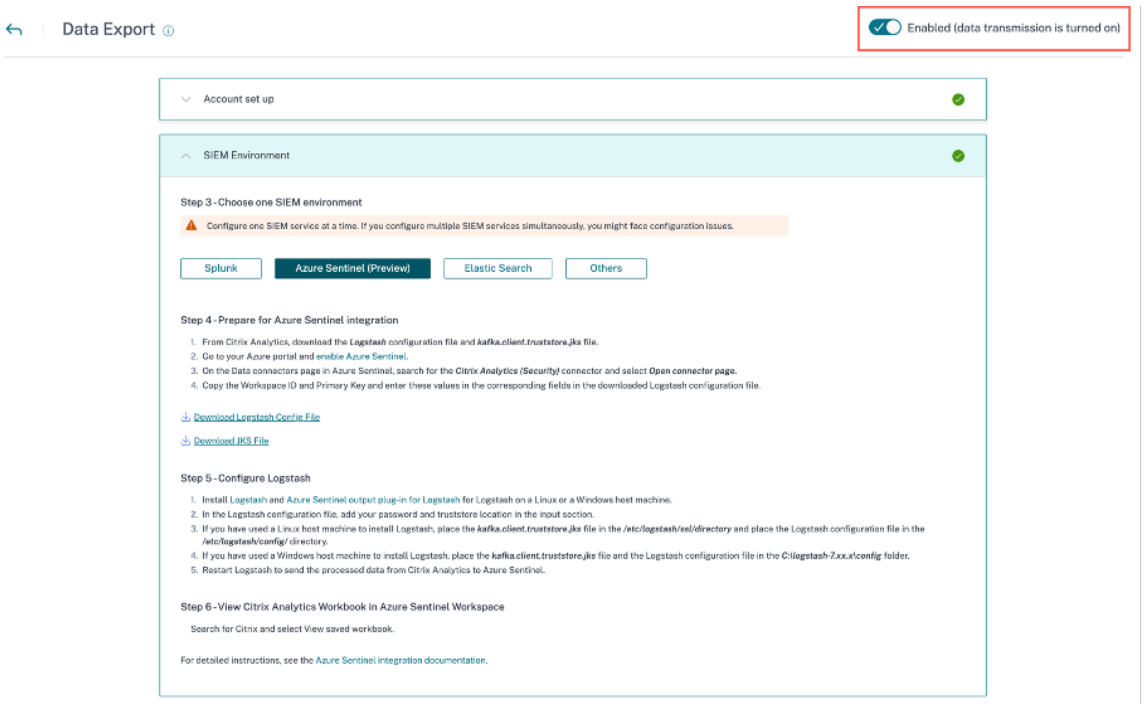
g) Accédez à votre espace de travail Microsoft Sentinel et affichez les données du classeur Citrix Analytics.

Activer ou désactiver la transmission des données

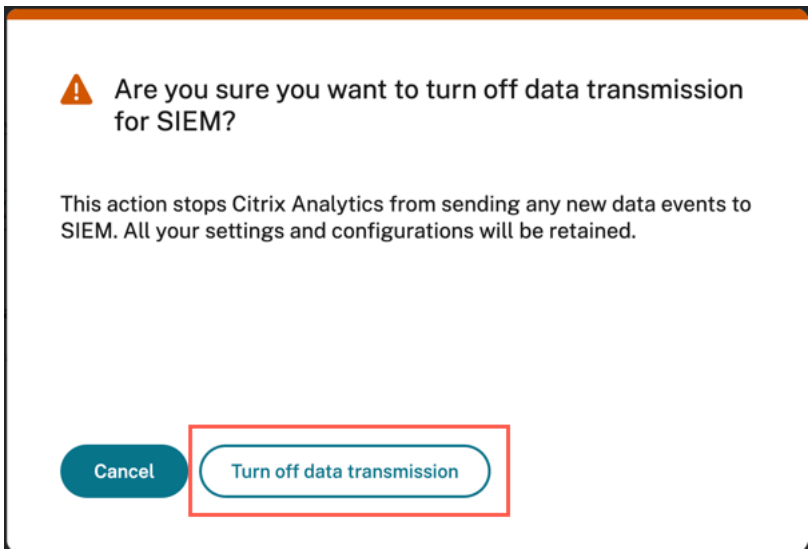
Une fois que Citrix Analytics for Security a préparé le fichier de configuration, la transmission des données est activée pour Microsoft Sentinel.

Pour arrêter de transmettre des données depuis Citrix Analytics for Security, procédez comme suit :

1. Accédez à **Réglages > Exportations de données**.
2. Désactivez le bouton pour désactiver la **transmission de données**. Par défaut, la transmission de données est toujours activée.



Une fenêtre d'avertissement apparaît pour votre confirmation. Cliquez sur le bouton **Désactiver la transmission de données** pour arrêter l'activité de transmission.



Pour réactiver la transmission de données, activez le bouton.

Pour en savoir plus sur l'intégration de Microsoft Sentinel, consultez les liens suivants :

- Intégration de Citrix Analytics à Microsoft Sentinel
- Améliorez votre capacité à détecter les menaces avec Citrix Analytics for Security et Microsoft Sentinel

Classeur Citrix Analytics pour Microsoft Sentinel

December 7, 2023

> **Remarque**
>
> Cette fonctionnalité est disponible dans la Tech Preview.

Cet article décrit le classeur Citrix Analytics disponible dans votre espace de travail Microsoft Sentinel.

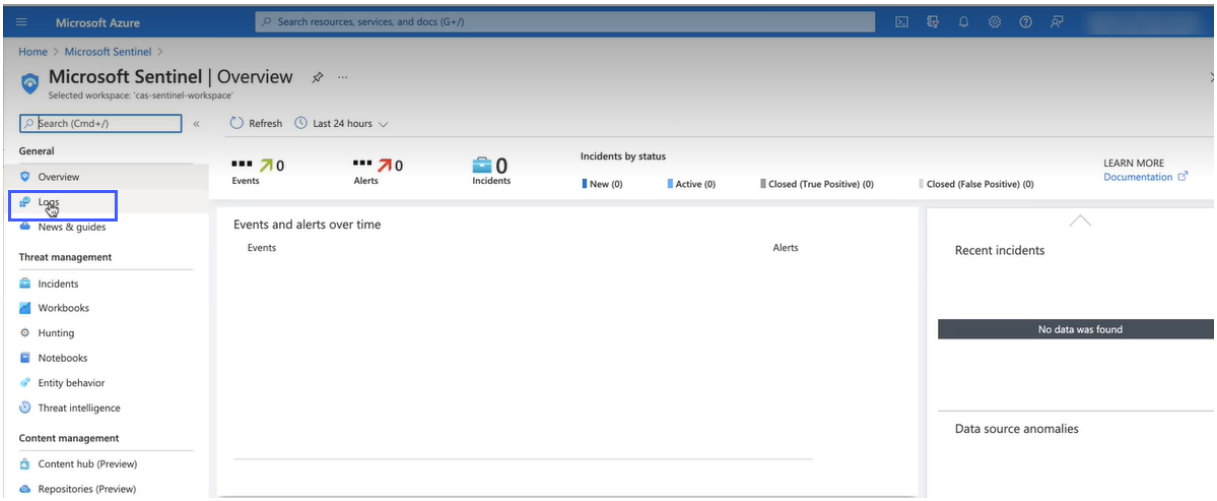
Conditions préalables

Pour utiliser le classeur Citrix Analytics, assurez-vous d'avoir déjà intégré Microsoft Sentinel à Citrix Analytics for Security. Pour plus d'informations, consultez la section Intégration de Microsoft Sentinel.

Afficher les événements Citrix Analytics

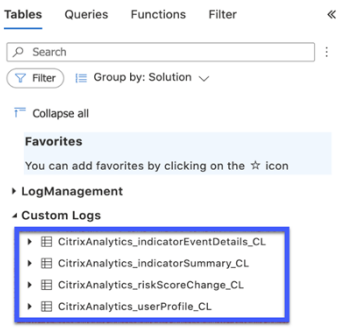
Après avoir intégré Citrix Analytics for Security à Microsoft Sentinel, le connecteur Logstash commence à transférer les événements de Citrix Analytics for Security vers l'espace de travail Microsoft Sentinel. Sur votre **portail Azure**, ouvrez l'espace de travail Microsoft Sentinel que vous avez utilisé pour l'intégration.

Pour vérifier que Microsoft Sentinel reçoit les événements de Citrix Analytics for Security, sélectionnez **Journaux > Journaux personnalisés**.



Dans la section **Journaux personnalisés**, vous pouvez afficher les tables de journaux créées automatiquement pour stocker les événements reçus de Citrix Analytics for Security. Ces tables de journaux servent de source pour les tableaux de bord du classeur Citrix Analytics.

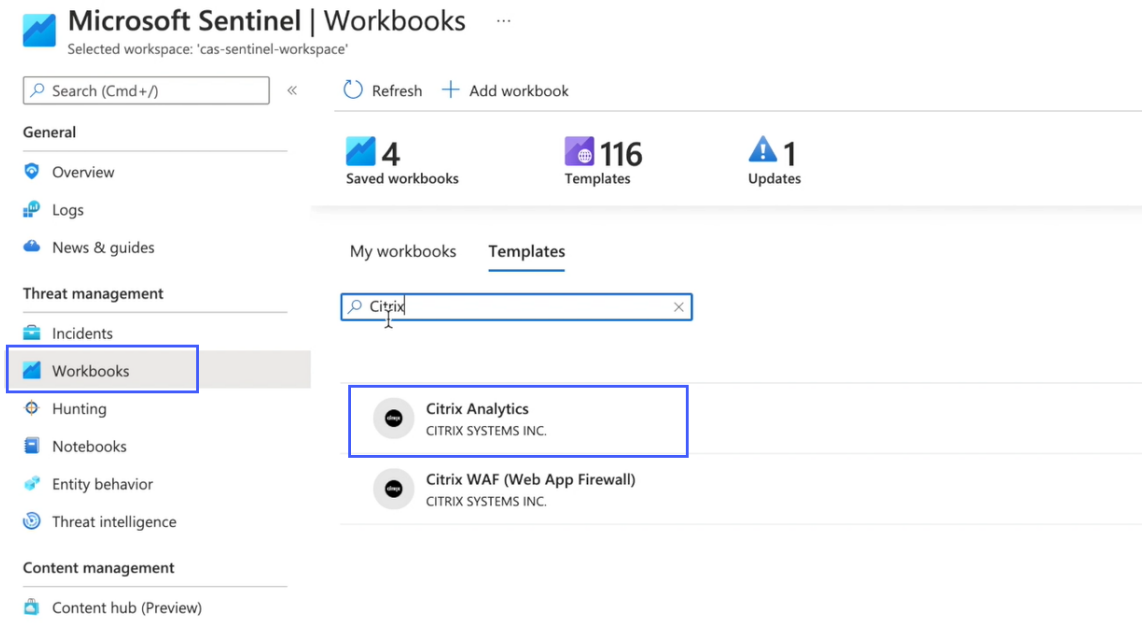
> **Remarque**
>
> Les événements envoyés par Citrix Analytics for Security peuvent prendre quelques heures pour apparaître dans l'espace de travail Microsoft Sentinel. Par conséquent, vous pouvez constater un retard dans la création des tables de journaux pour les événements.



Afficher le classeur Citrix Analytics

Lorsque les tables de journaux sont correctement créées, procédez comme suit :

1. Sélectionnez **Classeurs** et recherchez **Citrix Analytics**. Sélectionnez **Citrix Analytics**.

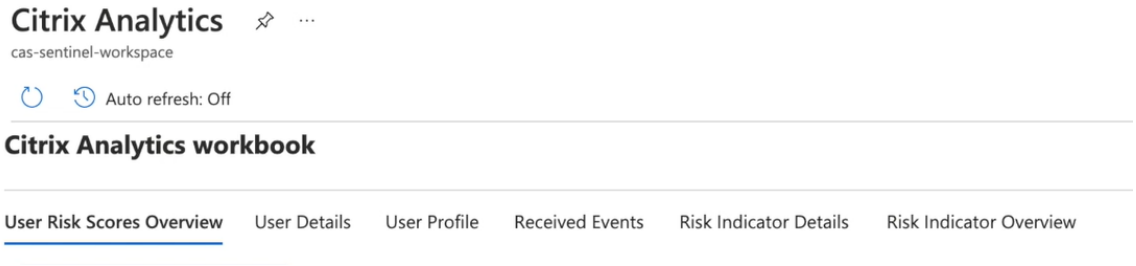


2. Sélectionnez **Afficher le modèle** pour ouvrir le classeur Citrix Analytics.

Dans le classeur Citrix Analytics, vous pouvez afficher les événements utilisateur dans les tableaux de bord suivants :

- **Vue d'ensemble des scores de risque utilisateur** : fournit une vue consolidée des utilisateurs à risque de votre organisation.

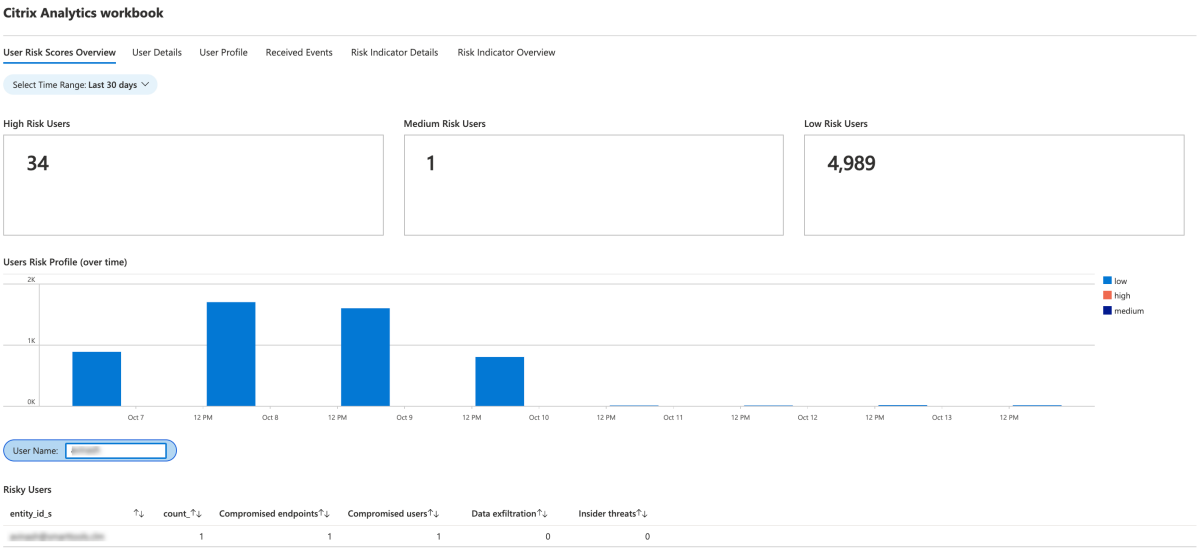
- **Détails de l'utilisateur** : fournit des détails sur les utilisateurs et leur comportement à risque.
- **Profil utilisateur** : fournit les mesures d'événement associées aux utilisateurs.
- **Événements reçus** : fournit les événements reçus de Citrix Analytics for Security.
- **Détails de l'indicateur de risque** : fournit des détails sur les indicateurs de risque intégrés et personnalisés déclenchés par les utilisateurs.
- **Vue d'ensemble des indicateurs de risque** : fournit une vue consolidée des indicateurs de risque déclenchés par les utilisateurs.



Aperçu du score de risque utilisateur

Ce tableau de bord fournit une vue consolidée des utilisateurs à risque de votre organisation. Les utilisateurs sont classés en fonction des niveaux de risque : élevé, moyen et faible. Les niveaux de risque sont basés sur les anomalies des activités de l'utilisateur et, par conséquent, un score de risque est attribué. Pour plus d'informations sur les types d'utilisateurs à risque, consultez le tableau de bord Utilisateurs.

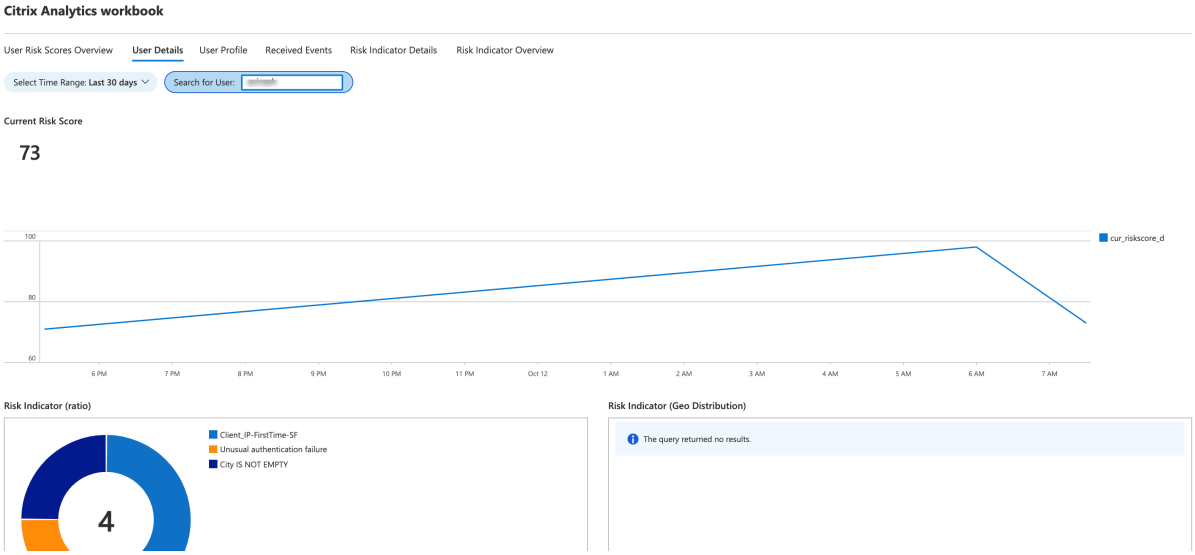
Sélectionnez une période pour voir les utilisateurs à risque de votre organisation.



Détails de l'utilisateur

Ce tableau de bord fournit le score de risque et les indicateurs de risque associés à un utilisateur.

Recherchez un utilisateur et affichez ses activités à risque susceptibles de constituer une menace pour votre organisation. Pour atténuer la menace, vous pouvez prendre les mesures appropriées sur les comptes d'utilisateurs en fonction de la gravité de leur risque.



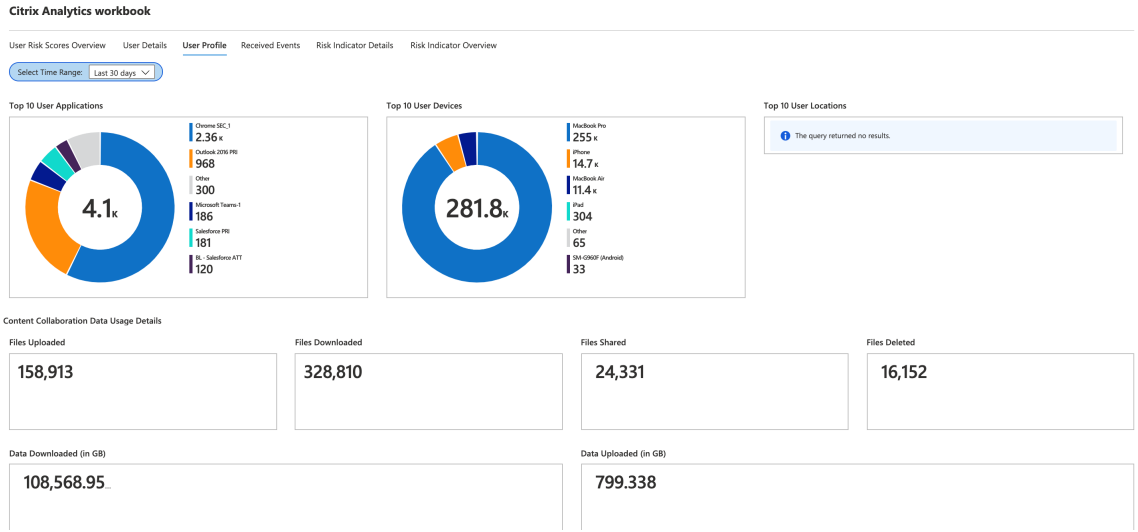
Profil utilisateur

Ce tableau de bord fournit les détails des mesures d'événement associées à vos utilisateurs pour une période donnée. Les mesures fournissent des informations sur les activités des utilisateurs, telles que :

- 10 applications les plus utilisées par les utilisateurs
- Les 10 principaux appareils utilisés par les utilisateurs
- Les 10 principaux emplacements depuis lesquels les utilisateurs se sont connectés

À l'aide des rapports, vous pouvez :

- Identifiez la tendance d'utilisation de vos utilisateurs
- Découvrez les appareils non conformes utilisés pour accéder aux ressources
- Vérifiez tout accès risqué potentiel de la part de vos utilisateurs

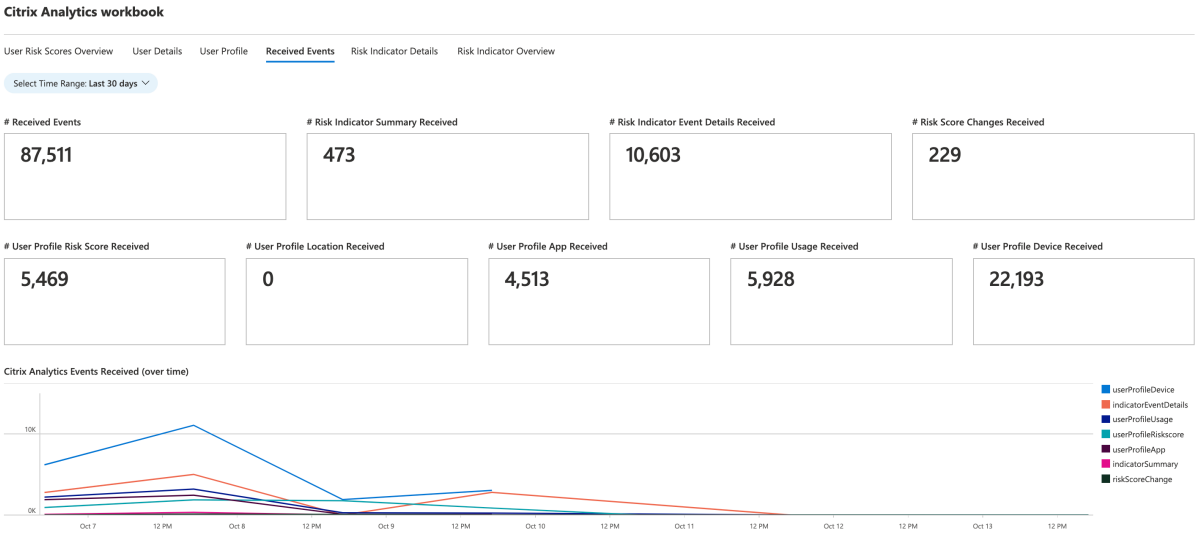


Événements reçus

Pour une période donnée, vous pouvez afficher le nombre total d'événements reçus de Citrix Analytics for Security. Le nombre total d'événements reçus comprend les éléments suivants :

- Résumé des indicateurs de risque : indique les événements associés au résumé des indicateurs de risque utilisateur. Pour plus d'informations sur divers événements récapitulatifs d'indicateurs de risque, voir Schéma des indicateurs de risque.
- Détails de l'événement de l'indicateur de risque : indique les événements associés aux détails des indicateurs de risque utilisateur. Pour plus d'informations sur les différents événements détaillés des indicateurs de risque, voir Schéma des indicateurs de risque.
- Score de risque du profil utilisateur : indique les événements associés au score de risque des utilisateurs. Pour plus d'informations, voir Tableau de bord des utilisateurs
- Changements du score de risque : indique les événements associés au changement du score de risque des utilisateurs. Pour plus d'informations, voir Tableau de bord des utilisateurs
- Emplacements du profil utilisateur : indique les événements associés aux emplacements à partir desquels les utilisateurs se sont connectés.
- Application de profil utilisateur : indique les événements associés aux applications utilisées par les utilisateurs.
- Utilisation du profil utilisateur : indique les événements associés à l'utilisation des données par les utilisateurs.
- Appareil de profil utilisateur : indique les événements associés aux appareils utilisés par les utilisateurs.

En examinant le tableau de bord à intervalles réguliers, vous pouvez vous assurer que les événements se déroulent correctement dans votre espace de travail Microsoft Sentinel. Toute différence dans le nombre total d'événements reçus peut indiquer des problèmes d'intégration avec Citrix Analytics for Security. Vous pouvez effectuer les étapes nécessaires pour déboguer les problèmes.

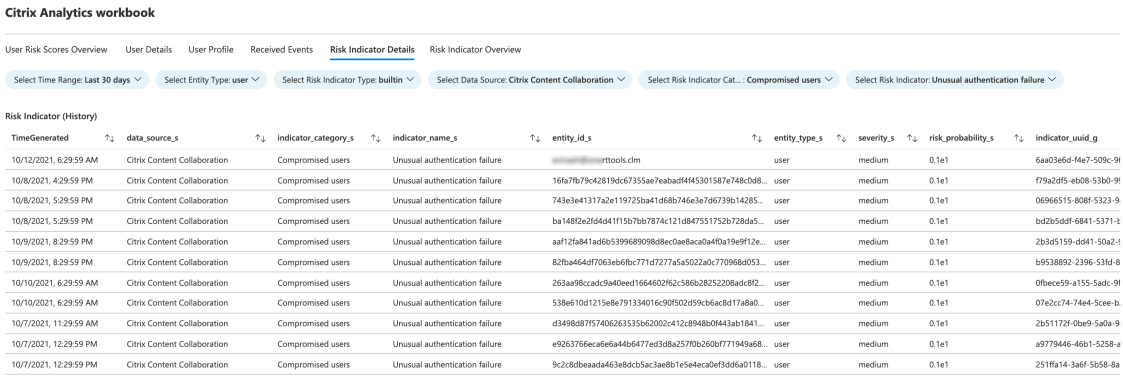


Détails de l'indicateur de risque

Ce tableau de bord fournit les détails des indicateurs de risque déclenchés par vos utilisateurs.

Vous pouvez afficher les détails de l'indicateur de risque en sélectionnant une ou plusieurs catégories :

- Plage de temps : sélectionnez une plage de temps pour afficher les détails des indicateurs de risque déclenchés au cours de la période.
- Type d'entité : sélectionnez un utilisateur pour afficher les détails des indicateurs de risque associés.
- Type d'indicateur de risque : sélectionnez des indicateurs de risque intégrés ou personnalisés pour afficher leurs détails.
- Source de données : sélectionnez une source de données pour afficher les indicateurs de risque associés.
- Catégorie d'indicateur de risque : sélectionnez la catégorie de risque pour afficher les indicateurs de risque associés.
- Indicateur de risque : sélectionnez un indicateur de risque par son nom et affichez ses détails.

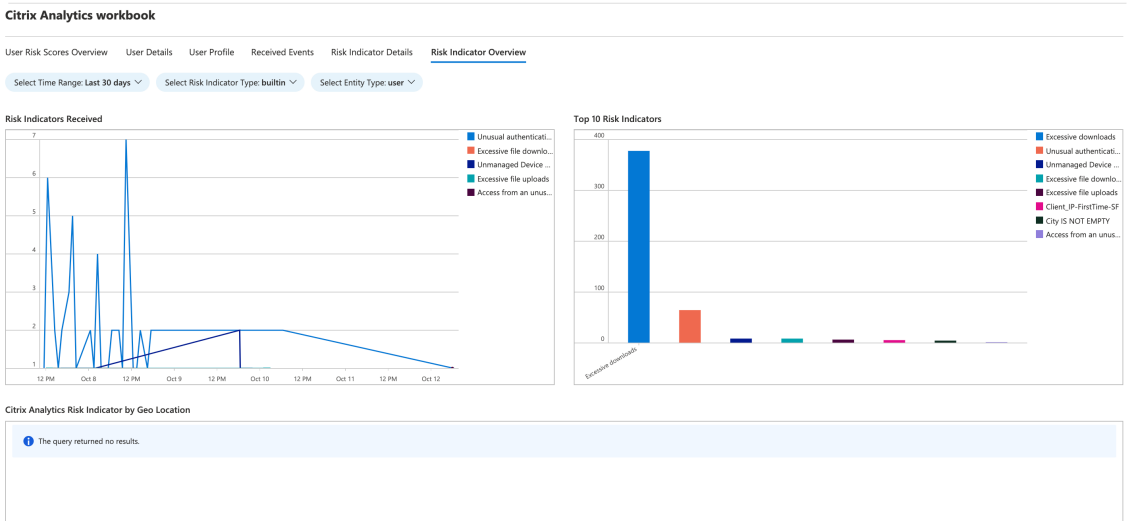


Aperçu des indicateurs de risque

Ce tableau de bord fournit une vue consolidée de tous les indicateurs de risque déclenchés par vos utilisateurs.

Vous pouvez consulter les indicateurs de risque en sélectionnant une ou plusieurs catégories :

- Plage de temps : sélectionnez une période pour afficher les indicateurs de risque qui sont déclenchés au cours de cette période.
- Type d'indicateur de risque : sélectionnez intégré ou personnalisé pour afficher les indicateurs de risque associés.
- Type d'entité : sélectionnez l'un des utilisateurs pour afficher les indicateurs de risque associés.



Conseils de résolution des problèmes liés à l'intégration de Sentinel via Logstash

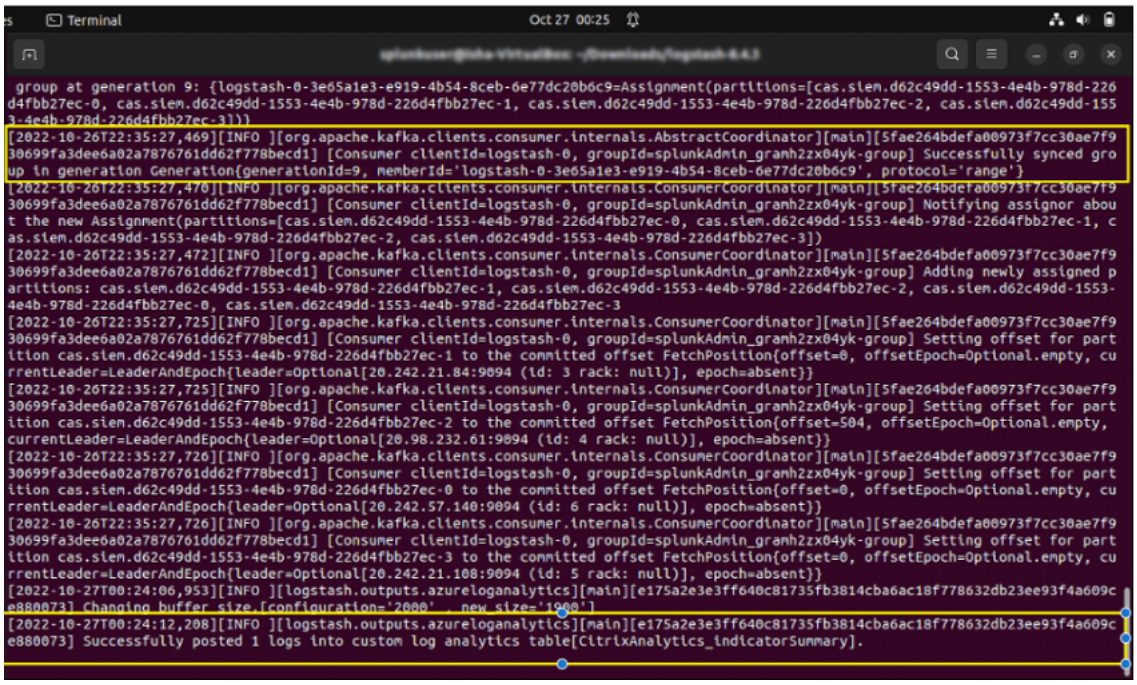
May 2, 2023

Cet article répertorie les conseils à suivre pour résoudre un problème que vous pourriez rencontrer lorsque vous intégrez Microsoft Sentinel à Citrix Analytics à l'aide de Logstash. Pour en savoir plus à ce sujet, consultez l'intégration SIEM à l'aide de Kafka ou d'un connecteur de données basé sur Logstash.

Vérifiez les journaux du serveur Logstash

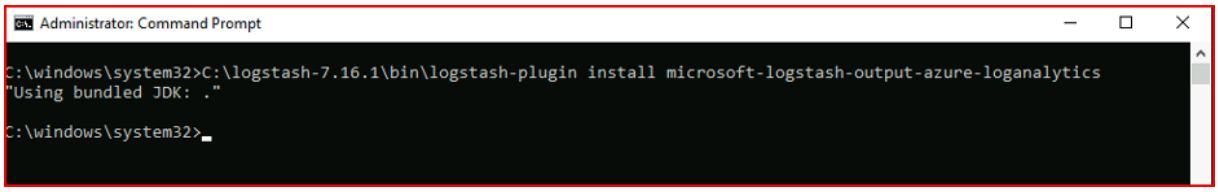
Vous pouvez consulter les journaux du serveur Logstash qui apparaissent dans la fenêtre de votre terminal pour vérifier si les données ont été correctement ingérées dans les tables de journaux personnalisées de votre espace de travail Sentinel.

1. Pour consulter les détails du journal, vous devez télécharger le fichier de configuration Logstash depuis **Paramètres > Exportations de données > onglet Configuration ****** développer l'environnement**SIEM**. Dans**Azure Sentinel (version préliminaire)**, cliquez sur**Télécharger le fichier de configuration Logstash**.
2. Une fois que vous avez démarré le serveur Logstash à l'aide du fichier de configuration, vous pouvez consulter les journaux suivants dans la même fenêtre de terminal qui indiquent une connexion réussie avec l'espace de travail Log Analytics hébergé par Microsoft Azure.

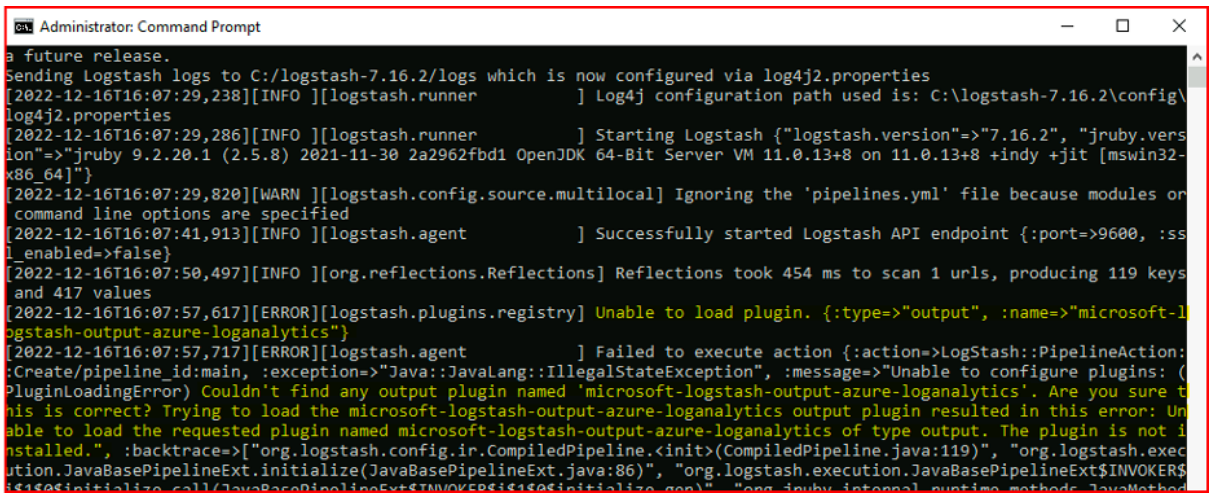


Erreur courante : utilisation du JDK intégré

Lorsque vous essayez d'installer le plug-in Microsoft Log Analytics, une erreur courante est signalée ci-dessous :



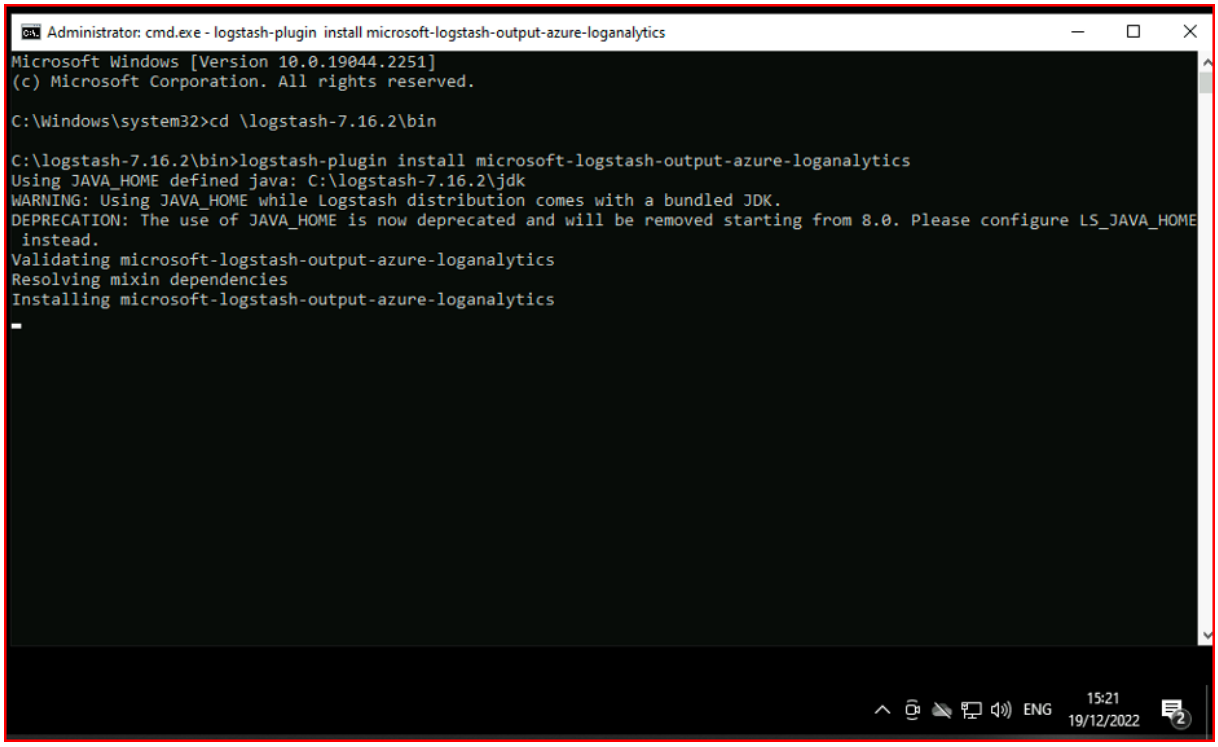
Ensuite, lorsque vous essayez d'exécuter le serveur Logstash, l'erreur suivante peut s'afficher :



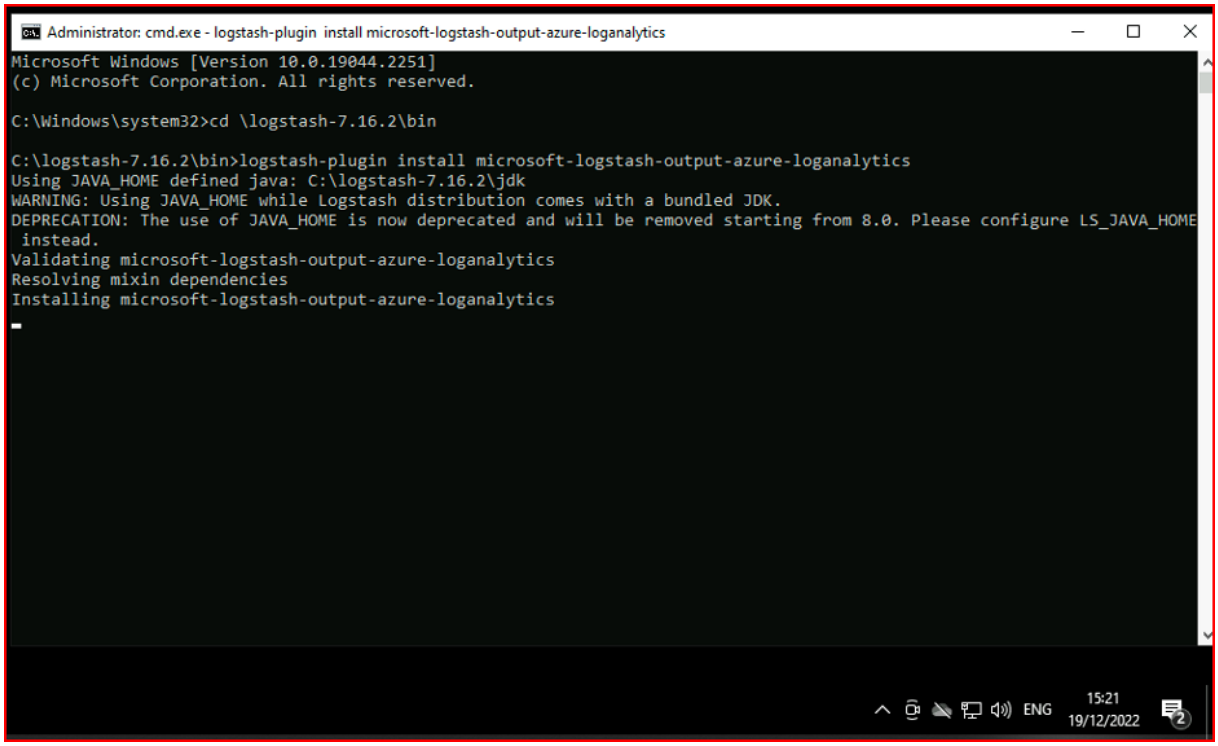
Pour résoudre ce problème, définissez JAVA_HOME sur le JDK intégré :

1. Accédez aux variables d'environnement Windows
2. Créez une nouvelle variable système avec le nom « JAVA_HOME »
3. < path_to_logstash >Ajoutez le chemin vers le JDK Logstash intégré (/Logstash-x.x.x/JDK)

Après avoir suivi les étapes ci-dessus, lorsque vous essayez à nouveau d'installer le plug-in, l'écran suivant s'affiche :

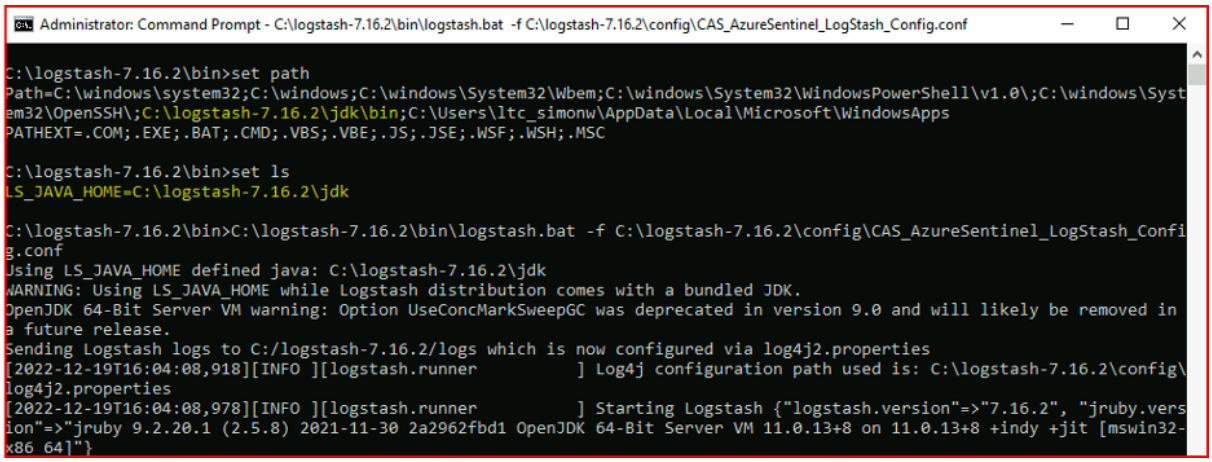


Si vous utilisez LS_JAVA_HOME (car JAVA_HOME est obsolète), vous devez également spécifier l'emplacement du JDK intégré dans la variable système PATH, et ce chemin doit pointer vers le dossier jdk \ bin (contrairement à la variable LS_JAVA_HOME) :



Si vous utilisez LS_JAVA_HOME (car JAVA_HOME est obsolète), vous devez également spécifier l'em-

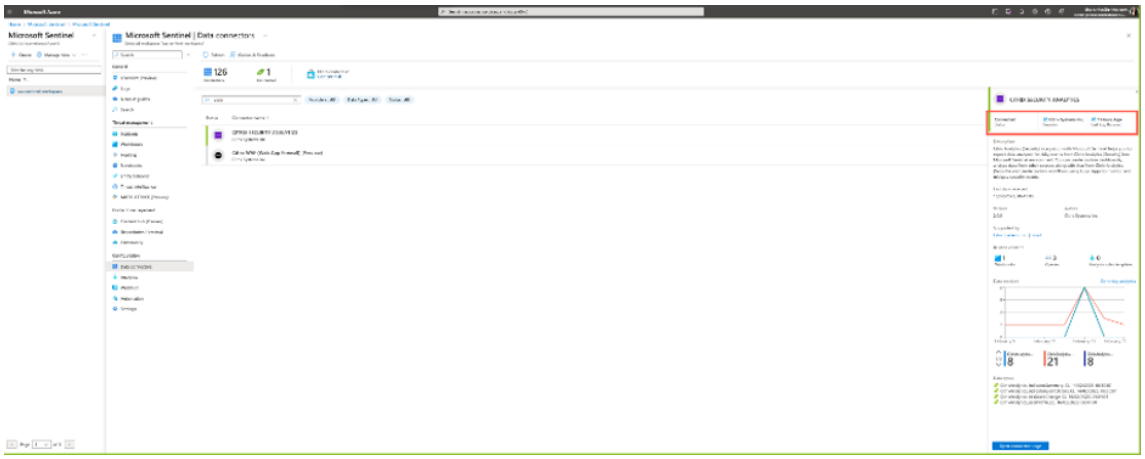
placement du JDK intégré dans la variable système PATH, et ce chemin doit pointer vers le dossier jdk \ bin (contrairement à la variable LS_JAVA_HOME) **:**



Consultez le classeur Microsoft Sentinel

Pour vérifier si les données envoyées par Citrix Analytics ont bien été saisies dans la table de journal personnalisée appropriée dans l'espace de travail Log Analytics (pour en savoir plus sur l'intégration de Microsoft Sentinel à Citrix Analytics, consultez l'intégration de Microsoft Sentinel) :

1. **Accédez au**portail Azure > Microsoft Sentinel > Select appropriate_workspace > Connecteurs de données > sélectionnez et cliquez sur Citrix** Security Analytics.**
2. Consultez la barre supérieure pour vérifier l'état de la connectivité.

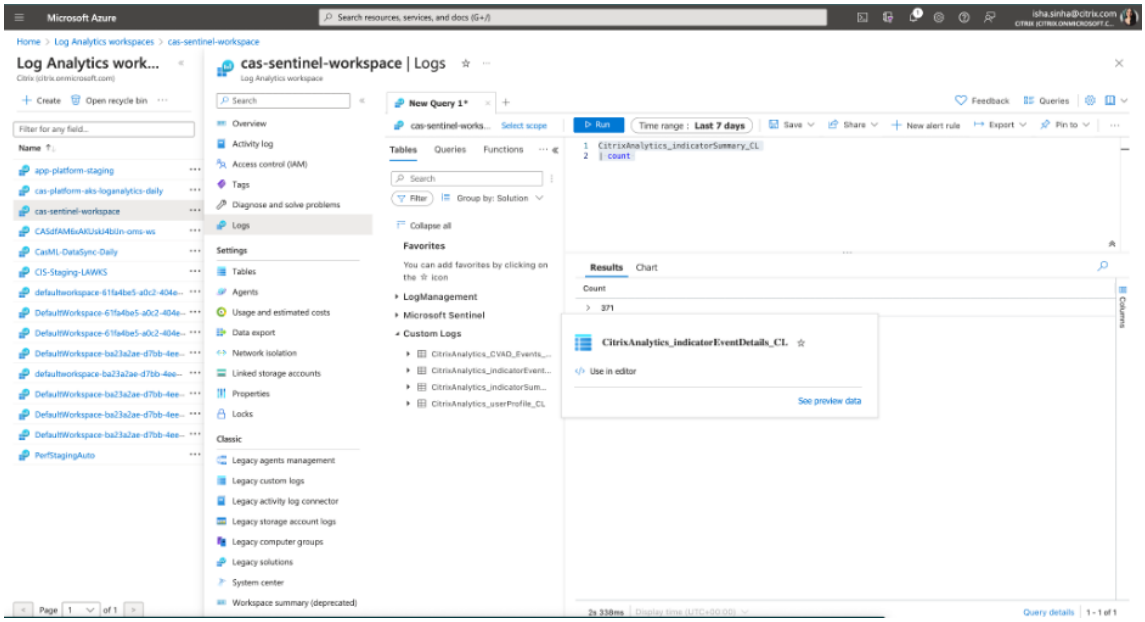


3. Dans les classeurs, vous pouvez utiliser des filtres intuitifs pour approfondir les données afin d'obtenir des informations sur les indicateurs de risque. Pour obtenir les informations, accédez au **portail Azure > Microsoft Sentinel > Connecteurs de données > CITRIX SECURITY ANALYTICS**Classeurs.

Vérifiez les journaux de l'espace de travail Log Analytics avec KQL

Vous pouvez également vérifier si les données correctes ont été transmises à votre espace de travail LogAnalytics en exécutant des requêtes KQL sur les tables de journaux personnalisées respectives.

1. Accédez au **portail Azure > Espaces de travail Log Analytics** et recherchez l'espace de travail approprié.
2. Dans le panneau de gauche, sélectionnez **Journaux** et recherchez le tableau d'analyse des journaux personnalisé sous l'onglet **Tableaux** .
3. Sélectionnez le tableau d'analyse des journaux personnalisé et cliquez sur **Utiliser dans l'éditeur**. (Pour obtenir des conseils sur les requêtes KQL dans l'espace de travail Log Analytics, consultez le didacticiel Log Analytics).
4. Cliquez sur **Exécuter**.



Intégration Elasticsearch

November 16, 2023

> **Remarque**
>
> Contactez CAS-PM-Ext@cloud.com pour demander de l'aide concernant l'intégration d'Elasticsearch, l'exportation de données vers Elasticsearch ou pour nous faire part de vos commentaires.

Intégrez Citrix Analytics for Security à Elasticsearch à l'aide du moteur Logstash. Cette intégration vous permet d'exporter et de corréler les données des utilisateurs de votre environnement informatique Citrix vers Elasticsearch et d'obtenir des informations plus approfondies sur le niveau de sécurité de votre organisation. Vous pouvez également utiliser Elasticsearch avec les services de visualisation et les SIEM tels que Kibana et LogRhythm respectivement.

Pour plus d'informations sur les avantages de l'intégration et le type de données traitées qui sont envoyées à votre SIEM, voir Intégration des informations de sécurité et de la gestion des événements.

Conditions préalables

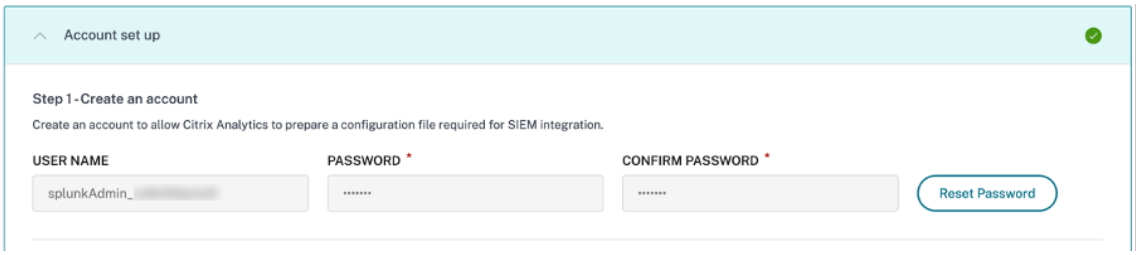
- Activez le traitement des données pour au moins une source de données. Il aide Citrix Analytics for Security à démarrer le processus d'intégration Elasticsearch.

- Assurez-vous que le point de terminaison suivant figure dans la liste d'autorisation de votre réseau.

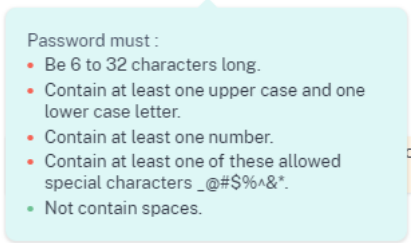
Point de terminaison	Région des États-Unis	Région de l'Union européenne	Région Asie-Pacifique Sud
Brokers Kafka	casnb-0.citrix.com:9094 casnb-1.citrix.com:9094 casnb-2.citrix.com:9094 casnb-3.citrix.com:9094	casnb-eu-0.citrix.com:9094 casnb-eu-1.citrix.com:9094 casnb-eu-2.citrix.com:9094	casnb-aps-0.citrix.com:9094 casnb-aps-1.citrix.com:9094 casnb-aps-2.citrix.com:9094

Intégration à Elasticsearch

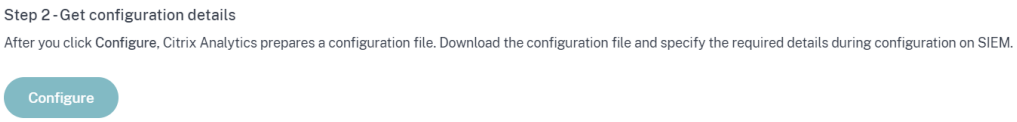
1. Accédez à **Réglages > Exportations de données**.
2. Dans la section **Configuration du compte**, créez un compte en spécifiant le nom d'utilisateur et le mot de passe. Ce compte est utilisé pour préparer un fichier de configuration, qui est nécessaire à l'intégration.



3. Assurez-vous que le mot de passe répond aux conditions suivantes :



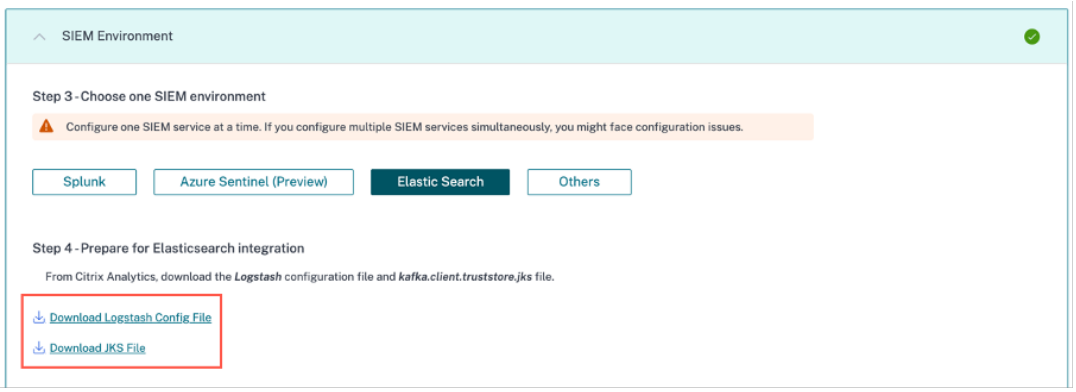
4. Cliquez sur **Configurer** pour générer le fichier de configuration Logstash.



5. Sélectionnez l'onglet **Elastic Search** dans la section Environnement SIEM pour télécharger les fichiers de configuration :

   - **Fichier de configuration Logstash** : contient les données de configuration (sections d'entrée, de filtre et de sortie) pour l'envoi d'événements de Citrix Analytics for Security à Elasticsearch à l'aide du moteur de collecte de données Logstash. Pour plus d'informations sur la structure du fichier de configuration Logstash, consultez la documentation Logstash .
   - **Fichier JKS** : contient les certificats nécessaires à la connexion SSL.

     > **Remarque**
     >
     > Ces fichiers contiennent des informations sensibles. Conservez-les dans un endroit sûr et sécurisé.



6. Configurez Logstash :

   a) Sur votre machine hôte Linux ou Windows, installez Logstash. Vous pouvez également utiliser votre instance Logstash existante.

   b) Sur la machine hôte sur laquelle vous avez installé Logstash, placez les fichiers suivants dans le répertoire spécifié :

Type de machine hôte	Nom du fichier	Chemin du répertoire
Linux	CAS_Elasticsearch_LogStash_Config.conf	Pour les paquets Debian et RPM : `/etc/logstash/conf.d/`

Type de machine hôte	Nom du fichier	Chemin du répertoire
Windows	CAS_Elasticsearch_LogStash_Config.conf kafka.client.truststore.jks	Pour les archives .zip et .tar.gz : `{ extract.path } / config` Pour les paquets Debian et RPM : `/etc/logstash/ssl/` Pour les archives .zip et .tar.gz : `{ extract.path } /ssl` `C:\Logstash-7.xx.x\config`

Pour plus d'informations sur la structure de répertoire par défaut des packages d'installation Logstash, consultez la documentation Logstash .

c) Ouvrez le fichier de configuration Logstash et procédez comme suit :

i. Dans la section de saisie du fichier, saisissez les informations suivantes :

- **Mot**de passe : mot de passe du compte que vous avez créé dans Citrix Analytics for Security pour préparer le fichier de configuration.
- **Emplacement du truststore SSL** : emplacement de votre certificat client SSL. Il s'agit de l'emplacement du fichier kafka.client.truststore.jks sur votre machine hôte.

```
input {
  kafka {
    bootstrap_servers => "
    topics => [
    group_id =>
    session_timeout_ms => 60000
    auto_offset_reset => "earliest"
    security_protocol => "SASL_SSL"
    sasl_mechanism => "SCRAM-SHA-256"
    ssl_endpoint_identification_algorithm => ""
    sasl_jaas_config => "org.apache.kafka.common.security.scram.ScramLoginModule required username='
    ssl_truststore_location => "/etc/logstash/ssl/kafka.client.truststore.jks"
  }
```

ii. Dans la section de sortie du fichier, saisissez l'adresse de votre machine hôte ou du cluster sur lequel Elasticsearch est exécuté.

```
}
output {
  elasticsearch {
    hosts => ["<your logstash host : port>"]
    index => "citrixanalytics-%{+YYYY.MM.dd}"
  }
}
```


d) Redémarrez votre machine hôte pour envoyer les données traitées de Citrix Analytics for Security à Elasticsearch.

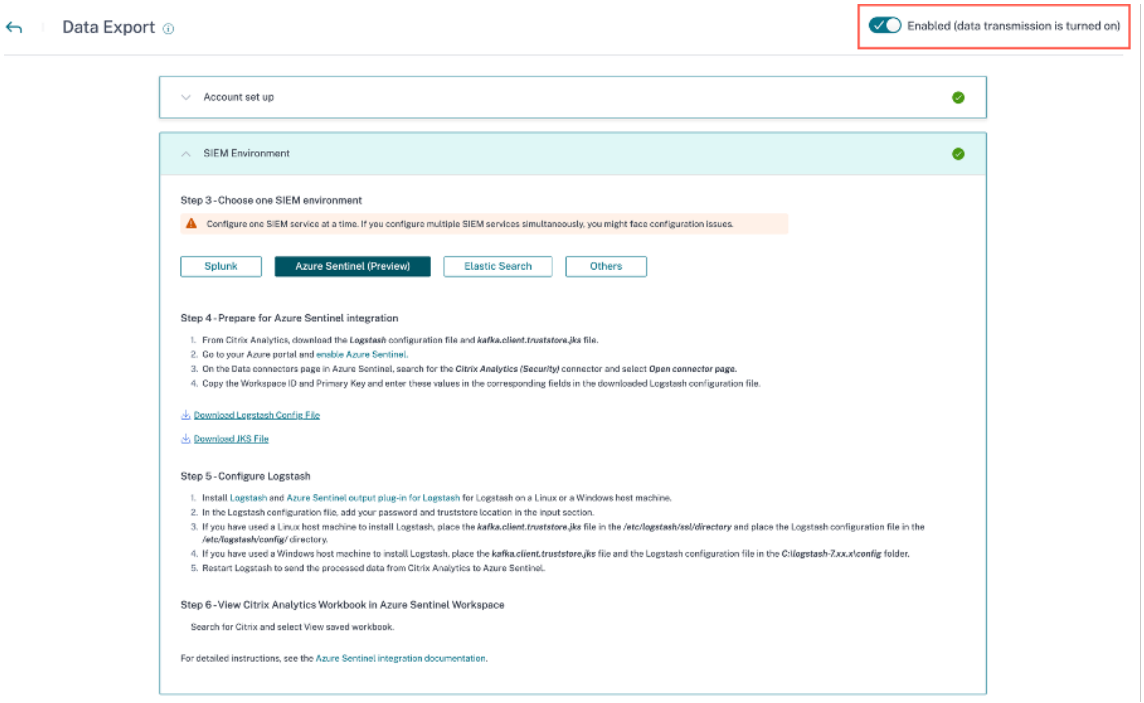
Une fois la configuration terminée, vérifiez que vous pouvez afficher les données Citrix Analytics dans votre Elasticsearch.

Activer ou désactiver la transmission des données

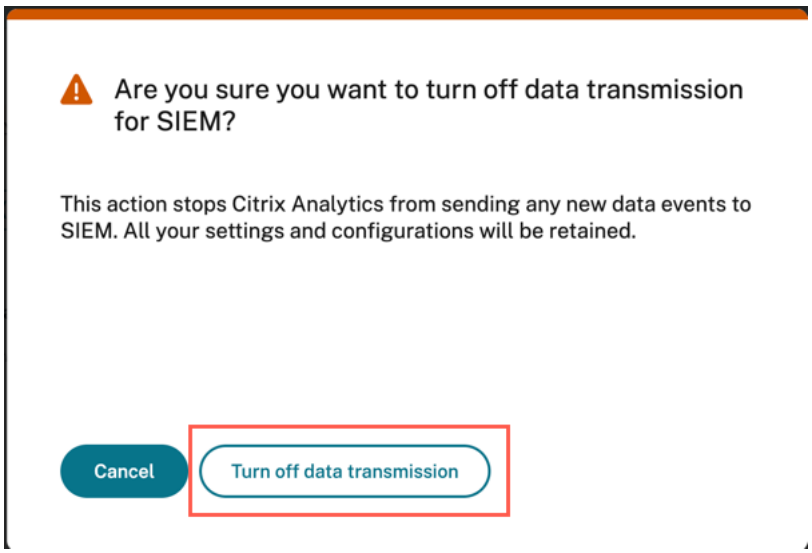
Une fois que Citrix Analytics for Security a préparé le fichier de configuration, la transmission des données est activée pour Elasticsearch.

Pour arrêter de transmettre des données depuis Citrix Analytics for Security, procédez comme suit :

1. Accédez à **Réglages > Exportations de données**.
2. Désactivez le bouton pour désactiver la transmission de données. Par défaut, la **transmission de données** est toujours activée.



Une fenêtre d'avertissement apparaît pour votre confirmation. Cliquez sur le bouton **Désactiver la transmission de données** pour arrêter l'activité de transmission.



Pour réactiver la transmission de données, activez le bouton.

Intégration SIEM à l'aide d'un connecteur de données basé sur Kafka ou Logstash

November 16, 2023

L'intégration de Citrix Analytics for Security SIEM vous permet d'exporter et de corréler les données des utilisateurs depuis Citrix Analytics vers votre environnement SIEM et d'obtenir des informations plus détaillées sur le niveau de sécurité de votre entreprise.

Pour plus d'informations sur les avantages de l'intégration et le type d'événements de données (informations sur les risques et événements liés aux sources de données) envoyés à votre SIEM, consultez la section Intégration des informations de sécurité et de la gestion des événements.

Vous pouvez intégrer Citrix Analytics for Security à vos solutions SIEM via les deux mécanismes suivants (pris en charge par votre déploiement SIEM et informatique) :

1. Connectez-vous via des points de terminaison Kafka
2. Connectez-vous via Logstash Data Broker avec une ingestion basée sur Kafka

Conditions préalables

- Activez le traitement des données pour au moins une source de données. Il aide Citrix Analytics for Security à commencer l'intégration avec votre outil SIEM.

- Assurez-vous que le point de terminaison suivant figure dans la liste d'autorisation 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`

Intégration à un service SIEM à l'aide de Kafka

Kafka est un logiciel open source utilisé pour le streaming de données en temps réel. À l'aide de Kafka, vous pouvez analyser les données en temps réel pour obtenir des informations plus rapidement. La plupart du temps, les grandes organisations qui gèrent des données adéquates utilisent Kafka.

Northbound Kafka est une couche intermédiaire interne qui permet à Citrix Analytics de partager des flux de données en temps réel avec les clients SIEM via des points de terminaison Kafka. Si votre SIEM prend en charge les points de terminaison Kafka, utilisez les paramètres fournis dans le fichier de configuration Logstash et les détails du certificat dans le fichier JKS ou le fichier PEM pour intégrer votre SIEM à Citrix Analytics for Security.

Les paramètres suivants sont nécessaires pour intégrer Kafka :

Nom de l'attribut	Description	Exemple de données de configuration
Nom d'utilisateur	Nom d'utilisateur fourni par Kafka.	`'sasl.username': cas_siem_user_name,`
Hôte	Nom d'hôte du serveur Kafka auquel vous souhaitez vous connecter.	`'bootstrap.servers': cas_siem_host,`
Nom du sujet/ID client	ID client attribué à chaque locataire.	`'client.id': cas_siem_topic,`

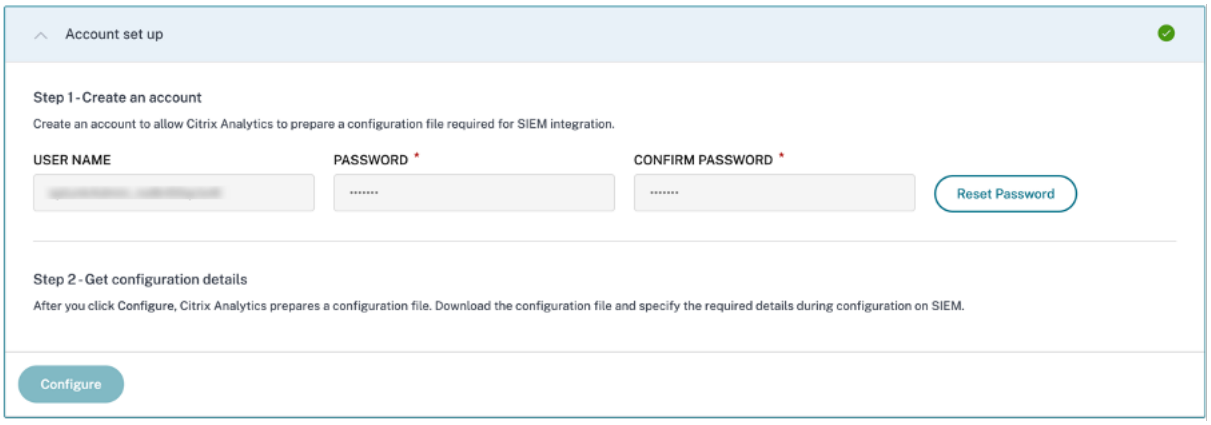
Nom de l'attribut	Description	Exemple de données de configuration
Nom/ID du groupe	Nom du groupe dont vous avez besoin pour lire les messages partagés par les consommateurs.	`'group.id': cas_siem_group_id,`
Protocole de sécurité	Nom du protocole de sécurité.	`'security.protocol': 'SASL_SSL',`
Mécanismes SASL	Mécanisme d'authentification généralement utilisé pour le chiffrement afin de mettre en œuvre une authentification sécurisée.	`'sasl.mechanisms': 'SCRAM-SHA-256',`
Emplacement du truststore SSL	Emplacement où vous pouvez stocker le fichier de certificat. Le mot de passe du client truststore est facultatif et devrait rester vide.	`'ssl.ca.location': ca_location`
Expiration de session	Délai d'expiration de session utilisé pour détecter les défaillances du client lors de l'utilisation de Kafka.	`'session.timeout.ms': 60000,`
Réinitialisation automatique du décalage	Définit le comportement lors de la consommation de données provenant d'une partition de sujet lorsqu'il n'y a pas de décalage initial. Vous pouvez définir des valeurs telles que « la plus récente », « la plus ancienne » ou « aucune ».	`'auto.offset.reset': 'earliest',`

Voici un exemple de sortie de configuration :

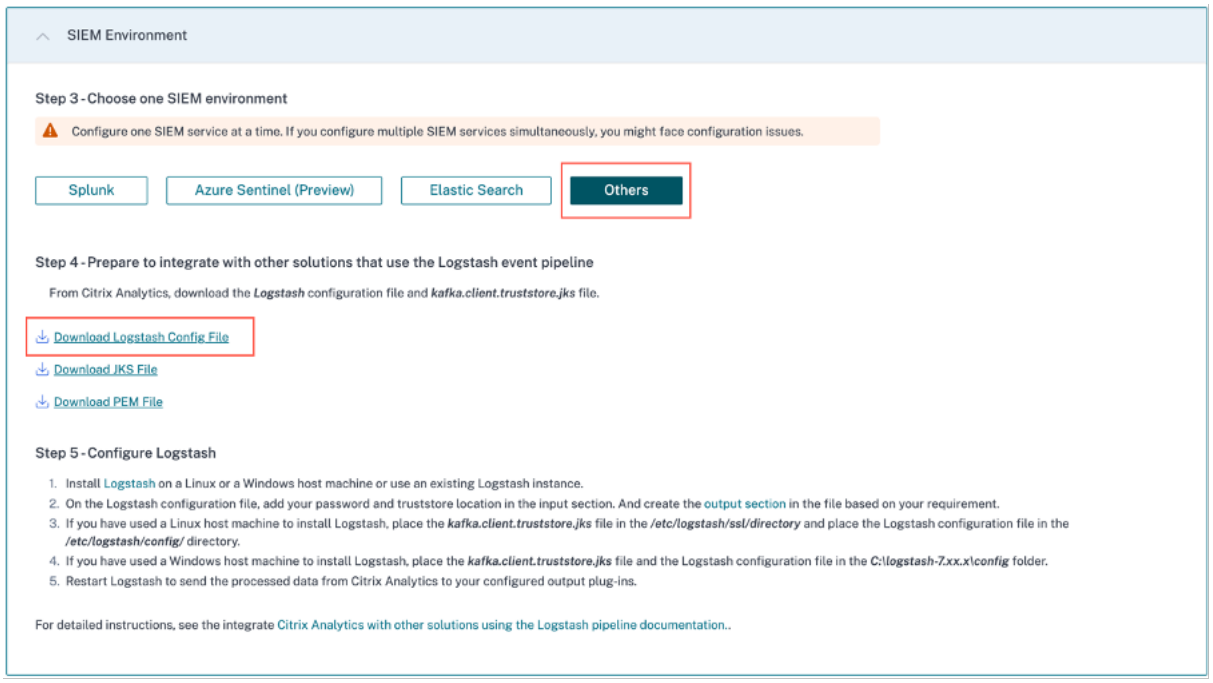
```
{
 'bootstrap.servers': cas_siem_host,
                      'client.id': cas_siem_topic,
                      'group.id': cas_siem_group_id,
                      'session.timeout.ms': 60000,
                      'auto.offset.reset': 'earliest',
                      'security.protocol': 'SASL_SSL',
```



```
                    'sasl.mechanisms': 'SCRAM-SHA-256',
                    'sasl.username': cas_siem_user_name,
                    'sasl.password': self.CLEAR_PASSWORD,
                    'ssl.ca.location': ca_location
                }


<!--NeedCopy-->
```



Les paramètres ci-dessus sont disponibles dans le fichier de configuration de Logstash. Pour télécharger le fichier de configuration, accédez à **Paramètres > Exportations de données > Environnement SIEM** sélectionnez l'onglet **Autres** > cliquez sur **Télécharger le fichier de configuration Logstash**.



Pour comprendre/en savoir plus sur les valeurs de configuration, consultez Configuration.

Flux de données

La communication des données d'authentification s'effectue entre les brokers côté serveur Kafka (Citrix Analytics for Security cloud) et les clients Kafka. Toutes les communications des brokers/clients externes utilisent le protocole de sécurité SASL_SSL activé et ciblent le port 9094 pour l'accès public.

Apache Kafka possède un composant de sécurité qui crypte les données en cours de transport à l'aide du cryptage SSL.
La transmission de données sur le réseau est cryptée et sécurisée lorsque le cryptage est activé et que les certificats SSL sont définis. Seules la première et la dernière machine ont la capacité de déchiffrer les paquets envoyés via SSL.

Authentifications

Deux niveaux d'authentification sont disponibles, comme indiqué ci-dessous :

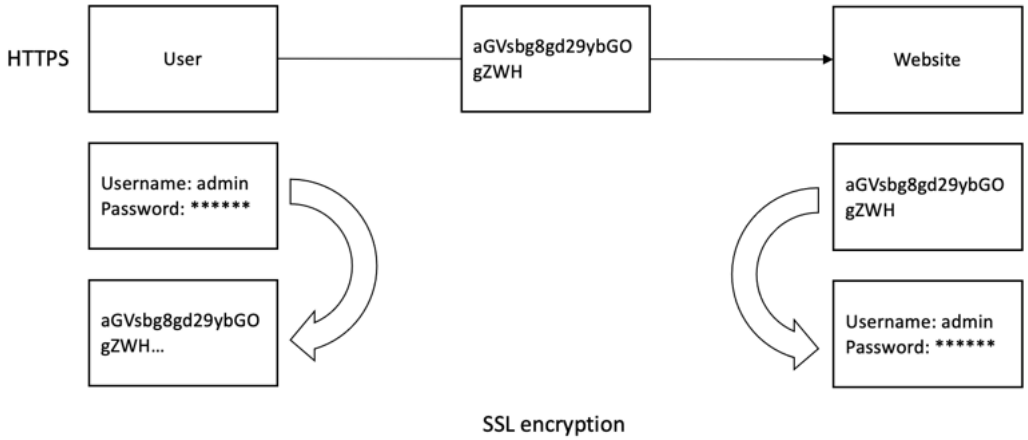
1. TLS/Entre le client et le serveur.
    - Les certificats de serveur (clés publiques) pour l'échange d'authentification TLS entre le client et le serveur.
    - L'authentification basée sur le client ou les authentifications bidirectionnelles ne sont pas prises en charge (lorsque des certificats de clé privée client sont requis).
2. Nom d'utilisateur/mot de passe pour le contrôle d'accès aux sujets/points de terminaison
    - Garantit qu'un client spécifique ne peut lire qu'un sujet spécifique
    - Le SASL/SCRAM est utilisé pour le mécanisme d'authentification par nom d'utilisateur/-mot de passe ainsi que le cryptage TLS pour implémenter une authentification sécurisée.

Chiffrement avec SSL et authentification avec SASL/SSL&SASL/PLAINTEXT

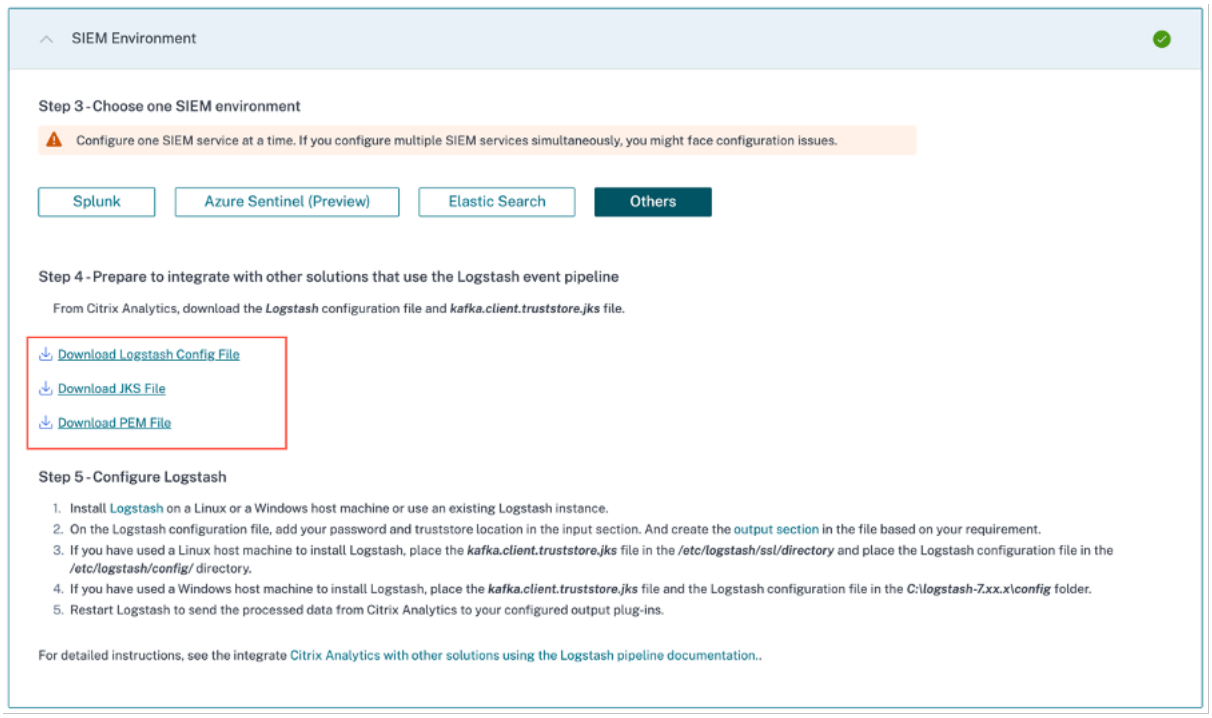
Par défaut, Apache Kafka communique en mode PLAINTEXT, où toutes les données sont envoyées en clair et tous les routeurs peuvent lire le contenu des données. Apache Kafka possède un composant de sécurité qui crypte les données en cours de transport à l'aide du cryptage SSL. Le cryptage étant activé et les certificats SSL soigneusement configurés, les données sont désormais cryptées et transmises en toute sécurité sur le réseau. Avec le cryptage SSL, seules la première et la dernière machine ont la capacité de déchiffrer le paquet envoyé.

Comme le cryptage SSL bidirectionnel est utilisé, la connexion par nom d'utilisateur/mot de passe est sécurisée pour les communications externes.

Le cryptage se fait uniquement en cours de route et les données ne sont toujours pas cryptées sur le disque du broker.



Dans la configuration du client, le fichier JKS et le fichier PEM du client truststore (convertis à partir du fichier jks de truststore) sont requis. Vous pouvez télécharger ces fichiers depuis l'interface graphique de Citrix Analytics for Security, comme illustré dans la capture d'écran suivante :



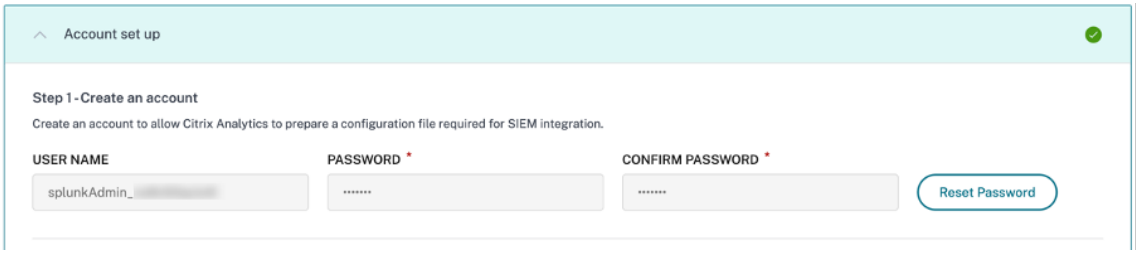
Intégration SIEM à l'aide de Logstash

Si votre SIEM ne prend pas en charge les terminaux Kafka, vous pouvez utiliser le moteur de collecte de **données Logstash** . Vous pouvez envoyer les événements de données depuis Citrix Analytics for Security vers l'un des plug-ins de sortie pris en charge par Logstash.

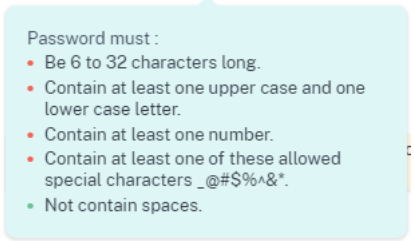
La section suivante décrit les étapes à suivre pour intégrer votre SIEM à Citrix Analytics for Security à l'aide de Logstash.

Intégration à un service SIEM à l'aide de Logstash

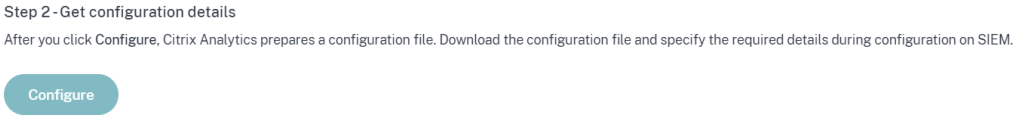
1. Accédez à **Réglages > Exportations de données**.
2. Sur la page de **configuration du compte**, créez un compte en spécifiant le nom d'utilisateur et le mot de passe. Ce compte est utilisé pour préparer un fichier de configuration, qui est nécessaire à l'intégration.



3. Assurez-vous que le mot de passe répond aux conditions suivantes :



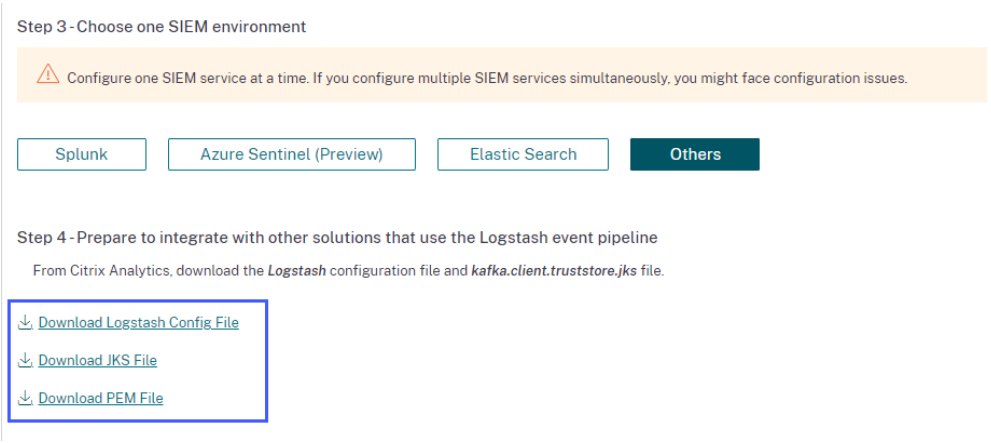
4. Sélectionnez **Configurer** pour générer le fichier de configuration Logstash.



5. Sélectionnez l'onglet **Autres** pour télécharger les fichiers de configuration.

   - **Fichier de configuration Logstash** : Ce fichier contient les données de configuration (sections d'entrée, de filtre et de sortie) pour l'envoi d'événements depuis Citrix Analytics for Security à l'aide du moteur de collecte de données Logstash. Pour plus d'informations sur la structure du fichier de configuration Logstash, consultez la documentation Logstash .
   - **Fichier JKS** : Ce fichier contient les certificats nécessaires à la connexion SSL. Ce fichier est nécessaire lorsque vous intégrez votre SIEM à l'aide de Logstash.
   - **Fichier PEM** : Ce fichier contient les certificats nécessaires à la connexion SSL. Ce fichier est nécessaire lorsque vous intégrez votre SIEM à l'aide de Kafka.

> **Remarque**
>
> Ces fichiers contiennent des informations sensibles. Conservez-les dans un endroit sûr et sécurisé.



6. Configurez Logstash :

   a) Sur votre machine hôte Linux ou Windows, installez Logstash (versions testées pour la compatibilité avec Citrix Analytics for Security : v7.17.7 et v8.5.3). Vous pouvez également utiliser votre instance Logstash existante.

   b) Sur la machine hôte sur laquelle vous avez installé Logstash, placez les fichiers suivants dans le répertoire spécifié :

Type de machine hôte	Nom du fichier	Chemin du répertoire
Linux	CAS_Others_LogStash_Config.config	Pour les paquets Debian et RPM : `/etc/logstash/conf.d/` Pour les archives .zip et .tar.gz : `{ extract.path } /config`
	kafka.client.truststore.jks	Pour les paquets Debian et RPM : `/etc/logstash/ssl/` Pour les archives .zip et .tar.gz : `{ extract.path } /ssl`
Windows	CAS_Others_LogStash_Config.config	`C:\logstash-7.xx.x\config`

Type de machine hôte	Nom du fichier	Chemin du répertoire
	kafka.client.truststore.jks	`C:\logstash-7.xx.x\config`

c) Le fichier de configuration Logstash contient des informations sensibles telles que les informations d'identification Kafka, les identifiants LogAnalytics Workspace et les clés primaires. Il est recommandé de ne pas stocker ces informations d'identification sensibles sous forme de texte brut. Pour sécuriser l'intégration, un magasin de clés Logstash peut être utilisé pour ajouter des clés avec leurs valeurs respectives, qui peuvent à leur tour être référencées à l'aide de noms de clés dans le fichier de configuration. Pour plus d'informations sur le keystore Logstash et sur la manière dont il renforce la sécurité de vos paramètres, consultez Secrets keystorepour les paramètres sécurisés.

d) Ouvrez le fichier de configuration Logstash et procédez comme suit :

Dans la section de saisie du fichier, saisissez les informations suivantes :

- **Mot**de passe : mot de passe du compte que vous avez créé dans Citrix Analytics for Security pour préparer le fichier de configuration.
- **Emplacement du truststore SSL** : emplacement de votre certificat client SSL. Il s'agit de l'emplacement du fichier kafka.client.truststore.jks sur votre machine hôte.

Dans la section de sortie du fichier, saisissez le chemin ou les détails de destination où vous souhaitez envoyer les données. Pour plus d'informations sur les plug-ins de sortie, consultez la documentation Logstash .

L'extrait suivant indique que la sortie est écrite dans un fichier journal local.

```
output {
        file {
        path => "./citrixanalytics-%{+YYYY.MM.dd}.log"
    }
}
```

e) Redémarrez votre machine hôte pour envoyer les données traitées de Citrix Analytics for Security à votre service SIEM.

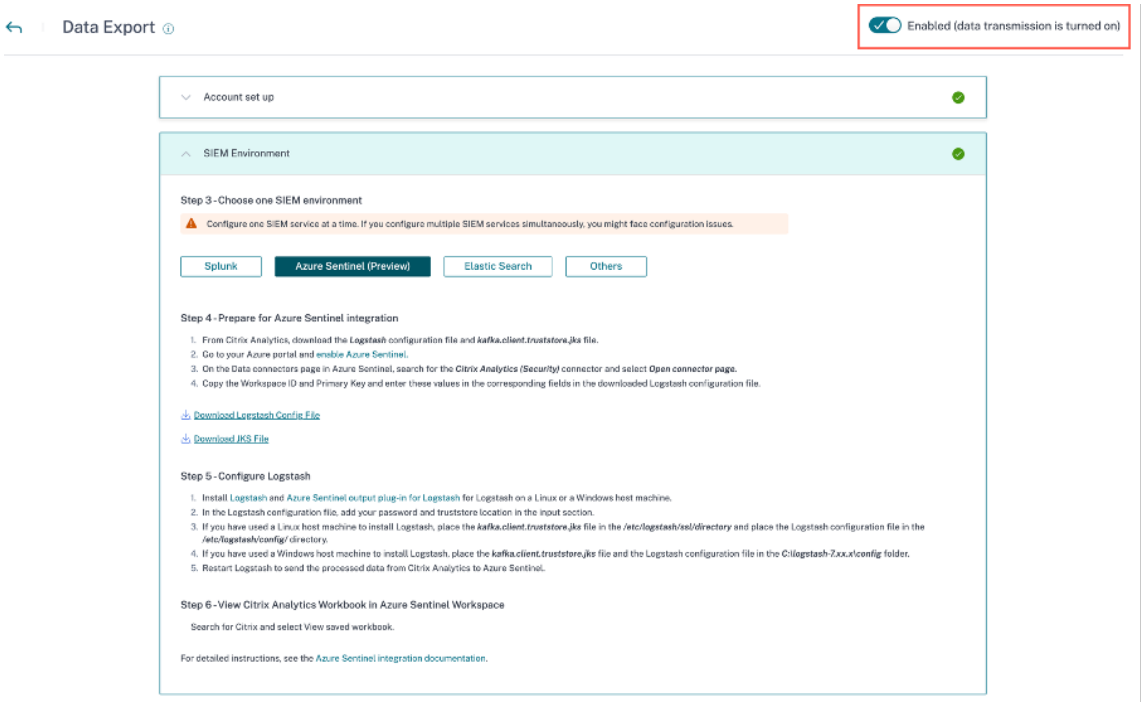
Une fois la configuration terminée, connectez-vous à votre service SIEM et vérifiez les données Citrix Analytics dans votre SIEM.

Activer ou désactiver la transmission des données

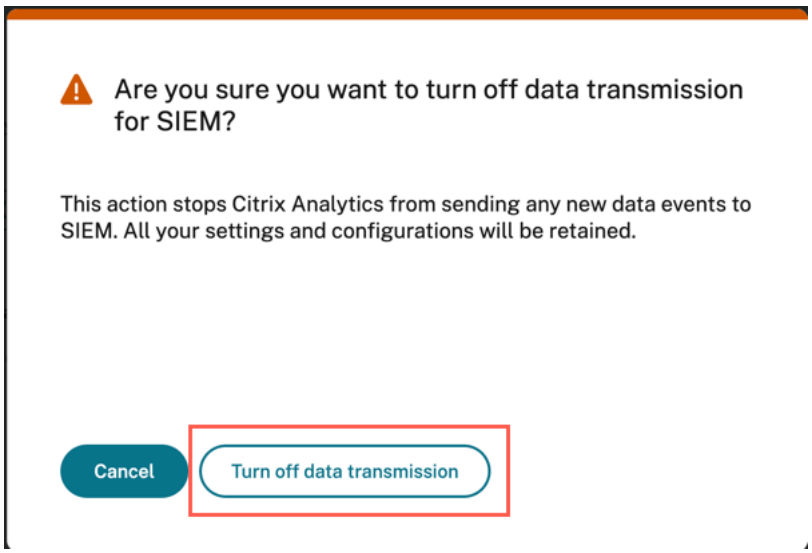
Une fois que Citrix Analytics for Security a préparé le fichier de configuration, la transmission des données est activée pour votre SIEM.

Pour arrêter de transmettre des données depuis Citrix Analytics for Security, procédez comme suit :

1. Accédez à **Réglages > Exportations de données**.
2. Désactivez le bouton pour désactiver la **transmission de données**. Par défaut, la transmission de données est toujours activée.



Une fenêtre d'avertissement apparaît pour votre confirmation. Cliquez sur le bouton **Désactiver la transmission de données** pour arrêter l'activité de transmission.



Pour réactiver la transmission de données, activez le bouton.

> **Remarque**
>
> Contactez CAS-PM-Ext@cloud.com pour demander de l'aide concernant l'intégration de votre SIEM, l'exportation de données vers votre SIEM ou pour nous faire part de vos commentaires.

Format d'exportation de données Citrix Analytics pour SIEM

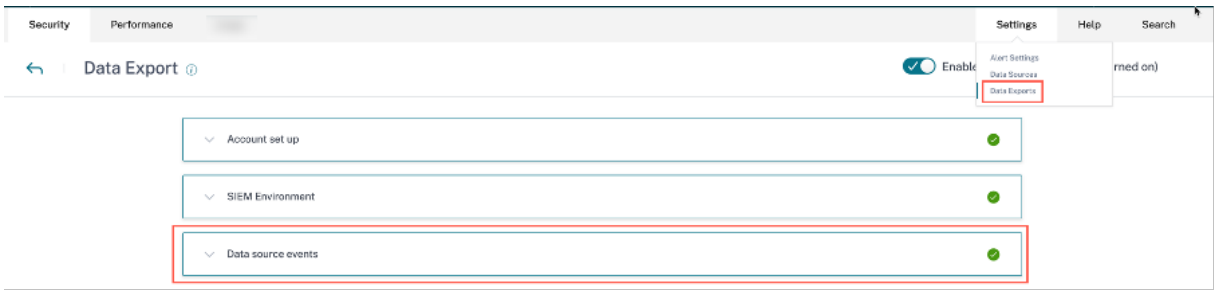
February 9, 2024

Citrix Analytics for Security vous permet d'intégrer vos services SIEM (Security Information and Event Management). Cette intégration permet à Citrix Analytics for Security d'envoyer des données à vos services SIEM et vous aide à mieux comprendre l'état des risques de sécurité de votre entreprise.

Actuellement, vous pouvez intégrer Citrix Analytics for Security aux services SIEM suivants :

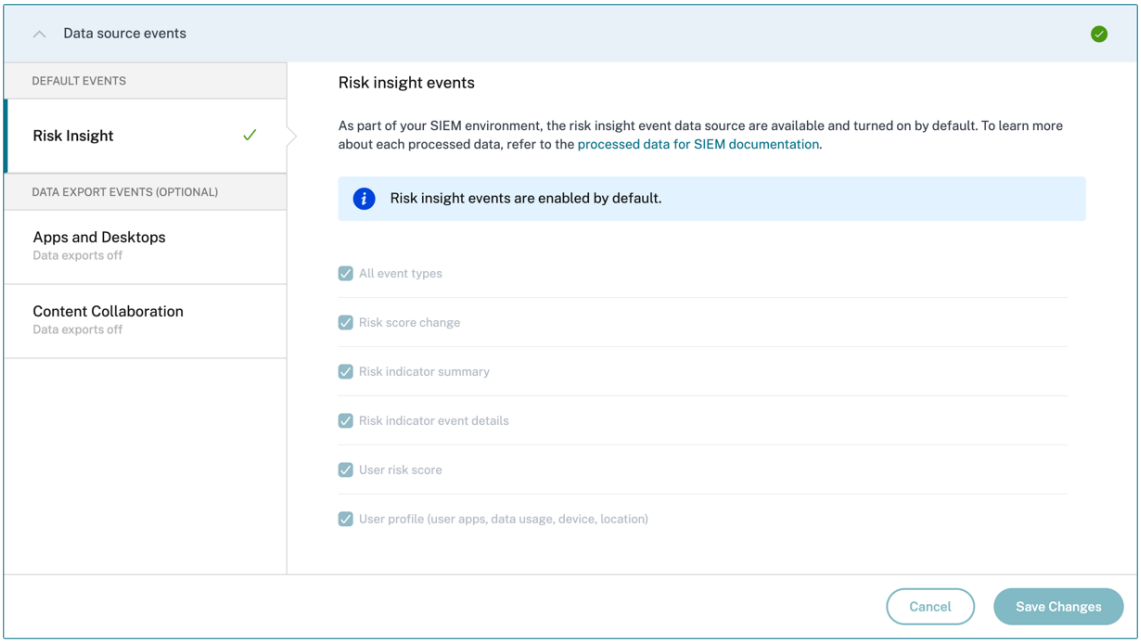
- Splunk
- Sentinelle Microsoft Azure
- Elasticsearch
- Autres SIEM utilisant un connecteur de données basé sur Kafka ou Logstash

L'**option Exportations de données** est désormais disponible dans le monde entier sous **Paramètres**. Pour afficher les événements de la source de données, accédez à **Paramètres > Exportations de données > Événements de la source de données**.



Les données d'analyse des risques envoyées par Citrix Analytics for Security à votre service SIEM sont de deux types :

- Événements d'analyse des risques (exportations par défaut)
- Événements relatifs aux sources de données (exportations facultatives)



Données d'analyse des risques pour le SIEM

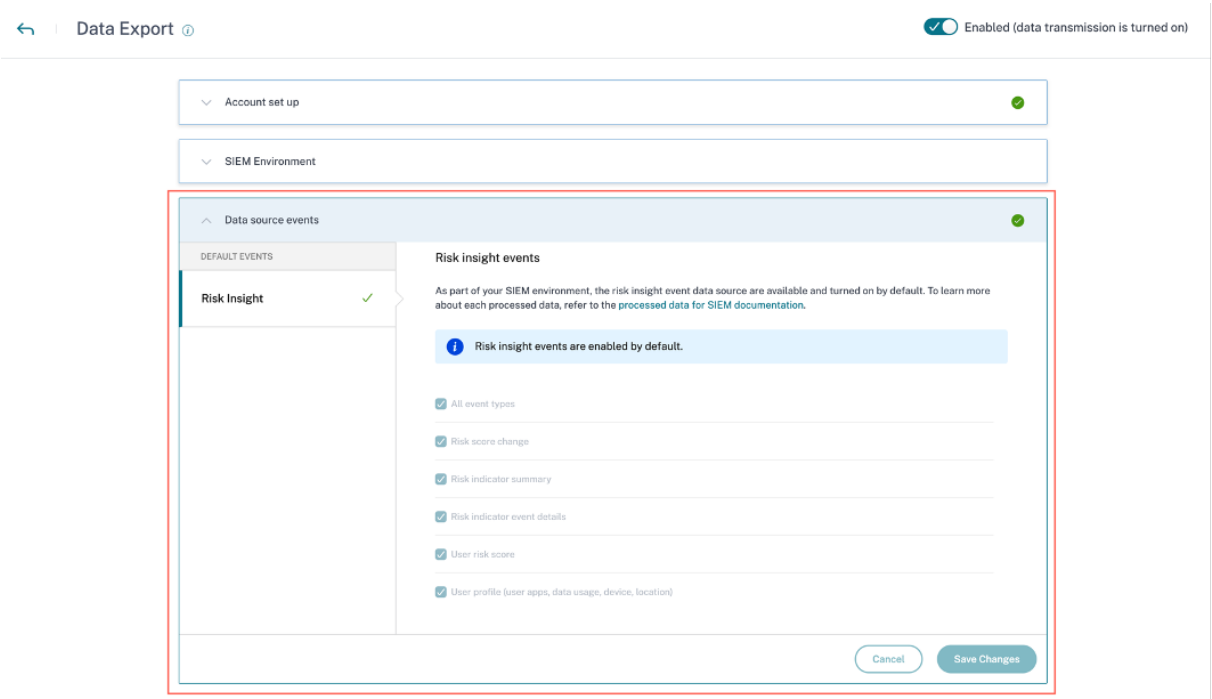
Une fois que vous avez terminé la configuration du compte et la configuration du SIEM, les ensembles de données par défaut (événements liés à l'analyse des risques) commencent à être intégrés à votre déploiement SIEM. Les ensembles de données d'informations sur les risques incluent les événements de score de risque des utilisateurs, les événements de profil utilisateur et les alertes relatives aux indicateurs de risque. Ils sont générés par les algorithmes d'apprentissage automatique de Citrix Analytics et l'analyse du comportement des utilisateurs, en tirant parti des événements utilisateur.

Les ensembles de données d'informations sur les risques d'un utilisateur incluent les éléments suivants :

- **Modification du score de risque** : indique un changement du score de risque de l'utilisateur. Lorsque la modification du score de risque d'un utilisateur est égale ou supérieure à 3 et que cette variation augmente à tout rythme ou baisse de plus de 10 %, les données sont envoyées au service SIEM.
- **Résumé des indicateurs de risque** : détails de l'indicateur de risque déclenché pour un utilisateur.
- **Détails de l'événement indicateur de risque** : événements utilisateur associés à un indicateur de risque. Citrix Analytics envoie un maximum de 1000 détails d'événements pour chaque occurrence d'indicateur de risque à votre service SIEM. Ces événements sont envoyés par ordre chronologique d'occurrence.
- **Événement relatif au score de risque utilisateur** : score de risque actuel d'un utilisateur. Citrix Analytics for Security envoie ces données au service SIEM toutes les 12 heures.
- **Profil utilisateur** : les données du profil utilisateur peuvent être classées dans les catégories suivantes :
  - **Applications utilisateur** : applications qu'un utilisateur a lancées et utilisées. Citrix Analytics for Security extrait ces données depuis Citrix Virtual Apps et les envoie au service SIEM toutes les 12 heures.
  - **Appareil utilisateur** : appareils associés à un utilisateur. Citrix Analytics for Security récupère ces données depuis Citrix Virtual Apps et Citrix Endpoint Management et les envoie au service SIEM toutes les 12 heures.
  - **Localisation de l'utilisateur** : ville dans laquelle un utilisateur a été détecté pour la dernière fois. Citrix Analytics for Security extrait ces données à partir de Citrix Virtual Apps and Desktops et de Citrix DaaS (anciennement Citrix Virtual Apps and Desktops service). Citrix Analytics for Security envoie ces informations à votre service SIEM toutes les 12 heures.
  - **IP du client utilisateur** : adresse IP du client de la machine utilisateur. Citrix Analytics for Security extrait ces données auprès de Citrix Virtual Apps and Desktops et de Citrix DaaS (anciennement Citrix Virtual Apps and Desktops service), et envoie ces informations à votre service SIEM toutes les 12 heures.

Si vous pouvez uniquement consulter les préférences relatives aux événements de la source de données, mais que vous ne pouvez pas les configurer, cela signifie que vous ne disposez pas des autorisations d'administrateur nécessaires.
Pour en savoir plus, consultez la section Gérer les rôles d'administrateur pour Security Analytics.

Dans l'exemple suivant, le bouton **Enregistrer les modifications** est désactivé. Les événements d'analyse des risques sont activés par défaut.



Détails du schéma des événements liés aux informations sur les risques

La section suivante décrit le schéma des données traitées générées par Citrix Analytics for Security.

> **Remarque**
>
> Les valeurs de champ indiquées dans les exemples de schéma suivants ne sont fournies qu'à des fins de représentation. Les valeurs de champ réelles varient en fonction du profil utilisateur, des événements utilisateur et de l'indicateur de risque.

Le tableau suivant décrit les noms de champs communs dans le schéma pour toutes les données de profil utilisateur, le score de risque utilisateur et la modification du score de risque.

Nom du champ	Description
`entity_id`	Identité associée à l'entité. Dans ce cas, l'entité est l'utilisateur.
`entity_type`	L'entité à risque. Dans ce cas, l'entité est l'utilisateur.
`event_type`	Type de données envoyées à votre service SIEM. Par exemple : l'emplacement de l'utilisateur, l'utilisation des données de l'utilisateur ou les informations d'accès à l'appareil de l'utilisateur.

Nom du champ	Description
tenant_id	L'identité unique du client.
timestamp	La date et l'heure de l'activité récente de l'utilisateur.
version	Version du schéma des données traitées. La version actuelle du schéma est 2.

Schéma de données de profil utilisateur

Schéma de localisation de l'utilisateur

```
{

  "tenant_id": "demo_tenant", "entity_id": "demo_user", "entity_type":
     "user", "timestamp": "2021-02-10T15:00:00Z", "event_type": "
     userProfileLocation", "country": "India", "city": "Bengaluru", "
     cnt": 4, "version": 2
   }


<!--NeedCopy-->
```

Description du champ pour l'emplacement de l'utilisateur

Nom du champ	Description
event_type	Type de données envoyées au service SIEM. Dans ce cas, le type d'événement est l'emplacement de l'utilisateur.
country	Le pays depuis lequel l'utilisateur s'est connecté.
city	Ville depuis laquelle l'utilisateur s'est connecté.
cnt	Nombre de fois où l'emplacement a été consulté au cours des 12 dernières heures.

Schéma IP du client utilisateur

```
{

  "client_ip": "149.147.136.10",
  "cnt": 3,
  "entity_id": "r2_up_user_1",
  "entity_type": "user",
  "event_type": "userProfileClientIps",
  "tenant_id": "xaxddaily1",
  "timestamp": "2023-09-18T10:45:00Z",
```



```
  "version": 2
 }



<!--NeedCopy-->
```

Description du champ pour l'adresse IP du client

Nom du champ	Description
client_ip	L'adresse IP de la machine utilisateur.
cnt	Le nombre de fois que l'utilisateur a accédé à l'appareil au cours des 12 dernières heures.
entity_id	Identité associée à l'entité. Dans ce cas, l'entité est l'utilisateur.
entity_type	L'entité à risque. Dans ce cas, le type d'événement est l'adresse IP du client de l'utilisateur.
event_type	Type de données envoyées à votre service SIEM. Par exemple : la localisation de l'utilisateur, son utilisation des données ou les informations d'accès à l'appareil de l'utilisateur.
tenant_id	L'identité unique du client.
timestamp	Date et heure de l'activité récente de l'utilisateur.
version	Version du schéma des données traitées. La version actuelle du schéma est 2.

Schéma d'utilisation des données utilisateur

```
{

  "data_usage_bytes": 87555255, "deleted_file_cnt": 0, "
     downloaded_bytes": 87555255, "downloaded_file_cnt": 5, "entity_id"
     : "demo@demo.com", "entity_type": "user", "event_type": "
     userProfileUsage", "shared_file_cnt": 0, "tenant_id": "demo_tenant
     ", "timestamp": "2021-02-10T21:00:00Z", "uploaded_bytes": 0, "
     uploaded_file_cnt": 0, "version": 2
   }


<!--NeedCopy-->
```

Description du champ pour l'utilisation des données utilisateur

Nom du champ	Description
data_usage_bytes	Quantité de données (en octets) utilisée par l'utilisateur. Il s'agit de l'agrégat du volume téléchargé et téléchargé pour un utilisateur.
deleted_file_cnt	Nombre de fichiers supprimés par l'utilisateur.
downloaded_bytes	La quantité de données téléchargées par l'utilisateur.
downloaded_file_count	Nombre de fichiers téléchargés par l'utilisateur.
event_type	Type de données envoyées au service SIEM. Dans ce cas, le type d'événement est le profil d'utilisation de l'utilisateur.
shared_file_count	Nombre de fichiers partagés par l'utilisateur.
uploaded_bytes	La quantité de données téléchargées par l'utilisateur.
uploaded_file_cnt	Nombre de fichiers téléchargés par l'utilisateur.

Schéma de la machine utilisateur

```
{

  "cnt": 2, "device": "user1612978536 (Windows)", "entity_id": "demo",
     "entity_type": "user", "event_type": "userProfileDevice", "
     tenant_id": "demo_tenant", "timestamp": "2021-02-10T21:00:00Z", "
     version": 2
   }


<!--NeedCopy-->
```

Description du champ de la machine utilisateur.

Nom du champ	Description
cnt	Nombre d'accès à l'appareil au cours des 12 dernières heures.
device	Le nom de l'appareil.
event_type	Type de données envoyées au service SIEM. Dans ce cas, le type d'événement correspond aux informations d'accès à l'appareil de l'utilisateur.

Schéma de l'application utilisateur

```
{
```



```
2
3   "tenant_id": "demo_tenant", "entity_id": "demo", "entity_type": "user
       ", "timestamp": "2021-02-10T21:00:00Z", "event_type": "
       userProfileApp", "version": 2, "session_domain": "99
       e38d488136f62f828d4823edd120b4f32d724396a7410e6dd1b0", "
       user_samaccountname": "testnameeikragz779", "app": "
       Chromeeikragz779", "cnt": 189
4    }
5
6
7   <!--NeedCopy-->
```

Description du champ pour l'application utilisateur.

Nom du champ	Description
event_type	Type de données envoyées au service SIEM. Dans ce cas, le type d'événement correspond aux informations d'accès à l'appareil de l'utilisateur.
session_domain	ID de la session à laquelle l'utilisateur s'est connecté.
user_samaccountname	Nom d'ouverture de session pour les clients et les serveurs d'une version précédente de Windows, telle que Windows NT 4.0, Windows 95, Windows 98 et LAN Manager. Ce nom est utilisé pour ouvrir une session sur Citrix StoreFront et également sur une machine Windows distante.
app	Le nom de l'application à laquelle l'utilisateur a accédé.
cnt	Nombre d'accès à l'application au cours des 12 dernières heures.

Schéma de score de risque utilisateur

```
1   {
2
3     "cur_riskscore": 7, "entity_id": "demo", "entity_type": "user", "
         event_type": "userProfileRiskscore", "last_update_timestamp": "
         2021-01-21T16:14:29Z", "tenant_id": "demo_tenant", "timestamp": "
         2021-02-10T20:45:00Z", "version": 2
4    }
5
6
7   <!--NeedCopy-->
```


Description du champ pour le score de risque de l'utilisateur.

Nom du champ	Description
cur_riskscore	Le score de risque actuel attribué à l'utilisateur. Le score de risque varie de 0 à 100 en fonction de la gravité de la menace associée à l'activité de l'utilisateur.
event_type	Type de données envoyées au service SIEM. Dans ce cas, le type d'événement est le score de risque de l'utilisateur.
last_update_timestamp	Heure de la dernière mise à jour du score de risque pour un utilisateur.
timestamp	Heure à laquelle l'événement de score de risque utilisateur est collecté et envoyé à votre service SIEM. Cet événement est envoyé à votre service SIEM toutes les 12 heures.

Schéma de changement du score de risque

Échantillon 1 :

```
{

  "alert_message": "Large risk score drop percent since last check", "
     alert_type": "riskscore_large_drop_pct", "alert_value": -21.73913,
      "cur_riskscore": 18, "entity_id": "demo_user", "entity_type": "
     user", "event_type": "riskScoreChange", "tenant_id": "demo_tenant"
     , "timestamp": "2021-02-11T05:45:00Z", "version": 2
   }


<!--NeedCopy-->
```

Échantillon 2 :

```
{

  "alert_message": "Risk score increase since last check", "alert_type"
     : "riskscore_increase", "alert_value": 39.0, "cur_riskscore": 76,
     "entity_id": "demo_user", "entity_type": "user", "event_type": "
     riskScoreChange", "tenant_id": "demo_tenant", "timestamp": "
     2021-02-11T03:45:00Z", "version": 2
   }


```



```
<!--NeedCopy-->
```

Description du champ pour la modification du score de risque.

Nom du champ	Description
alert_message	Le message affiché pour la modification du score de risque.
alert_type	Indique si l'alerte concerne une augmentation du score de risque ou une baisse significative du pourcentage de score de risque. Lorsque la variation du score de risque d'un utilisateur est égale ou supérieure à trois et que cette modification augmente à tout rythme ou diminue de plus de 10 %, les données sont envoyées au service SIEM.
alert_value	Une valeur numérique attribuée à la modification du score de risque. La modification du score de risque est la différence entre le score de risque actuel et le score de risque précédent pour un utilisateur. La valeur de l'alerte varie de -100 à 100.
cur_riskscore	Le score de risque actuel attribué à l'utilisateur. Le score de risque varie de 0 à 100 en fonction de la gravité de la menace associée à l'activité de l'utilisateur.
event_type	Type de données envoyées au service SIEM. Dans ce cas, le type d'événement est la modification du score de risque de l'utilisateur.
timestamp	Date et heure auxquelles la dernière modification du score de risque est détectée pour l'utilisateur.

Schéma des indicateurs de risque

Le schéma des indicateurs de risque comprend deux parties : le schéma récapitulatif des indicateurs et le schéma détaillé des événements indicateurs. En fonction de l'indicateur de risque, les champs et leurs valeurs dans le schéma changent en conséquence.

Le tableau suivant décrit les noms de champs communs à tous les schémas récapitulatifs des indicateurs.

Nom du champ	Description
data source	Les produits qui envoient des données à Citrix Analytics for Security. Par exemple : Citrix Secure Private Access, Citrix Gateway et Citrix Apps and Desktops.
data_source_id	ID associé à une source de données. ID 1 = Citrix Gateway, ID 2 = Citrix Endpoint Management, ID 3 = Citrix Apps and Desktops, ID 4 = Citrix Secure Private Access
entity_type	L'entité à risque. Il peut s'agir d'un utilisateur.
entity_id	ID associé à l'entité à risque.
event_type	Type de données envoyées au service SIEM. Dans ce cas, le type d'événement est le résumé de l'indicateur de risque.
indicator_category	Indique les catégories d'indicateurs de risque. Les indicateurs de risque sont regroupés dans l'une des catégories de risque : point de terminaison compromis, utilisateurs compromis, exfiltration de données ou menaces internes.
indicator_id	ID unique associé à l'indicateur de risque.
indicator_category_id	ID associé à une catégorie d'indicateurs de risque. ID 1 = Exfiltration de données, ID 2 = menaces internes, ID 3 = utilisateurs compromis, ID 4 = point de terminaison compromis
indicator_name	Le nom de l'indicateur de risque. Pour un indicateur de risque personnalisé, ce nom est défini lors de la création de l'indicateur.
indicator_type	Indique si l'indicateur de risque est par défaut (intégré) ou personnalisé.
indicator_uuid	ID unique associé à l'instance de l'indicateur de risque.

Nom du champ	Description
indicator_vector_name	Indique le vecteur de risque associé à un indicateur de risque. Les vecteurs de risque sont les indicateurs de risque basés sur l'appareil, les indicateurs de risque basés sur l'emplacement, les indicateurs de risque basés sur les échecs de connexion, les indicateurs de risque basés sur IP, les indicateurs de risque basés sur les données, les indicateurs de risque basés sur les fichiers et d'autres indicateurs de risque.
indicator_vector_id	ID associé à un vecteur de risque. ID 1 = Indicateurs de risque basés sur l'appareil, ID 2 = Indicateurs de risque basés sur la localisation, ID 3 = Indicateurs de risque basés sur l'échec de la connexion, ID 4 = Indicateurs de risque basés sur IP, ID 5 = Indicateurs de risque basés sur les données, ID 6 = Indicateurs de risque basés sur les fichiers, ID 7 = Autres indicateurs de risque et ID 999 = Non disponible
occurrence_details	Les détails sur la condition de déclenchement de l'indicateur de risque.
risk_probability	Indique les chances de risque associées à l'événement utilisateur. La valeur varie de 0 à 1,0. Pour un indicateur de risque personnalisé, la valeur risk_probability est toujours de 1,0 car il s'agit d'un indicateur basé sur une stratégie.
severity	Indique la gravité du risque. Il peut être faible, moyen ou élevé.
tenant_id	L'identité unique du client.
timestamp	La date et l'heure de déclenchement de l'indicateur de risque.
ui_link	Le lien vers la vue chronologique de l'utilisateur sur l'interface utilisateur de Citrix Analytics.

observation_start_time	Heure à partir de laquelle Citrix Analytics commence à surveiller l'activité des utilisateurs jusqu'à l'horodatage. Si un comportement anormal est détecté pendant cette période, un indicateur de risque est déclenché.

Le tableau suivant décrit les noms de champs communs à l'ensemble du schéma des détails des événements de l'indicateur.

Nom du champ	Description
data_source_id	ID associé à une source de données. ID 1 = Citrix Gateway, ID 2 = Citrix Endpoint Management, ID 3 = Citrix Apps and Desktops, ID 4 = Citrix Secure Private Access
indicator_category_id	ID associé à une catégorie d'indicateurs de risque. ID 1 = Exfiltration de données, ID 2 = menaces internes, ID 3 = utilisateurs compromis, ID 4 = point de terminaison compromis
entity_id	ID associé à l'entité à risque.
entity_type	L'entité à risque. Il peut être utilisateur.
event_type	Type de données envoyées au service SIEM. Dans ce cas, le type d'événement correspond aux détails de l'événement indicateur de risque.
indicator_id	ID unique associé à l'indicateur de risque.
indicator_uuid	ID unique associé à l'instance de l'indicateur de risque.
indicator_vector_name	Indique le vecteur de risque associé à un indicateur de risque. Les vecteurs de risque sont les indicateurs de risque basés sur l'appareil, les indicateurs de risque basés sur l'emplacement, les indicateurs de risque basés sur les échecs de connexion, les indicateurs de risque basés sur IP, les indicateurs de risque basés sur les données, les indicateurs de risque basés sur les fichiers et d'autres indicateurs de risque.

Nom du champ	Description
indicator_vector_id	ID associé à un vecteur de risque. ID 1 = Indicateurs de risque basés sur l'appareil, ID 2 = Indicateurs de risque basés sur la localisation, ID 3 = Indicateurs de risque basés sur l'échec de la connexion, ID 4 = Indicateurs de risque basés sur IP, ID 5 = Indicateurs de risque basés sur les données, ID 6 = Indicateurs de risque basés sur les fichiers, ID 7 = Autres indicateurs de risque et ID 999 = Non disponible
tenant_id	L'identité unique du client.
timestamp	La date et l'heure de déclenchement de l'indicateur de risque.
version	Version du schéma des données traitées. La version actuelle du schéma est 2.
client_ip	L'adresse IP de l'appareil de l'utilisateur.

> **Remarque**
>
> - Si une valeur de champ de type de données entier n'est pas disponible, la valeur attribuée est -999. Par exemple `"latitude": -999`, `"longitude": -999`.
> - Si une valeur de champ de type de données de chaîne n'est pas disponible, la valeur attribuée est NA. Par exemple `"city": "NA"`, `"region": "NA"`.

Schéma des indicateurs de risque Citrix Secure Private Access

Tentative d'accès au schéma d'indicateur de risque d'URL sur liste noire

Schéma récapitulatif des indicateurs

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 401,
  "indicator_uuid": "8f2a39bd-c7c2-5555-a86a-5cfe5b64dfef",
  "indicator_category_id": 2,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "data_source_id": 4,
```



```
  "timestamp": "2018-03-15T10:59:58Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Insider threats",
  "indicator_name": "Attempt to access blacklisted URL",
  "severity": "low",
  "data_source": "Citrix Secure Private Access",
  "ui_link": "https://analytics.cloud.com/user/",
  "indicator_type": "builtin",
  "occurrence_details": {

    "observation_start_time": "2018-03-15T10:44:59Z",
    "relevant_event_type": "Blacklisted External Resource Access"
   }

 }


<!--NeedCopy-->
```

Schéma des détails de l'événement indicateur

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 401,
  "indicator_uuid": "c421f3f8-33d8-59b9-ad47-715b9d4f65f4",
  "indicator_category_id": 2,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "data_source_id": 4,
  "timestamp": "2018-03-15T10:57:21Z",
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "domain_name": "googleads.g.doubleclick.net",
  "executed_action": "blocked",
  "reason_for_action": "URL Category match",
  "client_ip": "157.xx.xxx.xxx"
 }


<!--NeedCopy-->
```

Le tableau suivant décrit les noms de champs spécifiques au schéma récapitulatif et au schéma des détails de l'événement pour Tentative d'accès à l'URL de la liste noire.

Nom du champ	Description
observation_start_time	Heure à partir de laquelle Citrix Analytics commence à surveiller l'activité des utilisateurs jusqu'à l'horodatage. Si un comportement anormal est détecté pendant cette période, un indicateur de risque est déclenché.
executed_action	L'action appliquée sur l'URL de la liste noire. L'action inclut Autoriser et Bloquer.
reason_for_action	Raison de l'application de l'action pour l'URL.

Schéma d'indicateur de risque de téléchargements de données excessifs

Schéma récapitulatif des indicateurs

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 403,
  "indicator_uuid": "67d21b81-a89a-531e-af0b-c5688c2e9d40",
  "indicator_category_id": 2,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "data_source_id": 4,
  "timestamp": "2018-03-16T10:59:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Insider threats",
  "indicator_name": "Excessive data download",
  "severity": "low",
  "data_source": "Citrix Secure Private Access",
  "ui_link": "https://analytics.cloud.com/user/",
  "indicator_type": "builtin",
  "occurrence_details": {

    "observation_start_time": "2018-03-16T10:00:00Z",
    "data_volume_in_bytes": 24000,
    "relevant_event_type": "External Resource Access"
   }

 }

```



```
34
35 <!--NeedCopy-->
```

Schéma des détails de l'événement indicateur

```
1  {
2
3    "tenant_id": "demo_tenant",
4    "indicator_id": 403,
5    "indicator_uuid": "67d21b81-a89a-531e-af0b-c5688c2e9d40",
6    "indicator_category_id": 2,
7    "indicator_vector": {
8
9      "name": "Other Risk Indicators",
10     "id": 7  }
11  ,
12   "data_source_id": 4,
13   "timestamp": "2018-03-16T10:30:00Z",
14   "event_type": "indicatorEventDetails",
15   "entity_type": "user",
16   "entity_id": "demo_user",
17   "version": 2,
18   "domain_name": "www.facebook.com",
19   "client_ip": "157.xx.xxx.xxx",
20   "downloaded_bytes": 24000
21  }
22
23
24 <!--NeedCopy-->
```

Le tableau suivant décrit les noms de champs spécifiques au schéma récapitulatif et au schéma des détails de l'événement pour les téléchargements de données excessifs.

Nom du champ	Description
observation_start_time	Heure à partir de laquelle Citrix Analytics commence à surveiller l'activité des utilisateurs jusqu'à l'horodatage. Si un comportement anormal est détecté pendant cette période, un indicateur de risque est déclenché.
data_volume_in_bytes	Quantité de données en octets téléchargée.
relevant_event_type	Indique le type de l'événement utilisateur.
domain_name	Nom du domaine à partir duquel les données sont téléchargées.
downloaded_bytes	Quantité de données en octets téléchargée.

Schéma d'indicateur de risque de volume de téléchargement inhabituel

Schéma récapitulatif des indicateurs

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 402,
  "indicator_uuid": "4f2a249c-9d05-5409-9c5f-f4c764f50e67",
  "indicator_category_id": 2,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "data_source_id": 4,
  "timestamp": "2018-03-16T10:59:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Insider threats",
  "indicator_name": "Unusual upload volume",
  "severity": "low",
  "data_source": "Citrix Secure Private Access",
  "ui_link": "https://analytics.cloud.com/user/",
  "indicator_type": "builtin",
  "occurrence_details": {

    "observation_start_time": "2018-03-16T10:00:00Z",
    "data_volume_in_bytes": 24000,
    "relevant_event_type": "External Resource Access"
   }

 }


<!--NeedCopy-->
```

Schéma des détails de l'événement indicateur

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 402,
  "indicator_uuid": "c6abf40c-9b62-5db4-84bc-5b2cd2c0ca5f",
  "indicator_category_id": 2,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "data_source_id": 4,
```



```
  "timestamp": "2018-03-16T10:30:00Z",
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "domain_name": "www.facebook.com",
  "client_ip": "157.xx.xxx.xxx",
  "uploaded_bytes": 24000
 }


<!--NeedCopy-->
```

Le tableau suivant décrit les noms de champs spécifiques au schéma récapitulatif et au schéma des détails de l'événement pour le volume de téléchargement inhabituel.

Noms de champs	Description
observation_start_time	Heure à partir de laquelle Citrix Analytics commence à surveiller l'activité des utilisateurs jusqu'à l'horodatage. Si un comportement anormal est détecté pendant cette période, un indicateur de risque est déclenché.
data_volume_in_bytes	Quantité de données en octets qui est téléchargée.
relevant_event_type	Indique le type de l'événement utilisateur.
domain_name	Le nom du domaine dans lequel les données sont téléchargées.
uploaded_bytes	Quantité de données en octets qui est téléchargée.

Schéma des indicateurs de risque Citrix Endpoint Management

Schéma des indicateurs détectés par un périphérique jailbreaké ou rooté

Schéma récapitulatif des indicateurs

```
{

  "data_source": "Citrix Endpoint Management",
  "data_source_id": 2,
  "indicator_id": 200,
  "indicator_name": "Jailbroken / Rooted Device Detected",
  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorSummary",
```



```
  "indicator_category": "Compromised endpoints",
  "indicator_category_id": 4,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "indicator_type": "builtin",
  "indicator_uuid": "aa872f86-a991-4219-ad01-2a070b6e633d",
  "occurrence_details": {
  }
 ,
  "risk_probability": 1.0,
  "severity": "low",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-04-13T17:49:05Z",
  "ui_link": "https://analytics.cloud.com/user/",
  "version": 2
 }


<!--NeedCopy-->
```

Schéma des détails de l'événement indicateur

```
{

  "indicator_id": 200,
  "client_ip": "122.xx.xx.xxx",
  "data_source_id": 2,
  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorEventDetails",
  "indicator_category_id": 4,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "indicator_uuid": "9aaaa9e1-39ad-4daf-ae8b-2fa2caa60732",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-04-09T17:50:35Z",
  "version": 2
 }


<!--NeedCopy-->
```

Appareil avec des applications sur la liste noire détectées

Schéma récapitulatif des indicateurs

```
{
```



```
 2
 3   "data_source": "Citrix Endpoint Management",
 4   "data_source_id": 2,
 5   "indicator_id": 201,
 6   "indicator_name": "Device with Blacklisted Apps Detected",
 7   "entity_id": "demo_user",
 8   "entity_type": "user",
 9   "event_type": "indicatorSummary",
10   "indicator_category": "Compromised endpoints",
11   "indicator_category_id": 4,
12   "indicator_vector": {
13
14     "name": "Other Risk Indicators",
15     "id": 7  }
16  ,
17   "indicator_type": "builtin",
18   "indicator_uuid": "3ff7bd54-4319-46b6-8b98-58a9a50ae9a7",
19   "occurrence_details": {
20   }
21  ,
22   "risk_probability": 1.0,
23   "severity": "low",
24   "tenant_id": "demo_tenant",
25   "timestamp": "2021-04-13T17:49:23Z",
26   "ui_link": "https://analytics.cloud.com/user/",
27   "version": 2
28  }
29
30
31 <!--NeedCopy-->
```

Schéma des détails de l'événement indicateur

```
 1 {
 2
 3   "indicator_id": 201,
 4   "client_ip": "122.xx.xx.xxx",
 5   "data_source_id": 2,
 6   "entity_id": "demo_user",
 7   "entity_type": "user",
 8   "event_type": "indicatorEventDetails",
 9   "indicator_category_id": 4,
10   "indicator_vector": {
11
12     "name": "Other Risk Indicators",
13     "id": 7  }
14  ,
15   "indicator_uuid": "743cd13a-2596-4323-8da9-1ac279232894",
16   "tenant_id": "demo_tenant",
17   "timestamp": "2021-04-09T17:50:39Z",
18   "version": 2
19  }
20
21
```



```
<!--NeedCopy-->
```

Périphérique non géré détecté

Schéma récapitulatif des indicateurs


```
{

  "data_source": "Citrix Endpoint Management",
  "data_source_id": 2,
  "indicator_id": 203,
  "indicator_name": "Unmanaged Device Detected",
  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorSummary",
  "indicator_category": "Compromised endpoints",
  "indicator_category_id": 4,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "indicator_type": "builtin",
  "indicator_uuid": "e28b8186-496b-44ff-9ddc-ae50e87bd757",
  "occurrence_details": {
  }
 ,
  "risk_probability": 1.0,
  "severity": "low",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-04-13T12:56:30Z",
  "ui_link": "https://analytics.cloud.com/user/",
  "version": 2
 }


<!--NeedCopy-->
```


Schéma des détails de l'événement indicateur


```
{

  "indicator_id": 203,
  "client_ip": "127.xx.xx.xxx",
  "data_source_id": 2,
  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorEventDetails",
  "indicator_category_id": 4,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
```



```
 ,
  "indicator_uuid": "dd280122-04f2-42b4-b9fc-92a715c907a0",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-04-09T18:41:30Z",
  "version": 2
 }


<!--NeedCopy-->
```

Schéma des indicateurs de risque Citrix Gateway

Schéma de l'indicateur de risque d'échec de l'analyse EPA

Schéma récapitulatif des indicateurs

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 100,
  "indicator_uuid": "3c17454c-86f5-588a-a4ac-0342693d8a70",
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "data_source_id": 1,
  "timestamp": "2017-12-21T07:14:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Compromised users",
  "indicator_name": "EPA scan failure",
  "severity": "low",
  "data_source": "Citrix Gateway",
  "ui_link": "https://analytics.cloud.com/user/",
  "indicator_type": "builtin",
  "occurrence_details": {

    "event_description": "Post auth failed, no quarantine",
    "observation_start_time": "2017-12-21T07:00:00Z",
    "relevant_event_type": "EPA Scan Failure at Logon"
   }

 }


<!--NeedCopy-->
```


Schéma des détails de l'événement indicateur

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 100,
  "indicator_uuid": "3c17454c-86f5-588a-a4ac-0342693d8a70",
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "data_source_id": 1,
  "timestamp": "2017-12-21T07:12:00Z",
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "event_description": "Post auth failed, no quarantine",
  "gateway_domain_name": "10.102.xx.xx",
  "gateway_ip": "56.xx.xxx.xx",
  "policy_name": "postauth_act_1",
  "client_ip": "210.91.xx.xxx",
  "country": "United States",
  "city": "San Jose",
  "region": "California",
  "cs_vserver_name": "demo_vserver",
  "device_os": "Windows OS",
  "security_expression": "CLIENT.OS(Win12) EXISTS",
  "vpn_vserver_name": "demo_vpn_vserver",
  "vserver_fqdn": "10.xxx.xx.xx"
 }

<!--NeedCopy-->
```

Le tableau décrit les noms de champs spécifiques au schéma récapitulatif et le schéma des détails de l'événement pour l'indicateur de risque d'échec de l'analyse EPA.

Noms de champs	Description
event_description	Décrit les raisons de l'échec de l'analyse EPA, telles que l'échec de la post-authentification et l'absence de groupe de quarantaine.
relevant_event_type	Indique le type de l'événement d'échec de l'analyse EPA.
gateway_domain_name	Le nom de domaine de Citrix Gateway.
gateway_ip	L'adresse IP de Citrix Gateway.

Noms de champs	Description
policy_name	Nom de la stratégie d'analyse EPA configuré sur Citrix Gateway.
country	Le pays à partir duquel l'activité de l'utilisateur a été détectée.
city	Ville à partir de laquelle l'activité de l'utilisateur a été détectée.
region	La région à partir de laquelle l'activité de l'utilisateur a été détectée.
cs_vserver_name	Le nom du serveur virtuel de commutateur de contenu.
device_os	Le système d'exploitation de l'appareil de l'utilisateur.
security_expression	Expression de sécurité configurée sur Citrix Gateway.
vpn_vserver_name	Le nom du serveur virtuel Citrix Gateway.
vserver_fqdn	Le nom de domaine complet du serveur virtuel Citrix Gateway.

Schéma d'indicateur de risque d'échec d'authentification excessif

Schéma récapitulatif des indicateurs


```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 101,
  "indicator_uuid": "4bc0f759-93e0-5eea-9967-ed69de9dd09a",
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "Logon-Failure-Based Risk Indicators",
    "id": 3  }
 ,
  "data_source_id": 1,
  "timestamp": "2017-12-21T07:14:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Compromised users",
  "indicator_name": "Excessive authentication failures",
  "severity": "medium",
  "data_source": "Citrix Gateway",
```



```
  "ui_link": "https://analytics.cloud.com/user/" ,
  "indicator_type": "builtin",
  "occurrence_details": {

    "observation_start_time": "2017-12-21T07:00:00Z",
    "relevant_event_type": "Logon Failure"
   }

 }

<!--NeedCopy-->
```

Schéma des détails de l'événement indicateur

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 101,
  "indicator_uuid": "a391cd1a-d298-57c3-a17b-01f159b26b99",
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "Logon-Failure-Based Risk Indicators",
    "id": 3  }
 ,
  "data_source_id": 1,
  "timestamp": "2017-12-21T07:10:00Z",
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
  "entity_id": "demo-user",
  "version": 2,
  "event_description": "Bad (format) password passed to nsaaad",
  "authentication_stage": "Secondary",
  "authentication_type": "LDAP",
  "auth_server_ip": "10.xxx.x.xx",
  "client_ip": "24.xxx.xxx.xx",
  "gateway_ip": "24.xxx.xxx.xx",
  "vserver_fqdn": "demo-fqdn.citrix.com",
  "vpn_vserver_name": "demo_vpn_vserver",
  "cs_vserver_name": "demo_cs_vserver",
  "gateway_domain_name": "xyz",
  "country": "United States",
  "region": "California",
  "city": "San Jose",
  "nth_failure": 5
 }


<!--NeedCopy-->
```

Le tableau suivant décrit les noms de champs spécifiques au schéma récapitulatif et le schéma des détails de l'événement en cas d'échec d'authentification excessif.

Noms de champs	Description
relevant_event_type	Indique le type d'événement, tel qu'un échec de connexion.
event_description	Décrit la raison de l'échec d'authentification excessif, tel qu'un mot de passe incorrect.
authentication_stage	Indique si la phase d'authentification est principale, secondaire ou tertiaire.
authentication_type	Indique les types d'authentification tels que LDAP, Local ou OAuth.
auth_server_ip	L'adresse IP du serveur d'authentification.
gateway_domain_name	Le nom de domaine de Citrix Gateway.
gateway_ip	L'adresse IP de Citrix Gateway.
cs_vserver_name	Le nom du serveur virtuel de commutateur de contenu.
vpn_vserver_name	Le nom du serveur virtuel Citrix Gateway.
vserver_fqdn	Le nom de domaine complet du serveur virtuel Citrix Gateway.
nth_failure	Nombre de fois où l'authentification de l'utilisateur a échoué.
country	Le pays à partir duquel l'activité de l'utilisateur a été détectée.
city	Ville à partir de laquelle l'activité de l'utilisateur a été détectée.
region	La région à partir de laquelle l'activité de l'utilisateur a été détectée.

Indicateur de risque de voyage impossible

Schéma récapitulatif des indicateurs

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": "111",
  "indicator_uuid": "83d68a6d-6588-5b77-9118-8a9e6a5b462b",
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "Location-Based Risk Indicators",
    "id": 2
   }
```



```
 ,
  "data_source_id": 1,
  "timestamp": "2020-06-06T12:14:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Compromised users",
  "indicator_name": "Impossible travel",
  "severity": "medium",
  "data_source": "Citrix Gateway",
  "ui_link": "https://analytics.cloud.com/user/",
  "indicator_type": "builtin",
  "occurrence_details": {

    "relevant_event_type": "Impossible travel",
    "distance": 7480.44718,
    "observation_start_time": "2020-06-06T12:00:00Z",
    "historical_logon_locations": "[{
"country":"United States","region":"Florida","city":"Miami","latitude"
   :25.7617,"longitude":-80.191,"count":28 }
,{
"country":"United States","latitude":37.0902,"longitude":-95.7129,"
   count":2 }
]",
    "historical_observation_period_in_days": 30
   }

}


<!--NeedCopy-->
```

Schéma des détails de l'événement indicateur

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": "111",
  "indicator_uuid": "83d68a6d-6588-5b77-9118-8a9e6a5b462b",
  "pair_id": 2,
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "Location-Based Risk Indicators",
    "id": 2
   }
 ,
  "data_source_id": 1,
  "timestamp": "2020-06-06T05:05:00Z",
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
  "entity_id": "demo_user",
```



```
19    "version": 2,
20    "client_ip": "95.xxx.xx.xx",
21     “ ip_organization ” :  “ global telecom ltd ” ,
22     “ ip_routing_type ” :  “ mobile gateway ” ,
23    "country": "Norway",
24    "region": "Oslo",
25    "city": "Oslo",
26    "latitude": 59.9139,
27    "longitude": 10.7522,
28    "device_os": "Linux OS",
29    "device_browser": "Chrome 62.0.3202.94"
30   }
31
32
33  <!--NeedCopy-->
```

Le tableau suivant décrit les noms de champ spécifiques au schéma récapitulatif et au schéma des détails de l'événement pour Impossible travel.

Nom du champ	Description
distance	La distance (km) entre les événements associés à un voyage impossible.
historical_logon_locations	Les emplacements auxquels l'utilisateur a accédé et le nombre de fois où chaque emplacement a été consulté pendant la période d'observation.
historical_observation_period_in_days	Chaque site est surveillé pendant 30 jours.
relevant_event_type	Indique le type d'événement, tel que l'ouverture de session.
observation_start_time	Heure à partir de laquelle Citrix Analytics commence à surveiller l'activité des utilisateurs jusqu'à l'horodatage. Si un comportement anormal est détecté pendant cette période, un indicateur de risque est déclenché.
country	Le pays depuis lequel l'utilisateur s'est connecté.
city	Ville depuis laquelle l'utilisateur s'est connecté.
region	Indique la région à partir de laquelle l'utilisateur s'est connecté.
latitude	Indique la latitude de l'emplacement depuis lequel l'utilisateur s'est connecté.

Nom du champ	Description
longitude	Indique la longitude de l'emplacement à partir duquel l'utilisateur s'est connecté.
device_browser	Le navigateur Web utilisé par l'utilisateur.
device_os	Le système d'exploitation de l'appareil de l'utilisateur.
ip_organization	Enregistrement de l'organisation de l'adresse IP du client
ip_routing_type	Type de routage IP du client

Ouverture de session à partir d'un schéma d'indicateur de risque IP suspect

Schéma récapitulatif des indicateurs

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 102,
  "indicator_uuid": "0100e910-561a-5ff3-b2a8-fc556d199ba5",
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "IP-Based Risk Indicators",
    "id": 4  }
 ,
  "data_source_id": 1,
  "timestamp": "2019-10-10T10:14:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 0.91,
  "indicator_category": "Compromised users",
  "indicator_name": "Logon from suspicious IP",
  "severity": "medium",
  "data_source": "Citrix Gateway",
  "ui_link": "https://analytics.cloud.com/user/",
  "indicator_type": "builtin",
  "occurrence_details": {

    "relevant_event_type": "Logon",
    "client_ip": "1.0.xxx.xx",
    "observation_start_time": "2019-10-10T10:00:00Z",
    "suspicion_reasons": "brute_force|external_threat"
   }

 }
```



```
34
35 <!--NeedCopy-->
```

Schéma des détails de l'événement indicateur

```
1  {
2
3    "tenant_id": "demo_tenant",
4    "indicator_id": 102,
5    "indicator_uuid": "4ba77b6c-bac0-5ad0-9b4a-c459a3e2ec33",
6    "indicator_category_id": 3,
7    "indicator_vector": {
8
9      "name": "IP-Based Risk Indicators",
10     "id": 4  }
11  ,
12   "data_source_id": 1,
13   "timestamp": "2019-10-10T10:11:00Z",
14   "event_type": "indicatorEventDetails",
15   "entity_type": "user",
16   "entity_id": "demo_user",
17   "version": 2,
18   "suspicion_reasons": "external_threat",
19   "gateway_ip": "gIP1",
20   "client_ip": "128.0.xxx.xxx",
21   "country": "Sweden",
22   "city": "Stockholm",
23   "region": "Stockholm",
24   "webroot_reputation": 14,
25   "webroot_threat_categories": "Windows Exploits|Botnets|Proxy",
26   "device_os": "Windows OS",
27   "device_browser": "Chrome"
28  }
29
30
31 <!--NeedCopy-->
```

Le tableau suivant décrit les noms de champs spécifiques au schéma récapitulatif et au schéma des détails des événements pour Se connecter à partir d'une adresse IP suspecte.

Nom du champ	Description
`suspicious_reasons`	La raison pour laquelle l'adresse IP a été identifiée comme suspecte.
`webroot_reputation`	L'indice de réputation IP fourni par le fournisseur de renseignements sur les menaces Webroot.
`webroot_threat_categories`	Catégorie de menace identifiée pour l'adresse IP suspecte par le fournisseur de renseignements sur les menaces Webroot.

Nom du champ	Description
device_os	Le système d'exploitation de la machine utilisateur.
device_browser	Le navigateur Web utilisé.
country	Le pays à partir duquel l'activité de l'utilisateur a été détectée.
city	Ville à partir de laquelle l'activité de l'utilisateur a été détectée.
region	La région à partir de laquelle l'activité de l'utilisateur a été détectée.

Schéma d'indicateur de risque d'échec d'authentification inhabituel

Schéma récapitulatif des indicateurs

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 109,
  "indicator_uuid": "dc0174c9-247a-5e48-a2ab-d5f92cd83d0f",
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "Logon-Failure-Based Risk Indicators",
    "id": 3  }
 ,
  "data_source_id": 1,
  "timestamp": "2020-04-01T06:44:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Compromised users",
  "indicator_name": "Unusual authentication failure",
  "severity": "medium",
  "data_source": "Citrix Gateway",
  "ui_link": "https://analytics.cloud.com/user/",
  "indicator_type": "builtin",
  "occurrence_details": {

    "relevant_event_type": "Logon Failure",
    "observation_start_time": "2020-04-01T05:45:00Z"
   }

 }


```



```
<!--NeedCopy-->
```

Schéma des détails de l'événement indicateur

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 109,
  "indicator_uuid": "ef4b9830-39d6-5b41-bdf3-84873a77ea9a",
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "Logon-Failure-Based Risk Indicators",
    "id": 3  }
 ,
  "data_source_id": 1,
  "timestamp": "2020-04-01T06:42:00Z",
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "event_description": "Success",
  "authentication_stage": "Secondary",
  "authentication_type": "LDAP",
  "client_ip": "99.xxx.xx.xx",
  "country": "United States",
  "city": "San Jose",
  "region": "California",
  "device_os": "Windows OS ",
  "device_browser": "Chrome",
  "is_risky": "false"
 }


<!--NeedCopy-->
```

Le tableau suivant décrit les noms de champs spécifiques au schéma récapitulatif et le schéma des détails de l'événement en cas d'échec d'authentification inhabituel.

Noms de champs	Description
`relevant_event_type`	Indique le type d'événement, tel qu'un échec de connexion.
`event_description`	Indique si la connexion a réussi ou échoué
`authentication_stage`	Indique si la phase d'authentification est principale, secondaire ou tertiaire.
`authentication_type`	Indique les types d'authentification tels que LDAP, Local ou OAuth.

Noms de champs	Description
is_risky	Pour une ouverture de session réussie, la valeur is_risky est false. En cas d'ouverture de session infructueuse, la valeur is_risky est true.
device_os	Le système d'exploitation de la machine utilisateur.
device_browser	Le navigateur Web utilisé par l'utilisateur.
country	Le pays à partir duquel l'activité de l'utilisateur a été détectée.
city	Ville à partir de laquelle l'activité de l'utilisateur a été détectée.
region	La région à partir de laquelle l'activité de l'utilisateur a été détectée.

Indicateur de risque de connexion suspect

Schéma récapitulatif des indicateurs


```
{

  "tenant_id": "demo_tenant",
  "indicator_id": "110",
  "indicator_uuid": "67fd935-a6a3-5397-b596-636aa1588c",
  "indicator_category_id": 3,
  "indicator_vector": [
    {

      "name": "Location-Based Risk Indicators",
      "id": 2
     }
 ,
    {

      "name": "IP-Based Risk Indicators",
      "id": 4
     }
 ,
    {

      "name": "Other Risk Indicators",
      "id": 7
     }

  ],
  "data_source_id": 1,
  "timestamp": "2020-06-06T12:14:59Z",
```



```
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 0.71,
  "indicator_category": "Compromised users",
  "indicator_name": "Suspicious logon",
  "severity": "medium",
  "data_source": "Citrix Gateway",
  "ui_link": "https://analytics.cloud.com/user/",
  "indicator_type": "builtin",
  "occurrence_details": {

    "observation_start_time": "2020-06-06T12:00:00Z",
    "relevant_event_type": "Logon",
    "event_count": 1,
    "historical_observation_period_in_days": 30,
    "country": "United States",
    "region": "Florida",
    "city": "Miami",
    "historical_logon_locations": "[{
"country":"United States","region":"New York","city":"New York City","
    latitude":40.7128,"longitude":-74.0060,"count":9 }
]",
    "user_location_risk": 75,
    "device_id": "",
    "device_os": "Windows OS",
    "device_browser": "Chrome",
    "user_device_risk": 0,
    "client_ip": "99.xxx.xx.xx",
    "user_network_risk": 75,
    "webroot_threat_categories": "Phishing",
    "suspicious_network_risk": 89
   }

}



<!--NeedCopy-->
```

Schéma des détails de l'événement indicateur

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": "110",
  "indicator_uuid": "67fd6935-a6a3-5397-b596-63856aa1588c",
  "indicator_category_id": 3,
  "indicator_vector": [
    {

      "name": "Location-Based Risk Indicators",
      "id": 2
```



```
      }
  ,
     {

       "name": "IP-Based Risk Indicators",
       "id": 4
      }
  ,
     {

       "name": "Other Risk Indicators",
       "id": 7
      }

   ],
   "data_source_id": 1,
   "timestamp": "2020-06-06T12:08:40Z",
   "event_type": "indicatorEventDetails",
   "entity_type": "user",
   "entity_id": "demo_user",
   "version": 2,
   "country": "United States",
   "region": "Florida",
   "city": "Miami",
   "latitude": 25.7617,
   "longitude": -80.1918,
   "device_browser": "Chrome",
   "device_os": "Windows OS",
   "device_id": "NA",
   "client_ip": "99.xxx.xx.xx"
  }


<!--NeedCopy-->
```

Le tableau suivant décrit les noms de champs spécifiques au schéma récapitulatif et au schéma des détails de l'événement pour l'ouverture de session suspecte.

Nom du champ	Description
historical_logon_locations	Les emplacements auxquels l'utilisateur a accédé et le nombre de fois où chaque emplacement a été consulté pendant la période d'observation.
historical_observation_period_in_days	Chaque site est surveillé pendant 30 jours.
relevant_event_type	Indique le type d'événement, tel que l'ouverture de session.

Nom du champ	Description
observation_start_time	Heure à partir de laquelle Citrix Analytics commence à surveiller l'activité des utilisateurs jusqu'à l'horodatage. Si un comportement anormal est détecté pendant cette période, un indicateur de risque est déclenché.
occurrence_event_type	Indique le type d'événement utilisateur, tel que la connexion au compte.
country	Le pays depuis lequel l'utilisateur s'est connecté.
city	Ville depuis laquelle l'utilisateur s'est connecté.
region	Indique la région à partir de laquelle l'utilisateur s'est connecté.
latitude	Indique la latitude de l'emplacement depuis lequel l'utilisateur s'est connecté.
longitude	Indique la longitude de l'emplacement à partir duquel l'utilisateur s'est connecté.
device_browser	Le navigateur Web utilisé par l'utilisateur.
device_os	Le système d'exploitation de l'appareil de l'utilisateur.
device_id	Le nom de l'appareil utilisé par l'utilisateur.
user_location_risk	Indique le niveau de suspicion de l'emplacement à partir duquel l'utilisateur s'est connecté. Niveau de suspicion faible : 0—69, niveau de suspicion moyen : 70—89 et niveau de suspicion élevé : 90—100
user_device_risk	Indique le niveau de suspicion de l'appareil à partir duquel l'utilisateur s'est connecté. Niveau de suspicion faible : 0—69, niveau de suspicion moyen : 70—89 et niveau de suspicion élevé : 90—100
user_network_risk	Indique le niveau de suspicion du réseau ou du sous-réseau à partir duquel l'utilisateur s'est connecté. Niveau de suspicion faible : 0—69, niveau de suspicion moyen : 70—89 et niveau de suspicion élevé : 90—100

Nom du champ	Description
suspicious_network_risk	Indique le niveau de menace IP en fonction du flux Webroot IP Threat Intelligence. Niveau de menace faible : 0—69, niveau de menace moyen : 70—89 et niveau de menace élevé : 90-100
webroot_threat_categories	Indique les types de menaces détectés à partir de l'adresse IP en fonction du flux Webroot IP Threat Intelligence. Les catégories de menaces peuvent être les sources de spam, les exploits Windows, les attaques Web, les réseaux de zombies, les scanners, le déni de service, la réputation, l'hameçonnage, le proxy, les menaces non spécifiées, les menaces mobiles et le proxy Tor

Schéma des indicateurs de risque Citrix DaaS et Citrix Virtual Apps and Desktops

Indicateur de risque de voyage impossible

Schéma récapitulatif des indicateurs


```
{

  "tenant_id": "demo_tenant",
  "indicator_id": "313",
  "indicator_uuid": "c78d1dd4-5e70-5642-ba6f-1cdf31bc6ab2",
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "Location-Based Risk Indicators",
    "id": 2
   }
 ,
  "data_source_id": 3,
  "timestamp": "2020-06-06T12:14:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Compromised users",
  "indicator_name": "Impossible travel",
  "severity": "medium",
  "data_source": "Apps and Desktops",
```



```
  "ui_link": "https://analytics.cloud.com/user/",
  "indicator_type": "builtin",
  "occurrence_details": {

    "relevant_event_type": "Impossible travel",
    "distance": 7480.44718,
    "observation_start_time": "2020-06-06T12:00:00Z",
    "historical_logon_locations": "[{
 "country":"United States","region":"Florida","city":"Miami","latitude"
    :25.7617,"longitude":-80.191,"count":28 }
 ,{
 "country":"United States","latitude":37.0902,"longitude":-95.7129,"
    count":2 }
 ]",
    "historical_observation_period_in_days": 30
   }

 }


<!--NeedCopy-->
```

Schéma des détails de l'événement indicateur

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": "313",
  "indicator_uuid": "c78d1dd4-5e70-5642-ba6f-1cdf31bc6ab2",
  "pair_id": 2,
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "Location-Based Risk Indicators",
    "id": 2
   }
 ,
  "data_source_id": 3,
  "timestamp": "2020-06-06T05:05:00Z",
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "occurrence_event_type": "Account.Logon",
  "client_ip": "95.xxx.xx.xx",
   “ip_organization”: “global telecom ltd”,
   “ip_routing_type”: “mobile gateway”,
  "country": "Norway",
  "region": "Oslo",
  "city": "Oslo",
  "latitude": 59.9139,
  "longitude": 10.7522,
  "device_id": "device1",
  "receiver_type": "XA.Receiver.Linux",
```



```
31    "os": "Linux OS",
32    "browser": "Chrome 62.0.3202.94"
33   }
34
35
36  <!--NeedCopy-->
```

Le tableau suivant décrit les noms de champ spécifiques au schéma récapitulatif et au schéma des détails de l'événement pour Impossible travel.

Nom du champ	Description
distance	La distance (km) entre les événements associés à un voyage impossible.
historical_logon_locations	Les emplacements auxquels l'utilisateur a accédé et le nombre de fois où chaque emplacement a été consulté pendant la période d'observation.
historical_observation_period_in_days	Chaque site est surveillé pendant 30 jours.
relevant_event_type	Indique le type d'événement, tel que l'ouverture de session.
observation_start_time	Heure à partir de laquelle Citrix Analytics commence à surveiller l'activité des utilisateurs jusqu'à l'horodatage. Si un comportement anormal est détecté pendant cette période, un indicateur de risque est déclenché.
country	Le pays depuis lequel l'utilisateur s'est connecté.
city	Ville depuis laquelle l'utilisateur s'est connecté.
region	Indique la région à partir de laquelle l'utilisateur s'est connecté.
latitude	Indique la latitude de l'emplacement depuis lequel l'utilisateur s'est connecté.
longitude	Indique la longitude de l'emplacement à partir duquel l'utilisateur s'est connecté.
browser	Le navigateur Web utilisé par l'utilisateur.
os	Le système d'exploitation de l'appareil de l'utilisateur.
device_id	Le nom de l'appareil utilisé par l'utilisateur.

Nom du champ	Description
receiver_type	Type d'application Citrix Workspace ou de Citrix Receiver installé sur la machine de l'utilisateur.
ip_organization	Enregistrement de l'organisation de l'adresse IP du client
ip_routing_type	Type de routage IP du client

Indicateur de risque potentiel d'exfiltration de données

Schéma récapitulatif des indicateurs

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 303,
  "indicator_uuid": "fb649ff7-5b09-5f48-8a04-12836b9eed85",
  "indicator_category_id": 1,
  "indicator_vector": {

    "name": "Data-Based Risk Indicators",
    "id": 5  }
 ,
  "data_source_id": 3,
  "timestamp": "2018-04-02T10:59:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Data exfiltration",
  "indicator_name": "Potential data exfiltration",
  "severity": "low",
  "data_source": "Citrix Apps and Desktops",
  "ui_link": "https://analytics.cloud.com/user/ ",
  "indicator_type": "builtin",
  "occurrence_details": {

    "relevant_event_type": "Download/Print/Copy",
    "observation_start_time": "2018-04-02T10:00:00Z",
    "exfil_data_volume_in_bytes": 1172000
   }

 }


<!--NeedCopy-->
```


Schéma des détails de l'événement indicateur

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 303,
  "indicator_uuid": "fb649ff7-5b09-5f48-8a04-12836b9eed85",
  "indicator_category_id": 1,
  "indicator_vector": {

    "name": "Data-Based Risk Indicators",
    "id": 5  }
 ,
  "data_source_id": 3,
  "timestamp": "2018-04-02T10:57:36Z",
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "occurrence_event_type": "App.SaaS.Clipboard",
  "file_size_in_bytes": 98000,
  "file_type": "text",
  "device_id": "dvc5",
  "receiver_type": "XA.Receiver.Windows",
  "app_url": "https://www.citrix.com",
  "client_ip": "10.xxx.xx.xxx",
  "entity_time_zone": "Pacific Standard Time"
 }


<!--NeedCopy-->
```

Le tableau suivant décrit les champs spécifiques au schéma récapitulatif et au schéma des détails de l'événement pour l'exfiltration de données potentielle.

Nom du champ	Description
observation_start_time	Heure à partir de laquelle Citrix Analytics commence à surveiller l'activité des utilisateurs jusqu'à l'horodatage. Si un comportement anormal est détecté pendant cette période, un indicateur de risque est déclenché.
relevant_event_type	Indique l'activité de l'utilisateur, telle que le téléchargement, l'impression ou la copie des données.
exfil_data_volume_in_bytes	Quantité d'exfiltration de données.
occurrence_event_type	Indique comment l'exfiltration des données s'est produite, comme l'opération de presse-papiers dans une application SaaS.

Nom du champ	Description
file_size_in_bytes	La taille du fichier.
file_type	Type de fichier.
device_id	ID de la machine utilisateur.
receiver_type	L'application Citrix Workspace ou Citrix Receiver est installée sur la machine utilisateur.
app_url	URL de l'application à laquelle l'utilisateur accède.
entity_time_zone	Le fuseau horaire de l'utilisateur.

Schéma d'indicateur de risque d'ouverture de session suspecte

Schéma récapitulatif des indicateurs

```
{

  "tenant_id": "tenant_1",
  "indicator_id": "312",
  "indicator_uuid": "1b97c3be-abcd-efgh-ijkl-1234567890",
  "indicator_category_id": 3,
  "indicator_vector":
  [
    {

      "name": "Other Risk Indicators",
      "id": 7
     }
,
    {

      "name":"Location-Based Risk Indicators",
      "id":2
     }
,
    {

      "name":"IP-Based Risk Indicators",
      "id":4
     }
,
    {

      "name": "Device-Based Risk Indicators",
      "id": 1
     }
,
 ],
```



```
  "data_source_id": 3,
  "timestamp": "2020-06-06T12:14:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "user2",
  "version": 2,
  "risk_probability": 0.78,
  "indicator_category": "Compromised users",
  "indicator_name": "Suspicious logon",
  "severity": "medium",
  "data_source": "Citrix Apps and Desktops",
  "ui_link": "https://analytics.cloud.com/user/ ",
  "indicator_type": "builtin",
  "occurrence_details":
  {

    "user_location_risk": 0,
    "city": "Some_city",
    "observation_start_time": "2020-06-06T12:00:00Z",
    "event_count": 1,
    "user_device_risk": 75,
    "country": "United States",
    "device_id": "device2",
    "region": "Some_Region",
    "client_ip": "99.xx.xx.xx",
    "webroot_threat_categories": "'Spam Sources', 'Windows Exploits', '
       Web Attacks', 'Botnets', 'Scanners', 'Denial of Service'",
    "historical_logon_locations": "[{
 "country":"United States","latitude":45.0,"longitude":45.0,"count":12
    }
 ,{
 "country":"United States","region":"Some_Region_A","city":"Some_City_A
    ","latitude":0.0,"longitude":0.0,"count":8 }
 ]",
    "relevant_event_type": "Logon",
    "user_network_risk": 100,
    "historical_observation_period_in_days": 30,
    "suspicious_network_risk": 0
   }

 }


<!--NeedCopy-->
```

Schéma des détails de l'événement indicateur

```
{

  "tenant_id": "tenant_1",
  "indicator_id": "312",
  "indicator_uuid": "1b97c3be-abcd-efgh-ijkl-1234567890",
  "indicator_category_id": 3,
  "indicator_vector":
```



```
  [
    {

      "name": "Other Risk Indicators",
      "id": 7
     }
,
    {

      "name":"Location-Based Risk Indicators",
      "id":2
     }
,
    {

      "name":"IP-Based Risk Indicators",
      "id":4
     }
,
    {

      "name": "Device-Based Risk Indicators",
      "id": 1
     }
,
 ],
 "data_source_id": 3,
 "timestamp": "2020-06-06 12:02:30",
 "event_type": "indicatorEventDetails",
 "entity_type": "user",
 "entity_id": "user2",
 "version": 2,
 "occurrence_event_type": "Account.Logon",
 "city": "Some_city",
 "country": "United States",
 "region": "Some_Region",
 "latitude": 37.751,
 "longitude": -97.822,
 "browser": "Firefox 1.3",
 "os": "Windows OS",
 "device_id": "device2",
 "receiver_type": "XA.Receiver.Chrome",
 "client_ip": "99.xxx.xx.xx"
}


<!--NeedCopy-->
```

Le tableau suivant décrit les noms de champs spécifiques au schéma récapitulatif et au schéma des détails de l'événement pour l'ouverture de session suspecte.

Nom du champ	Description
historical_logon_locations	Les emplacements auxquels l'utilisateur a accédé et le nombre de fois où chaque emplacement a été consulté pendant la période d'observation.
historical_observation_period_in_days	Chaque site est surveillé pendant 30 jours.
relevant_event_type	Indique le type d'événement, tel que l'ouverture de session.
observation_start_time	Heure à partir de laquelle Citrix Analytics commence à surveiller l'activité des utilisateurs jusqu'à l'horodatage. Si un comportement anormal est détecté pendant cette période, un indicateur de risque est déclenché.
occurrence_event_type	Indique le type d'événement utilisateur, tel que la connexion au compte.
country	Le pays depuis lequel l'utilisateur s'est connecté.
city	Ville depuis laquelle l'utilisateur s'est connecté.
region	Indique la région à partir de laquelle l'utilisateur s'est connecté.
latitude	Indique la latitude de l'emplacement depuis lequel l'utilisateur s'est connecté.
longitude	Indique la longitude de l'emplacement à partir duquel l'utilisateur s'est connecté.
browser	Le navigateur Web utilisé par l'utilisateur.
os	Le système d'exploitation de l'appareil de l'utilisateur.
device_id	Le nom de l'appareil utilisé par l'utilisateur.
receiver_type	Type d'application Citrix Workspace ou de Citrix Receiver installé sur la machine de l'utilisateur.
user_location_risk	Indique le niveau de suspicion de l'emplacement à partir duquel l'utilisateur s'est connecté. Niveau de suspicion faible : 0—69, niveau de suspicion moyen : 70—89 et niveau de suspicion élevé : 90—100

Nom du champ	Description
user_device_risk	Indique le niveau de suspicion de l'appareil à partir duquel l'utilisateur s'est connecté. Niveau de suspicion faible : 0—69, niveau de suspicion moyen : 70—89 et niveau de suspicion élevé : 90—100
user_network_risk	Indique le niveau de suspicion du réseau ou du sous-réseau à partir duquel l'utilisateur s'est connecté. Niveau de suspicion faible : 0—69, niveau de suspicion moyen : 70—89 et niveau de suspicion élevé : 90—100
suspicious_network_risk	Indique le niveau de menace IP en fonction du flux Webroot IP Threat Intelligence. Niveau de menace faible : 0—69, niveau de menace moyen : 70—89 et niveau de menace élevé : 90-100
webroot_threat_categories	Indique les types de menaces détectés à partir de l'adresse IP en fonction du flux Webroot IP Threat Intelligence. Les catégories de menaces peuvent être les sources de spam, les exploits Windows, les attaques Web, les réseaux de zombies, les scanners, le déni de service, la réputation, l'hameçonnage, le proxy, les menaces non spécifiées, les menaces mobiles et le proxy Tor

Indicateur Microsoft Active Directory

Schéma récapitulatif des indicateurs

```
{

  "data_source": "Microsoft Graph Security",
  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorSummary",
  "indicator_category": "Compromised users",
  "indicator_id": 1000,
  "indicator_name": "MS Active Directory Indicator",
  "indicator_vector": {

    "name": "IP-Based Risk Indicators",
    "id": 4  }
```



```
 ,
  "indicator_type": "builtin",
  "indicator_uuid": "9880f479-9fbe-4ab0-8348-a613f9de5eba",
  "occurrence_details": {
  }
 ,
  "risk_probability": 1.0,
  "severity": "low",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-01-27T16:03:46Z",
  "ui_link": "https://analytics-daily.cloud.com/user/",
  "version": 2
 }


<!--NeedCopy-->
```

Schéma des détails de l'événement indicateur

```
{

  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorEventDetails",
  "indicator_id": 1000,
  "indicator_vector": {

    "name": "IP-Based Risk Indicators",
    "id": 4  }
 ,
  "indicator_uuid": "9880f479-9fbe-4ab0-8348-a613f9de5eba",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-01-27T16:03:46Z",
  "version": 2
 }


<!--NeedCopy-->
```

Schéma d'indicateur de risque personnalisé

La section suivante décrit le schéma de l'indicateur de risque personnalisé.

> **Remarque**
>
> Actuellement, Citrix Analytics envoie les données relatives aux indicateurs de risque personnalisés de Citrix DaaS et de Citrix Virtual Apps and Desktops à votre service SIEM.

Le tableau suivant décrit les noms des champs du schéma récapitulatif des indicateurs de risque personnalisés.

Nom du champ	Description
data source	Les produits qui envoient des données à Citrix Analytics for Security. Par exemple : Citrix Secure Private Access, Citrix Gateway et Citrix Apps and Desktops.
data_source_id	ID associé à une source de données. ID 1 = Citrix Gateway, ID 2 = Citrix Endpoint Management, ID 3 = Citrix Apps and Desktops, ID 4 = Citrix Secure Private Access
entity_id	ID associé à l'entité à risque.
entity_type	L'entité à risque. Dans ce cas, l'entité est un utilisateur.
event_type	Type de données envoyées au service SIEM. Dans ce cas, le type d'événement est le résumé de l'indicateur de risque.
indicator_category	Indique les catégories d'indicateurs de risque. Les indicateurs de risque sont regroupés dans l'une des catégories de risque : point de terminaison compromis, utilisateurs compromis, exfiltration de données ou menaces internes.
indicator_id	ID unique associé à l'indicateur de risque.
indicator_category_id	L'identifiant associé à la catégorie d'indicateur de risque. ID 1 = Exfiltration de données, ID 2 = menaces internes, ID 3 = utilisateurs compromis, ID 4 = points de terminaison compromis
indicator_name	Le nom de l'indicateur de risque. Pour un indicateur de risque personnalisé, ce nom est défini lors de la création de l'indicateur.
indicator_type	Indique si l'indicateur de risque est par défaut (intégré) ou personnalisé.
indicator_uuid	ID unique associé à l'instance de l'indicateur de risque.
occurrence_details	Les détails sur la condition de déclenchement de l'indicateur de risque.
pre_configured	Indique si l'indicateur de risque personnalisé est préconfiguré.

Nom du champ	Description
risk_probability	Indique les chances de risque associées à l'événement utilisateur. La valeur varie de 0 à 1,0. Pour un indicateur de risque personnalisé, la valeur risk_probability est toujours de 1,0 car il s'agit d'un indicateur basé sur une stratégie.
severity	Indique la gravité du risque. Il peut être faible, moyen ou élevé.
tenant_id	L'identité unique du client.
timestamp	La date et l'heure de déclenchement de l'indicateur de risque.
ui_link	Le lien vers la vue chronologique de l'utilisateur sur l'interface utilisateur de Citrix Analytics.
version	Version du schéma des données traitées. La version actuelle du schéma est 2.

Le tableau suivant décrit les noms de champs communs dans le schéma de détails d'événement d'indicateur de risque personnalisé.

Nom du champ	Description
data_source_id	ID associé à une source de données. ID 1 = Citrix Gateway, ID 2 = Citrix Endpoint Management, ID 3 = Citrix Apps and Desktops, ID 4 = Citrix Secure Private Access
indicator_category_id	L'identifiant associé à la catégorie d'indicateur de risque. ID 1 = Exfiltration de données, ID 2 = menaces internes, ID 3 = utilisateurs compromis, ID 4 = points de terminaison compromis
event_type	Type de données envoyées au service SIEM. Dans ce cas, le type d'événement correspond aux détails de l'événement indicateur de risque.
tenant_id	L'identité unique du client.
entity_id	ID associé à l'entité à risque.
entity_type	L'entité à risque. Dans ce cas, il s'agit de l'utilisateur.
indicator_id	ID unique associé à l'indicateur de risque.

Nom du champ	Description
indicator_uuid	ID unique associé à l'instance de l'indicateur de risque.
timestamp	La date et l'heure de déclenchement de l'indicateur de risque.
version	Version du schéma des données traitées. La version actuelle du schéma est 2.
event_id	ID associé à l'événement utilisateur.
occurrence_event_type	Indique le type d'événement utilisateur tel que l'ouverture de session, le lancement de session et la connexion au compte.
product	Indique le type d'application Citrix Workspace, telle que l'application Citrix Workspace pour Windows.
client_ip	L'adresse IP de l'appareil de l'utilisateur.
session_user_name	Nom d'utilisateur associé à la session Citrix Apps and Desktops.
city	Le nom de la ville à partir de laquelle l'activité de l'utilisateur est détectée.
country	Le nom du pays à partir duquel l'activité de l'utilisateur est détectée.
device_id	Le nom de l'appareil utilisé par l'utilisateur.
os_name	Système d'exploitation installé sur l'appareil de l'utilisateur. Pour plus d'informations, consultez la section Recherche en libre-service d'applications et de bureaux.
os_version	Version du système d'exploitation qui est installée sur l'appareil de l'utilisateur. Pour plus d'informations, consultez la section Recherche en libre-service d'applications et de bureaux.
os_extra_info	Les détails supplémentaires associés au système d'exploitation installé sur l'appareil de l'utilisateur. Pour plus d'informations, consultez la section Recherche en libre-service d'applications et de bureaux.

Indicateur de risque personnalisé pour Citrix DaaS et Citrix Virtual Apps and Desktops

Schéma récapitulatif des indicateurs

```
{

  "data_source": " Citrix Apps and Desktops",
  "data_source_id": 3,
  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorSummary",
  "indicator_category": "Compromised users",
  "indicator_category_id": 3,
  "indicator_id": "ca97a656ab0442b78f3514052d595936",
  "indicator_name": "Demo_user_usage",
  "indicator_type": "custom",
  "indicator_uuid": "8e680e29-d742-4e09-9a40-78d1d9730ea5",
  "occurrence_details": {

    "condition": "User-Name ~ demo_user", "happen": 0, "new_entities":
       "", "repeat": 0, "time_quantity": 0, "time_unit": "", "type": "
       everyTime" }
 ,
  "pre_configured": "N",
  "risk_probability": 1.0,
  "severity": "low",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-02-10T14:47:25Z",
  "ui_link": "https://analytics.cloud.com/user/ ",
  "version": 2
 }


<!--NeedCopy-->
```

Schéma des détails de l'événement d'indicateur pour l'événement d'ouverture de session

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "Session.Logon",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
```



```
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "app_name": "notepad",
  "launch_type": "Application",
  "domain": "test_domain",
  "server_name": "SYD04-MS1-S102",
  "session_guid": "f466e318-9065-440c-84a2-eec49d978a96",
 }


<!--NeedCopy-->
```

Le tableau suivant décrit les noms de champ spécifiques au schéma des détails de l'événement pour l'événement d'ouverture de session.

Nom du champ	Description
app_name	Nom d'une application ou d'un bureau lancé.
launch_type	Indique une application ou un bureau.
domain	Le nom de domaine du serveur qui a envoyé la demande.
server_name	Nom du serveur.
session_guid	Le GUID de la session active.

Schéma des détails de l'événement indicateur pour l'événement de lancement de session

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "Session.Launch",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
```



```
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "app_name": "notepad",
  "launch_type": "Application",
 }


<!--NeedCopy-->
```

Le tableau suivant décrit les noms de champ spécifiques au schéma des détails de l'événement pour l'événement de lancement de session.

Nom du champ	Description
app_name	Nom d'une application ou d'un bureau lancé.
launch_type	Indique une application ou un bureau.

Schéma des détails de l'événement indicateur pour l'événement d'ouverture de session de compte :

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "Account.Logon",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "app_name": "notepad",
 }


<!--NeedCopy-->
```

Le tableau suivant décrit les noms de champ spécifiques au schéma des détails de l'événement pour

l'événement d'ouverture de session de compte.

Nom du champ	Description
app_name	Nom d'une application ou d'un bureau lancé.

Schéma des détails de l'événement indicateur pour l'événement de fin de session

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "Session.End",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "app_name": "notepad",
  "launch_type": "Application",
  "domain": "test_domain",
  "server_name": "test_server",
  "session_guid": "f466e318-9065-440c-84a2-eec49d978a96",
 }


<!--NeedCopy-->
```

Le tableau suivant décrit les noms de champ spécifiques au schéma des détails de l'événement pour l'événement de fin de session.

Nom du champ	Description
app_name	Nom d'une application ou d'un bureau lancé.
launch_type	Indique une application ou un bureau.

Nom du champ	Description
domain	Le nom de domaine du serveur qui a envoyé la demande.
server_name	Nom du serveur.
session_guid	Le GUID de la session active.

Schéma des détails de l'événement indicateur pour l'événement de démarrage de l'application

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "App.Start",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "app_name": "notepad",
  "launch_type": "Application",
  "domain": "test_domain",
  "server_name": "test_server",
  "session_guid": "f466e318-9065-440c-84a2-eec49d978a96",
  "module_file_path": "/root/folder1/folder2/folder3"
 }


<!--NeedCopy-->
```

Le tableau suivant décrit les noms de champ spécifiques au schéma des détails de l'événement pour l'événement de démarrage de l'application.

Nom du champ	Description
app_name	Nom d'une application ou d'un bureau lancé.
launch_type	Indique une application ou un bureau.
domain	Le nom de domaine du serveur qui a envoyé la demande.
server_name	Nom du serveur.
session_guid	Le GUID de la session active.
module_file_path	Chemin d'accès de l'application utilisée.

Schéma des détails de l'événement indicateur pour l'événement de fin d'application

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "App.End",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "app_name": "notepad",
  "launch_type": "Application",
  "domain": "test_domain",
  "server_name": "test_server",
  "session_guid": "f466e318-9065-440c-84a2-eec49d978a96",
  "module_file_path": "/root/folder1/folder2/folder3"
 }


<!--NeedCopy-->
```

Le tableau suivant décrit les noms de champ spécifiques au schéma des détails de l'événement pour l'événement de fin d'application.

Nom du champ	Description
app_name	Nom d'une application ou d'un bureau lancé.
launch_type	Indique une application ou un bureau.
domain	Le nom de domaine du serveur qui a envoyé la demande.
server_name	Nom du serveur.
session_guid	Le GUID de la session active.
module_file_path	Chemin d'accès de l'application utilisée.

Schéma des détails de l'événement Indicateur pour l'événement de téléchargement de fichiers

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "File.Download",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "file_download_file_name": "File5.txt",
  "file_download_file_path": "/root/folder1/folder2/folder3",
  "file_size_in_bytes": 278,
  "launch_type": "Desktop",
  "domain": "test_domain",
  "server_name": "test_server",
  "session_guid": "f466e318-9065-440c-84a2-eec49d978a96",
  "device_type": "USB"
 }


<!--NeedCopy-->
```


Le tableau suivant décrit les noms de champ spécifiques au schéma des détails de l'événement pour l'événement de téléchargement de fichiers.

Nom du champ	Description
file_download_file_name	Nom du fichier de téléchargement.
file_download_file_path	Chemin d'accès de destination dans lequel le fichier est téléchargé.
launch_type	Indique une application ou un bureau.
domain	Le nom de domaine du serveur qui a envoyé la demande.
server_name	Nom du serveur.
session_guid	Le GUID de la session active.
device_type	Indique le type de périphérique sur lequel le fichier est téléchargé.

Schéma des détails de l'événement indicateur pour l'événement d'impression

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "Printing",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "printer_name": "Test-printer",
  "launch_type": "Desktop",
  "domain": "test_domain",
  "server_name": "test_server",
  "session_guid": "f466e318-9065-440c-84a2-eec49d978a96",
  "job_details_size_in_bytes": 454,
  "job_details_filename": "file1.pdf",
```



```
  "job_details_format": "PDF"
 }


<!--NeedCopy-->
```

Le tableau suivant décrit les noms de champ spécifiques au schéma des détails de l'événement pour l'événement d'impression.

Nom du champ	Description
printer_name	Nom de l'imprimante utilisée pour la tâche d'impression.
launch_type	Indique une application ou un bureau.
domain	Le nom de domaine du serveur qui a envoyé la demande.
server_name	Nom du serveur.
session_guid	Le GUID de la session active.
job_details_size_in_bytes	Taille du travail d'impression, tel qu'un fichier ou un dossier.
job_details_filename	Nom du fichier imprimé.
job_details_format	Format de la tâche d'impression.

Schéma des détails de l'événement indicateur pour l'événement de lancement SaaS de l'application

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "App.SaaS.Launch",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
```



```
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "launch_type": "Desktop",
 }


<!--NeedCopy-->
```

Le tableau suivant décrit les noms de champ spécifiques au schéma des détails de l'événement pour l'événement de lancement SaaS de l'application.

Nom du champ	Description
launch_type	Indique une application ou un bureau.

Schéma des détails de l'événement indicateur pour l'événement de fin SaaS de l'application

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "App.SaaS.End",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "launch_type": "Desktop",
 }


<!--NeedCopy-->
```

Le tableau suivant décrit les noms de champ spécifiques au schéma des détails de l'événement pour l'événement de fin SaaS de l'application.

Nom du champ	Description
`launch_type`	Indique une application ou un bureau.

Événements de source de données

En outre, vous pouvez configurer la fonctionnalité d'exportation de données pour exporter les événements utilisateur à partir de vos sources de données de produits compatibles avec Citrix Analytics for Security. Lorsque vous effectuez une activité dans l'environnement Citrix, les événements de la source de données sont générés. Les événements exportés sont des données d'utilisation des utilisateurs et des produits en temps réel non traitées, disponibles dans la vue en libre-service. Les métadonnées contenues dans ces événements peuvent également être utilisées pour une analyse plus approfondie des menaces, la création de nouveaux tableaux de bord et la mise en relation avec d'autres événements provenant de sources de données autres que Citrix dans votre infrastructure informatique et de sécurité.

Actuellement, Citrix Analytics for Security envoie les événements utilisateur à votre SIEM pour la source de données Citrix Virtual Apps and Desktops.

Détails du schéma des événements de la source de données

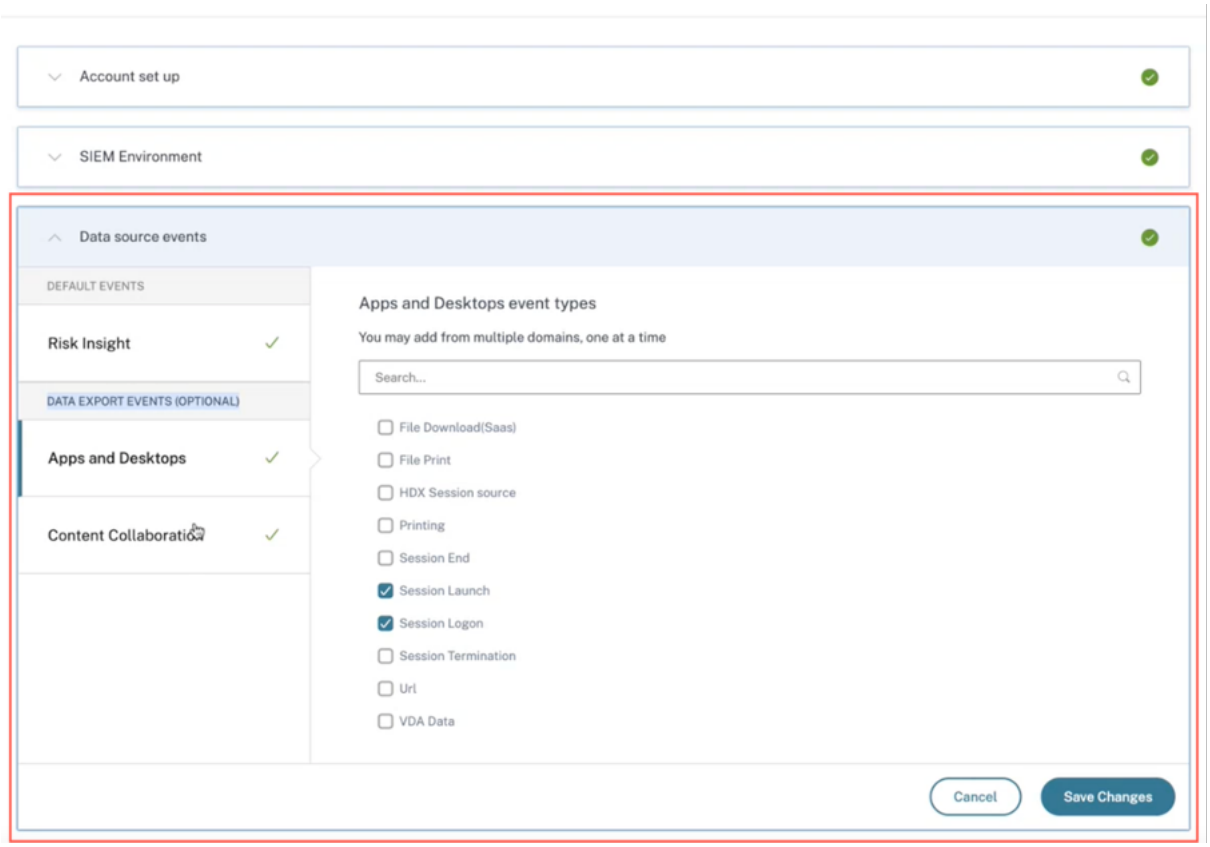
Événements Citrix Virtual Apps and Desktops

Les événements utilisateur sont reçus en temps réel dans Citrix Analytics for Security lorsque les utilisateurs utilisent des applications ou des bureaux virtuels. Pour plus d'informations, consultez Citrix Virtual Apps and Desktops et Source de données Citrix DaaS. Vous pouvez consulter les événements utilisateur suivants associés à Citrix Virtual Apps and Desktops dans votre SIEM :

- Tous les types d'événements
- Connexion au compte
- Application (début, lancement, fin)
- Presse-papiers
- Fichier (impression, téléchargement)
- Téléchargement de fichiers (SaaS)
- Source de session HDX
- Impression
- Session (ouverture de session, lancement, fin, fin)
- Url
- Données VDA
- Création de processus VDA

Pour plus d'informations sur les événements et leurs attributs, voir Recherche en libre-service pour les Virtual Apps and Desktops.

Vous pouvez vérifier quels types d'événements sont activés et transmis au SIEM. Vous pouvez configurer ou supprimer le type d'événement applicable à un locataire et cliquer sur le bouton **Enregistrer les modifications** pour enregistrer vos paramètres.



Utilisation du modèle de données SIEM de Citrix Analytics pour l'analyse des menaces et la corrélation des données

June 19, 2023

Cet article explique la relation entre les données de l'entité qui est mise en évidence par les événements envoyés à l'environnement SIEM d'un client. Pour mieux comprendre ce point, prenons l'exemple d'un scénario de chasse aux menaces dans lequel les attributs (adresse IP et système d'exploitation du client) sont les points focaux. Les méthodes suivantes pour corréler ces attributs à l'utilisateur seront discutées :

- Utilisation d'informations personnalisées sur les indicateurs de risque

- Utilisation des événements de source de données

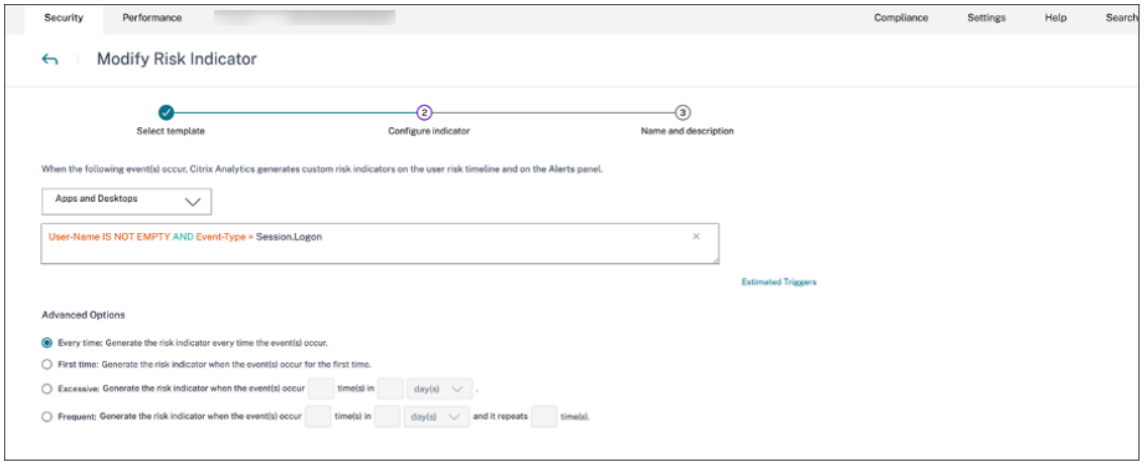
Splunk est l'environnement SIEM choisi pour être présenté dans l'exemple suivant. Une corrélation de données similaire peut également être effectuée sur Sentinel à l'aide d'un modèle de classeur de Citrix Analytics. Pour en savoir plus, consultez le classeur Citrix Analytics pour Microsoft Sentinel.

Informations sur les indicateurs de risque personnalisés

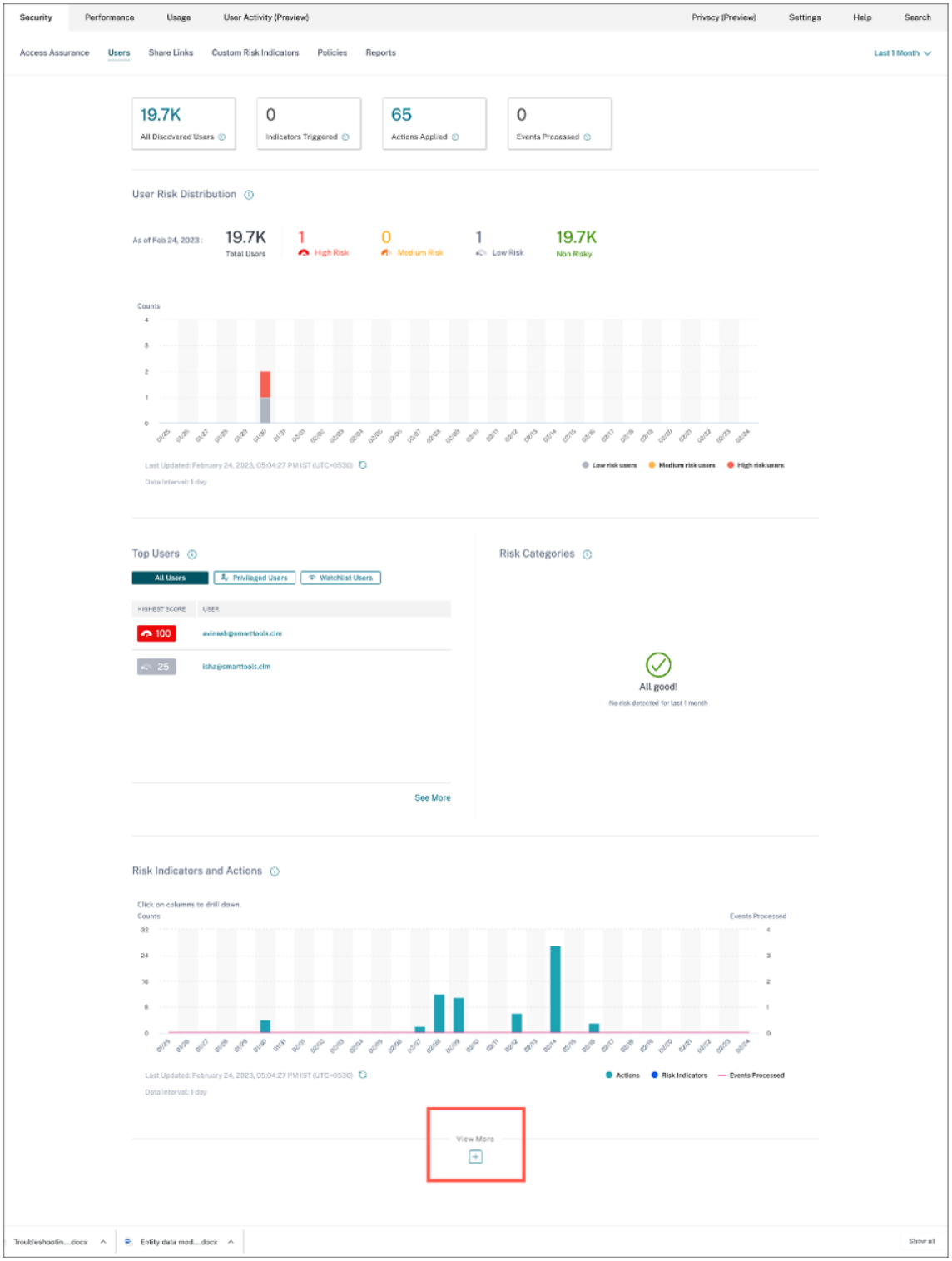
Comme indiqué dans le format d'exportation de données Citrix Analytics pour SIEM, le résumé des indicateurs et les informations détaillées sur les événements font partie de l'ensemble de données d'informations sur les risques par défaut. Pour le jeu de données d'indicateurs Citrix Virtual Apps and Desktops, l'adresse IP et le système d'exploitation du client sont exportés par défaut. Par conséquent, si un administrateur configure un indicateur personnalisé avec ou sans la condition d'inclure ces champs, ces points de données seront acheminés vers votre environnement Splunk.

Configuration d'un indicateur de risque personnalisé dans Citrix Analytics

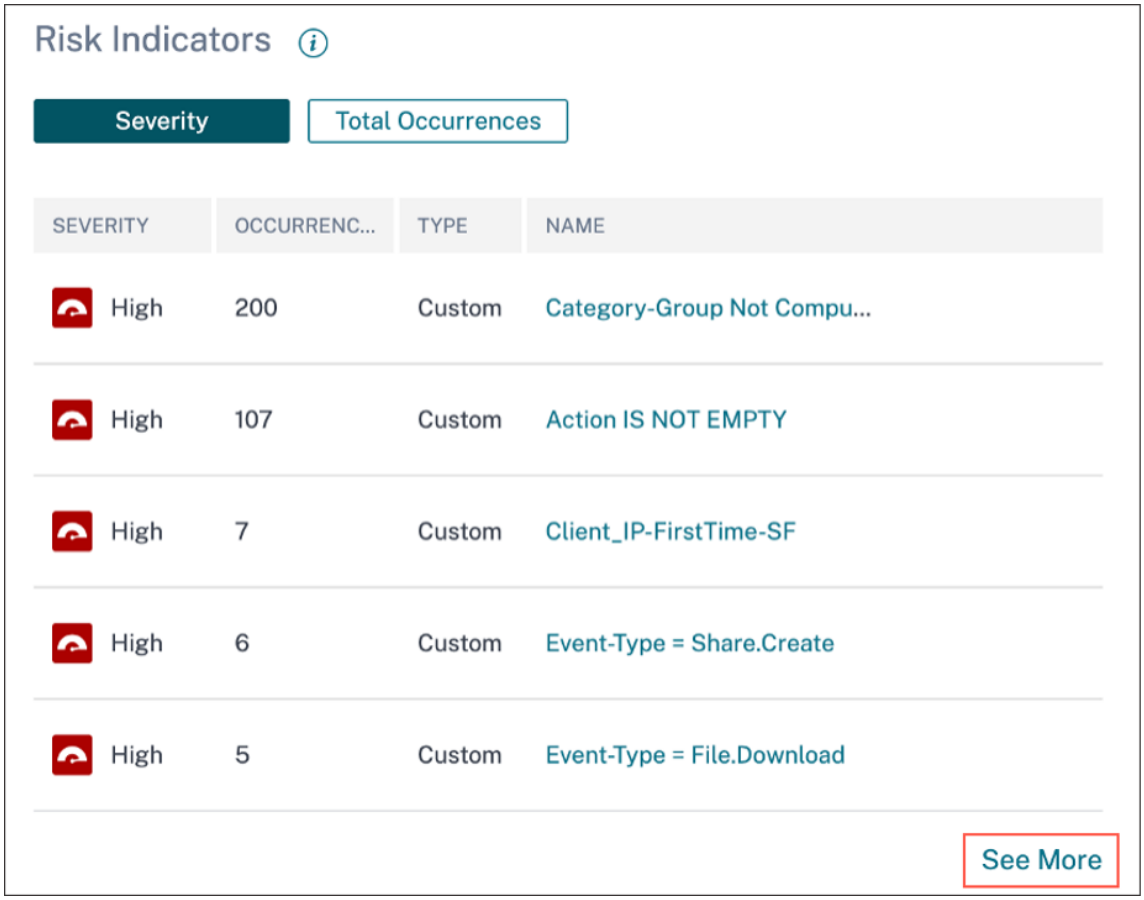
1. Accédez au tableau de **bord de Citrix Analytics for Security > Indicateurs de risque personnalisés > Créer un indicateur**. Vous pouvez créer un indicateur de risque personnalisé avec n'importe quelle condition qui vous aide à surveiller le comportement de l'utilisateur. Une fois que vous avez configuré l'indicateur personnalisé, tous les utilisateurs qui déclenchent la condition associée sont visibles dans votre environnement Splunk.



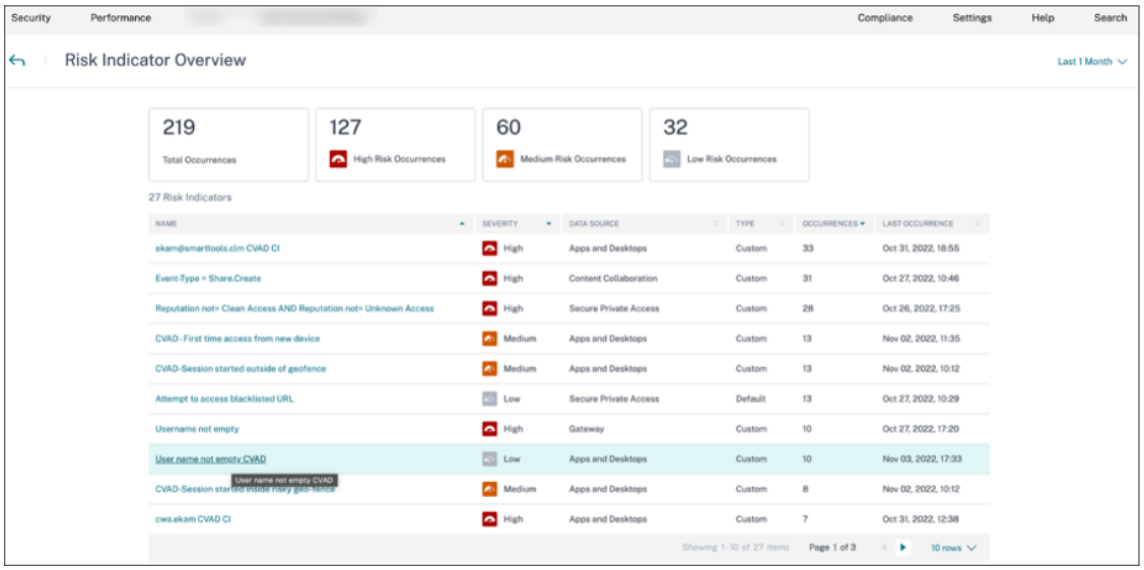
2. Pour afficher les occurrences des indicateurs de risque créées sur Citrix Analytics for Security, accédez à **Sécurité > Utilisateurs. Accédez au bas de la page et cliquez sur l'icône plus (+)**.



La carte des indicateurs de risque s'affiche. Vous pouvez consulter les détails de l'indicateur de risque, de la gravité et de l'occurrence.

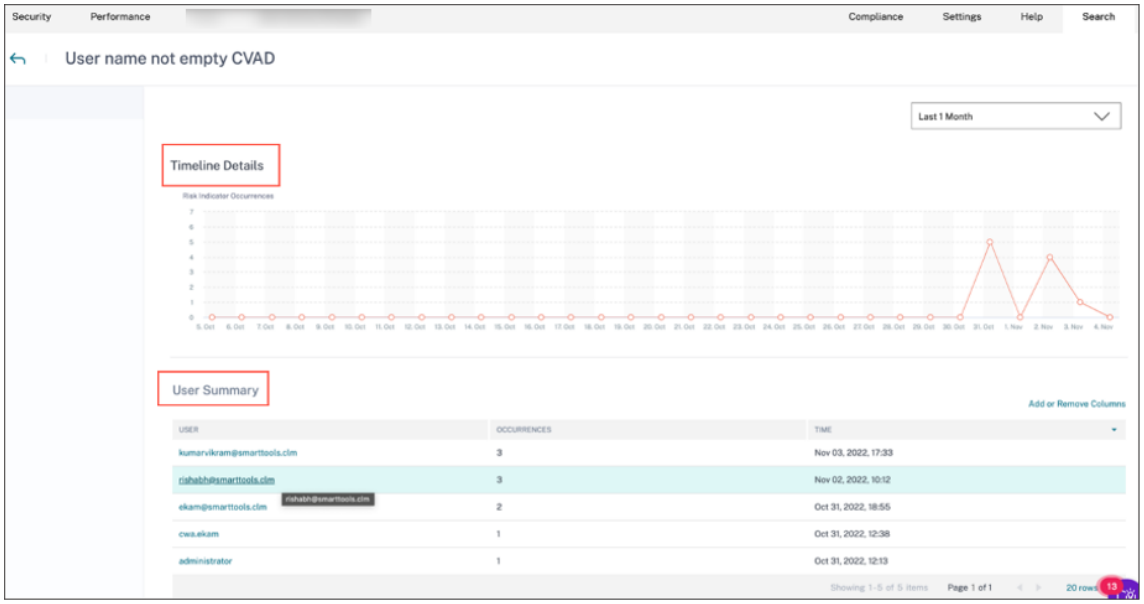


3. Cliquez sur **Voir plus**. La page de **présentation** de l'indicateur de risque s'affiche.



Sur la page Vue d'ensemble de l'indicateur de risque, vous pouvez consulter les détails de l'utilisateur qui a déclenché l'indicateur grâce à une chronologie détaillée et à un résumé de l'utilisateur. Pour en savoir plus sur la chronologie, voir Chronologie et profil des risques de l'

utilisateur.

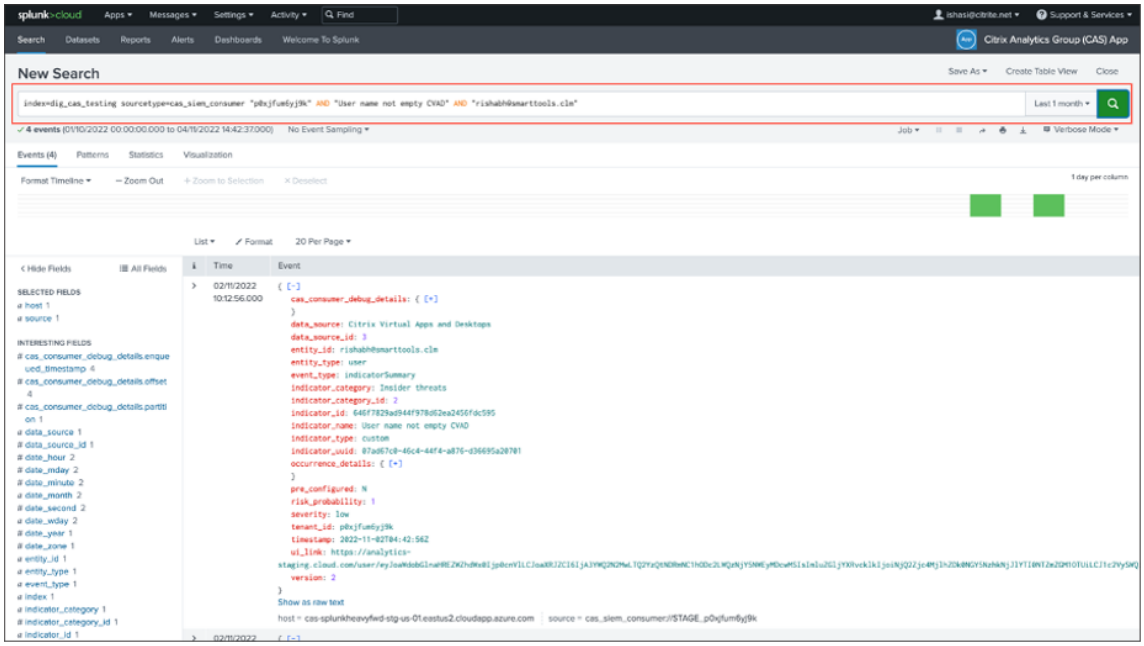


Occurrences d'indicateurs de risque sur Splunk - Raw Queries

Vous pouvez également obtenir les informations relatives à l'adresse IP et au système d'exploitation du client en utilisant l'index et le type de source utilisés par l'administrateur de l'infrastructure Splunk lors de la configuration de la saisie des données sur le module complémentaire Splunk Enterprise pour Citrix Analytics for Security.

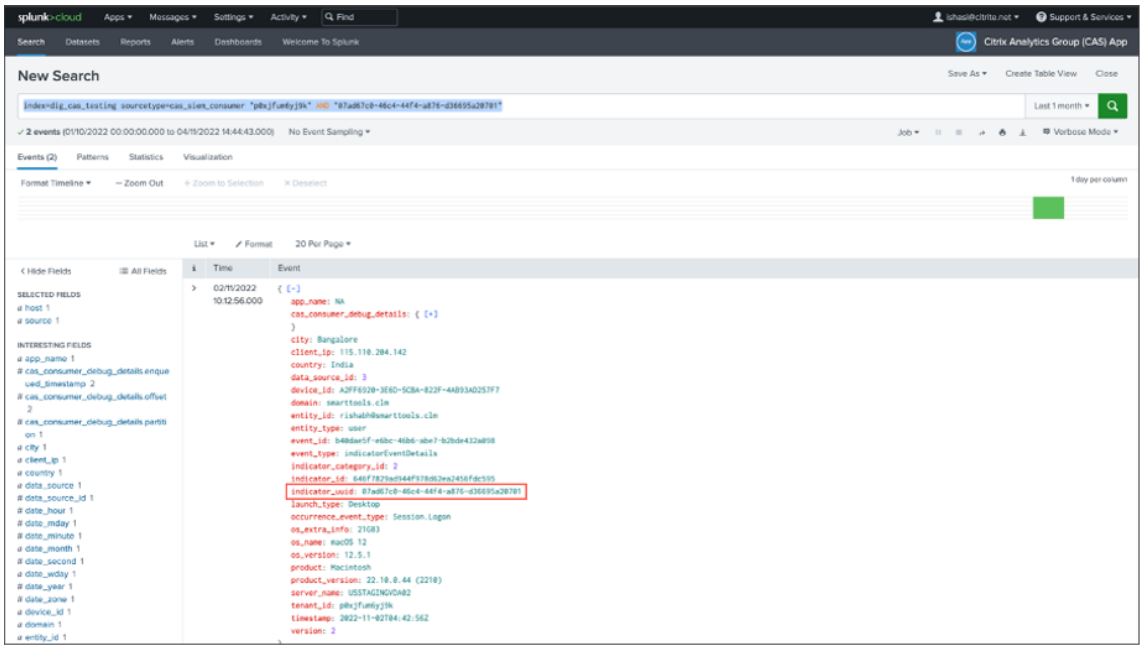
1. Accédez à **Splunk > Nouvelle recherche**. Dans la requête de recherche, saisissez et exécutez la requête suivante :

```
index=<index configured by you> sourcetype=<sourcetype configured
    by you> AND "<tenant_id>" AND "<indicator name configured by
    you on CAS>" AND "<user you are interested in>"

<!--NeedCopy-->
```

2. Choisissez le fichier indicator_uuid et exécutez la requête suivante :

```
index=<index configured by you> sourcetype=<sourcetype configured
    by you> "<tenant_id>" AND "<indicator_uuid>"

<!--NeedCopy-->
```



Le résultat de l'événement contient le **résumé de l'événement indicateuret les détails**de l'événement indicateur (l'activité déclenchée par votre indicateur). Le détail de l'événement contient l'**adresse IP du client**et les**informations sur le système d'exploitation** (nom, version, informations supplémentaires).

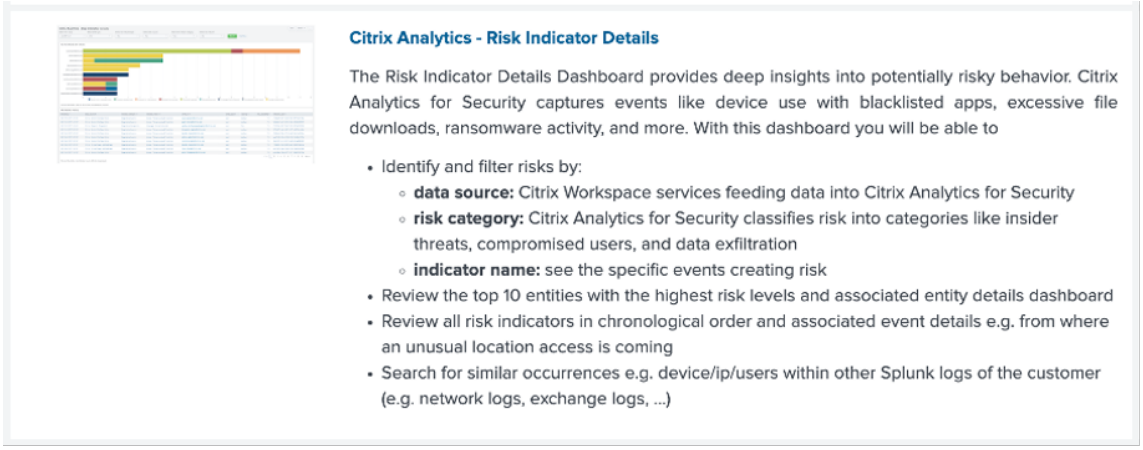
Pour en savoir plus sur le format de données, consultez le format d'exportation de données Citrix Analytics pour SIEM.

Événements liés aux indicateurs de risque sur Splunk - Application de tableau de bord

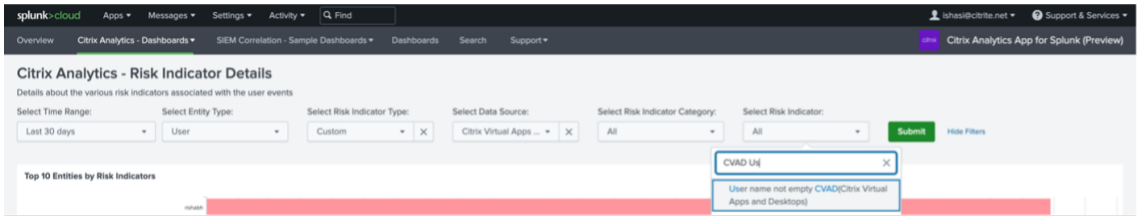
Consultez les articles suivants pour savoir comment installer l'application Citrix Analytics pour Splunk :

- Application Citrix Analytics pour Splunk
- Tableaux de bord Citrix Analytics pour Splunk

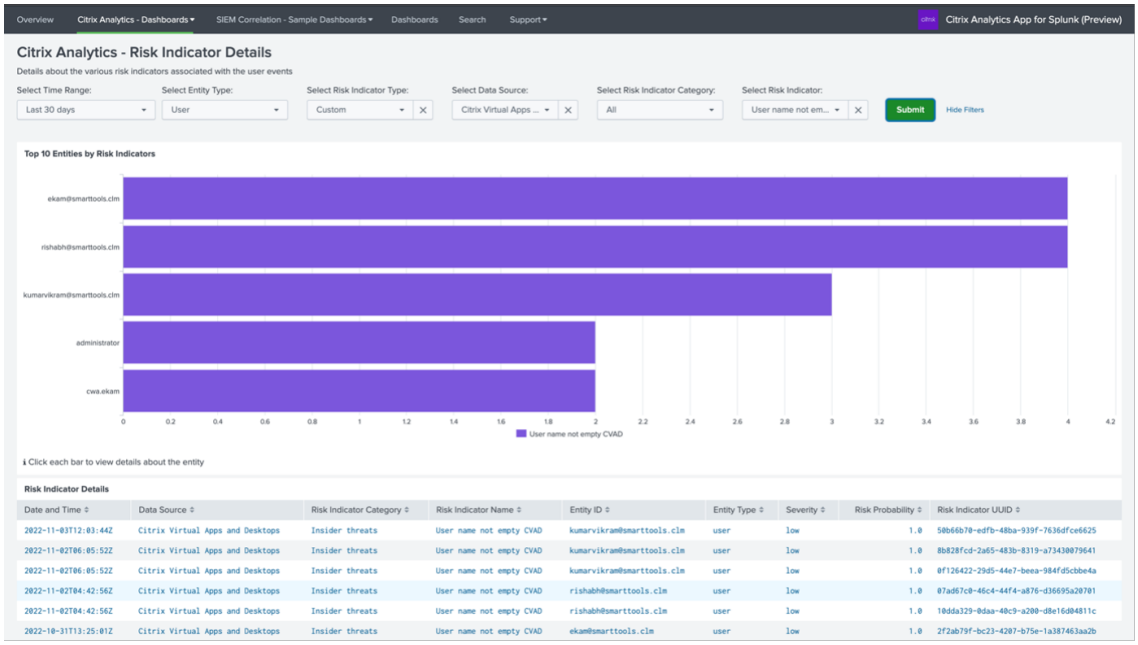
1. Cliquez sur l'onglet **Citrix Analytics** —**Tableau de bord** et sélectionnez l'option **Détails de l'indicateur de risque** dans la liste déroulante.



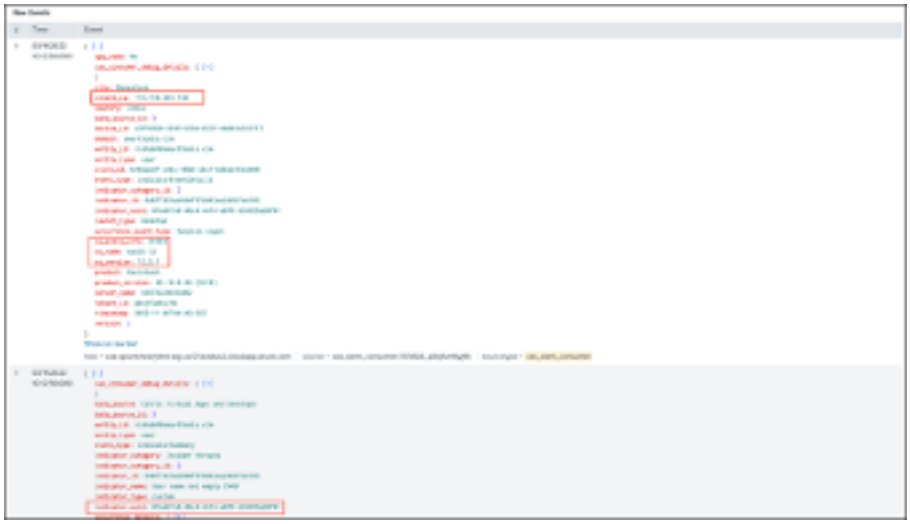
2. Filtrez le contenu de manière appropriée dans la liste déroulante et cliquez sur **Soumettre**.



3. Cliquez sur l'instance utilisateur pour obtenir les détails.



4. Vous pouvez consulter les **informations relatives à l'adresse IP et au système d'exploitationdu client** (nom, version, informations supplémentaires) au bas de cette page :

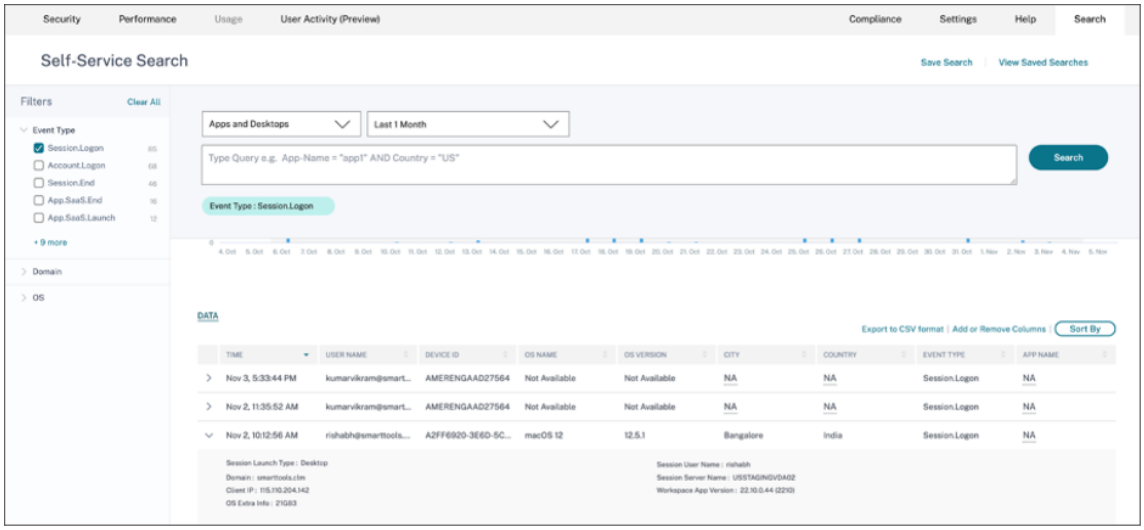


Événements de source de données

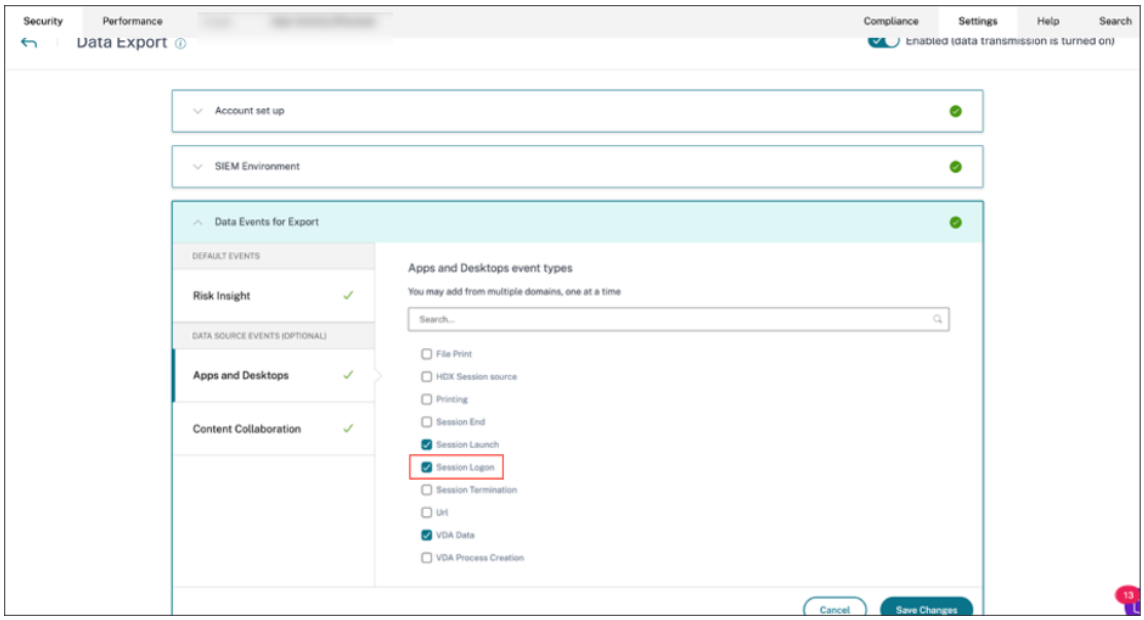
Une autre méthode pour obtenir les détails de l'adresse IP et du système d'exploitation du client dans votre environnement Splunk consiste à configurer les événements de source de données pour l'exportation. Cette fonctionnalité permet aux événements présents dans la vue Self-Service Search d'être transférés directement dans votre environnement Splunk. Pour plus d'informations sur la façon de configurer les types d'événements pour les Virtual Apps and Desktops à exporter vers SIEM, consultez les articles suivants :

- Événements de données exportés depuis Citrix Analytics for Security vers votre service SIEM.
- Événements de source de données

1. Accédez au tableau de **bord de Citrix Analytic for Security > Rechercher**. Sur cette page de recherche en libre-service, tous les types d'événements et les informations associées sont disponibles. Vous pouvez voir le type d'événement **Session.Logon à** titre d'exemple dans la capture d'écran suivante :



2. Configurez les événements **Session.Logon** in Data Source pour l'exportation et cliquez sur **Enregistrer** pour les intégrer à votre environnement Splunk.



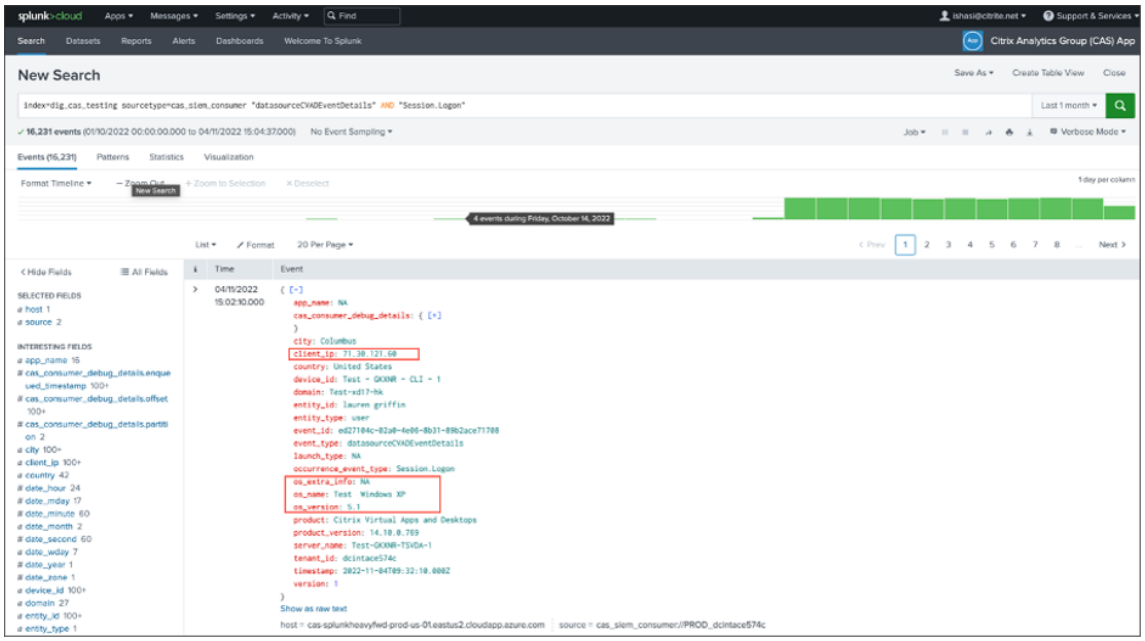
3. Accédez à Splunk, puis saisissez et exécutez la requête suivante :

```
index="<index you configured>" sourcetype="<sourcetype you
    configured>" "<tenant_id>" AND "datasourceCVADEventDetails" AND
```



```
        "Session.Logon"  AND "<user you're interested in>"

<!--NeedCopy-->
```

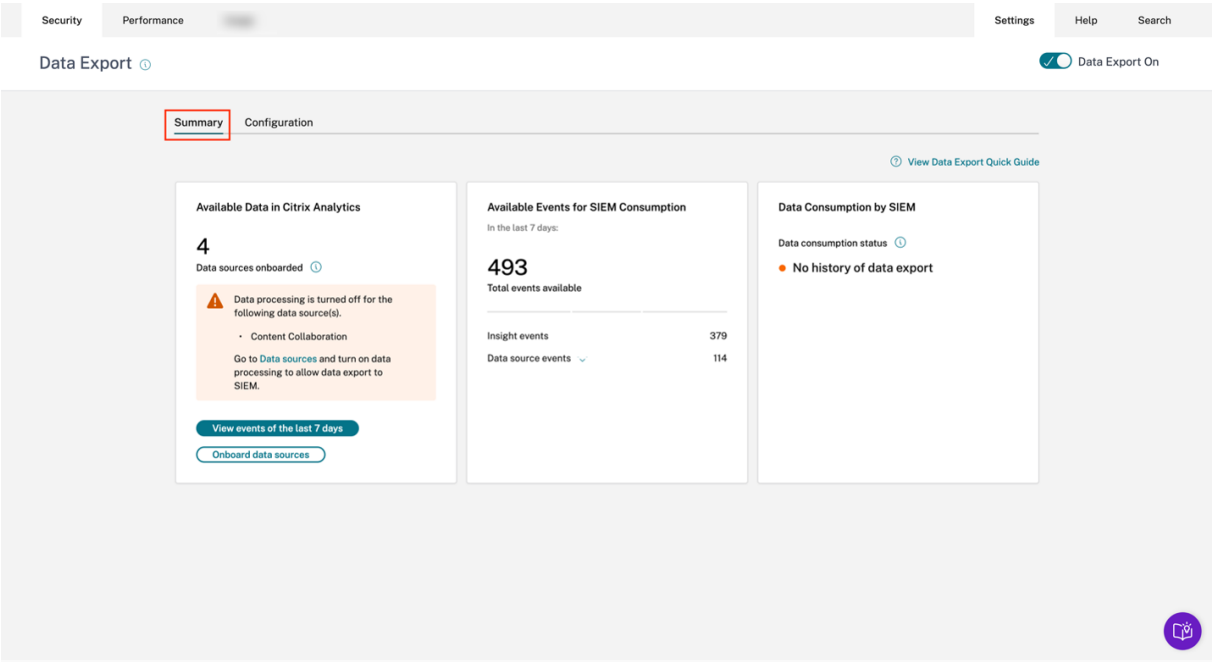
Les champs relatifs à l'adresse IP et au système d'exploitation du client sont surlignés.



Résolution des problèmes d'exportation de données

December 7, 2023

La vue Exportations de données pour la sécurité inclut un onglet **Résumé** qui aide les administrateurs à résoudre les problèmes liés à leur intégration SIEM avec Citrix Analytics. Le tableau de bord **récapitulatif** fournit une visibilité sur l'état et le flux des données en les guidant vers les points de contrôle qui facilitent le processus de résolution des problèmes.

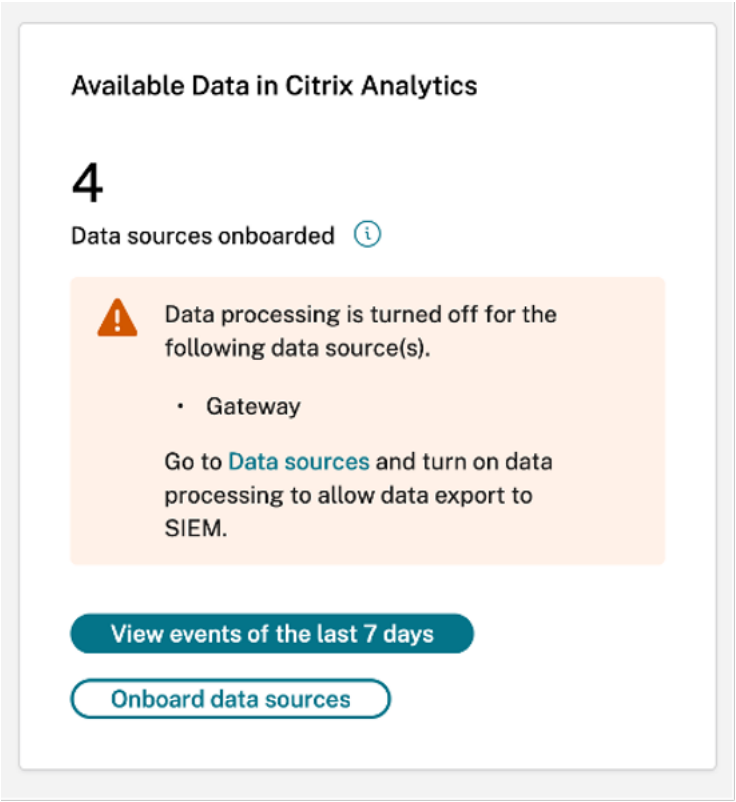


Onglet Résumé

L'onglet **Résumé** constitue la base du processus de résolution des problèmes en libre-service dans la vue Exportations de données. Il décrit votre configuration SIEM à l'aide de ces trois cartes :

- **Données disponibles dans Citrix Analytics** : cette carte indique l'état des configurations de vos sources de données.
- **Événements disponibles pour la consommation SIEM** : Cette carte indique le nombre d'événements prêts à être consommés par votre environnement SIEM.
- **Consommation de données par SIEM** : Cette carte affiche l'état du flux de données dans votre environnement SIEM.

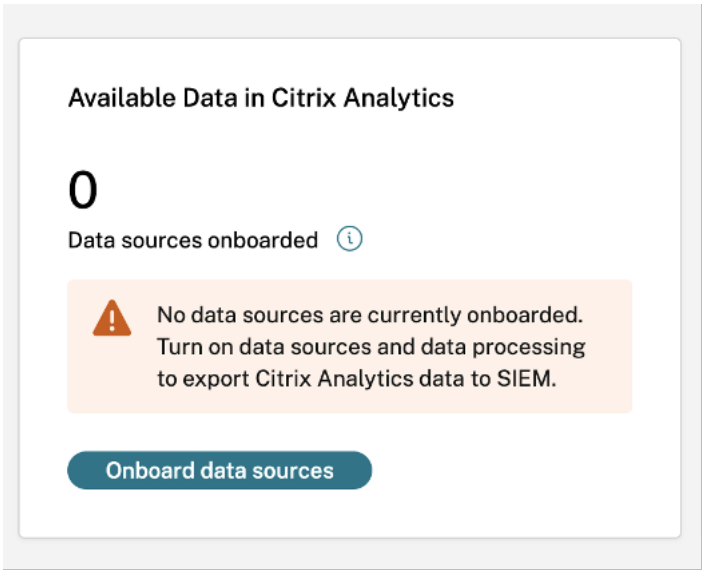
Données disponibles dans Citrix Analytics



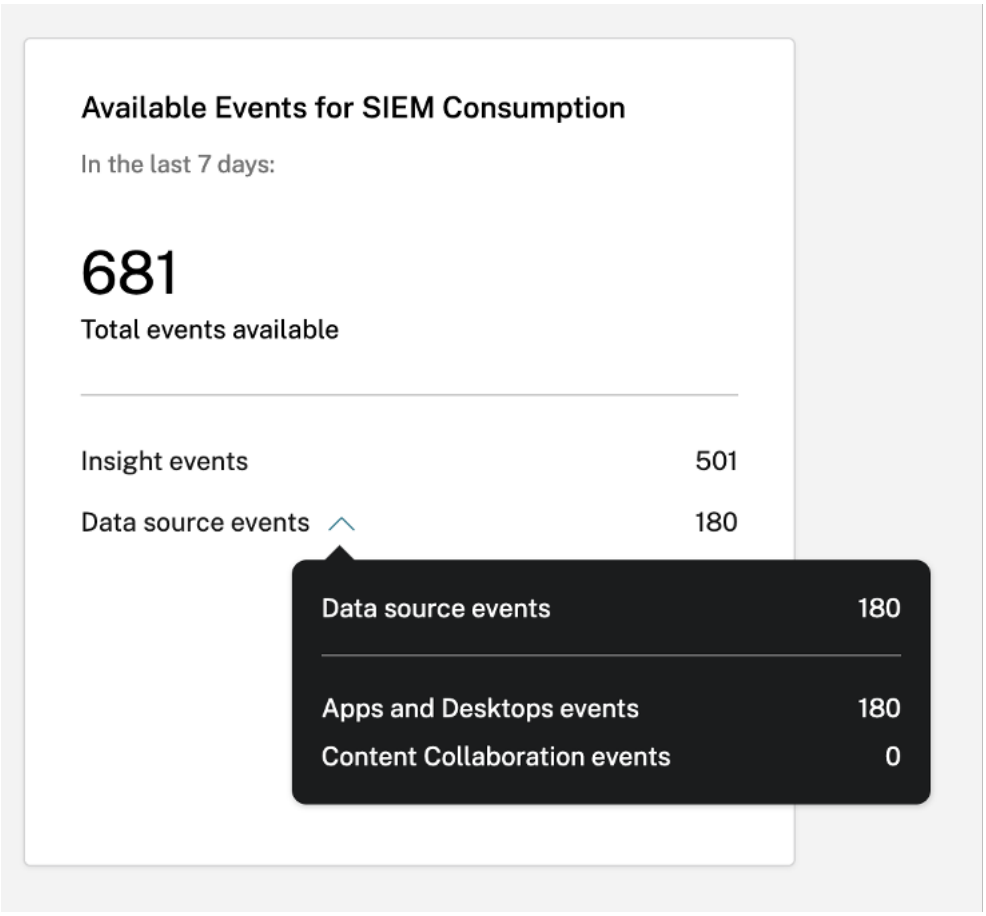
La fiche **Données disponibles dans Citrix Analytics** indique le nombre de sources de données pouvant éventuellement contribuer aux informations SIEM intégrées à Citrix Analytics for Security. Trois sources de données sont actuellement prises en charge pour les exportations de données : Apps and Desktops, Gateway et Secure Private Access. Même si ces sources de données ont été intégrées, l'exportation de données ne fonctionnera pas pour les sources de données dont le traitement des données est désactivé. Un message d'avertissement approprié tel que celui illustré dans l'image ci-dessus s'affiche lorsque de telles sources de données sont détectées.

Le bouton **Afficher les événements des 7 derniers jours** redirige l'administrateur vers la vue de recherche en libre-service, grâce à laquelle les administrateurs peuvent vérifier que les événements ont été transmis à Citrix Analytics for Security. Le bouton **Sources de données intégrées** redirige vers la vue Sources de données où vous pouvez suivre en détail le processus d'intégration.

S'il n'y a aucune source de données intégrée, un message d'avertissement approprié s'affiche, comme illustré dans la capture d'écran suivante :



Événements disponibles pour la consommation du SIEM



La carte **Available Events for SIEM Consumption** affiche le nombre d'événements Insight et Data Source ainsi que leur répartition qui devraient affecter votre environnement SIEM. Lors de l'exten-

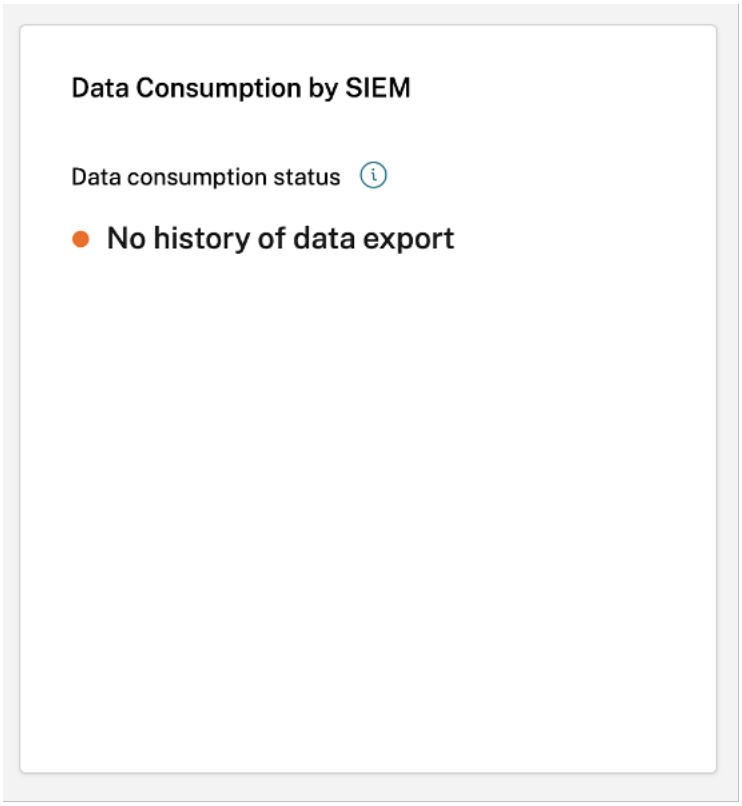
sion, une ventilation plus détaillée de chaque type d'événement de données à exporter est également disponible.

Consommation de données par SIEM

La fiche **Consommation de données par SIEM** décrit l'état du flux de données préparé par Citrix Analytics vers votre environnement SIEM. L'état de consommation des données est basé sur le mouvement du décalage au sein de votre rubrique **Kafka** . Lorsqu'elle est disponible, la carte affiche également l'horodatage de la dernière détection d'une consommation de données réussie. L'état de consommation des données et l'horodatage sont actualisés toutes les 10 minutes. Cliquez ici pour en savoir plus sur la gestion des groupes de consommateurs et de la compensation dans Kafka.

L'état de consommation des données peut prendre les états suivants :

1. **Consommation inactive**
    - **Aucun historique d'exportation de données** : cet état est représenté par un point orange pour indiquer qu'aucune donnée préparée par Citrix Analytics n'a jamais été transférée avec succès dans votre environnement SIEM.



Cela peut être dû à :

- Configuration de la source de données incorrecte/incomplète. La fiche **Données disponibles dans Citrix Analytics** peut être utilisée pour vérifier s'il existe suff-

isamment de sources de données et si le traitement des données est activé pour permettre l'exportation.

- Absence d'activité des utilisateurs. Le bouton **Afficher les événements des 7 derniers jours** de la carte **Données disponibles dans Citrix Analytics** peut être utilisé pour vérifier l'absence d'activité de l'utilisateur. En outre, la carte **Available Events for SIEM Consumption** peut être utilisée pour vérifier s'il existe des événements Insight ou Data Source préparés par Citrix Analytics pour être transférés dans votre SIEM.
- Configuration SIEM incorrecte/incomplète. Vérifiez que l'étape de configuration du compte dans l'onglet **Configuration** s'est bien déroulée. Une coche verte est visible à l'étape de configuration du compte si la configuration est terminée.

  Si l'état ne change pas même après une configuration de compte réussie, poursuivez la résolution des problèmes en vérifiant :

  * Problèmes de pare-feu ou paramètres SIEM mal configurés : voir Configuration de l'environnement SIEM.
  * Problèmes d'identification liés à la configuration du compte Kafka ou à votre environnement SIEM : voir Intégration SIEM à l'aide de Kafka.

- **Aucune consommation active détectée** : cet état indique qu'au moins au cours des 10 dernières minutes, les données n'ont pas été transférées correctement dans votre environnement SIEM. La carte affichera également l'horodatage du dernier mouvement de données réussi. Comme dans le cas **de l'absence d'historique d'exportation de données**, vous pouvez résoudre ce problème à l'aide des cartes **Available Data in Citrix Analytics** et **Available Events for SIEM Consumption**. Si l'activité des utilisateurs est suffisante et que le nombre d'événements disponibles augmente, il serait judicieux de se concentrer sur le dernier horodatage réussi pour vérifier si des modifications du pare-feu ou des rotations de mots de passe se sont produites après cet horodatage.

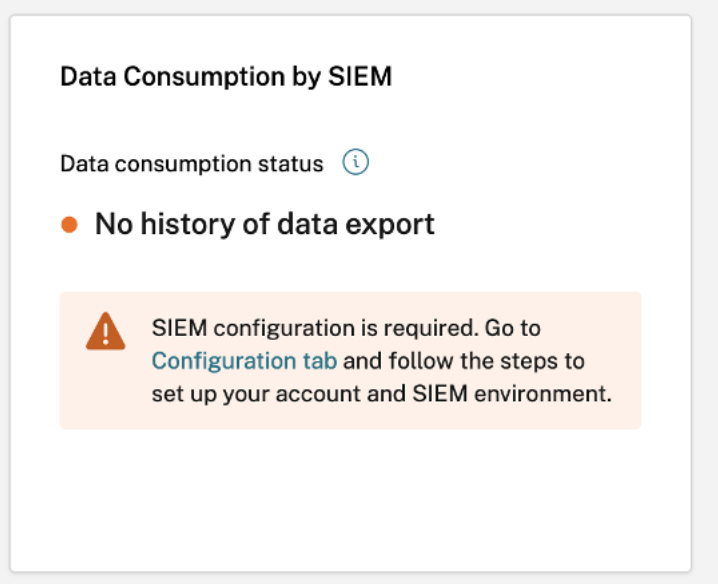
- **Exporté il y a plus de 7 jours** : cet état indique que la consommation active sur votre SIEM a été détectée pour la dernière fois il y a plus d'une semaine. Comme dans les deux états ci-dessus, utilisez les **données disponibles dans Citrix Analytics** et les cartes **Available Events for SIEM Consumption pour résoudre les problèmes de configuration de votre SIEM s'il s'agit de l'état de consommation** de données détecté.

> **Remarque**
>
> **Stratégie de conservation de Kafka** : les rubriques Kafka de Citrix Analytics con-

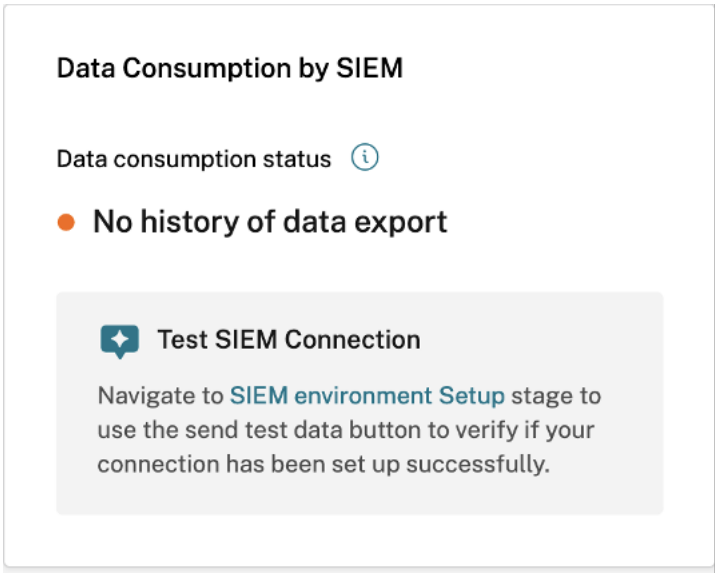
> servent les événements pendant une durée maximale de 7 jours uniquement. Pour éviter ou empêcher toute perte de données potentielle, il est recommandé de définir un intervalle entre les interrogations de données ne dépassant pas 7 jours.

En cas de consommation inactive, vous pouvez consulter les messages d'avertissement suivants pour vous aider à naviguer dans le processus de résolution des problèmes.

Comme indiqué dans le cas **Aucun historique d'exportation de données**, si la configuration du SIEM n'est pas terminée, aucune donnée ne circule dans l'environnement SIEM. L'utilisateur est donc redirigé vers l'onglet **Configuration** pour terminer la configuration du compte, comme illustré dans la capture d'écran suivante :

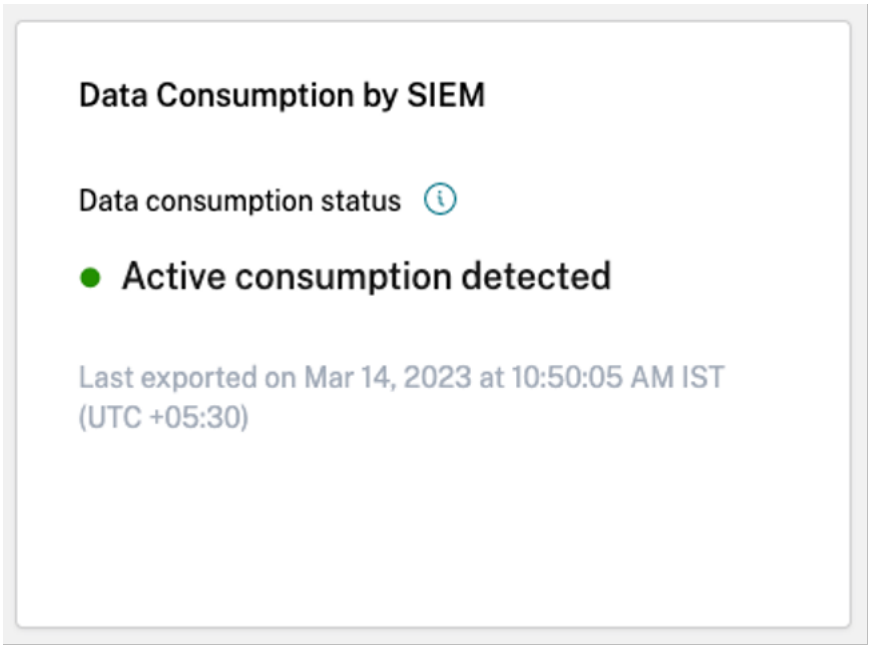


Si la configuration du SIEM est terminée, il se peut que les données ne circulent pas activement, comme indiqué dans l'état **Aucune consommation active détectée** ou **exportée il y a plus de 7 jours** . L'utilisateur est donc invité à accéder à la section **Génération d'événements** de test pour tester la connexion SIEM, comme indiqué dans le message d'avertissement suivant.



2. **Consommation active**

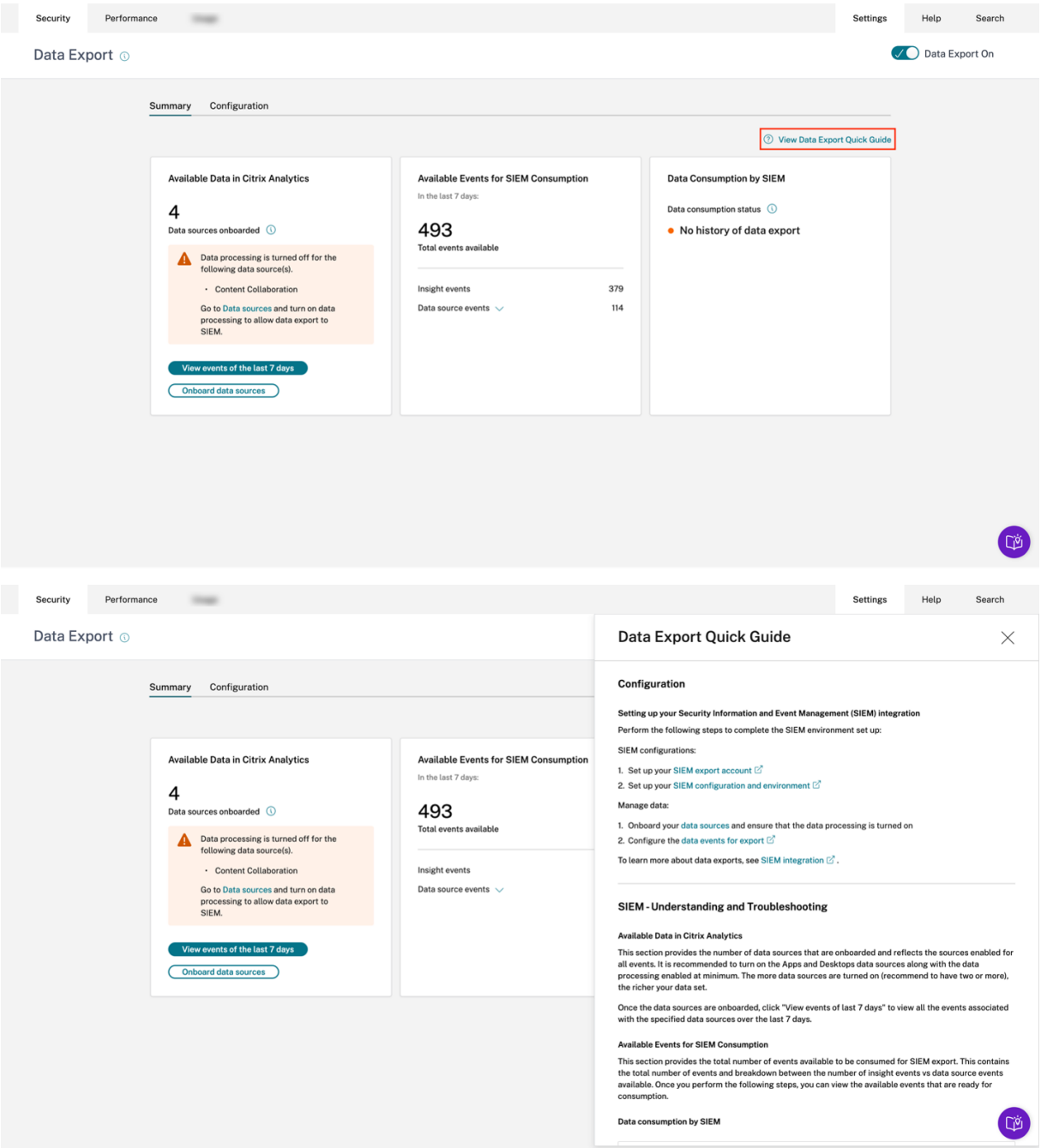
   - **Consommation active détectée** : Cet état indique qu'une consommation active a été détectée sur votre SIEM.

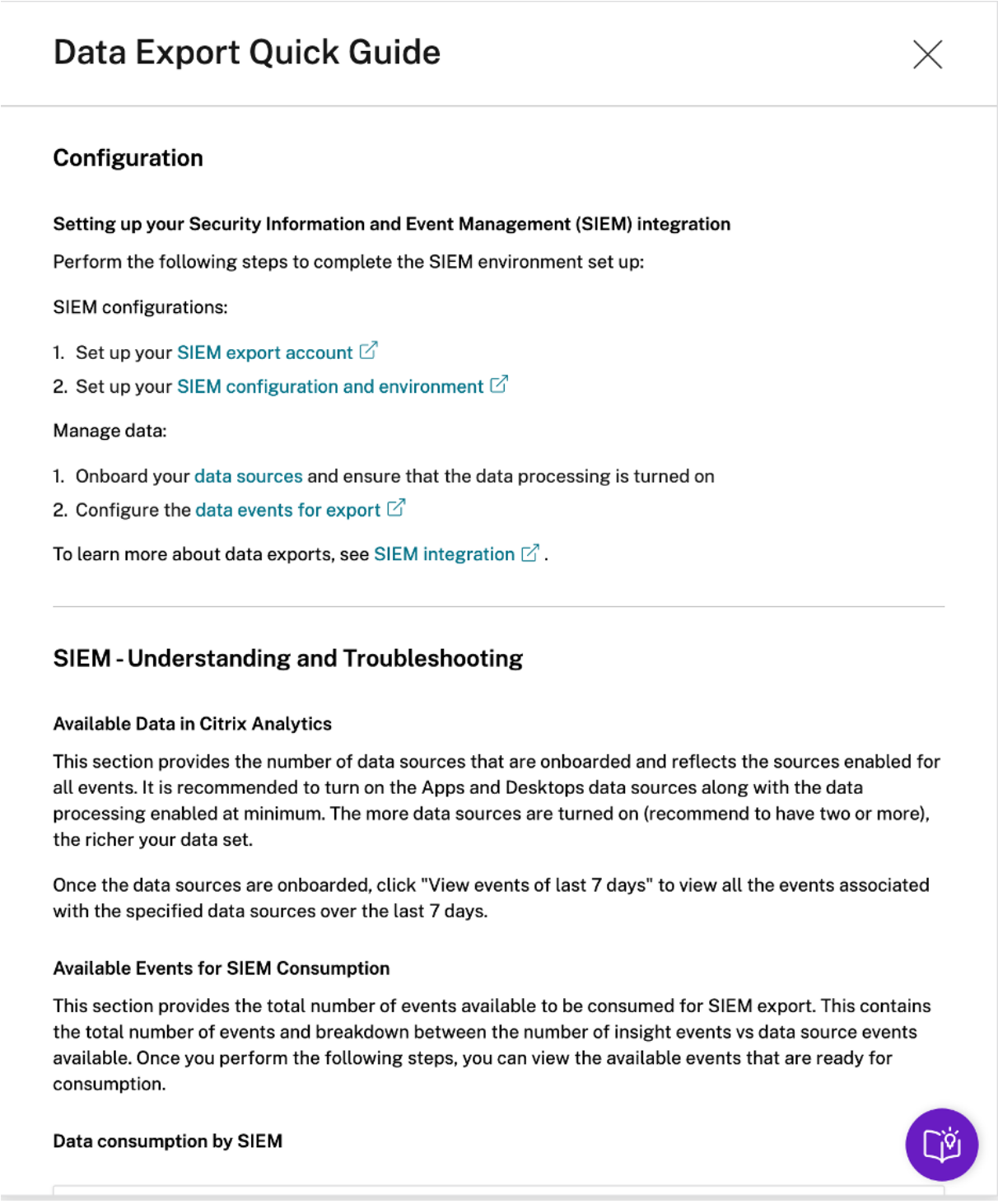


Guide rapide d'exportation de données

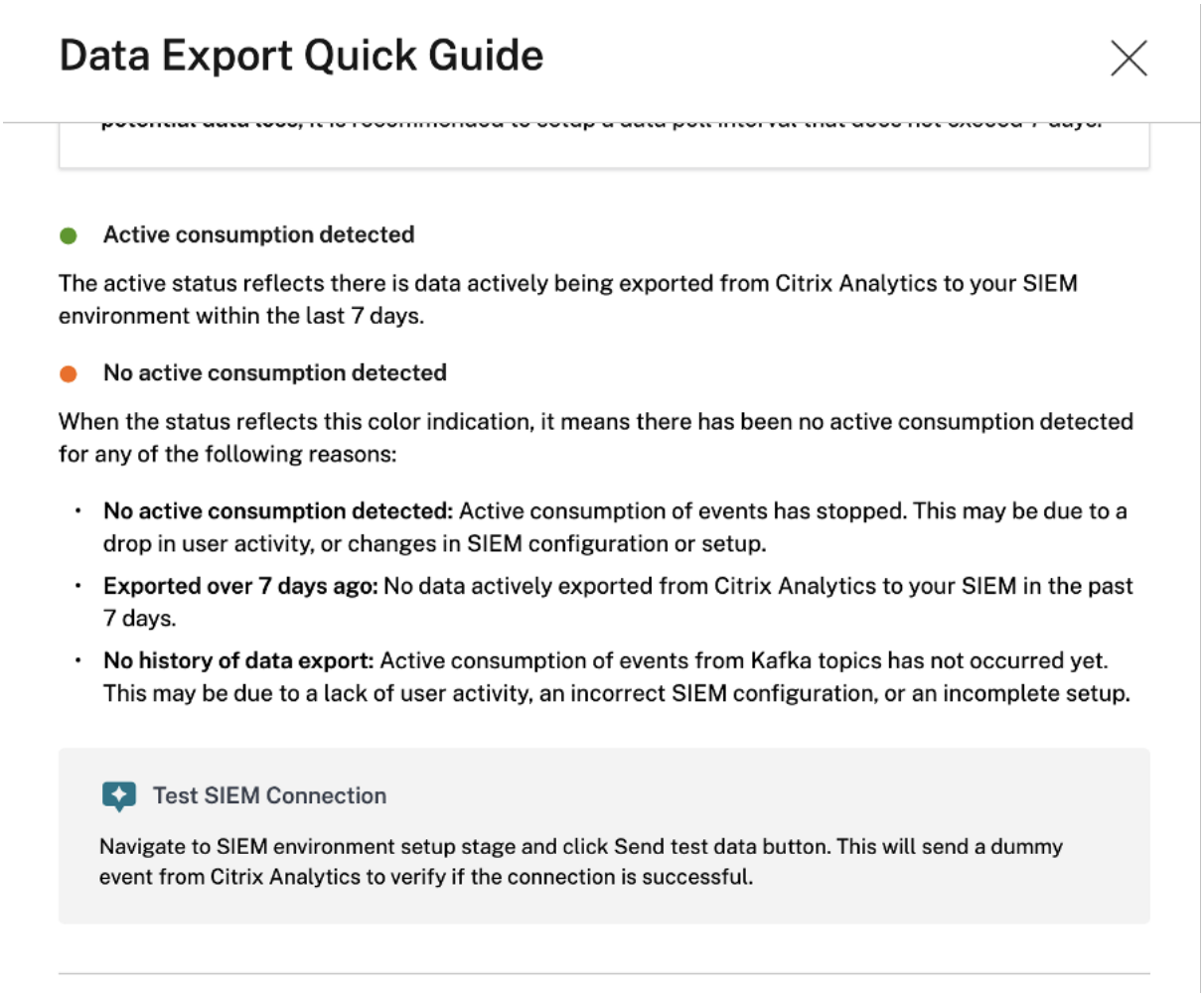
L'onglet **Résumé** est complété par la lame du **guide rapide d'exportation des données** pour faciliter le déploiement, la gestion et le dépannage de vos configurations SIEM. Outre un guide complet sur la vue Exportation de données à des fins de sécurité, le guide rapide inclut également des conseils utiles

sur la manière de configurer et de gérer votre environnement SIEM en fournissant des liens vers la documentation pertinente.



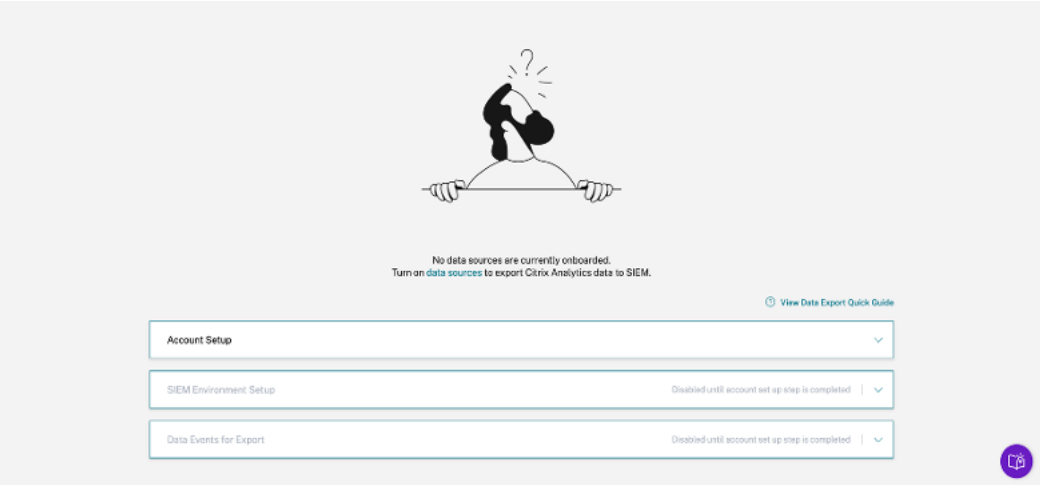


Il existe également une section **Test de connexion SIEM** dans la lame Quick Guide qui redirige l'utilisateur vers l'étape Test de connexion SIEM au sein de la phase de configuration de l'environnement SIEM. Cela permet à l'utilisateur de vérifier si l'intégration SIEM est elle-même interrompue, éliminant ainsi la possibilité de problèmes liés au traitement des événements par Citrix Analytics for Security. L'utilisateur peut ensuite corriger la connexion SIEM pour activer le flux de données.

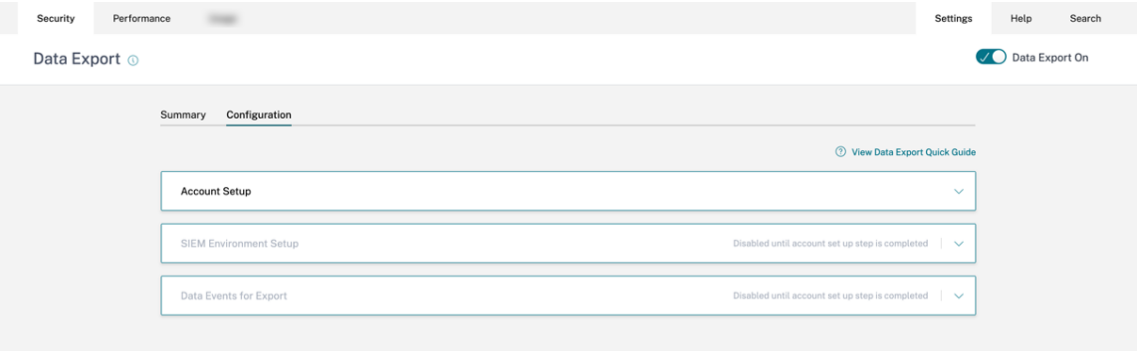


L'onglet **Configuration**, tout en guidant la configuration du déploiement, fournit également aux administrateurs des conseils utiles, des messages d'avertissement et des pièges courants lors de la configuration de leur SIEM. Des avertissements appropriés s'affichent lorsque :

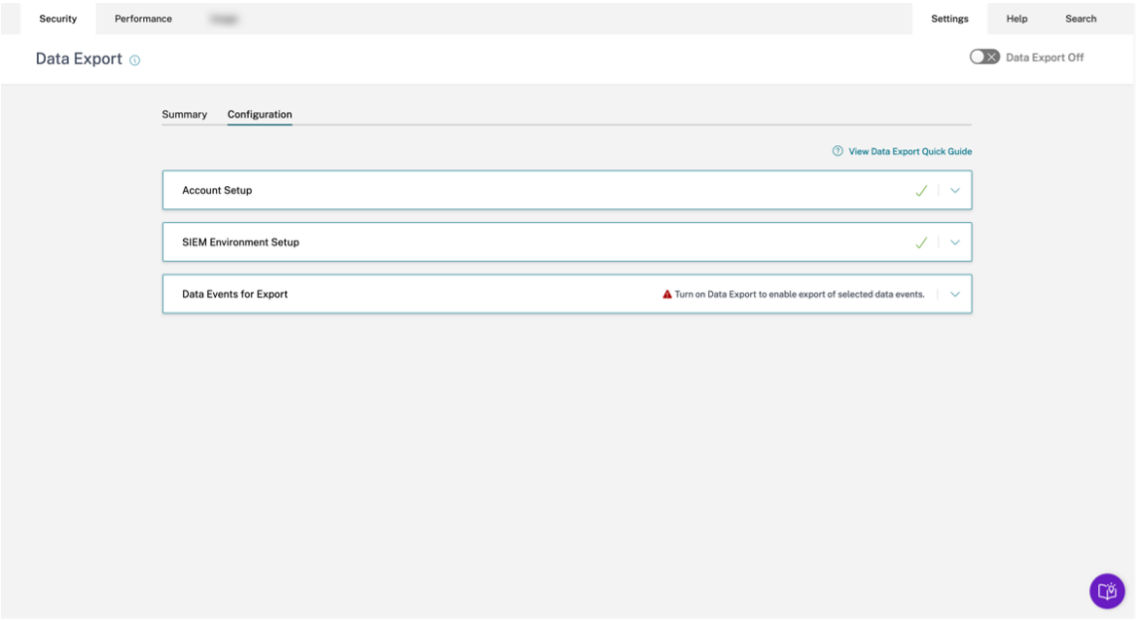
- Citrix Analytics détecte qu'aucune source de données n'a été intégrée. Il est recommandé d'intégrer Apps and Desktops pour collecter des données télémétriques en fonction de l'activité des utilisateurs. En l'absence de source de données intégrée, aucun flux de données n'est observé, même si la configuration de votre SIEM a peut-être été effectuée avec succès.



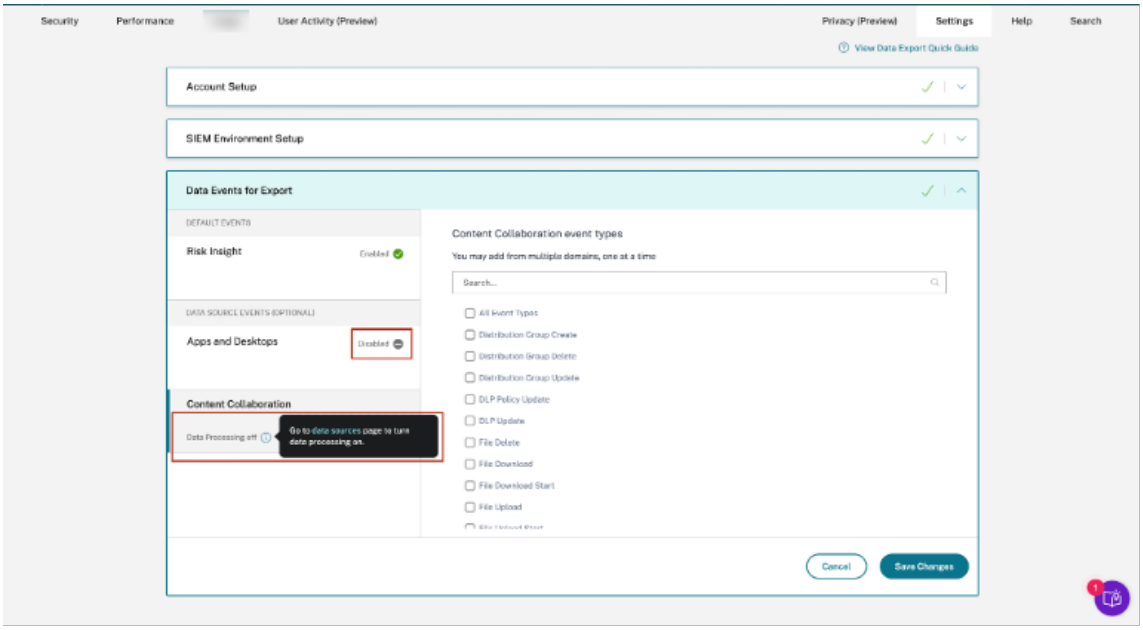
- Comme l'illustre l'image suivante, la configuration de l'environnement SIEM et les événements de données pour les étapes d'exportation sont désactivés jusqu'à ce que la configuration du compte soit terminée avec succès.



- Les exportations de données ont été désactivées. L'avertissement affiché à l'étape Data Events for Export sert de rappel pour permettre aux exportations de données d'effectuer toute modification.



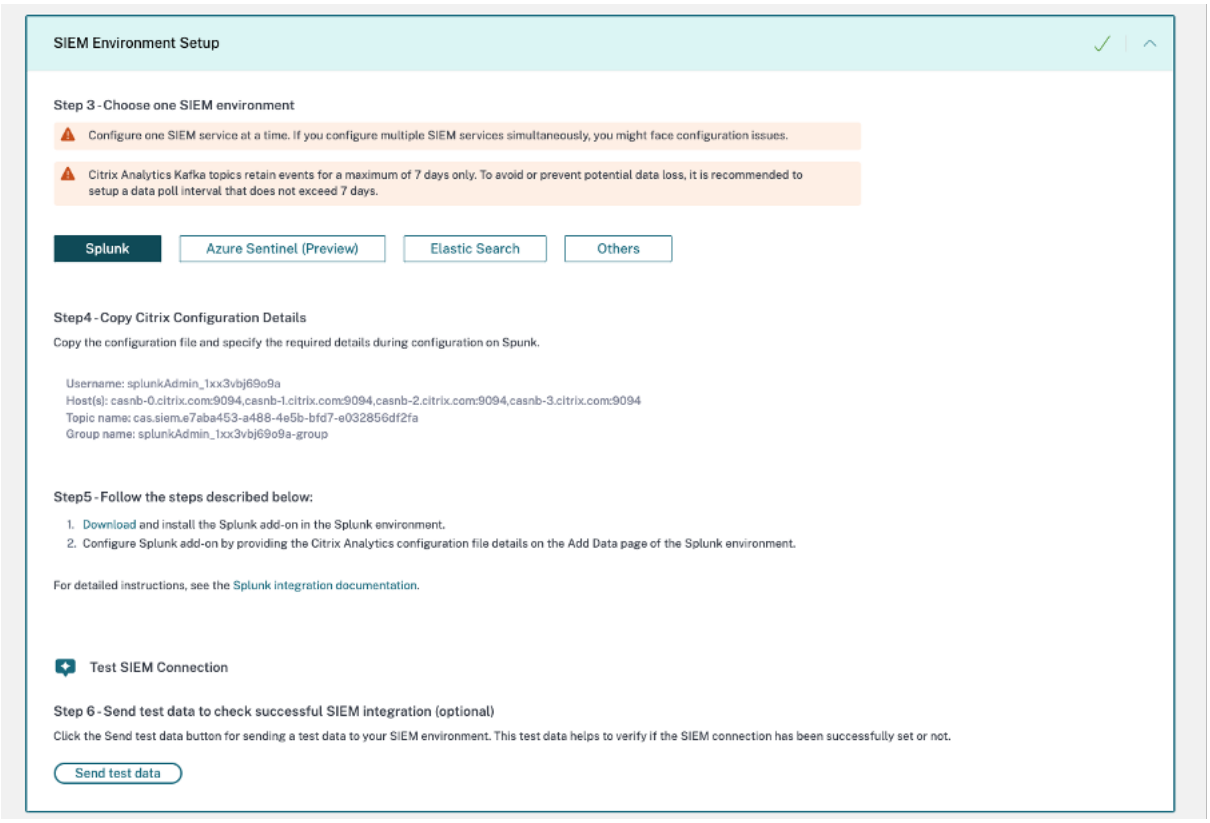
- Au stade Data Events for Export, si l'exportation de données pour une source de données particulière est désactivée, aucun événement de source de données n'est transmis au SIEM. Vous devez activer cette option en configurant et en sélectionnant les types d'événements de source de données souhaités. En outre, assurez-vous que le traitement des données pour la source de données correspondante est activé afin de garantir que les données parviennent à Citrix Analytics.



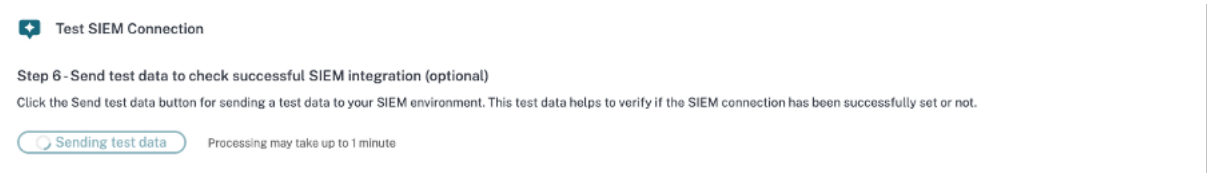
Génération d'événements de test

La génération d'événements de test est fournie dans le cadre de la phase de **configuration de l'environnement SIEM** afin d'améliorer l'expérience de dépannage. Une fois qu'un utilisateur a terminé la configuration du SIEM, la génération d'événements de test permet de tester rapidement la connexion SIEM en envoyant un événement de test directement dans la rubrique Kafka sur l'exportation de données SIEM du client.

Il permet également aux nouveaux utilisateurs de tester rapidement leur intégration SIEM avec Citrix Analytics sans avoir à intégrer explicitement une nouvelle source de données et à générer ensuite une activité utilisateur.

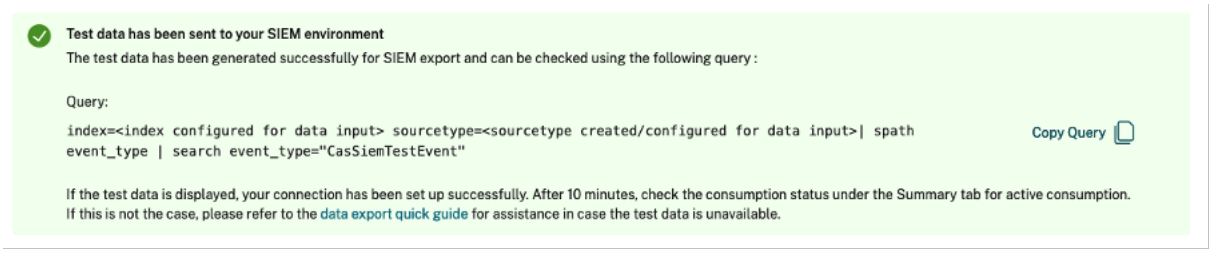


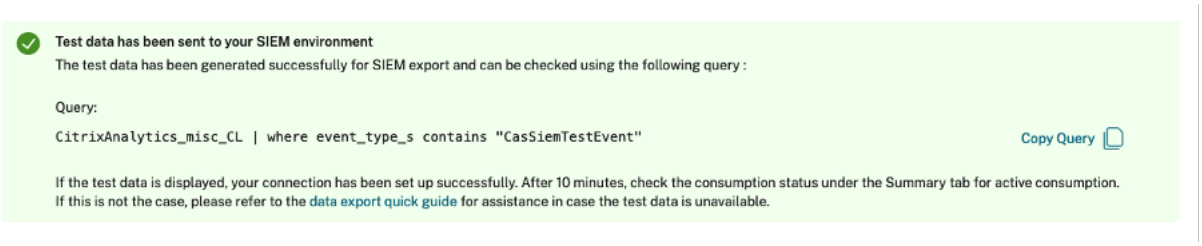
Pour tester cette fonctionnalité, l'utilisateur doit cliquer sur le bouton **Envoyer les données de test** . Cela génère un événement de test fictif et l'envoie à la rubrique Kafka d'exportation de données SIEM du client. Ce processus de génération d'événements de test peut prendre jusqu'à 1 minute, comme le montre la capture d'écran suivante :



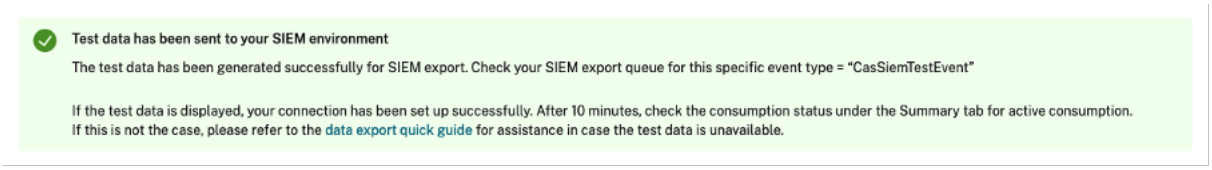
Si les données de l'événement de test sont correctement écrites dans la rubrique client Kafka, un

message de réussite s'affiche, indiquant que la connexion SIEM est réussie. Selon l'environnement que vous avez choisi (Splunk et Sentinel), les administrateurs peuvent copier la requête et vérifier la présence de l'événement de test dans leur environnement SIEM.

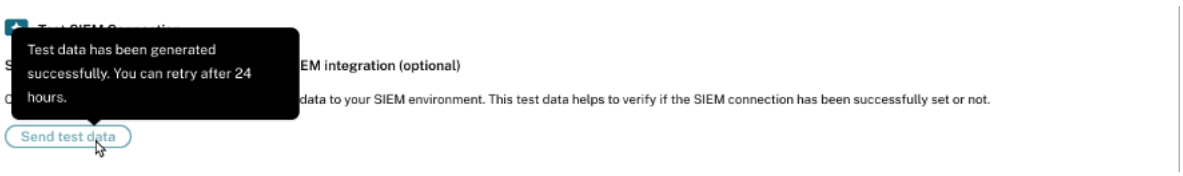




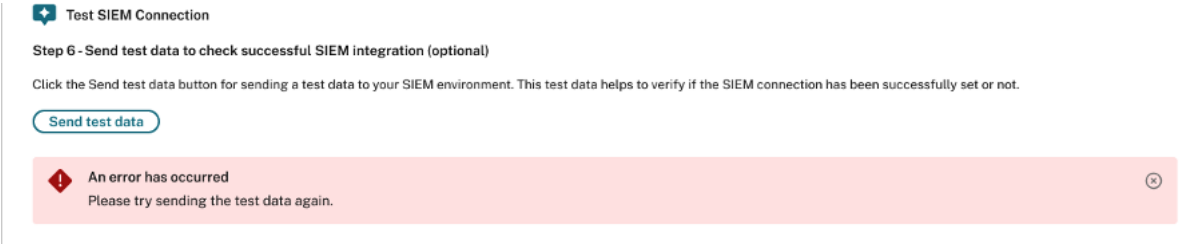
Pour Elasticsearch et les autres environnements, le message de réussite suivant s'affiche.



> **Remarque**
>
> Une fois qu'un événement de test est généré, le bouton **Envoyer les données de test** est désactivé pendant les 24 heures suivantes, et les utilisateurs voient apparaître la fenêtre contextuelle suivante lorsqu'ils passent la souris sur le bouton. 24 heures après le dernier horodatage de réussite, le bouton est activé pour permettre aux utilisateurs de tester à nouveau la fonctionnalité.



Si les données de l'événement de test ne sont pas correctement écrites dans la rubrique client Kafka, un message d'échec s'affiche, comme illustré dans la capture d'écran suivante. L'utilisateur peut renvoyer les données pour tester la connexion.



Alerte e-mail SIEM

Citrix Analytics envoie des alertes par e-mail pour informer les administrateurs des scénarios susceptibles d'entraîner une interruption du flux de données vers leur environnement SIEM. Il contient des informations situationnelles sur les activités susceptibles d'entraîner une perte de données temporaire ou permanente liée à la sécurité. Il permet également de suivre le processus de résolution des problèmes en libre-service pour l'exportation de données SIEM.

Voici quelques propriétés importantes de cet ensemble d'alertes par e-mail pour vous aider à les retrouver dans votre boîte de réception :

- L'e-mail est distribué aux administrateurs Citrix Cloud, aux administrateurs complets de Security, aux administrateurs en lecture seule Security et aux administrateurs en lecture seule Security and Performance.
- L'expéditeur est Citrix Cloud **donotreplynotifications@citrix.com**.
- L'objet du message est le suivant :
  - **Alerte d'exportation de données SIEM - Le mot de passe a été réinitialisé** pour les alertes par e-mail de réinitialisation du mot de passe.
  - **Alerte d'exportation de données SIEM : le flux de données s'est arrêté en raison** d' alertes par e-mail d'interruption du flux de données.

Comment activer les notifications par e-mail ?

Si vous êtes administrateur Citrix Cloud et que vous disposez d'autorisations d'accès personnalisées (Security Full Admin, Security Read Only Admin, Security et Performance Read Only) pour gérer Security Analytics, les notifications par e-mail sont toujours activées pour votre compte Citrix Cloud. Par défaut, les notifications hebdomadaires par e-mail sont envoyées à la liste par défaut des Citrix Security Administrators. Vous pouvez également modifier la liste de distribution qui reçoit cette alerte. Pour plus d'informations, consultez la section .

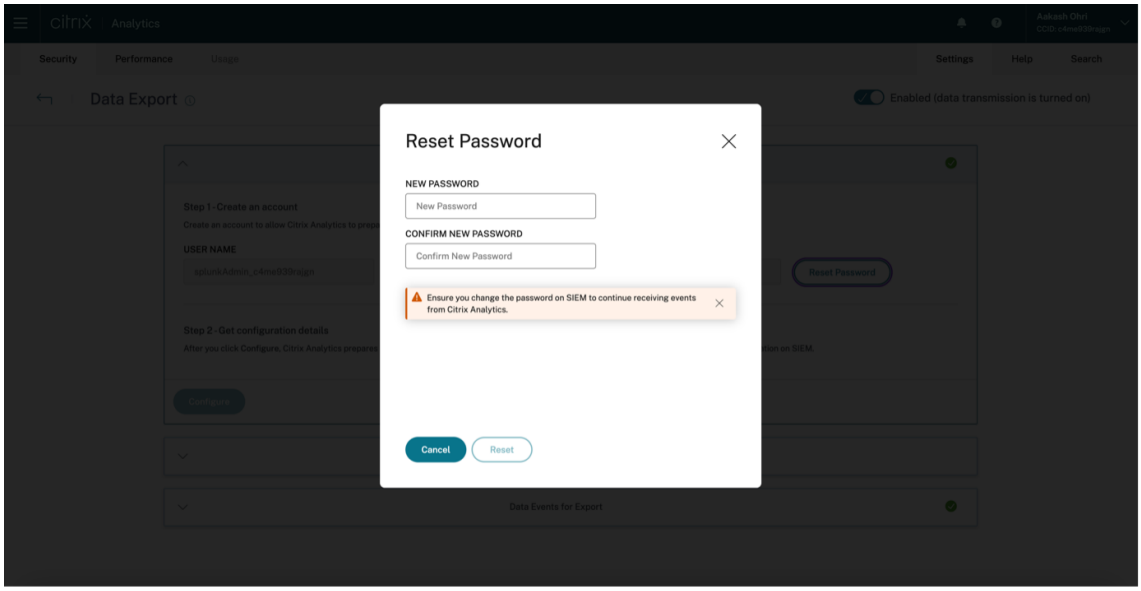
Si vous êtes un administrateur Citrix Cloud disposant d'autorisations d'accès personnalisées (administrateur complet de sécurité, administrateur en lecture seule de sécurité, lecture seule de sécurité

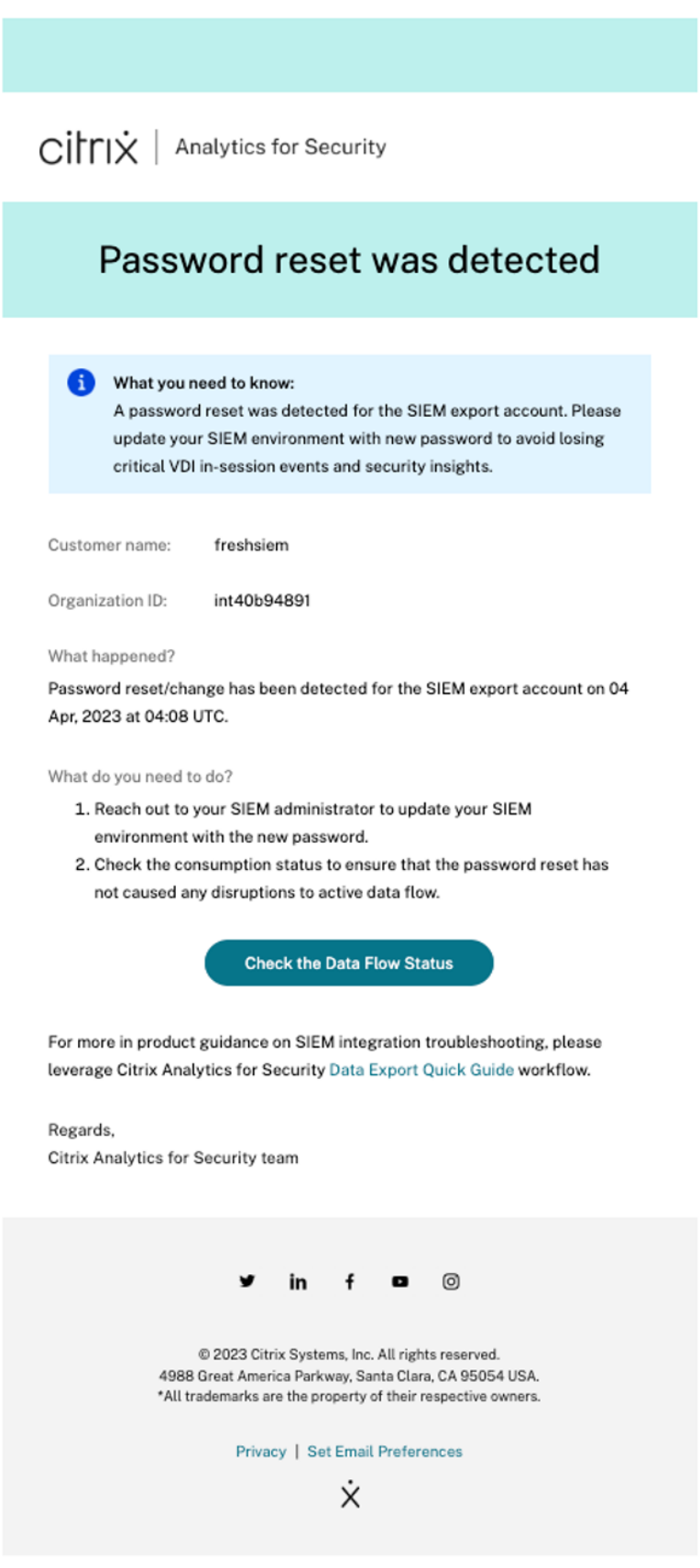
et de performances) pour gérer Security Analytics, les notifications par e-mail sont toujours activées pour votre compte Citrix Cloud.

Types d'alerte e-mail SIEM

1. **Alerte e-mail de réinitialisation du mot de passe SIEM**

   L'e-mail d'alerte de réinitialisation du mot de passe SIEM est reçu lorsque le mot de passe du compte est réinitialisé via la page Exportations de données. La réinitialisation du mot de passe SIEM uniquement sur l'interface utilisateur de Citrix Analytics peut entraîner une incompatibilité du mot de passe avec celui configuré sur votre SIEM. Cela entraîne une perturbation du flux de données. Cette alerte par e-mail contient l'heure à laquelle le mot de passe a été réinitialisé. Si le flux de données s'arrête, vous pouvez accéder à l'onglet **Résumé**, vérifier si l'horodatage du « dernier export à » est proche de l'horodatage de réinitialisation du mot de passe, et ainsi relayer les modifications de mot de passe nécessaires. Cela raccourcit le processus de débogage et vous aide à rétablir un flux de données efficace dans votre environnement SIEM en un rien de temps.





citrix | Analytics for Security

Password reset was detected

What you need to know:
A password reset was detected for the SIEM export account. Please update your SIEM environment with new password to avoid losing critical VDI in-session events and security insights.

Customer name: freshsiem

Organization ID: int40b94891

What happened?

Password reset/change has been detected for the SIEM export account on 04 Apr, 2023 at 04:08 UTC.

What do you need to do?

1. Reach out to your SIEM administrator to update your SIEM environment with the new password.
2. Check the consumption status to ensure that the password reset has not caused any disruptions to active data flow.

Check the Data Flow Status

For more in product guidance on SIEM integration troubleshooting, please leverage Citrix Analytics for Security Data Export Quick Guide workflow.

Regards,
Citrix Analytics for Security team

2. **Alerte par e-mail d'interruption du flux de données pendant 24 heures**

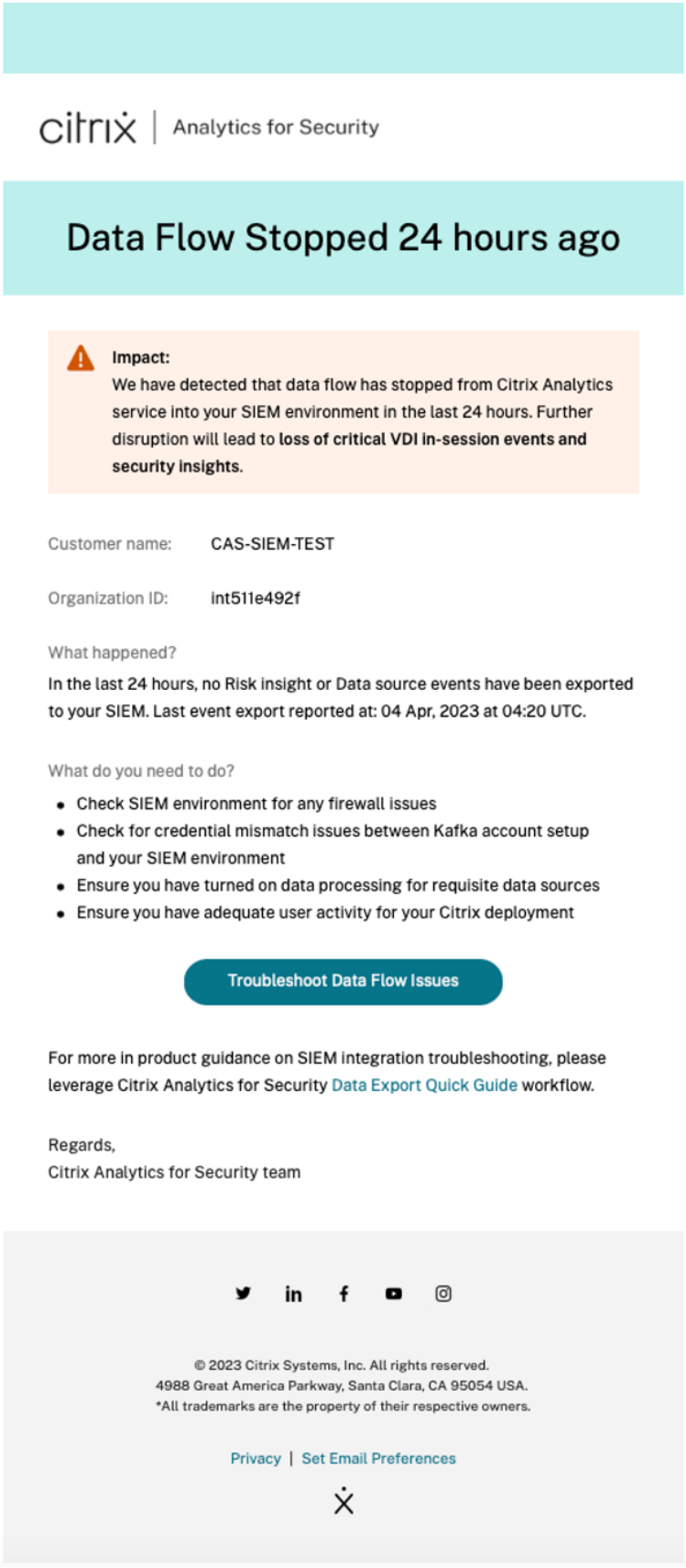
   Cette alerte par e-mail est envoyée lorsque le flux de données du service Citrix Analytics vers votre environnement SIEM est interrompu pendant plus de 24 heures. L'e-mail inclut l'heure à laquelle le dernier événement a été exporté ainsi que des conseils de dépannage utiles qui peuvent être appliqués pour rétablir le flux de données. Ce serait le bon moment pour rétablir rapidement le flux de données afin de ne pas perdre les données sécurisées.

3. **Alerte e-mail d'interruption du flux de données pendant 7 jours**

   Cette alerte par e-mail est envoyée lorsque le flux de données du service Citrix Analytics vers votre environnement SIEM est interrompu pendant plus de 7 jours. Étant donné que la période de conservation du sujet Kafka du client est de 7 jours, il est essentiel de suivre les conseils de résolution des problèmes et de suivre le guide rapide disponible sur la page **Exportations de données** pour ne pas perdre d'autres données, car cet e-mail met en garde contre une situation de perte permanente des informations de sécurité.

4. **Alerte par e-mail d'interruption du flux de données pendant 30 jours**

   Cette alerte par e-mail est envoyée lorsque le flux de données du service Citrix Analytics vers votre environnement SIEM est interrompu pendant plus de 30 jours. À ce jour, le client a perdu des données sécurisées et il est impératif d'utiliser les fonctionnalités de dépannage pour rétablir le flux dès que possible.



citrix | Analytics for Security

Data Flow Stopped 24 hours ago

Impact:
We have detected that data flow has stopped from Citrix Analytics service into your SIEM environment in the last 24 hours. Further disruption will lead to **loss of critical VDI in-session events and security insights.**

Customer name: CAS-SIEM-TEST

Organization ID: int511e492f

What happened?

In the last 24 hours, no Risk insight or Data source events have been exported to your SIEM. Last event export reported at: 04 Apr, 2023 at 04:20 UTC.

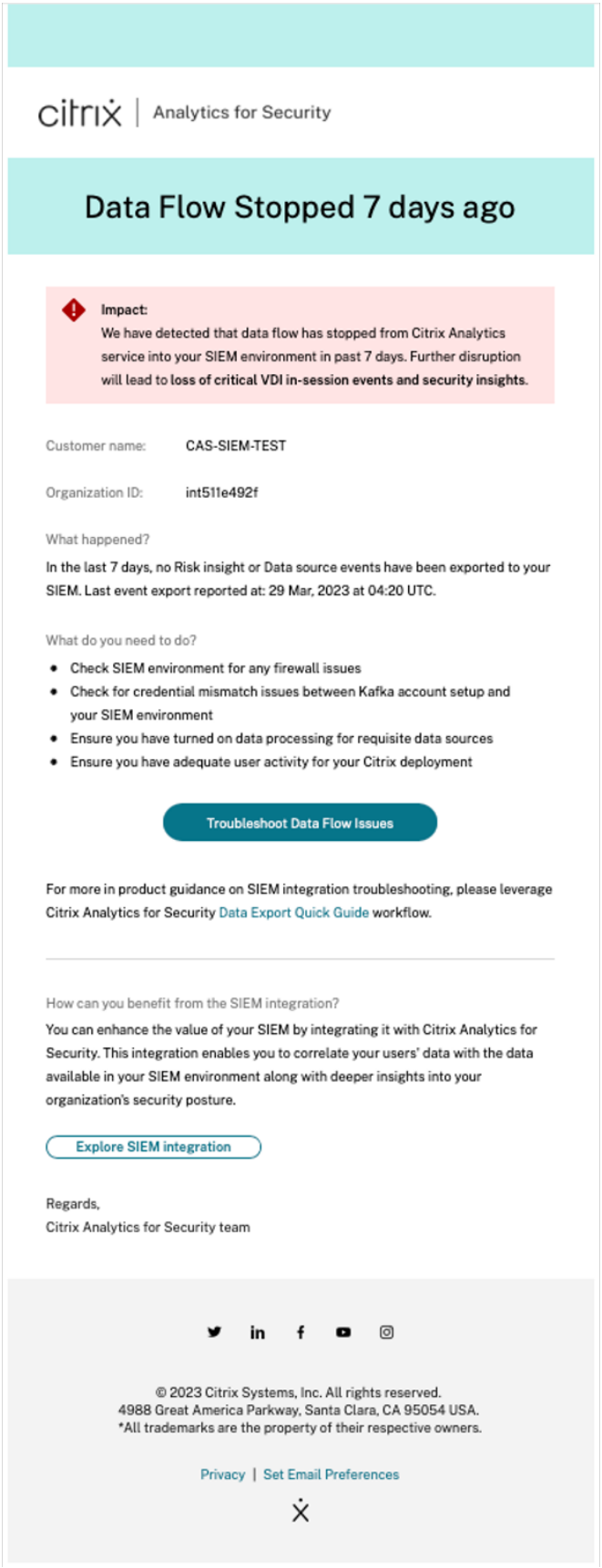
What do you need to do?

- Check SIEM environment for any firewall issues
- Check for credential mismatch issues between Kafka account setup and your SIEM environment
- Ensure you have turned on data processing for requisite data sources
- Ensure you have adequate user activity for your Citrix deployment

Troubleshoot Data Flow Issues

For more in product guidance on SIEM integration troubleshooting, please leverage Citrix Analytics for Security Data Export Quick Guide workflow.

Regards,
Citrix Analytics for Security team



citrix | Analytics for Security

Data Flow Stopped 7 days ago

Impact:
We have detected that data flow has stopped from Citrix Analytics service into your SIEM environment in past 7 days. Further disruption will lead to **loss of critical VDI in-session events and security insights.**

Customer name: CAS-SIEM-TEST

Organization ID: int511e492f

What happened?

In the last 7 days, no Risk insight or Data source events have been exported to your SIEM. Last event export reported at: 29 Mar, 2023 at 04:20 UTC.

What do you need to do?

- Check SIEM environment for any firewall issues
- Check for credential mismatch issues between Kafka account setup and your SIEM environment
- Ensure you have turned on data processing for requisite data sources
- Ensure you have adequate user activity for your Citrix deployment

Troubleshoot Data Flow Issues

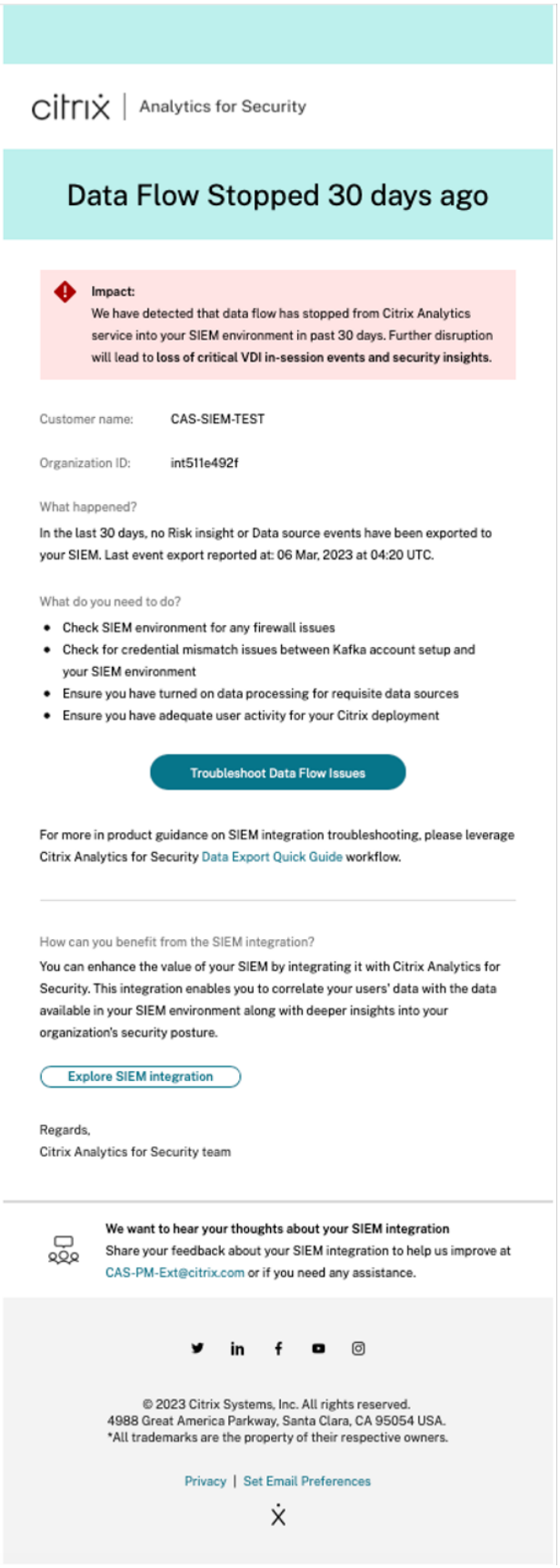
For more in product guidance on SIEM integration troubleshooting, please leverage Citrix Analytics for Security Data Export Quick Guide workflow.

How can you benefit from the SIEM integration?

You can enhance the value of your SIEM by integrating it with Citrix Analytics for Security. This integration enables you to correlate your users' data with the data available in your SIEM environment along with deeper insights into your organization's security posture.

Explore SIEM integration

Regards,
Citrix Analytics for Security team



citrix | Analytics for Security

Data Flow Stopped 30 days ago

Impact:
We have detected that data flow has stopped from Citrix Analytics service into your SIEM environment in past 30 days. Further disruption will lead to **loss of critical VDI in-session events and security insights.**

Customer name: CAS-SIEM-TEST

Organization ID: int511e492f

What happened?

In the last 30 days, no Risk insight or Data source events have been exported to your SIEM. Last event export reported at: 06 Mar, 2023 at 04:20 UTC.

What do you need to do?

- Check SIEM environment for any firewall issues
- Check for credential mismatch issues between Kafka account setup and your SIEM environment
- Ensure you have turned on data processing for requisite data sources
- Ensure you have adequate user activity for your Citrix deployment

Troubleshoot Data Flow Issues

For more in product guidance on SIEM integration troubleshooting, please leverage Citrix Analytics for Security Data Export Quick Guide workflow.

How can you benefit from the SIEM integration?

You can enhance the value of your SIEM by integrating it with Citrix Analytics for Security. This integration enables you to correlate your users' data with the data available in your SIEM environment along with deeper insights into your organization's security posture.

Explore SIEM integration

Regards,
Citrix Analytics for Security team

We want to hear your thoughts about your SIEM integration
Share your feedback about your SIEM integration to help us improve at CAS-PM-Ext@citrix.com or if you need any assistance.

Exemples de signatures Sigma pour Security Insights

December 7, 2023

Cette page contient des exemples de requêtes destinées à aider les administrateurs à obtenir des résultats significatifs à l'aide de Citrix Security Analytics.

Ces exemples couvrent les risques relevant des catégories suivantes :

- Points de terminaison compromis
- Menaces internes
- Exfiltration de données

Comment utiliser ces exemples

Afficher la source de données et activer le traitement des données

Pour afficher la source de données, cliquez sur **Paramètres > Sources de données > Sécurité** dans l'interface graphique de Citrix Analytics. La fiche de site de l'**application Apps and Desktops- Workspace** apparaît sur la page **Sources de données** . Cliquez **sur Activer le traitement des données** pour permettre à Citrix Analytics de commencer à traiter les données de cette source de données.

Citrix Analytics for Security envoie les deux types de données d'analyse des risques suivants à votre service SIEM :

- Événements d'analyse des risques (exportations par défaut)
- Événements relatifs aux sources de données (exportations facultatives)

Dans le cadre de votre environnement SIEM, les sources de données relatives aux événements liés à l'analyse des risques sont disponibles et toujours activées par défaut. Pour plus d'informations, consultez la section Événements liés aux données exportés depuis Citrix Analytics for Security vers votre service SIEM.

Vous pouvez utiliser des signatures CAS ou Sigma pour vérifier tout événement utilisateur particulier au sein de vos sources de données. Les requêtes CAS sont accessibles via la page de recherche en libre-service de votre interface graphique Citrix Analytics. Les signatures Sigma sont écrites dans un format simple ou convivial, ce qui les rend compatibles avec divers environnements SIEM.

Utilisation de requêtes CAS

Vous pouvez utiliser la requête CAS sur la page de recherche en **libre-service pour rechercher** et filtrer les événements utilisateur reçus de différentes sources de données. Cliquez sur **Rechercher**

dans votre interface graphique Citrix Analytics et saisissez la requête dans la zone de recherche. Pour plus de détails, consultez Comment utiliser la recherche en libre-service.

Vous pouvez également créer des indicateurs de risque personnalisés à l'aide des modèles existants. Pour créer un indicateur de risque personnalisé, accédez à **Sécurité > Indicateurs de risque personnalisés > Créer un indicateur**. Pour plus de détails, voir Création d'un indicateur de risque personnalisé.

Utiliser les signatures Sigma

Sigma est un format de signature ouverte convivial permettant de créer des requêtes textuelles que les analystes peuvent utiliser pour décrire les événements du journal, ce qui facilite la rédaction des détections. Il existe différentes manières de convertir une signature Sigma dans le langage de requête de votre outil SIEM.

- Vous pouvez utiliser les outils CLI et les SDK Python proposés par Sigma. Pour plus d'informations sur la signature Sigma, voir Utilisation des règles.
- Vous pouvez utiliser des outils publics tels que le moteur de traduction Sigma d'uncoder.io, qui propose un niveau gratuit.

Reportez-vous aux différents cas d'utilisation des indicateurs personnalisés suivants pour obtenir les différentes informations sur les risques :

- Navigateur non autorisé
- Système d'exploitation non autorisé
- Versions non autorisées de l'application Workspace
- Systèmes d'exploitation non autorisés en dehors de la liste des systèmes autorisés
- Adresse IP ou sous-réseaux non autorisés
- Applications virtuelles non autorisées
- Noms de bureau inhabituels
- Surveillez une application spécifique
- Impression à partir d'applications SaaS
- Utilisation du presse-papiers sur les applications SaaS

Points de terminaison compromis

November 16, 2023

Navigateur non autorisé

Cela se produit lorsqu'un utilisateur tente d'accéder à du contenu à partir d'un type ou d'une version de navigateur qui n'est pas autorisé par la stratégie informatique de l'entreprise ou en raison de failles de sécurité.

Détails

Source de données : applications et ordinateurs de bureau (application Workspace)

Requête CAS

```
Event-Type = "Session.Logon" AND Browser-Name !~ "<Browser-Name>"
<!--NeedCopy-->
```

L'événement Session.Logon se déclenche lorsqu'un utilisateur saisit ses informations d'identification et se connecte à sa session d'application ou de bureau.

Signature Sigma

```
author: Citrix
date: 2023/01/31
description: This occurs when a user accesses content from an
    authorized browser which might cause an undesirable event or action
    through the internet.
detection:
  condition: index_selection and selection and not filter
  filter:
  - browser_name|contains: '<Browser-Name>'
  index_selection:
    source: cas_siem_consumer://<env>_<tenant_identifier>
  selection:
  - occurrence_event_type: Session.logon
logsource:
  product: citrixanalytics
  service: security
title: Access from unauthorized browser
<!--NeedCopy-->
```

Systèmes d'exploitation non autorisés

Cela se produit lorsqu'un utilisateur tente d'accéder à un appareil dont le type ou la version du système d'exploitation n'est pas autorisé par la stratégie informatique de votre entreprise ou en raison de failles de sécurité.

Détails

Source de données : applications et ordinateurs de bureau (application Workspace)

Requête CAS

```
Event-Type = "Session.Logon" AND OS-Name ~ "<OS-Name>" AND OS-Version =
    "<OS-Version>" AND OS-Extra-Info = "<OS-Extra-Info>"
<!--NeedCopy-->
```

Signature Sigma

```
author: Citrix
date: 2023/01/31
description: This occurs when a user attempts to access apps from
   servers with blocked listed operating systems.
detection:
  condition: index_selection and selection
  filter_null: []
  index_selection:
    source: cas_siem_consumer://<env>_<tenant_identifier>
  selection:
    occurrence_event_type: Session.logon
    os_name|contains: '<OS-Name>'
    os_version: '<OS-Version>'
    os_extra_info: '<OS-Extra-Info>'
logsource:
  product: citrixanalytics
  service: security
title: Unauthorized operating systems in block list
<!--NeedCopy-->
```

Adresse IP ou sous-réseaux non autorisés

Cela se produit lorsqu'un utilisateur tente d'accéder à partir d'une adresse ou d'une plage IP marquée comme non autorisée par la stratégie informatique de votre entreprise.

Détails

Source de données : applications et ordinateurs de bureau (application Workspace)

Requête CAS


```
Event-Type = "Session.Logon" AND Client-IP = "<XX.YY.ZZ.*>"
<!--NeedCopy-->
```

Signature Sigma

```
author: Citrix
date: 2023/01/31
description: This occurs when a user accessing content from an
   unauthorized IPs which might cause an undesirable event or action
   through the internet.
detection:
  condition: selection and not filter_null and filter
  filter:
  - client_ip: '<IP>'
  filter_null:
  - client_ip: null
  selection:
  - occurrence_event_type: Session.Logon
logsource:
  product: citrixanalytics
  service: security
title: Access from unauthorized IP
<!--NeedCopy-->
```

Systèmes d'exploitation non autorisés en dehors de la liste des systèmes autorisés

Cela se produit lorsqu'un utilisateur tente d'accéder à des applications à partir de serveurs hébergeant des systèmes d'exploitation ne figurant pas dans la liste d'autorisation.

Détails

Source de données : applications et ordinateurs de bureau (application Workspace)

Requête CAS

```
Event-Type = "Session.Logon" AND OS-Name !~ "<OS-Name>" AND OS-Version
   != "<OS-Version>" AND OS-Extra-Info != "<OS-Extra-Info>"
<!--NeedCopy-->
```

Signature Sigma


```
author: Citrix
date: 2023/01/31
description: Unauthorized operating systems outside allow list
detection:
  condition: selection and not filter_null and not filter_os and not
     filter_os_version and not filter_os_extra
  filter_os:
  - os_name|contains: '<OS INFO>'
  filter_os_version:
  - os_version: '<OS Version>'
  filter_os_extra:
  - os_extra_info: '<OS Extra Info>'
  filter_null:
  - os_name: null
  - os_version: null
  - os_extra_info: null
  selection:
  - occurrence_event_type: Session.Logon
logsource:
  product: citrixanalytics
  service: security
title: Unauthorized operating systems outside allow list
<!--NeedCopy-->
```

Versions non autorisées de l'application Workspace

Cela se produit lorsqu'un utilisateur tente d'accéder à une version de l'application Workspace qui n'est pas une version cliente prise en charge. Dans ce cas, les utilisateurs doivent mettre à niveau leur client vers une version prise en charge. Pour plus d'informations, consultez la section Versions du client de support.

Détails

Source de données : applications et ordinateurs de bureau (application Workspace)

Requête CAS

```
Event-Type = "Session.Logon" AND Client-Type IN ("Windows", "Macintosh"
    , "Unix/Linux") AND Workspace-App-Version != "20*" AND Workspace-App
    -Version != "21*"
<!--NeedCopy-->
```

Signature Sigma


```
author: Citrix
date: 2023/01/31
description: Unsupported Workspace app versions
detection:
  condition: selection and not filter_null and filter_product and not
     filter_product_version
  filter_product:
  - product: ['Windows', 'Mac', '<Other type>']
  filter_product_version:
  - product_version|contains: ['<Product Version1>', '<Product Version2
     >']
  filter_null:
  - product: null
  - product_version: null
  selection:
  - occurrence_event_type: Session.Logon
logsource:
  product: citrixanalytics
  service: security
title: Unsupported Workspace app versions
<!--NeedCopy-->
```

Menaces internes

November 16, 2023

Noms de bureau inhabituels

Cela se produit lorsque l'utilisateur tente de lancer un poste de travail qui n'est pas considéré comme habituel.

Détails

Source de données : applications et ordinateurs de bureau (application Workspace)

Requête CAS

```
Event-Type = "Session.Logon" AND Session-Launch-Type = "desktop" AND
   App-Name ~ "<Desktop Name>"
<!--NeedCopy-->
```


Signature Sigma

```
author: Citrix
date: 2023/01/31
description: Unusual desktop names
detection:
  condition: selection1 and selection2 and not filter_null and
     filter_app_name
  filter_app_name:
  - app_name|contains: '<App Name>'
  filter_null:
  - app_name: null
  selection1:
  - occurrence_event_type: Citrix.EventMonitor.AppStart
  selection2:
  - launch_type: 'desktop'
logsource:
  product: citrixanalytics
  service: security
title: Unusual desktop names
<!--NeedCopy-->
```

Surveiller un processus spécifique

Cela se produit lorsque l'utilisateur lance une application publiée figurant dans la liste de surveillance. L'objectif pourrait être de surveiller l'utilisation de certaines applications publiées.

Détails

Source de données : applications et ordinateurs de bureau (enregistrement de session)

Requête CAS

```
Event-Type = "Citrix.EventMonitor.AppStart" AND App-Name IN ("<App-Name
   -1>", "<App-Name-2>")
<!--NeedCopy-->
```

Signature Sigma

```
author: Citrix
date: 2023/01/31
description: Monitor specific process
detection:
  condition: selection and not filter_null and filter_app_name
  filter_app_name:
```



```
  - app_name: ['<App-Name1>', '<App-Name2>']
  filter_null:
  - app_name: null
  selection:
  - occurrence_event_type: Citrix.EventMonitor.AppStart
logsource:
  product: citrixanalytics
  service: security
title: Monitor specific process
<!--NeedCopy-->
```

Applications virtuelles non autorisées

Cela se produit lorsque l'utilisateur accède à des applications virtuelles non autorisées.

Détails

Source de données : applications et ordinateurs de bureau (application Workspace)

Requête CAS

```
Event-Type = "App.Start" AND App-Name IN ("<App-Name1>", "<App-Name2>")
<!--NeedCopy-->
```

Signature Sigma

```
date: 2023/01/31
description: Unauthorized virtual apps
detection:
  condition: selection and not filter_null and filter_app_name
  filter_app_name:
  - app_name: ['<App-Name1>', '<App-Name2>']
  filter_null:
  - app_name: null
  selection:
  - occurrence_event_type: App.Start
logsource:
  product: citrixanalytics
  service: security
title: Unauthorized virtual apps
<!--NeedCopy-->
```


Exfiltration de données

November 16, 2023

Impression à partir d'applications SaaS

Cela se produit lorsqu'un fichier est imprimé à partir d'une application SaaS à partir de laquelle l'impression n'est pas autorisée. Il détecte les risques d'exfiltration de données lors des opérations d'impression dans les applications SaaS.

Détails

Source de données : Apps and Desktops (Citrix Enterprise Browser)

Requête CAS

```
Event-Type = "App.SaaS.File.Print" AND SaaS-App-Name = "<App-Name>"
<!--NeedCopy-->
```

Signature Sigma

```
author: Citrix
date: 2023/01/31
description: Printing from SaaS apps
detection:
  condition: selection and not filter_null and filter_saas_app_name
  filter_saas_app_name:
  - saas_app_name: '<App-Name>'
  filter_null:
  - saas_app_name: null
  selection:
  - occurrence_event_type: App.SaaS.File.Print
logsource:
  product: citrixanalytics
  service: security
title: Printing from SaaS apps
<!--NeedCopy-->
```


Utilisation du presse-papiers sur les applications SaaS

Cela se produit lorsqu'une activité de coupage, de copie ou de collage est effectuée à partir de n'importe quelle application SaaS. Il détecte l'exfiltration potentielle de données à partir des applications SaaS de votre organisation en surveillant le fonctionnement du presse-papiers.

Détails

Source de données : Apps and Desktops (Citrix Enterprise Browser)

Requête CAS

```
Event-Type = "App.SaaS.Clipboard" AND Clipboard-Result = "success" AND
   Clipboard-Operation IN ( "copy" , "cut" )
<!--NeedCopy-->
```

Signature Sigma

```
author: Citrix
date: 2023/01/31
description: Clipboard usage on SaaS apps
detection:
  condition: selection and not filter_null and
     filter_clipboard_details_result and filter_clipboard_operation
  filter_clipboard_details_result:
  - clipboard_details_result: 'success'
  filter_clipboard_operation:
  - clipboard_operation: ['cut', 'copy', '<Other Operation>']
  filter_null:
  - clipboard_operation: null
  - clipboard_details_result: null
  selection:
  - occurrence_event_type: App.SaaS.Clipboard
logsource:
  product: citrixanalytics
  service: security
title: Clipboard usage on SaaS apps
<!--NeedCopy-->
```

Tableau de bord des utilisateurs

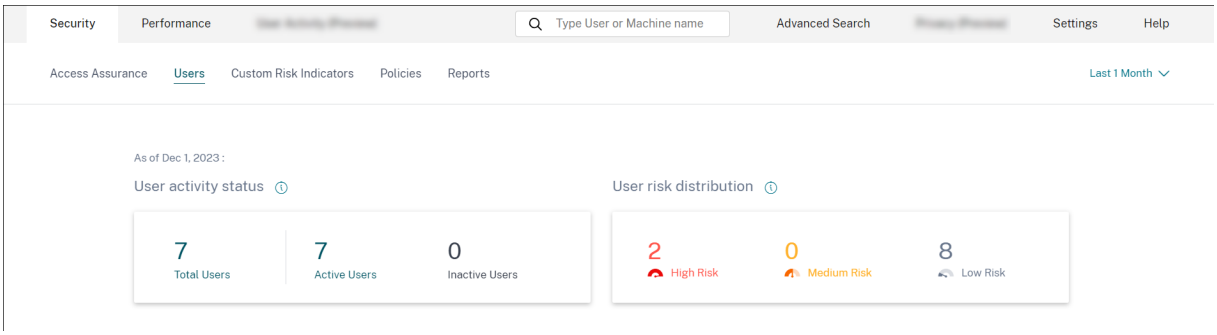
February 9, 2024

Vue d'ensemble

Le tableau de bord des **utilisateurs** est le point de départ de l'analyse du comportement des utilisateurs et de la prévention des menaces.

Ce tableau de bord fournit une visibilité sur les modèles de comportement des utilisateurs au sein d'une organisation. À l'aide de ces données, vous pouvez surveiller, détecter et signaler de manière proactive les comportements qui ne sont pas conformes à la norme, tels que les attaques de phishing ou de rançongiciel.

Pour afficher le tableau de bord des utilisateurs, accédez à **Sécurité > Utilisateurs**. Le tableau de bord Utilisateurs contient les sections suivantes :



- **État actif de l'utilisateur** : répartition du nombre total d'utilisateurs actifs et inactifs.
- Répartition des**risques pour les utilisateurs : répartition**du nombre total d'utilisateurs actifs, inactifs et répartition des utilisateurs à risque présentant un profil élevé, moyen et faible en fonction de leur score de risque calculé le plus élevé au cours de la période sélectionnée.
- **Principaux utilisateurs : Les**meilleurs utilisateurs sont triés en fonction de leur niveau de risque et segmentés en fonction de tous les utilisateurs, des utilisateurs privilégiés et des utilisateurs de la liste de surveillance.
- **Catégories de risques** : affiche les catégories de risques prises en charge par Citrix Analytics. Les indicateurs de risque présentant des modèles comportementaux similaires sont regroupés en catégories.
- **Indicateurs de risque et actions** : Distribution des indicateurs de risque et des actions tracés sur une durée sélectionnée pour tous les utilisateurs de votre organisation.
- **Résumé de l'accès : Récapitule**le nombre total de tentatives effectuées par les utilisateurs pour accéder aux ressources de votre organisation.
- **Stratégies et actions** : affiche les cinq principales stratégies et actions appliquées aux profils utilisateur.
- **Indicateurs de risque** : affiche les cinq principaux indicateurs de risque de votre organisation.

État de l'activité de l'utilisateur

Nombre total d'utilisateurs de votre organisation utilisant les sources de données pour lesquelles vous avez activé Analytics. Il se peut qu'ils aient ou non un score de risque associé à leur compte. Cette vignette indique le nombre d'utilisateurs actifs. Les utilisateurs actifs sont les utilisateurs dont les événements ont été détectés au cours de la période sélectionnée. Vous pouvez cliquer sur le menu déroulant de l'état de l'activité des utilisateurs pour voir la répartition du nombre total d'utilisateurs entre utilisateurs actifs et inactifs.

- Nombre total d'utilisateurs : nombre total d'utilisateurs au cours de la période sélectionnée.
- Utilisateurs actifs : utilisateurs dont les événements ont été détectés au cours de la période sélectionnée.
- Utilisateurs inactifs : utilisateurs pour lesquels aucun événement n'a été détecté au cours de la période sélectionnée.

Le nombre total d'utilisateurs figurant sur le tableau de bord des **utilisateurs** peut être supérieur au nombre d'utilisateurs à risque, car on ne s'attend pas à ce que tous les utilisateurs soient exposés à des risques.

> **Remarque**
>
> Sur la page **Utilisateurs**, le nombre total d'utilisateurs est affiché au cours des 30 derniers jours, quelle que soit la période sélectionnée.

Facettes

Filtrez les événements utilisateur en fonction des catégories suivantes :

- **Score de risque** : événements utilisateur basés sur des scores de haut risque, de risque moyen, de risque faible et de risque zéro.
- **Utilisateur** : événements utilisateur basés sur les privilèges d'administrateur, les privilèges exécutifs et les utilisateurs de la liste de suivi.
- **Sources de données découvertes** : événements utilisateur basés sur la source de données que vous avez intégrée.

Boîte de recherche

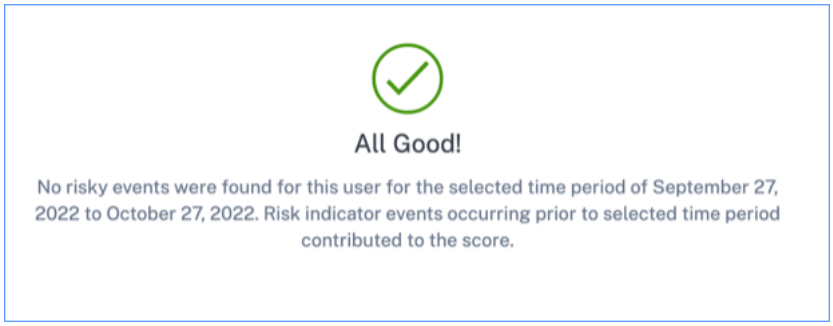
Utilisez la zone de recherche pour rechercher des événements pour les utilisateurs. Vous pouvez utiliser des opérateurs dans votre requête pour affiner le focus de votre recherche. Pour plus d'informations sur les opérateurs valides que vous pouvez utiliser dans votre requête, consultez la rubrique Recherche en libre-service.

Dernier score

Le score de risque détermine le niveau de risque qu'un utilisateur pose à une organisation pendant une période spécifique. La valeur du score de risque est dynamique et varie en fonction de l'analyse du comportement des utilisateurs. Sur la base du dernier score de risque, un utilisateur peut appartenir à l'une des catégories suivantes : utilisateur à haut risque, utilisateur à risque moyen, utilisateur à faible risque et utilisateur sans score de risque nul.

Utilisateur

Liste de tous les utilisateurs découverts par Analytics. Sélectionnez un nom d'utilisateur pour afficher les informations utilisateur et la chronologie des risques pour l'utilisateur. Il se peut que l'utilisateur ait déclenché ou non un indicateur de risque. Si aucun événement risqué n'est associé à cet utilisateur, le message suivant s'affiche.



S'il y a des événements à risque associés à un utilisateur, les indicateurs de risque figurent sur son calendrier de risque. Sélectionnez l'utilisateur pour afficher la chronologie des risques.

Un utilisateur peut être marqué comme `privileged` et ajouté à la liste de suivi.

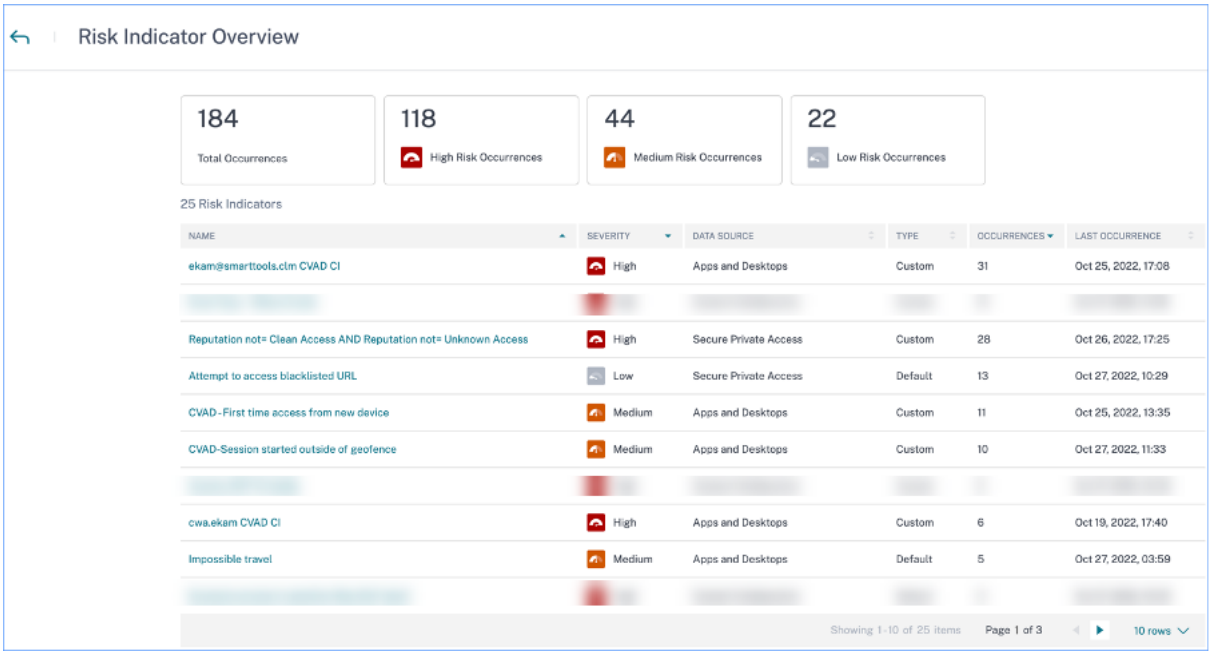
Source de données découverte

Source de données associée à un utilisateur. Lorsqu'un utilisateur utilise activement la source de données, Analytics reçoit les événements utilisateur de cette source de données. Pour recevoir des événements utilisateur, vous devez activer le traitement des données sur la fiche de site de la source de données, disponible sur la page **Sources de données** .

Indicateurs déclenchés

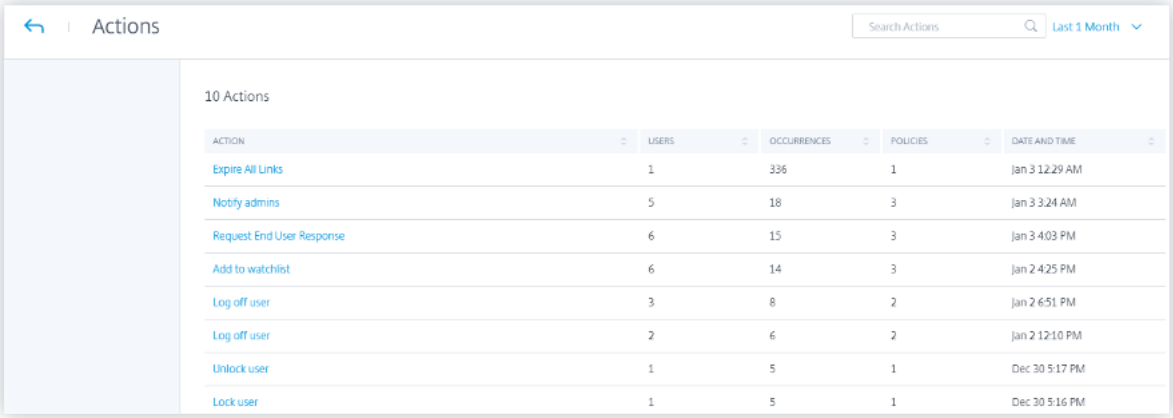
Indique le nombre d'indicateurs de risque déclenchés par les utilisateurs pendant la durée sélectionnée. Cliquez sur la vignette **Indicateurs déclenchés** pour afficher les détails des indicateurs de risque. Le tableau des indicateurs de risque fournit les informations suivantes :

- **Nom : nom**de l'indicateur de risque.
- **Gravité** : gravité du risque associé à l'événement. Le risque peut être élevé, moyen ou faible.
- **Source de données : source**de données à laquelle s'applique le modèle d'indicateur de risque.
- **Type** : Type d'indicateur de risque. Un indicateur de risque peut être par défaut ou personnalisé.
- **Occurrences** : nombre de fois qu'un indicateur de risque est déclenché pour un utilisateur. Lorsque vous sélectionnez la période, les occurrences de l'indicateur de risque changent en fonction de la sélection de l'heure.
- **Dernière occurrence** : affiche la date et l'heure de la dernière occurrence.



Actions appliquées

Indique le nombre d'actions appliquées aux utilisateurs pendant la durée sélectionnée. Cela inclut les actions appliquées manuellement par les administrateurs et les actions pilotées par des stratégies. Cliquez sur la vignette **Action appliquée** pour afficher les détails de l'action. Cette section n'affiche pas les actions que vous avez appliquées manuellement sur les profils utilisateur.

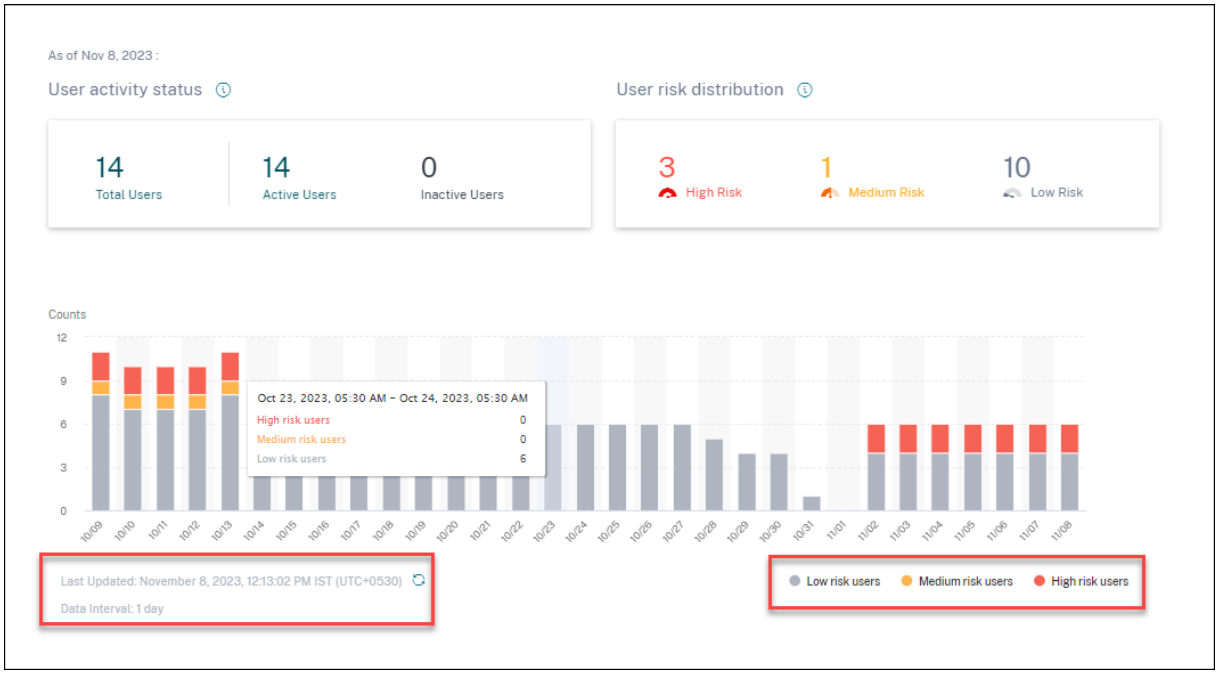


Le tableau des **actions** fournit les informations suivantes :

- **Action** : nom de l'action appliquée conformément à la stratégie.
- **Utilisateurs** : nombre d'utilisateurs auxquels l'action a été appliquée.
- **Occurrences** : nombre d'occurrences de l'action.
- **Date et heure** : date et heure de l'action appliquée.

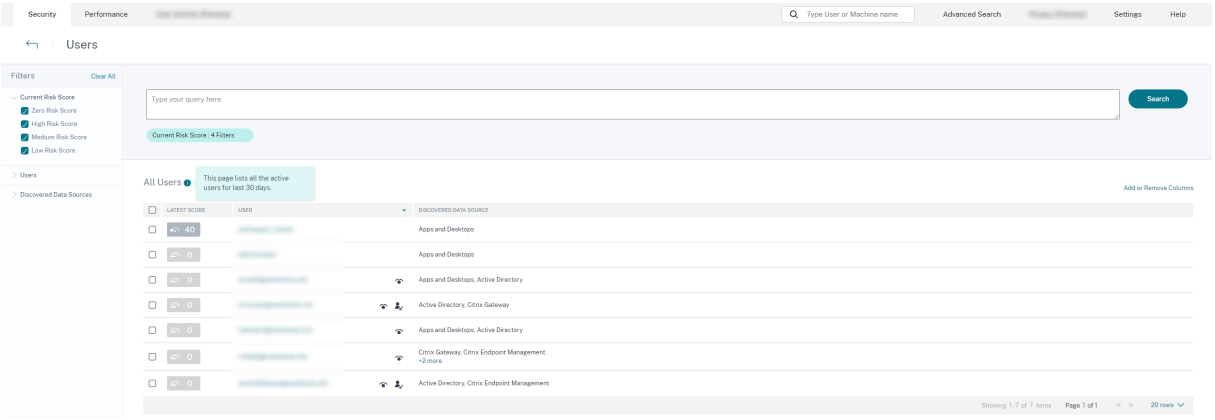
Événements traités

Nombre total d'événements utilisateur reçus à partir de vos sources de données connectées et traités par Analytics.



Répartition des risques pour les utilisateurs

Vous pouvez consulter le nombre d'utilisateurs présentant un profil élevé, moyen ou faible en fonction de leur score de risque calculé le plus élevé au cours de la période sélectionnée. En dessous des chiffres globaux, un graphique à barres montre l'évolution au fil du temps de la répartition des utilisateurs présentant un risque faible, moyen et élevé.



Le niveau de risque est classé selon trois codes de couleur.

- **Rouge** : représente les utilisateurs à haut risque.
- **Orange** —Représente les utilisateurs présentant un risque moyen.
- **Gris** —Représente les utilisateurs à faible risque.

Vous pouvez consulter le nombre d'utilisateurs à risque (élevé, moyen et faible) en passant votre souris sur les barres de couleur en fonction d'une période spécifique. Vous pouvez consulter les détails de la dernière mise à jour (date et heure) à l'aide des informations relatives à l'intervalle de données. Cliquez sur n'importe quelle barre de couleur pour voir les utilisateurs à risque pendant cette durée. Cliquez sur l'option d'actualisation pour obtenir les données mises à jour.

Utilisateurs risqués

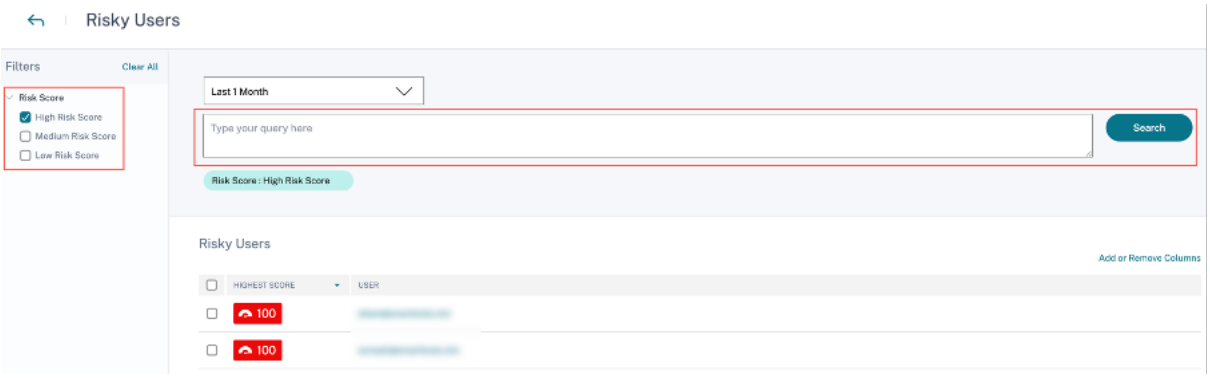
Les utilisateurs à risque sont des utilisateurs auxquels sont associés des événements risqués et qui ont déclenché au moins un indicateur de risque. Le niveau de risque qu'un utilisateur pose au réseau pendant une période de temps spécifique est déterminé par le score de risque associé à l'utilisateur. La valeur du score de risque est dynamique et repose sur l'analyse du comportement des utilisateurs.

Le risque de chaque utilisateur est régulièrement mis à jour au fil du temps en fonction de l'activité de l'utilisateur. Par conséquent, un utilisateur peut présenter un risque moyen ou élevé à un moment donné, mais chuter à un niveau de risque inférieur plus tard. Sur la base du score de risque, un utilisateur à risque peut appartenir à l'une des catégories suivantes :

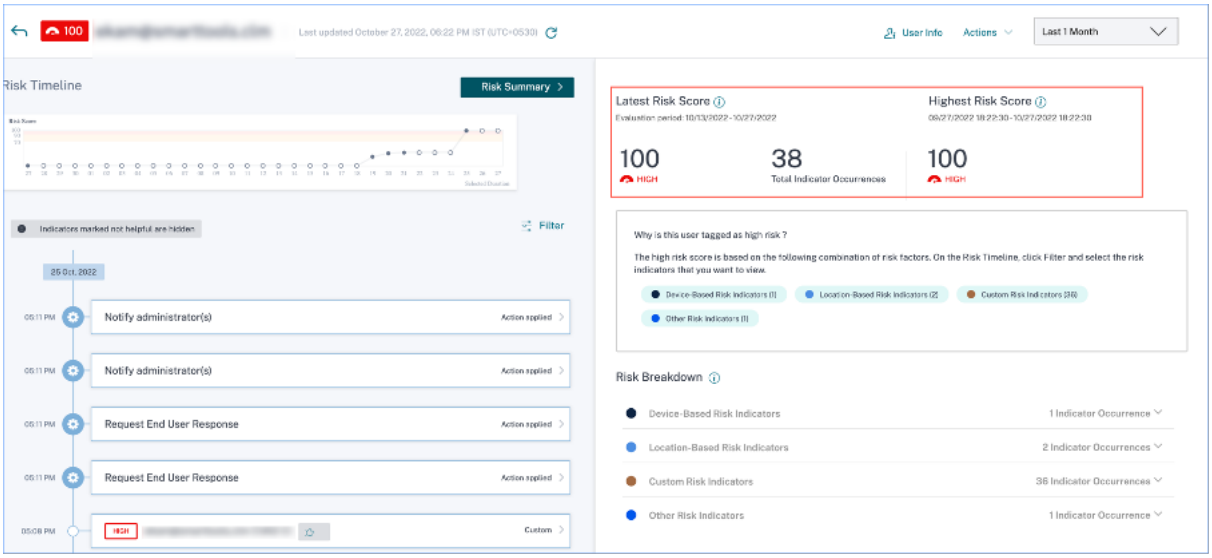
- Risque élevé

- Risque moyen
- Risque faible

Sur la page **Utilisateurs à risque**, vous pouvez utiliser les facettes pour filtrer en fonction des niveaux de risque associés à la période sélectionnée, et la barre de recherche pour rechercher un ou plusieurs utilisateurs spécifiques.



Cliquez sur l'adresse e-mail de l'utilisateur pour afficher la page de **chronologie des risques** pour cet utilisateur sélectionné en particulier. Cette page affiche les indicateurs de risque ainsi que les détails des **scores de risque les plus récentset les plus élevés** en fonction de la période sélectionnée.



Risque élevé

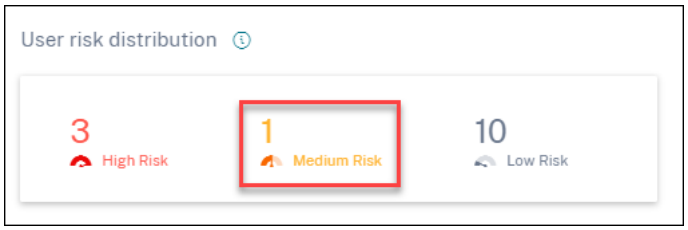
Utilisateurs dont le score de risque est compris entre 90 et 100. Ces utilisateurs ont présenté de multiples comportements correspondant à des facteurs de risque modérés à graves et peuvent représenter une menace immédiate pour l'organisation.

Sur le tableau de bord des **utilisateurs**, vous pouvez consulter le nombre d'utilisateurs à haut risque en fonction du score de risque calculé le plus élevé au cours de la période sélectionnée.

Cliquez sur l'option **Risque élevé** pour afficher la page **Utilisateurs à risque** . La page affiche les détails concernant les utilisateurs à haut risque.

Risque moyen

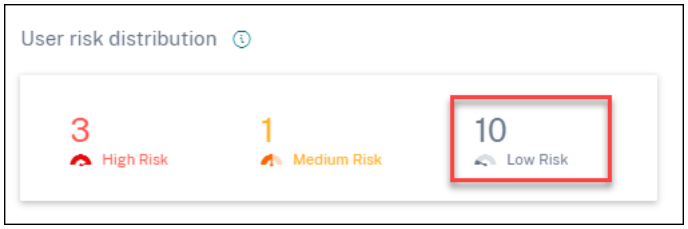
Utilisateurs dont le score de risque est compris entre 70 et 89. Ces utilisateurs ont généralement une ou plusieurs activités qui semblent potentiellement suspectes et/ou anormales et qui méritent d'être surveillées de près.



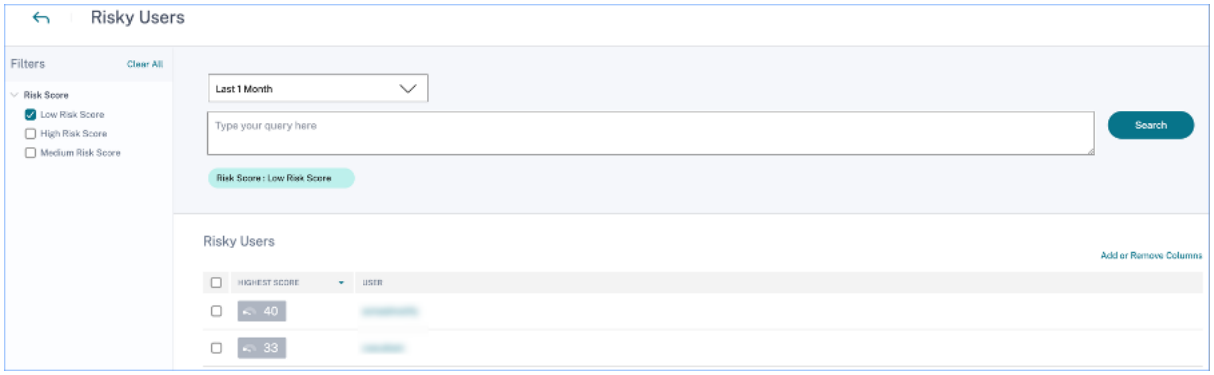
Cliquez sur l'option **Risque moyen** pour afficher la page **Utilisateurs à risque** . La page affiche les détails concernant les utilisateurs présentant un risque moyen.

Risque faible

Utilisateurs dont le score de risque est compris entre 1 et 69. Ces utilisateurs disposent d'au moins un indicateur de risque reflétant un comportement inhabituel ou inattendu, mais pas suffisamment pour mériter une classification de risque plus grave.

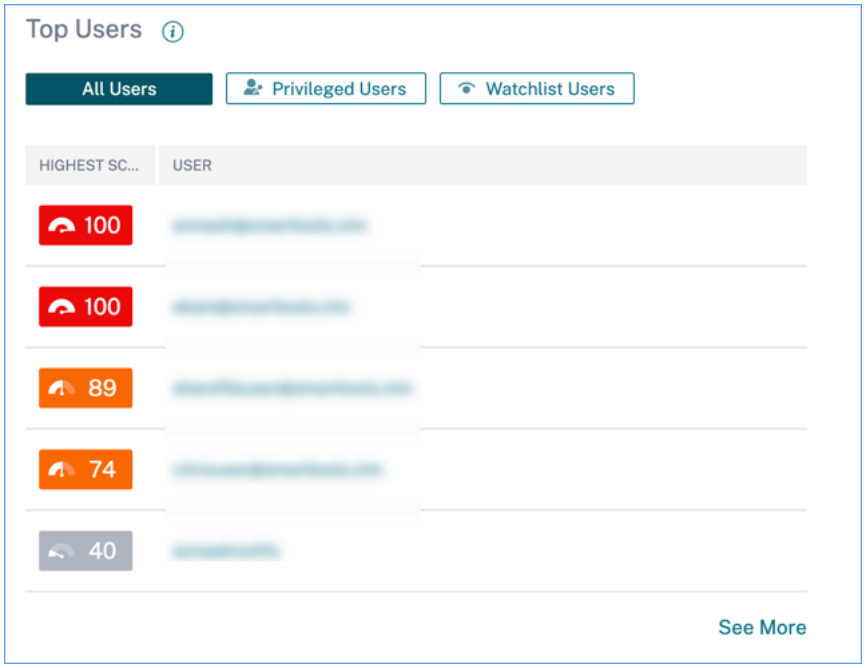


Cliquez sur l'option **Risque faible** pour afficher la page **Utilisateurs à risque** . La page affiche les détails concernant les utilisateurs à faible risque.



Les meilleurs utilisateurs

Vous pouvez consulter les meilleurs utilisateurs dans différentes catégories d'utilisateurs, triés selon les scores de risque les plus élevés pour la période sélectionnée. Le tableau des **principaux utilisateurs** suivant présente les cinq utilisateurs les plus exposés au risque (tous les utilisateurs, les utilisateurs privilégiés et les utilisateurs de la liste de surveillance) en fonction de leur score de risque calculé sur la période sélectionnée, plutôt que du score de risque le plus récent.

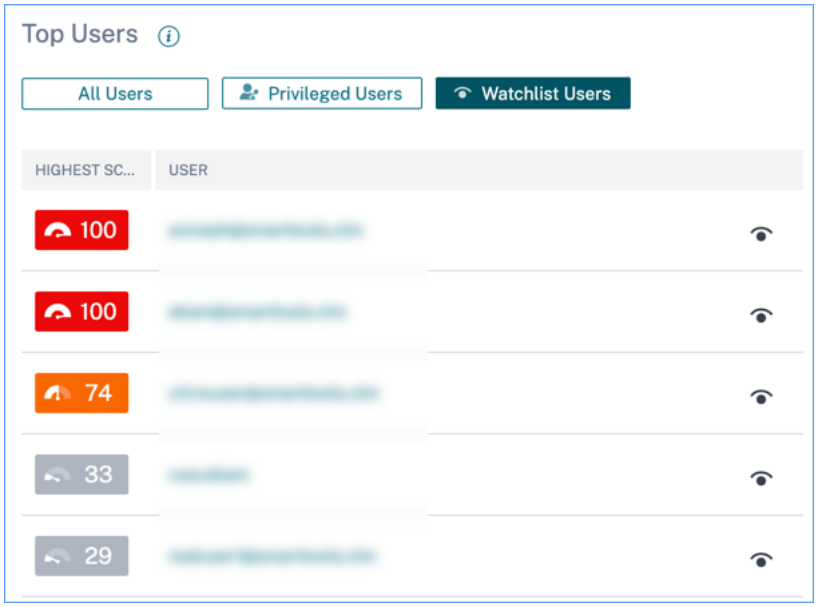


> **Remarque**
>
> Dans les versions précédentes, le tableau des principaux utilisateurs affichait toujours le score de risque le plus récent, quelle que soit la période sélectionnée.

Utilisateurs de la liste de surveillance

Liste des utilisateurs surveillés de près pour détecter les menaces potentielles. Par exemple, vous pouvez surveiller les utilisateurs qui ne sont pas des employés à temps plein au sein de votre organisation en ajoutant ces utilisateurs à la liste de suivi. Vous pouvez également surveiller les utilisateurs qui déclenchent fréquemment un indicateur de risque spécifique. Vous pouvez soit ajouter un utilisateur à la liste de suivi manuellement, soit définir des stratégies pour ajouter des utilisateurs à la liste de suivi.

Si vous avez ajouté des utilisateurs à la liste de suivi, vous pouvez consulter les cinq meilleurs utilisateurs de la liste de suivi en fonction du score le plus élevé.



Cliquez sur le lien **Voir plus** dans le volet **Tous les utilisateurs** pour afficher la **page Utilisateurs**. La page affiche la liste de tous les utilisateurs de la liste de suivi.

> **Remarque**
>
> Sur le tableau de bord **Utilisateurs** et la page **Utilisateurs**, le nombre d'utilisateurs dans la liste de suivi est affiché pour les 13 derniers mois, quelle que soit la période sélectionnée. Lorsque vous sélectionnez une période, les occurrences de l'indicateur de risque changent en fonction de la sélection de l'heure.

En savoir plus : Liste de surveillance

Catégories de risque

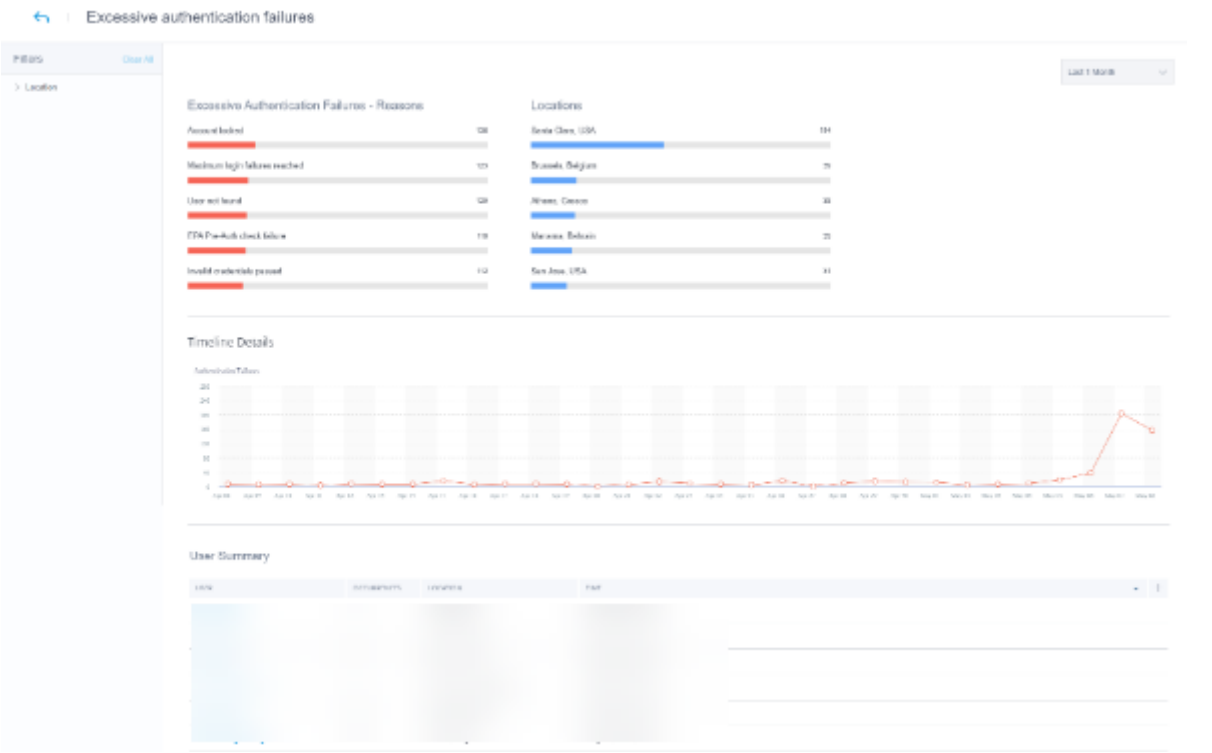
Le graphique en anneau des **catégories de risques** résume le nombre d'occurrences d'indicateurs par catégorie de risque au cours de la période sélectionnée. Le nombre d'utilisateurs uniques est affiché

lorsque vous passez la souris sur chaque segment du graphique, qui renvoie à son tour à la page d'aperçu de la **catégorie d'indicateurs de risque** correspondante. La catégorisation des risques est prise en charge par des indicateurs de risque par défaut et personnalisés.

L'objectif du tableau de bord des **catégories de risques** est de permettre aux administrateurs de Citrix Virtual Apps and Desktops et Citrix DaaS de gérer les risques liés aux utilisateurs et de discuter de manière simplifiée avec leurs homologues en matière de sécurité sans avoir besoin de connaissances de niveau expert en matière de sécurité. Il permet à l'application de la sécurité de prendre effet au niveau de l'organisation et n'est pas limité aux seuls administrateurs de sécurité.

Cas d'utilisation

Considérez que vous êtes un administrateur Citrix Virtual Apps and Desktops et que vous gérez les droits d'accès aux applications des employés de votre organisation. Si vous accédez à la section **Catégories de risque** > **Utilisateurs compromis** > **Échecs d'authentification excessifs - Indicateur de risque Citrix Gateway**, vous pouvez évaluer si les employés auxquels vous avez accordé l'accès ont été compromis. Si vous naviguez plus loin, vous pouvez obtenir des informations plus précises sur cet indicateur de risque, telles que les raisons de l'échec, les emplacements de connexion, les détails de la chronologie et le résumé utilisateur. Si vous remarquez des divergences entre les utilisateurs auxquels l'accès a été accordé et ceux dont l'accès a été compromis, vous pouvez en informer l'administrateur de sécurité. Cette notification en temps opportun à l'administrateur de la sécurité contribue à l'application de la sécurité au niveau de l'organisation.

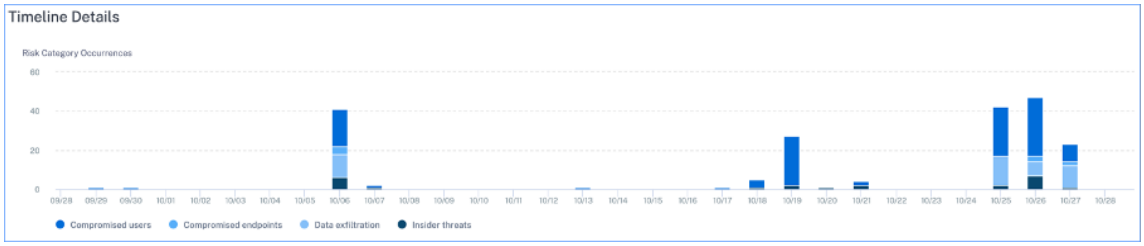


Comment analyser le tableau de bord des catégories de risques ?

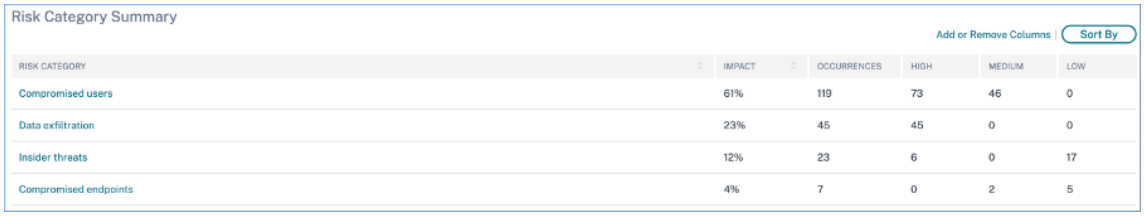
Lorsque vous sélectionnez **Voir plus** sur le tableau de bord **Catégories de risques**, vous êtes redirigé vers la page qui récapitule les détails des catégories de risque. Cette page contient les informations suivantes :

- **Rapport de catégorie de risque** : représente le nombre total d'occurrences d'indicateurs de risque de chaque catégorie pour une période sélectionnée.

- **Détails de la chronologie** : fournit une représentation graphique du nombre total d'occurrences d'indicateurs de risque de chaque catégorie de risque pour une période sélectionnée. Si vous accédez au bas de cette section, vous pouvez effectuer un tri en fonction des catégories de risque pour obtenir des informations plus précises sur les indicateurs de risque.



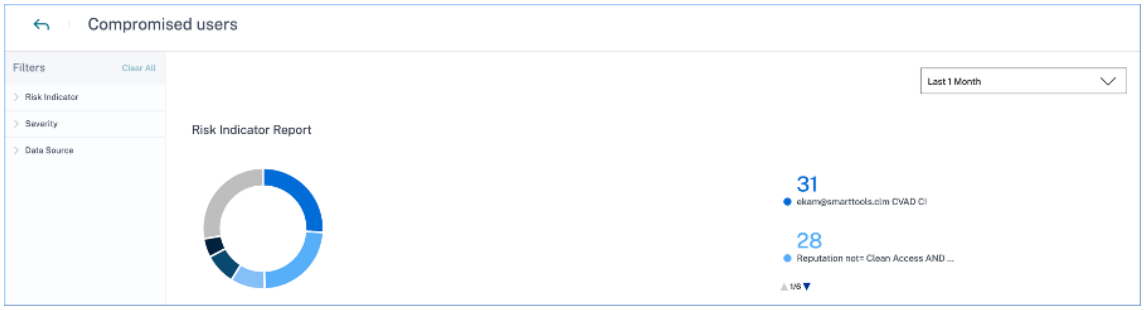
- **Résumé des catégories de risques** : Cette section fournit des détails tels que l'impact, les occurrences et la gravité des indicateurs de risque associés à chaque catégorie. Sélectionnez n'importe quelle catégorie de risque pour afficher des détails sur les indicateurs de risque associés à cette catégorie. Par exemple, lorsque vous sélectionnez la catégorie **Utilisateurs compromis**, vous êtes redirigé vers la page **Utilisateurs compromis** .



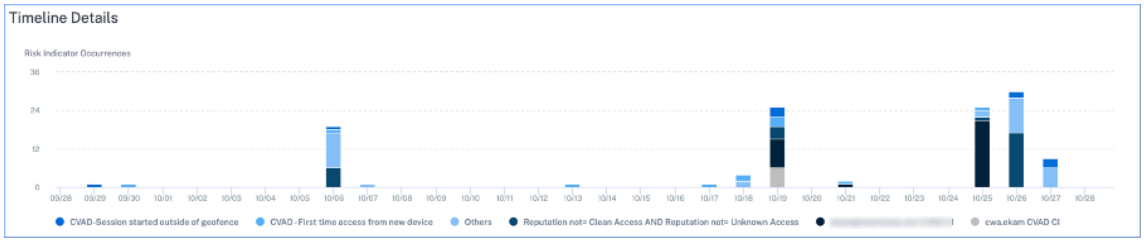
RISK CATEGORY	IMPACT	OCCURRENCES	HIGH	MEDIUM	LOW
Compromised users	61%	119	73	46	0
Data exfiltration	23%	45	45	0	0
Insider threats	12%	23	6	0	17
Compromised endpoints	4%	7	0	2	5

La page **Utilisateurs compromis** affiche les informations suivantes :

- **Rapport des indicateurs**de risque : affiche les indicateurs de risque qui appartiennent à la catégorie Utilisateurs compromis pour une période sélectionnée. Il affiche également le nombre total d'occurrences des indicateurs de risque qui ont été déclenchés au cours de la période sélectionnée.

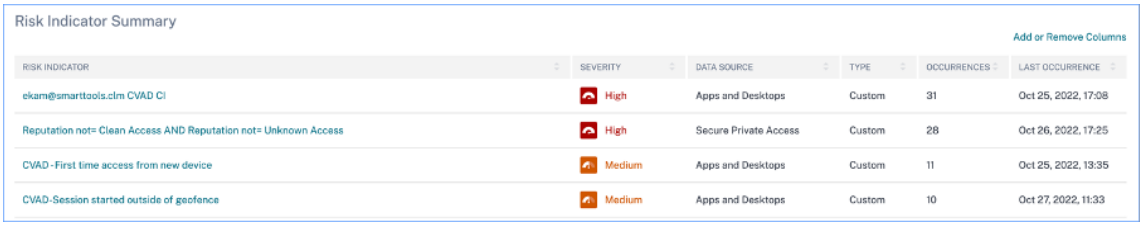


- **Détails de la chronologie** : fournit une représentation graphique des occurrences de l'indicateur de risque pour une période sélectionnée.

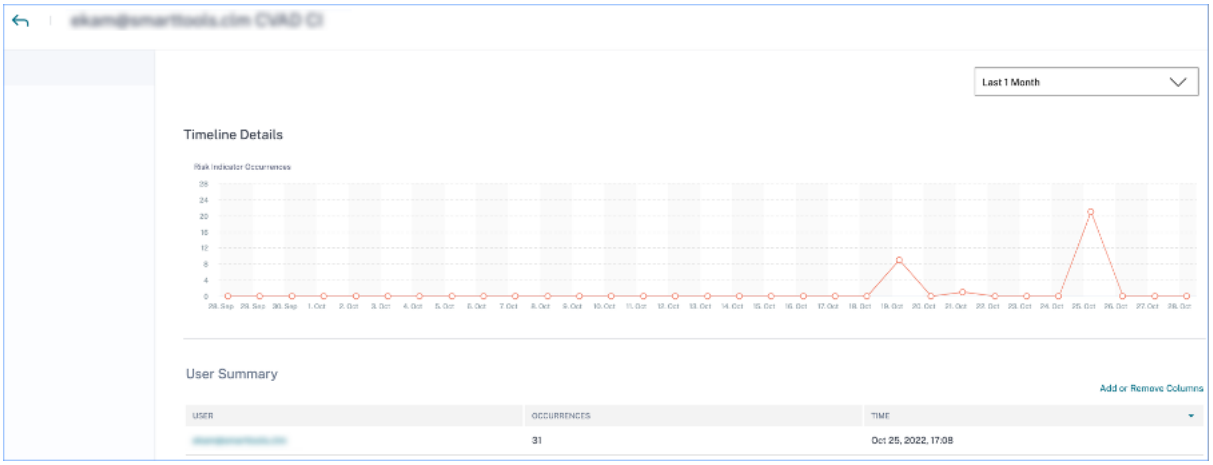


- **Résumé des indicateurs de risque** : affiche un résumé des indicateurs de risque générés dans

la catégorie des utilisateurs compromis. Cette section affiche également la gravité, la source de données, le type d'indicateur de risque, les occurrences et la dernière occurrence.



Lorsque vous sélectionnez un indicateur de risque, vous êtes redirigé vers la page qui résume les détails de cet indicateur. Par exemple, si vous sélectionnez l'indicateur de risque **Premier accès à partir d'un nouvel appareil**, vous êtes redirigé vers la page qui récapitule les détails de cet indicateur. Le résumé inclut des détails chronologiques sur les occurrences de cet événement et un résumé utilisateur répertoriant les utilisateurs qui ont déclenché cet indicateur de risque, les occurrences de l'indicateur de risque et l'heure de l'événement. Lorsque vous sélectionnez un utilisateur, vous êtes redirigé vers la chronologie des risques de l'utilisateur.



> **Remarque**
>
> Citrix Analytics regroupe les indicateurs de risque par défaut dans la catégorie de risque appropriée. Pour les indicateurs de risque personnalisés, vous devez sélectionner une catégorie de risque sur la page **Créer un indicateur** . Pour plus d'informations, consultez la section Indicateurs de risque personnalisés.

Types de catégories de risques

Exfiltration de données Cette catégorie regroupe les indicateurs de risque déclenchés par des logiciels malveillants ou par des employés qui effectuent des transferts de données non autorisés ou des vols de données vers ou depuis un appareil d'une organisation. Vous pouvez obtenir des informations sur toutes les activités d'exfiltration de données qui ont eu lieu au cours d'une période donnée et at-

ténuer les risques associés à cette catégorie en appliquant de manière proactive des actions sur les profils utilisateur.

La catégorie de risque d'exfiltration de données regroupe les indicateurs de risque suivants :

Sources de données	Indicateurs de risque utilisateur
Citrix Virtual Apps and Desktops et Citrix DaaS	Exfiltration potentielle des données

Menaces internes Cette catégorie regroupe les indicateurs de risque déclenchés par les employés au sein d'une organisation. Étant donné que les employés disposent de niveaux d'accès plus élevés aux applications spécifiques à l'entreprise, les entreprises sont plus exposées à des risques de sécurité. Les activités risquées peuvent être intentionnellement causées par un initié malveillant ou être le résultat d'une erreur humaine. Dans l'un ou l'autre des scénarios, l'impact sur la sécurité de l'organisation est préjudiciable. Cette catégorie fournit des informations sur toutes les activités liées aux menaces internes qui ont eu lieu au cours d'une période donnée. À l'aide de ces informations, vous pouvez atténuer les risques associés à cette catégorie en appliquant de manière proactive des actions sur les profils utilisateur.

La catégorie de risques liés aux menaces internes regroupe les indicateurs de risque suivants :

Sources de données	Indicateurs de risque utilisateur
Citrix Secure Private Access	tentative d'accès à l'URL de la liste noire
Citrix Secure Private Access	Téléchargement excessif de données
Citrix Secure Private Access	Accès à un site Web risqué
Citrix Secure Private Access	Volume de téléchargement inhabituel

Utilisateurs compromis Cette catégorie regroupe les indicateurs de risque dans lesquels les utilisateurs présentent des comportements inhabituels, tels que des connexions suspectes et des échecs de connexion. Les tendances inhabituelles peuvent également résulter de la compromission des comptes d'utilisateurs. Vous pouvez obtenir des informations sur tous les événements utilisateur compromis qui se sont produits au cours d'une période spécifiée et atténuer les risques associés à cette catégorie en appliquant des actions proactives sur les profils utilisateur.

La catégorie de risque des utilisateurs compromis regroupe les indicateurs de risque suivants :

Sources de données	Indicateurs de risque utilisateur
Citrix Gateway	Échec de l'analyse du point final
Citrix Gateway	Échec excessif de l'authentification
Citrix Gateway	Voyages impossibles
Citrix Gateway	Ouverture de session à partir d'une adresse IP suspecte
Citrix Gateway	Échec d'authentification inhabituel
Citrix Virtual Apps and Desktops et Citrix DaaS	Ouverture de session suspecte
Citrix Virtual Apps and Desktops et Citrix DaaS	Voyages impossibles
Microsoft Graph Security	Indicateurs de risque Azure AD Identity Protection
Microsoft Graph Security	Indicateurs de risque Microsoft Defender for Endpoint

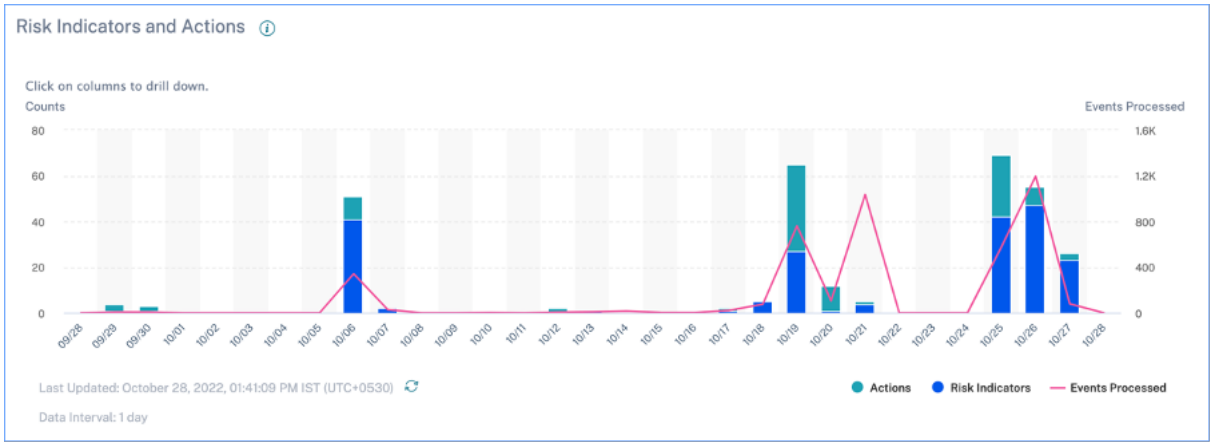
Points de terminaison compromis Cette catégorie regroupe les indicateurs de risque qui sont déclenchés lorsque les appareils présentent un comportement non sécurisé pouvant indiquer une compromission.

La catégorie de risque des points de terminaison compromis regroupe les indicateurs de risque suivants :

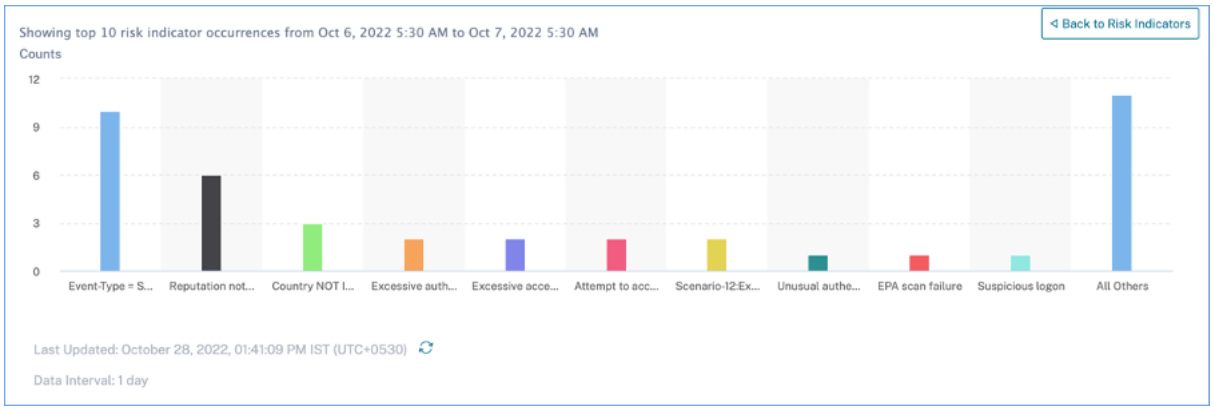
Sources de données	Indicateurs de risque utilisateur
Citrix Endpoint Management	Périphérique non géré détecté
Citrix Endpoint Management	Appareil jailbreaké ou rooté détecté
Citrix Endpoint Management	Appareil avec des applications sur la liste noire détectées

Indicateurs de risque et actions

Vous pouvez consulter les indicateurs de risque déclenchés et les actions appliquées à vos utilisateurs pour la période sélectionnée. Le nouveau diagramme à barres **des indicateurs de risque et des actions** fournit le détail du nombre d'indicateurs, d'actions et d'événements au fil du temps, la plage temporelle globale et l'intervalle de barres étant dérivés de la période sélectionnée.



Cliquez sur un segment de barre correspondant à des indicateurs ou à des actions pour afficher une visualisation détaillée des chiffres par indicateur ou action, respectivement.



Dans la liste déroulante des indicateurs, cliquez sur une barre d'indicateur individuelle pour accéder à la page de l'indicateur de risque correspondant, pour la période sélectionnée.

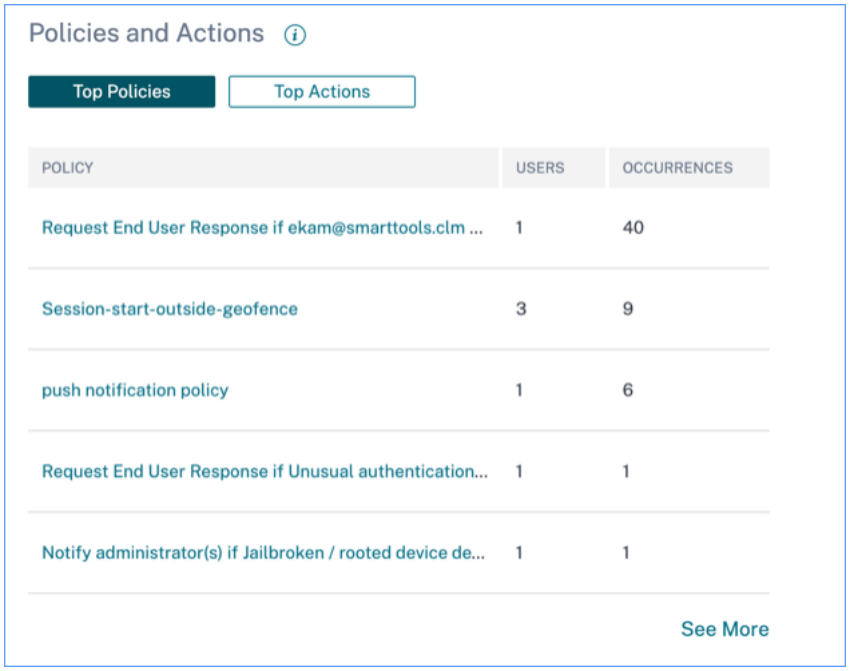
Résumé des accès

Ce tableau de bord récapitule tous les événements d'accès à la passerelle pendant une période sélectionnée. Il affiche le nombre total d'accès, d'accès réussis et d'accès échoué via Citrix Gateway.

Cliquez sur les pointeurs du graphique pour afficher la page Recherche en libre-service de passerelle . Pour les scénarios de connexion réussis, les événements d'accès à la passerelle sont triés en fonction du code d'état sur la page.

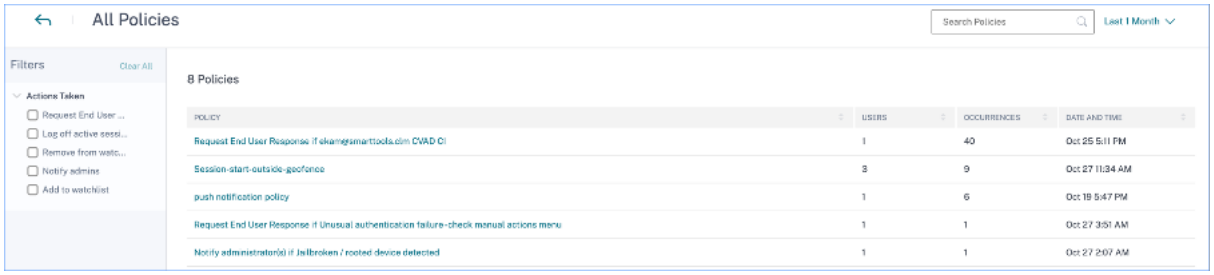
Stratégies et actions

Affiche les cinq principales stratégies et actions appliquées aux profils utilisateur pendant une période sélectionnée. Cliquez sur le lien **Voir plus** dans le volet **Stratégies et actions** pour obtenir des informations détaillées sur les stratégies et les actions.



Principales stratégies

Les cinq principales stratégies configurées sont déterminées en fonction du nombre d'occurrences. Lorsque vous êtes dans la section **Principales stratégies** du tableau de bord et que vous sélectionnez **Voir plus**, vous êtes redirigé vers la page **Toutes les stratégies** .



Toutes les stratégies Cette page fournit des informations détaillées sur toutes les stratégies configurées. Lorsque vous sélectionnez une stratégie, vous êtes redirigé vers la page Recherche de stratégies en libre-service . Dans le volet gauche, vous pouvez filtrer en fonction des actions appliquées.

Lorsque vous sélectionnez un nom d'utilisateur, vous êtes redirigé vers la chronologie des risques. L'action basée sur une stratégie est ajoutée à la chronologie des risques de l'utilisateur. Lorsque vous sélectionnez l'action, ses détails sont affichés dans le volet droit de la chronologie des risques.

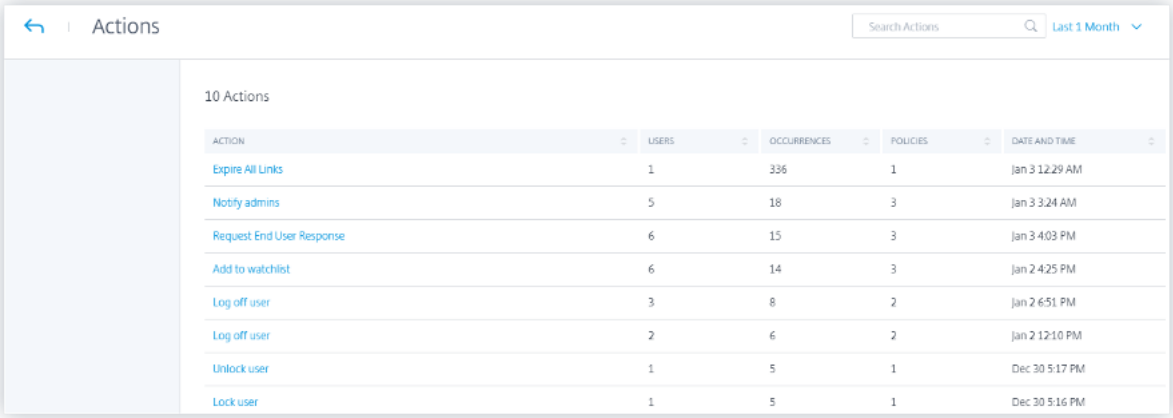
Principales actions

Les cinq principales actions associées aux stratégies appliquées aux profils utilisateur. Cette section n'affiche pas les actions que vous avez appliquées manuellement sur les profils utilisateur. Les principales actions sont déterminées par le nombre d'occurrences.

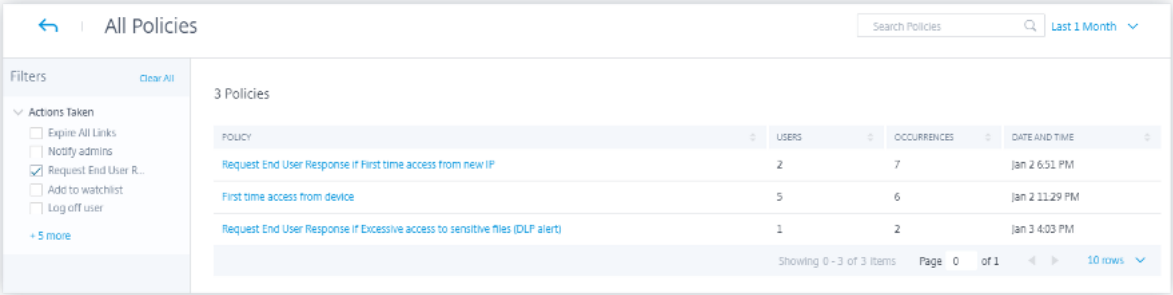
Cliquez sur **Voir plus** pour afficher toutes les actions basées sur des stratégies sur la page **Actions** .

Actions La page fournit la liste de toutes les actions basées sur des stratégies qui ont été appliquées à vos utilisateurs pendant la période sélectionnée. Vous affichez les informations suivantes :

- Nom de l'action appliquée conformément à la stratégie
- Nombre d'utilisateurs auxquels l'action a été appliquée
- Nombre d'occurrences de l'action
- Nombre de stratégies associées à l'action
- Date et heure de l'action appliquée



Cliquez sur une action pour afficher toutes les stratégies associées. Ces stratégies sont triées en fonction du nombre d'occurrences. Par exemple, cliquez sur **Demander une réponse de l'utilisateur final** sur la page **Actions** . La page **Toutes les stratégies** affiche toutes les stratégies associées à l'action **Demander une réponse de l'utilisateur final** .



Sur la page **Toutes les stratégies**, cliquez sur une stratégie pour afficher les événements utilisateur auxquels l'action a été appliquée.

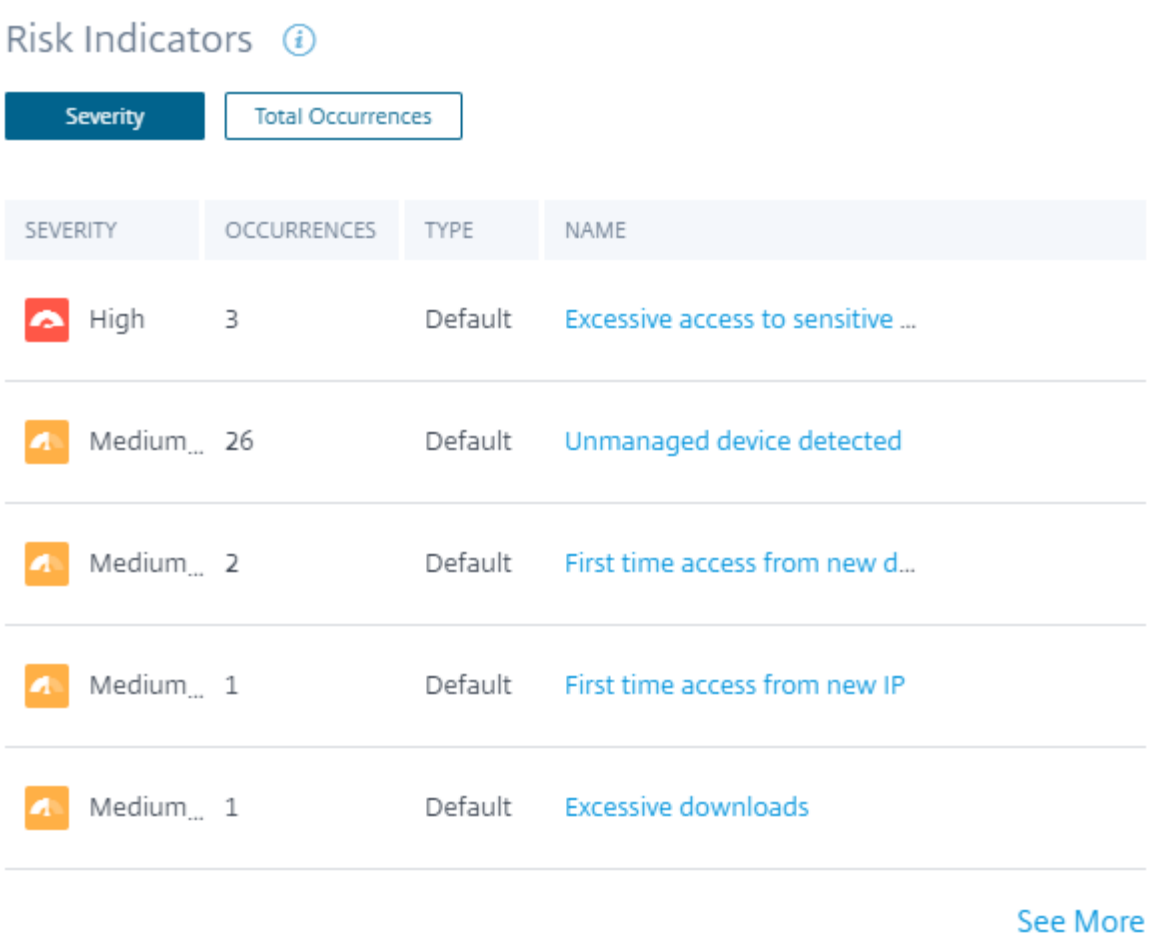
Indicateurs de risque

Résume les cinq principaux indicateurs de risque pour une période sélectionnée. Les indicateurs de risque peuvent être par défaut ou personnalisés. Pour les indicateurs de risque par défaut, Citrix Analytics collecte des données à partir des sources de données découvertes et sur lesquelles le traitement des données est activé.

Pour les indicateurs de risque personnalisés, Citrix Analytics collecte des données à partir des sources de données suivantes en fonction des événements risqués générés :

- Citrix Gateway
- Citrix Secure Private Access
- Citrix Virtual Apps and Desktops
- Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service)

Dans le volet **Indicateurs de risque**, vous pouvez afficher les cinq principaux indicateurs de risque et les trier en fonction du nombre total d'occurrences ou de leur gravité.



Cliquez sur **Voir plus** dans le volet **Indicateurs de risque** pour afficher la page **Aperçu des indicateurs de risque** .

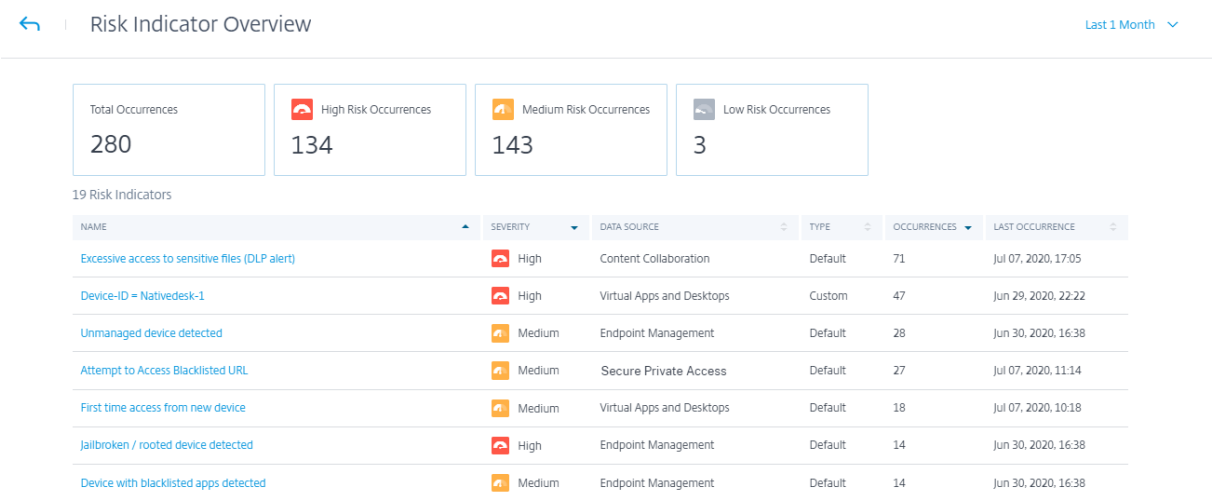


Tableau de bord de garantie des accès

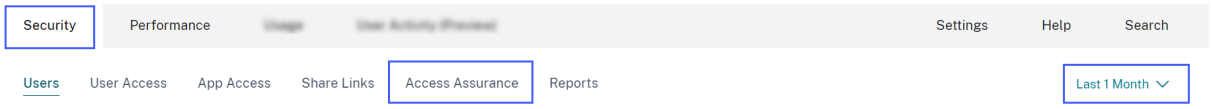
December 5, 2022

Compte tenu de l'augmentation du travail à distance, en tant qu'administrateur informatique Citrix, vous souhaiterez peut-être avoir l'assurance que vos utilisateurs accèdent à Citrix Virtual Apps and Desktops ou Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) depuis leur emplacement habituel et sécurisé. Si des utilisateurs se sont connectés à partir d'emplacements inconnus ou de nouveaux emplacements, vous pouvez valider leurs informations d'ouverture de session et prendre les mesures nécessaires pour atténuer les menaces pesant sur votre environnement informatique Citrix.

Le tableau de bord Access Assurance fournit une vue d'ensemble des emplacements et des réseaux à partir desquels vos utilisateurs accèdent à des applications virtuelles ou à des bureaux virtuels. Citrix Analytics for Security reçoit ces événements d'ouverture de session utilisateur de l'application Citrix Workspace installée sur les appareils des utilisateurs. Pour plus de détails sur les versions prises en charge, consultez la matrice des versions de l'application Citrix Workspace.

Afficher le tableau de bord

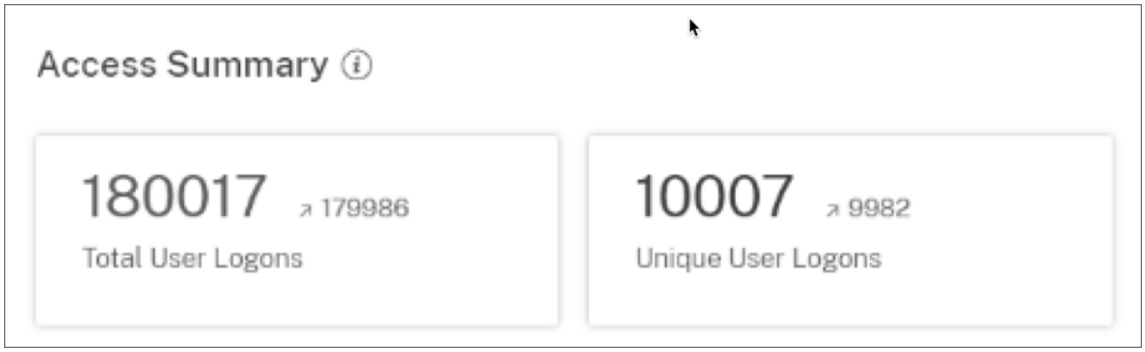
Pour afficher le tableau de bord, cliquez sur **Sécurité > Access Assurance**. Sélectionnez la période pour laquelle vous souhaitez afficher les informations de connexion.



Résumé de l'accès

La section récapitulative du tableau de bord fournit les informations suivantes pour une période sélectionnée :

1. Nombre total de connexions d'utilisateurs sur l'ensemble des sites (dans le monde entier).
2. Nombre total de connexions utilisateur uniques sur l'ensemble des sites (dans le monde entier).



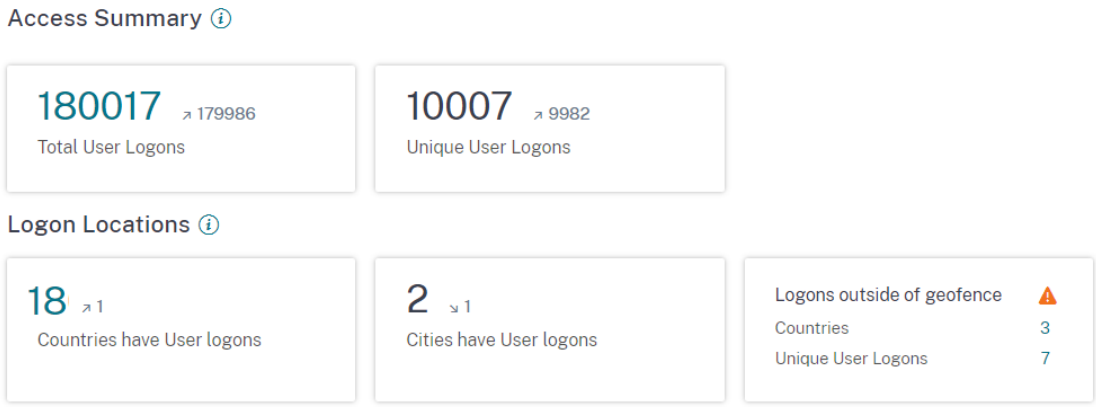
Emplacement de connexion

La section **Emplacements de connexion** fournit les informations suivantes pour une période sélectionnée :

- Nombre total de pays depuis lesquels les utilisateurs se sont connectés.
- Nombre total de villes à partir desquelles les utilisateurs se sont connectés.
- Le nombre total de pays et les ouvertures de session uniques des utilisateurs dans les zones de géofencing. Pour afficher les détails d'ouverture de session à partir des zones de géofencing, activez le géofencing.
- Top 10 des emplacements avec des ouvertures de session utilisateur uniques. Parfois, les ouvertures de session uniques les plus importantes proviennent également de villes et de pays inconnus et elles sont répertoriées sous l'onglet **Unknown Locations (Emplacements inconnus**). La liste des emplacements inconnus est également un sous-ensemble des 10 premiers emplacements. Pour connaître les raisons pour lesquelles certains emplacements ne sont pas identifiés, consultez la section Emplacements identifiés comme non disponibles.

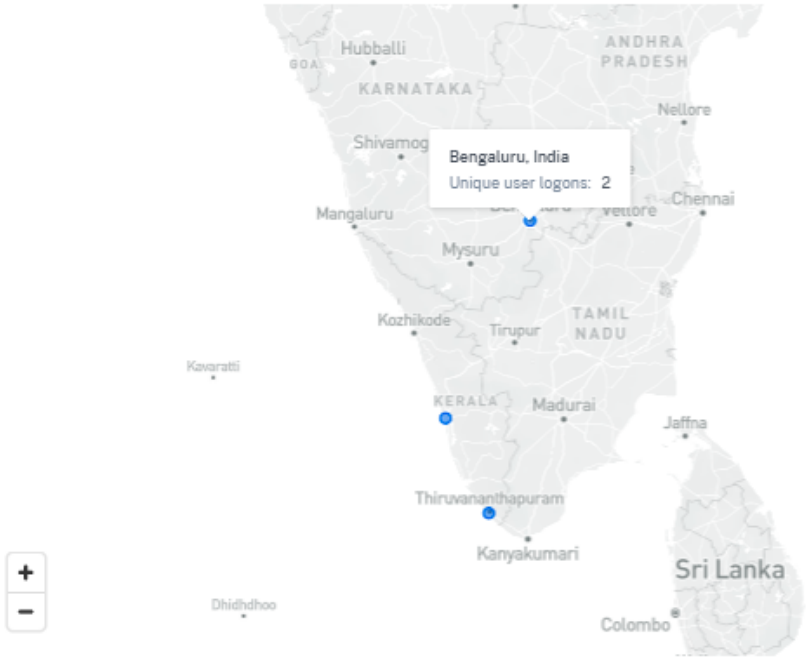
Vous pouvez également consulter la tendance à la hausse ou à la baisse du nombre total de connexions utilisateur dans le monde et du nombre total d'ouvertures de session d'utilisateurs uniques dans le monde. Pour les 10 premiers emplacements, la colonne **ÉCART** indique la modification (positive (+) ou négative (-)) des ouvertures de session utilisateur pour chaque emplacement. Cette comparaison est basée sur la période sélectionnée et la période précédente de durée égale. Par exemple, si vous sélectionnez la période du **dernier mois**, la tendance de connexion de l'utilisateur et l'écart sont comparés entre le dernier mois et le précédent au dernier mois.

> **Remarque**
>
> Les informations de localisation sont fournies au niveau de la ville et du pays et ne représentent pas une géolocalisation précise. Pour plus de détails sur la garantie d'accès et la géolocalisation, consultez la FAQ.

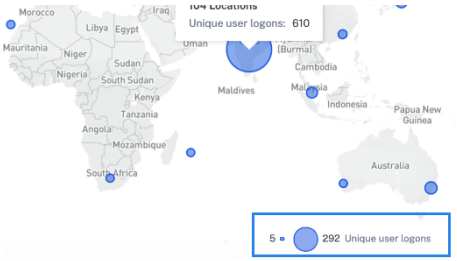


Dans le tableau **Les 10 principaux emplacements d'ouverture de session uniques**, sélectionnez un emplacement pour afficher les utilisateurs, leurs profils d'accès et les détails d'ouverture de session.

La carte affiche le nombre d'utilisateurs uniques de différents emplacements pour une période sélectionnée. Survolez la bulle bleue ou effectuez un zoom avant sur un emplacement pour afficher le nombre total d'ouvertures de session utilisateur uniques à partir de cet emplacement. Cliquez sur la bulle bleue pour afficher les détails d'accès d'un point de vente.



Dans le coin inférieur droit de la carte, vous pouvez afficher la plage des ouvertures de session uniques des utilisateurs. Pour une période sélectionnée, la petite bulle indique le nombre minimum d'ouvertures de session utilisateur uniques dans les emplacements. La grande bulle indique le nombre maximal d'ouvertures de session utilisateur uniques dans les emplacements.

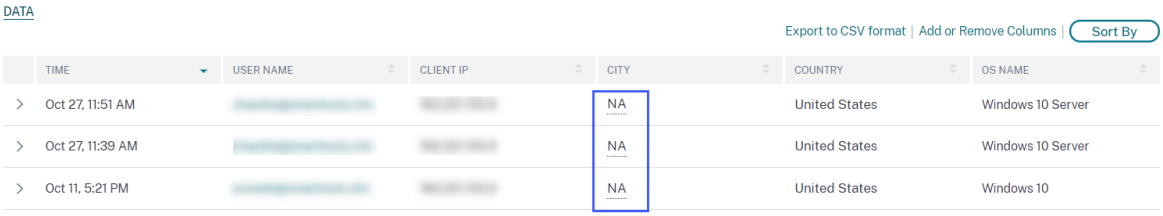


Emplacements identifiés comme non disponibles

Dans le tableau **Les 10 principaux emplacements d'ouverture de session uniques**, vous pouvez constater que certains emplacements sont inconnus ou indisponibles. Cliquez sur un emplacement inconnu pour afficher les informations de connexion utilisateur correspondantes sur la page Ouverture de **session utilisateur** .

Sur la page Ouverture de **session utilisateur**, le tableau **DONNÉES** affiche l'étiquette **NA** si des informations de pays ou de ville ne sont pas disponibles.

Survolez l'étiquette **NA** pour voir la raison pour laquelle les informations de localisation ne sont pas disponibles.



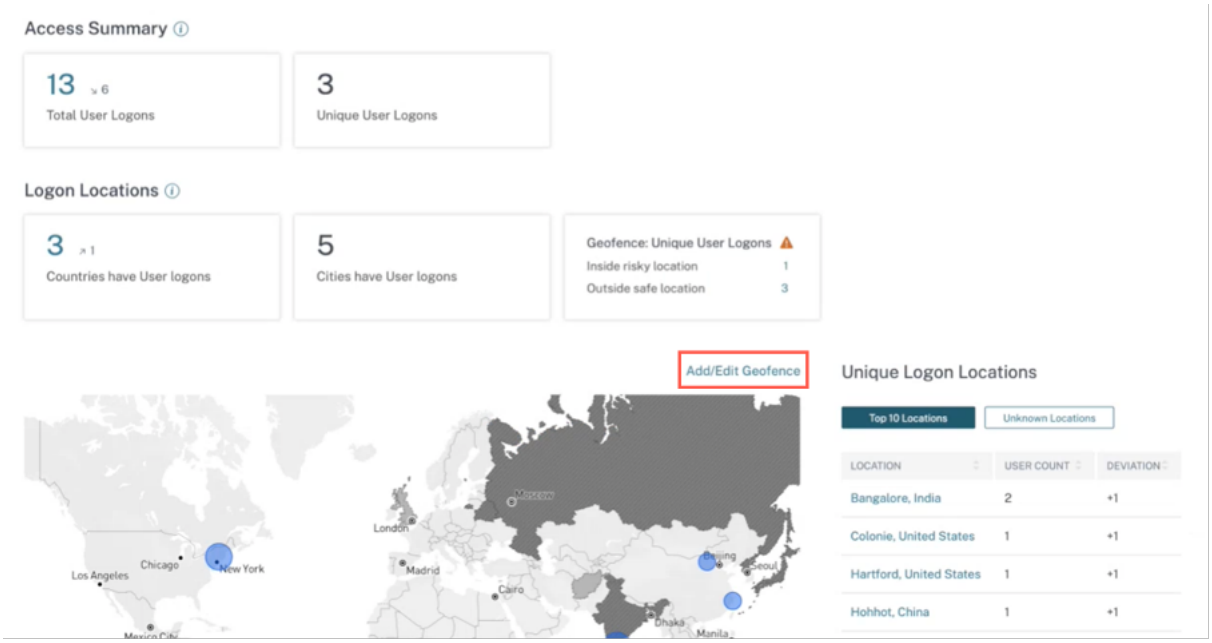
L'un des scénarios suivants peut s'afficher en cas d'indisponibilité d'un emplacement :

Scénario	Raisons
Le nom de la ville et le nom du pays ne sont pas disponibles.	Un des composants suivants 1. Les utilisateurs utilisent une version non prise en charge de l'application Citrix Workspace. Pour afficher les informations de localisation, mettez à jour le client vers une version prise en charge.
Emplacements dotés d'adresses IP privées	L'appareil de l'utilisateur se trouve dans un réseau privé. Dans ce cas, les informations de localisation ne sont pas disponibles pour Citrix Analytics.
Le nom du pays est disponible, mais le nom de la ville n'est pas disponible.	L'appareil de l'utilisateur utilise peut-être une adresse IP d'entreprise. Les plages IP de l'entreprise sont masquées dans le service de géolocalisation externe. Par conséquent, les informations d'emplacement ne sont pas disponibles pour Citrix Analytics.

Activer le géofencing

Le géorepérage vous permet d'identifier les utilisateurs qui accèdent à des applications virtuelles ou à des bureaux virtuels depuis l'extérieur d'une barrière de sécurité et à l'intérieur de zones de géofence à risque. Pour consulter la page **Récapitulatif des accès**, accédez à **Sécurité > Assurance de l'accès**.

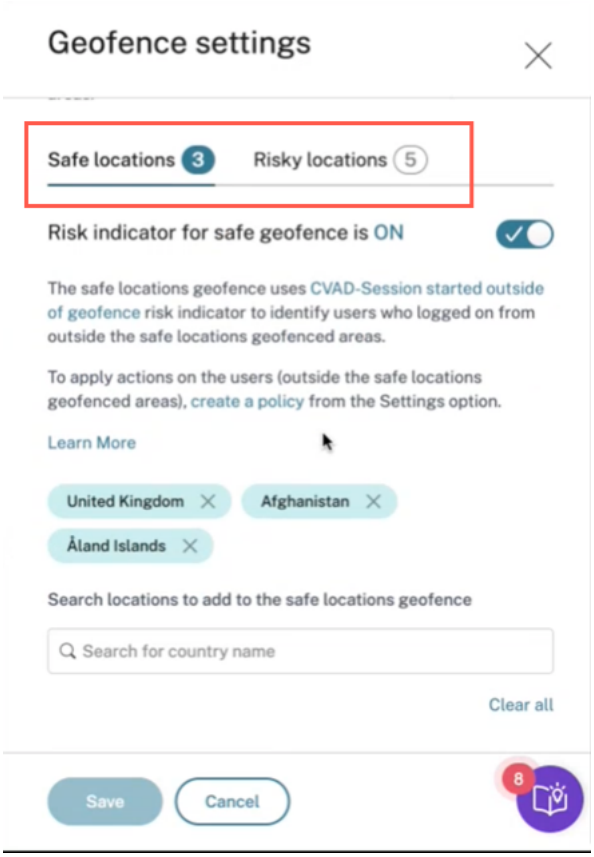
Par défaut, les **paramètres Geofence** sont toujours activés. Pour configurer votre limite géographique, cliquez sur **Ajouter/Modifier la limite géographique**.



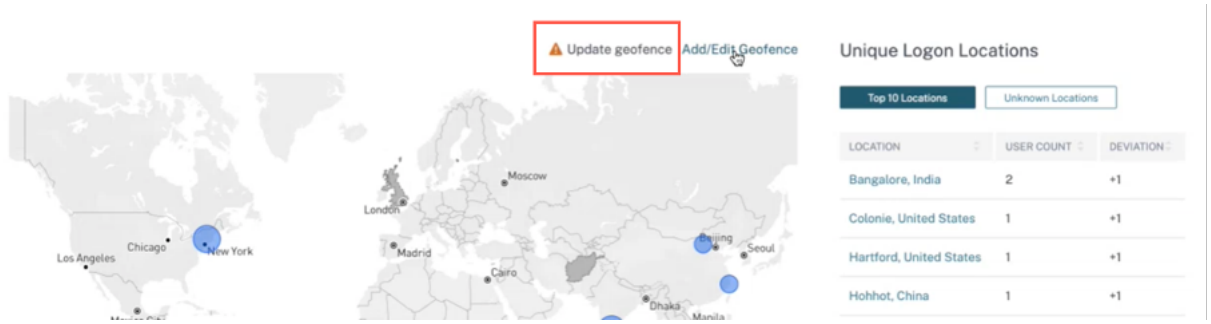
La fenêtre des **paramètres de Geofence** s'affiche avec deux onglets :

- **Endroits sécurisés** : vous pouvez configurer ou supprimer les pays qui font partie de la zone de localisation sécurisée.
- **Lieux à risque** : vous pouvez configurer ou supprimer les pays classés dans la catégorie des zones à risque.

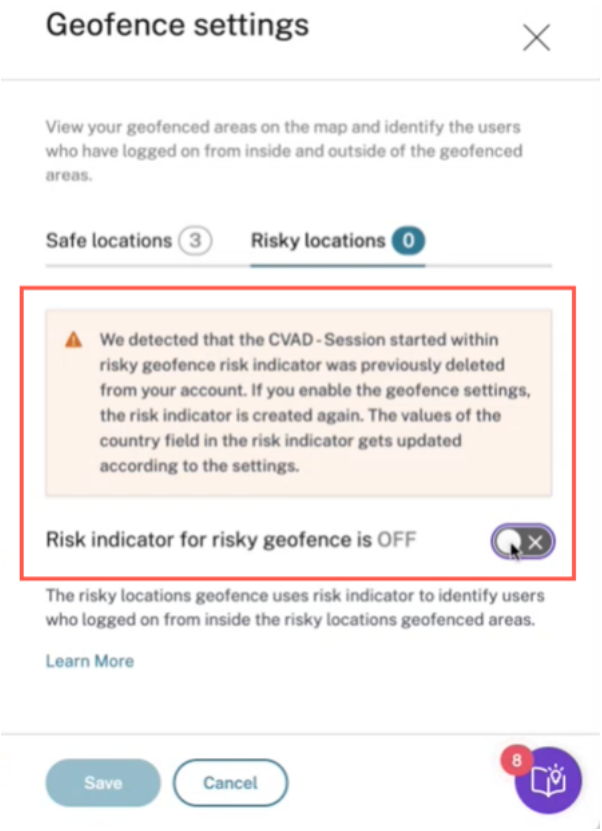
  Vous pouvez également consulter le nombre total d'emplacements sûrs et risqués configurés sur chaque onglet. Pour supprimer ou retirer un pays d'une géofence de localisation sécurisée ou d'une clôture de localisation à risque, cliquez sur le signe de fermeture (X) à côté du pays. Cliquez sur **Enregistrer** pour enregistrer les paramètres de Geofence.



Vous pouvez configurer les pays qui relèvent de la zone de géofence des lieux à risque. Si aucun indicateur de risque n'est ajouté pour la géofence des emplacements risqués ou si les indicateurs de risque sont supprimés, un message d'avertissement de **mise à jour de la géofence** peut s'afficher à côté **de Ajouter/modifier une clôture géographique**.



Pour recréer l'indicateur, accédez à l'onglet **Lieux à risque** et activez l'**indicateur de risque pour les géofences** à risque.



L'indicateur est créé avec la liste par défaut des emplacements à risque.

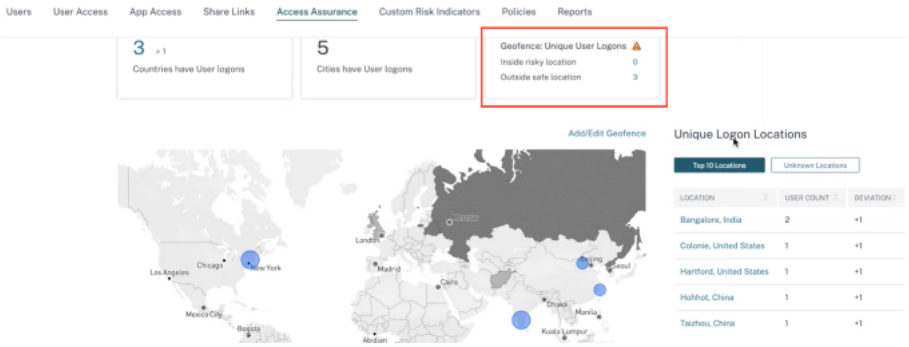
La page de **résumé des accès** affiche également les pays sûrs et risqués Geofenced.

- Les pays sécurisés géofencés sont signalés par un cercle gris clair.
- Géofencés Les pays à risque sont signalés par un cercle gris foncé.

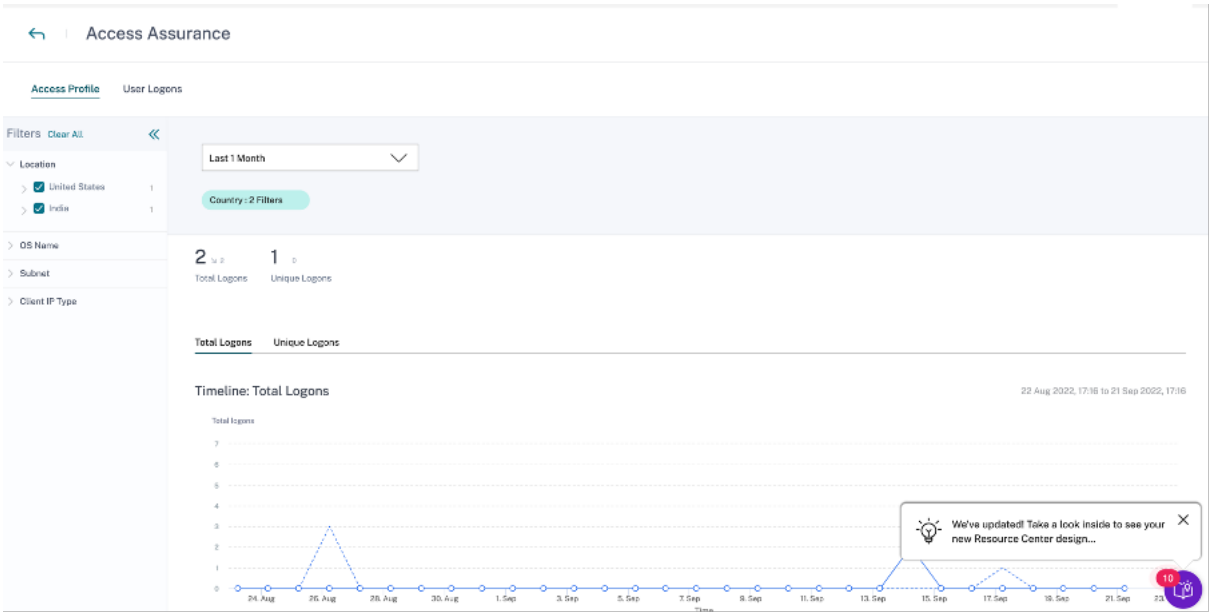
Geofence : connexions utilisateur uniques

Accédez à la page Résumé des accès pour voir Geofence : Unique User Logons. La carte indique le nombre d'emplacements intérieurs à risque et d'emplacements extérieurs sûrs.

- **À l'intérieur d'un emplacement à risque** : identifiez les utilisateurs qui se sont connectés depuis les zones à risque (zones géolocalisées).
- **Endroit extérieur sécurisé** Identifiez les utilisateurs qui se sont connectés depuis l'extérieur des zones sécurisées géo-clôturées.



Pour obtenir un résumé détaillé du nombre total et des ouvertures de session uniques des utilisateurs, cliquez sur le chiffre à côté de Emplacement à risque intérieur ou Emplacement sécurisé extérieur.



Cette fonctionnalité utilise l'indicateur de risque personnalisé préconfiguré suivant :

- La**session CVAD a démarré en dehors de Geofence** : pour surveiller les connexions des utilisateurs en dehors de la zone sécurisée de géofence.
- La**session CVAD a débuté dans une géofence à risque** : pour surveiller les connexions des utilisateurs à l'intérieur de la géofence à risque.

Si des ouvertures de session utilisateur sont détectées en dehors de la clôture géographique, l'indicateur de risque est déclenché et la stratégie Session démarrée en dehors de la zone géographique est appliquée à ces utilisateurs. La stratégie déclenche l'action *Demander une réponse de l'utilisateur final* et, en fonction de la réponse de l'utilisateur, vous pouvez prendre les mesures appropriées pour prévenir les menaces liées à toute ouverture de session suspecte. Pour plus d'informations, consultez la section Indicateurs de risque personnalisés préconfigurés.

> **Remarques**
>
> - Dans les **paramètres de Geofence**, lorsque vous modifiez les pays, la *session CVAD démarrée en dehors de l'indicateur de risque de géofence* est également mise à jour.
> - Par exemple, si vous sélectionnez et enregistrez les pays Australie et Inde en tant que nouveaux pays géo-clôturés, la condition préconfigurée de l'indicateur de risque est mise à jour avec les nouveaux pays, en plus des États-Unis (qui est la clôture géographique par défaut). Vous pouvez également supprimer le pays géofencé par défaut États-Unis.
>
>   Condition préconfigurée de l'indicateur de risque :
>
>   ```
>   Event-Type = \"Session.logon\" AND Country != \"\" AND Country
>    ~ \"\" AND Country != \"United States\"
>   ```
>
>   Après la mise à jour **des paramètres de géofencing**, l'état de l'indicateur de risque :
>
>   ```
>   Event-Type = \"Session.logon\" AND Country != \"\" AND Country
>    ~ \"\" AND Country NOT IN (\"Australia\", \"United States\",
>   \"India\"
>   ```
>
> - Si la *session CVAD démarrée en dehors de l'indicateur de risque de géofence* est précédemment supprimée de votre compte, l'activation des **paramètres de géofencing** crée à nouveau l'indicateur de risque. Les pays géoréférencés de l'indicateur de risque sont contrôlés à partir des **paramètres de Geofence**.

Après avoir activé les **paramètres de géofencing**, la carte affiche les zones délimitées et les ouvertures de session uniques des utilisateurs à partir de ces zones.

Réseau de connexion

Dans le tableau de bord Access Assurance, vous pouvez désormais consulter les informations supplémentaires suivantes sur les utilisateurs :

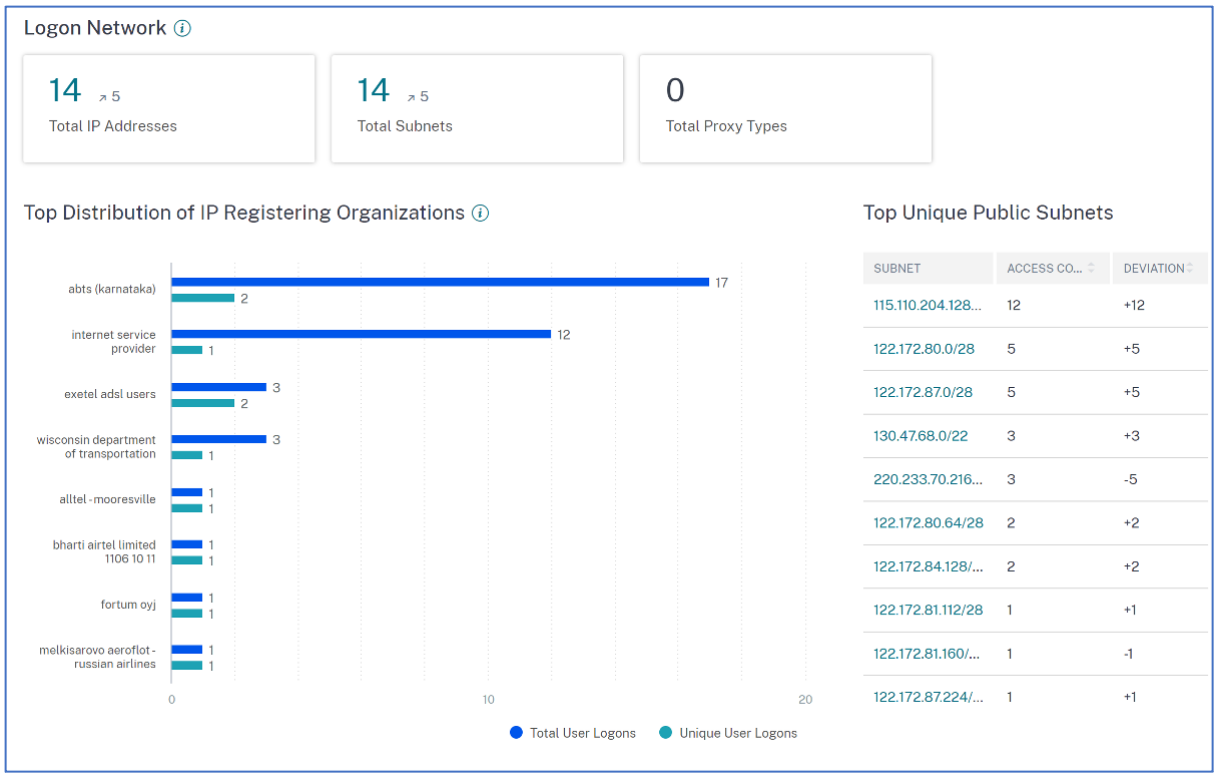
- Les organisations associées aux adresses IP à partir desquelles les utilisateurs se sont connectés. Ces organisations incluent des entités telles que les entreprises, le gouvernement, les entités éducatives et les fournisseurs de services Internet.

- Le total du sous-réseau public unique et du sous-réseau privé à partir duquel les utilisateurs se sont connectés.
- Les informations indiquant que l'utilisateur s'est connecté à l'aide de proxys et de services VPN privés.

À l'aide de ces informations supplémentaires, en tant qu'administrateur, vous pouvez valider les informations de connexion de l'utilisateur et vous assurer que l'ouverture de session de l'utilisateur répond aux attentes de sécurité de l'organisation.

Afficher les détails du réseau utilisateur

Accédez à **Sécurité > Assurance d'accès** et faites défiler l'écran vers le bas pour afficher les détails sous **Logon Network**.

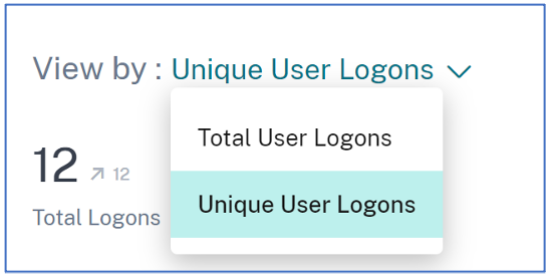


- **Nombre total d'adresses IP** : indique le nombre total d'adresses IP uniques utilisées pour se connecter aux sessions virtuelles.
- **Nombre total de sous-réseaux** : indique le nombre total de sous-réseaux utilisés pour se connecter aux sessions virtuelles.
- **Nombre total de types de proxy** : indique le nombre total de types de réseau ou de protocole utilisés par le serveur pour proxy la connexion utilisateur.

- Dans **la section Répartition principale des organisations enregistrant des adresses IP**, vous pouvez visualiser un aperçu du nombre total d'ouvertures de session utilisateur et des informations de connexion uniques de chaque organisation (ISP). Vous pouvez cliquer sur le graphique pour afficher les détails des utilisateurs, ainsi que leurs profils d'accès et informations de connexion associés à l'organisation sélectionnée.
- Sous **Total des sous-réseaux publics uniques**, vous pouvez visualiser une vue d'ensemble des sous-réseaux, du nombre total d'ouvertures de session utilisateur sur chaque sous-réseau et de la tendance d'écart dans chaque sous-réseau. Vous pouvez cliquer sur chaque sous-réseau pour afficher les détails des utilisateurs, ainsi que leurs profils d'accès et informations de connexion associés au sous-réseau sélectionné.

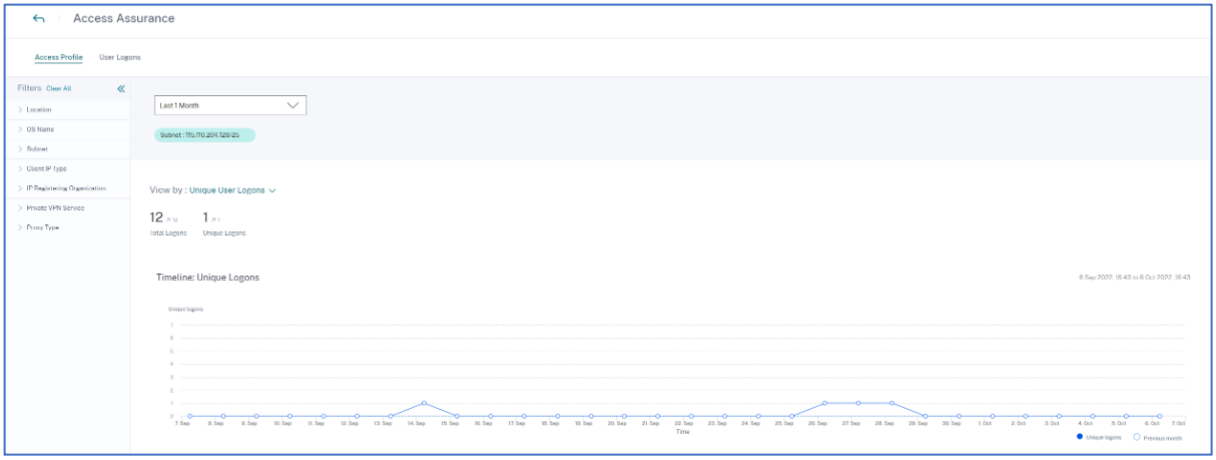
Afficher les profils d'accès des utilisateurs

Lorsque vous analysez une métrique (emplacement, organisation ou sous-réseau), la page **Access Profile** fournit le résumé des accès de vos utilisateurs aux applications virtuelles ou aux bureaux virtuels à partir des emplacements sélectionnés. Vous pouvez sélectionner l'option d'ouverture de session unique ou d'ouverture de session totale pour consulter l'analyse des tendances pour la période sélectionnée.



Vous pouvez consulter les principaux événements d'accès pour la métrique sélectionnée (emplacement, organisation ou sous-réseau). Ces informations vous aident à examiner les modèles d'accès et les détails pour l'investigation et l'analyse des menaces.

La tendance à la hausse ou à la baisse du nombre total d'ouvertures de session utilisateur et des ouvertures de session utilisateur uniques est comparée en fonction de la période sélectionnée et de la période précédente de durée égale. Par exemple, si vous sélectionnez la période comme **Dernier mois**, la tendance est comparée entre le dernier mois et le mois précédent.



Facettes

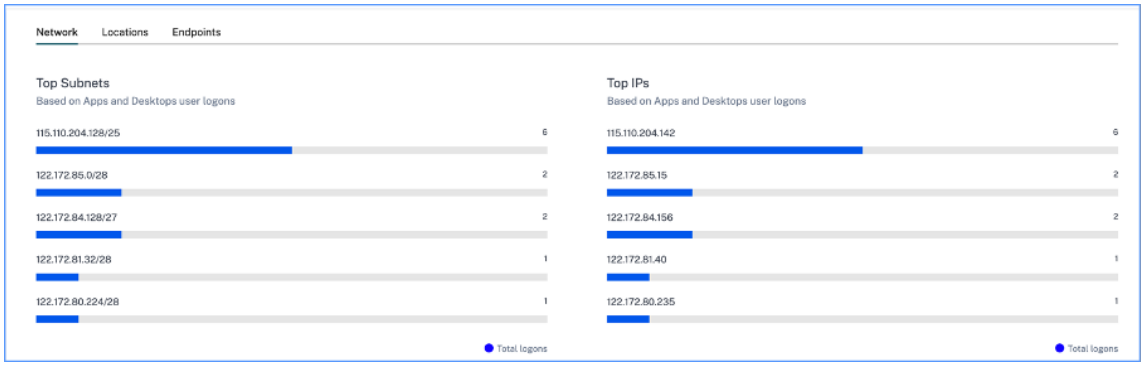
Vous pouvez utiliser les facettes suivantes pour les événements d'accès :

- **Lieu**- Filtrez les événements d'accès par pays et leurs villes.
- **OS**- Filtrez les événements d'accès en fonction des systèmes d'exploitation et de leurs versions.
- **Sous-réseau** : filtrez les événements d'accès par sous-réseaux.
- **Type d'adresse IP du client** : filtrez les événements d'accès par public ou privé.
- **Organisation d'enregistrement IP** : filtrez l'organisation associée à l'adresse IP publique.
- **Service VPN privé** : filtrez les événements d'accès en fonction des noms de réseaux VPN privés.
- **Type de proxy** : filtrez les événements d'accès selon les classifications des types de proxy tels que HTTP, Web, Tor et SOCKS.

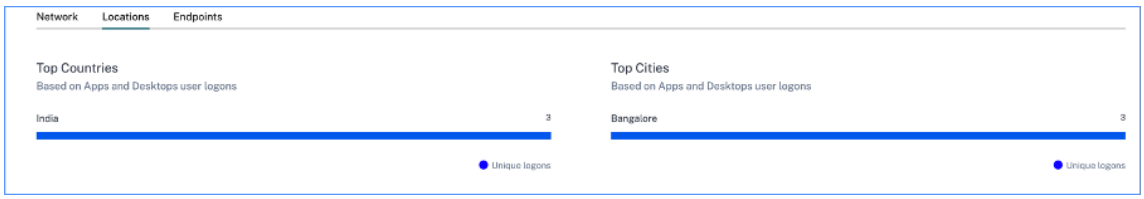
> **Remarque**
>
> L'étiquette non disponible peut également s'afficher si les données sont indisponibles ou non identifiées.

En fonction des filtres appliqués, affichez les informations suivantes pour le nombre total d'ouvertures de session utilisateur et les ouvertures de session utilisateur uniques :

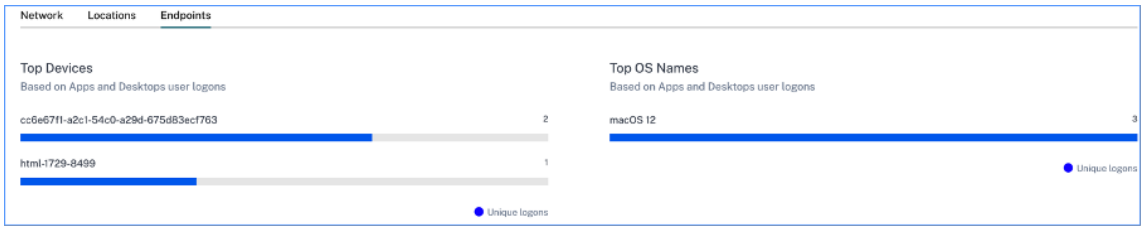
- **Réseau** : principaux sous-réseaux et adresses IP à partir desquels les utilisateurs se sont connectés à des applications virtuelles ou à des bureaux virtuels.



- **Emplacements** : principaux pays et villes à partir desquels les utilisateurs se sont connectés à des applications virtuelles ou à des bureaux virtuels.

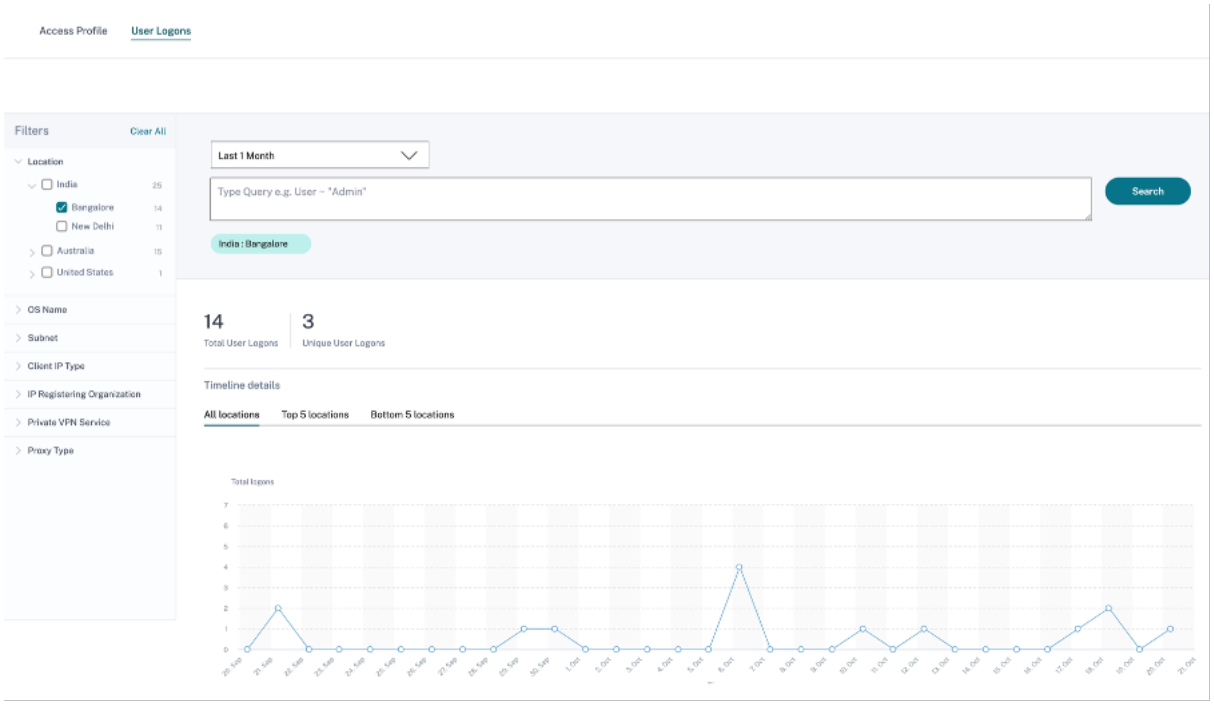


- **Endpoints** : principaux noms d'appareils et de systèmes d'exploitation en fonction des ouvertures de session des utilisateurs des applications et des ordinateurs de bureau.



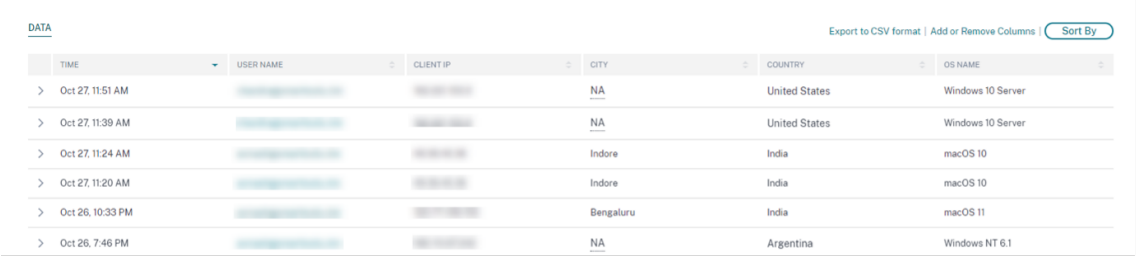
Afficher les détails des ouvertures de session des utilisateurs

La page Ouverture de **session utilisateur fournit les détails des ouvertures** de session utilisateur aux applications virtuelles ou aux bureaux virtuels à partir des emplacements sélectionnés. Ces informations vous aident lors de l'investigation et de l'analyse des menaces.



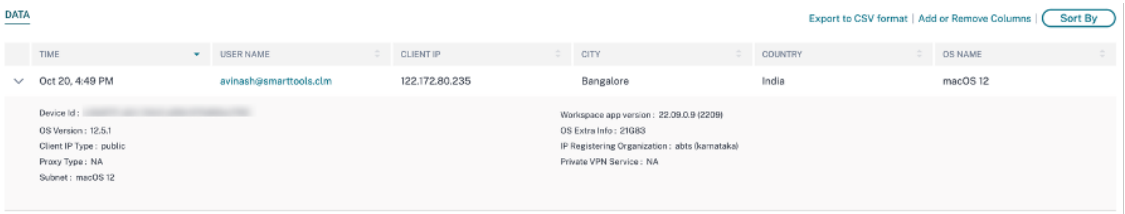
Le tableau **DATA** affiche les détails d'ouverture de session suivants pour les emplacements sélectionnés et la période :

- **Heure**. La date et l'heure auxquelles l'utilisateur s'est connecté.
- **Nom d'utilisateur**. L'identité de l'utilisateur.
- **Adresse IP du client**. L'adresse IP de la machine utilisateur.
- **Type d'adresse IP du client**. Type d'adresse IP de l'utilisateur (publique ou privée, par exemple).
- **Ville et pays**. Les emplacements à partir desquels l'utilisateur s'est connecté à des applications virtuelles ou à des bureaux virtuels.
- **ID du périphérique**. Code d'identité de la machine utilisateur.
- **Nom du système d'exploitation** Le système d'exploitation sur la machine utilisateur. Pour plus d'informations, consultez la section Recherche en libre-service d'applications et de bureaux.



Si vous élargissez chaque événement, vous pouvez voir les informations suivantes :

- **version du système d'exploitation** La version du système d'exploitation sur la machine utilisateur. Pour plus d'informations, consultez la section Recherche en libre-service d'applications et de bureaux.
- **Informations supplémentaires sur le système d'exploitation** : informations supplémentaires sur le système d'exploitation, telles que les numéros de version, les Service Packs et les correctifs. Pour plus d'informations, consultez la section Recherche en libre-service d'applications et de bureaux.
- **Version de l'application Workspace**. La version de génération de l'application Citrix Workspace ou de Citrix Receiver.



Dans le tableau **DATA**, vous pouvez effectuer les opérations suivantes :

- Cliquez sur **Ajouter ou supprimer des colonnes** pour mettre à jour les colonnes de la table en fonction de la façon dont vous souhaitez afficher les données.
- Cliquez sur **Trier par** et sélectionnez les éléments de données pour effectuer un tri sur plusieurs colonnes. Pour plus d'informations, consultez la section Tri multi-colonnes.
- Cliquez sur **Exporter au format CSV** pour télécharger les données affichées dans le tableau DATA dans un fichier CSV et les utiliser pour votre analyse.

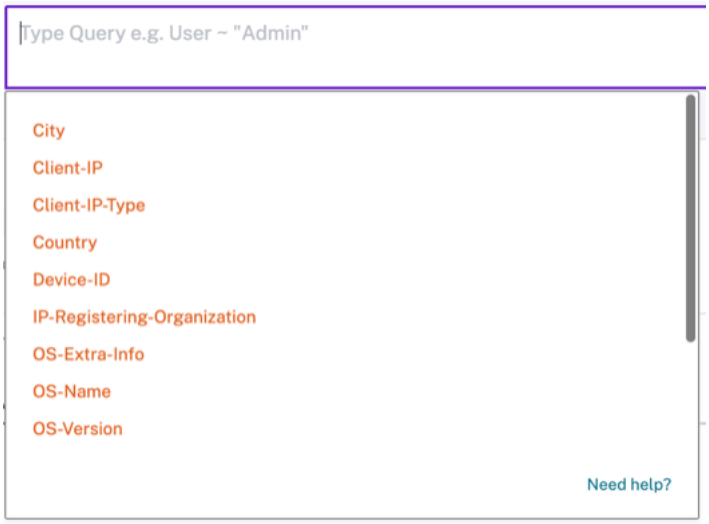
Barre de recherche

Vous pouvez également utiliser la barre de recherche pour définir votre requête à l'aide des dimensions associées à un événement d'ouverture de session.

Par exemple :

```
User = "test user" AND Client-IP = "10.xx.xx.xx AND Client-IP-Type =
public"
```

```
User = "demo_user@citrix.com" AND OS-Major-Version = "macOS 10.13" AND
 OS-Minor-Version = 6
```

Facettes

Vous pouvez utiliser les facettes suivantes pour les événements d'ouverture de session :

- **Emplacements** : filtrez les événements d'ouverture de session par pays et par ville.
- Système d'**exploitation**- Filtrez les événements d'ouverture de session par système d'exploitation et leurs versions.
- **Sous-réseau** : filtrez les événements d'accès par sous-réseaux.
- **Type d'adresse IP client**- Filtrez les événements d'accès par type d'adresse IP publique et privée.
- **Organisation d'enregistrement IP** : filtrez les événements d'accès par fournisseur de services Internet utilisé par l'utilisateur.
- **Service VPN privé** : filtrez les événements d'accès en fonction des noms de réseaux VPN privés.
- **Type de proxy** : filtrez les événements d'accès selon les classifications des types de proxy tels que HTTP, Web, Tor et SOCKS.

> **Remarque**
>
> L'étiquette non disponible peut également s'afficher si les données sont indisponibles ou non identifiées.

Chronologie et profil des risques utilisateur

December 7, 2023

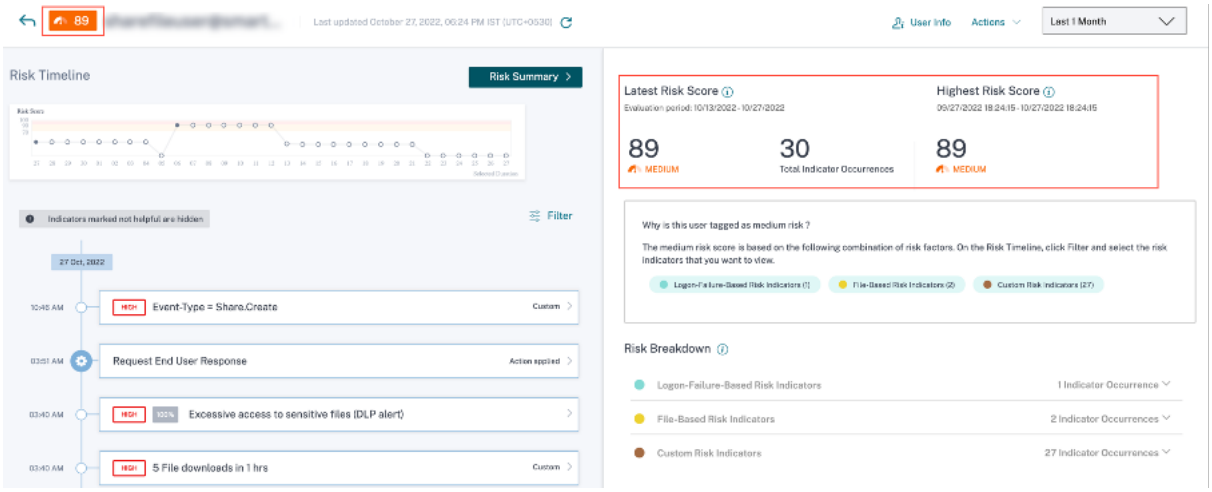
> **Remarque**
>
> **Attention** : Citrix Content Collaboration et ShareFile ont atteint leur fin de vie et ne sont plus disponibles pour les utilisateurs.

La chronologie des risques utilisateur sur le profil d'un utilisateur vous permet, en tant qu'administrateur Citrix Analytics, d'obtenir des informations plus approfondies sur le comportement risqué d'un utilisateur. Par défaut, la chronologie des risques utilisateur est affichée pour le dernier mois. Vous pouvez également voir les actions correspondantes effectuées sur leur compte pendant une période sélectionnée. À partir de la chronologie des risques utilisateur, vous pouvez approfondir le profil d'un utilisateur pour comprendre les éléments suivants :

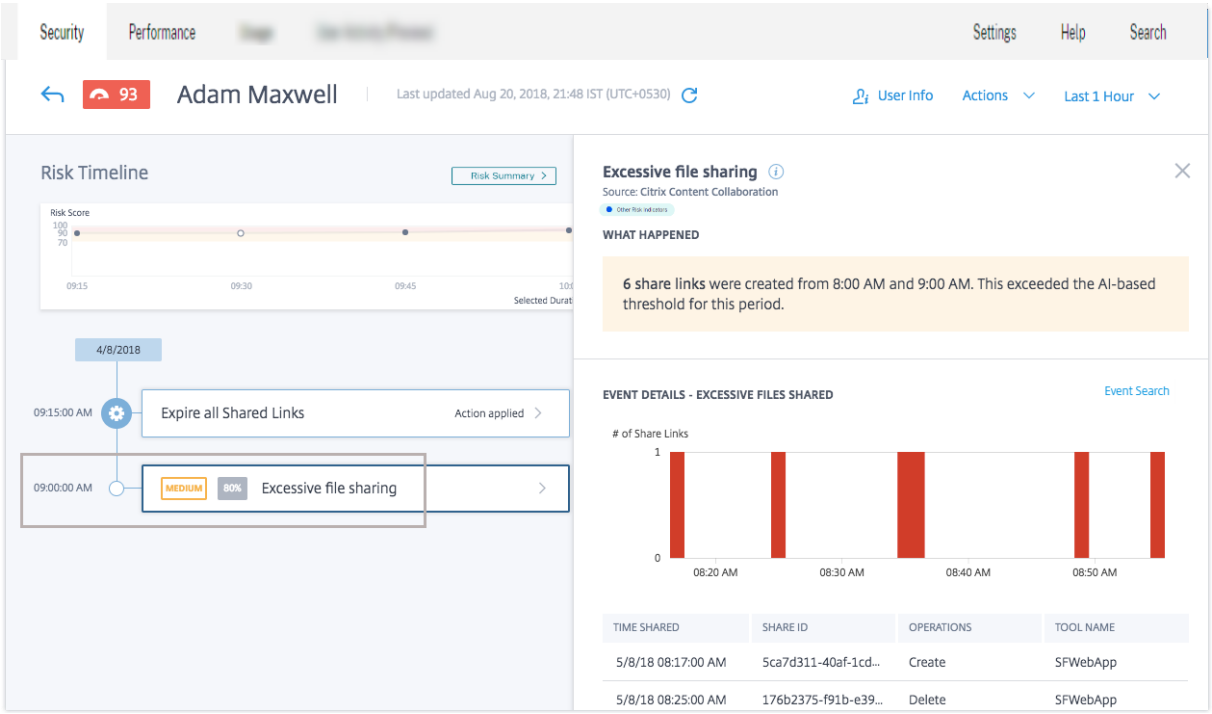
- Utilisation de l'application
- Utilisation des données
- Utilisation des appareils
- Utilisation des emplacements

Vous pouvez également afficher le score de risque et les tendances des indicateurs de risque pour l'utilisateur et déterminer s'il s'agit d'un utilisateur à haut risque ou non.

Vous pouvez consulter le dernier score de risque de l'utilisateur dans le coin supérieur gauche de la page Chronologie des risques utilisateur. Les rapports de visualisation du **résumé des risques** présentent à la fois les scores maximaux les plus récents et historiques.



Lorsque vous accédez à la chronologie des risques d'un utilisateur, vous pouvez sélectionner un indicateur de risque ou une action qui a été appliquée à son compte. Si vous choisissez l'une des options ci-dessus, le volet droit affiche la section Indicateur de risque ou la section Action.

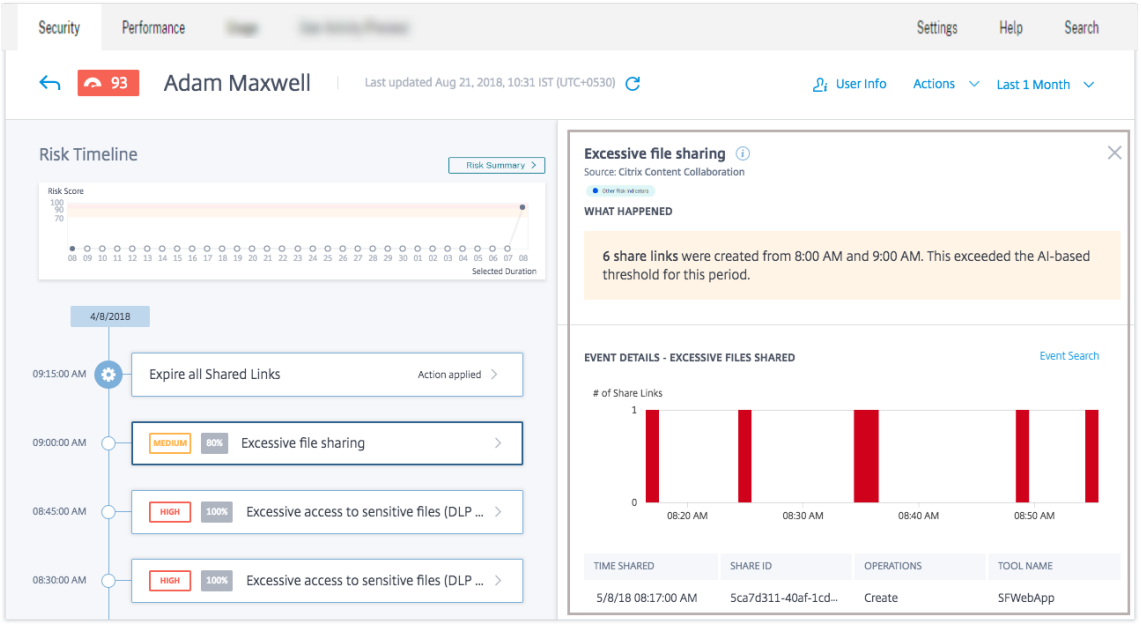


Chronologie des risques

La chronologie des risques affiche les informations suivantes :

- **Indicateurs de risque**. Les indicateurs de risque sont des activités des utilisateurs suspectes ou susceptibles de poser une menace à la sécurité de votre organisation. Les indicateurs sont déclenchés lorsque le comportement de l'utilisateur s'écarte de son comportement normal. Les indicateurs de risque peuvent être destinés aux sources de données suivantes :
  - Citrix Content Collaboration
  - Citrix Gateway
  - Citrix Endpoint Management
  - Citrix Virtual Apps and Desktops ou Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service)
  - Citrix Secure Private Access

  Lorsque vous sélectionnez un indicateur de risque dans la chronologie de l'utilisateur, la section Informations sur l'indicateur de risque s'affiche dans le volet droit. Vous pouvez consulter la raison de l'indicateur de risque ainsi que les détails de l'événement. Ils sont globalement classés dans les sections suivantes :



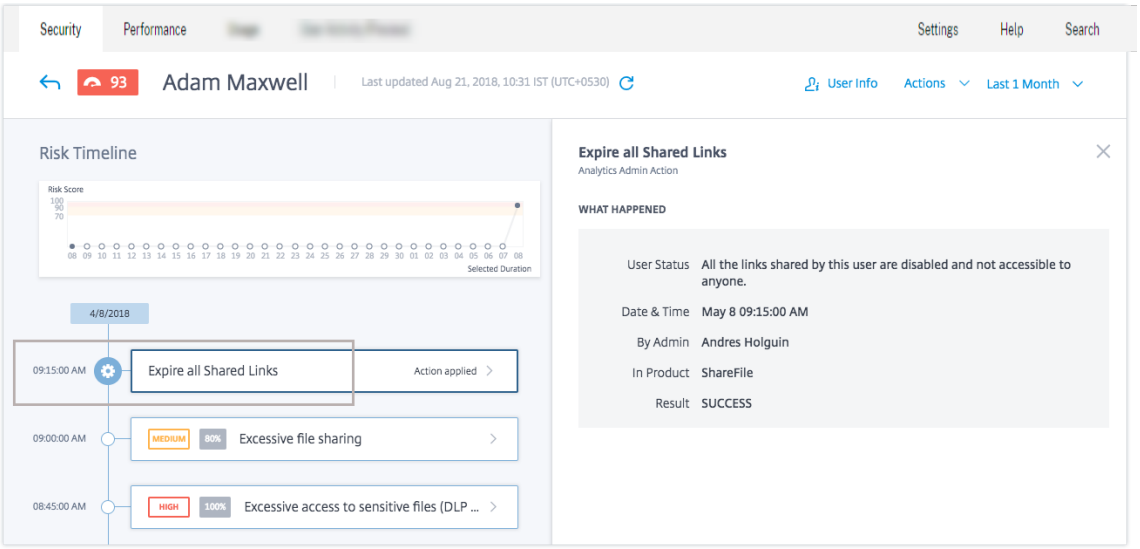
- **Que s'est-il passé** ? Vous pouvez consulter un résumé de l'indicateur de risque ici. Par exemple, si vous avez sélectionné l'indicateur de risque de **partage de fichiers excessif** . Dans la section Que s'est-il passé, vous pouvez afficher le nombre de liens de partage envoyés aux destinataires et le moment où l'événement de partage s'est produit.
- **Détails de l'événement**. Vous pouvez afficher les entrées d'événements individuels sous forme graphique et tabulaire, ainsi que les détails de l'événement. Cliquez sur **Recherche d'événements** pour accéder à la page de recherche en libre-service et afficher les événements correspondant à l'indicateur de risque de l'utilisateur. Pour plus d'informations, consultez la rubrique **Recherche en libre-service**.
- **Informations contextuelles supplémentaires**. Vous pouvez consulter les données partagées, le cas échéant, pendant la survenance d'un événement dans cette section.

Vous pouvez marquer manuellement les indicateurs de risque comme utiles ou inutiles. Pour plus d'informations, voir Fournir des commentaires sur les indicateurs de risque utilisateur.

En savoir plus : Indicateurs de risque

- **Des actions**. Les actions vous aident à réagir aux événements suspects et à prévenir de futurs événements anormaux. Les actions qui ont été appliquées au profil d'un utilisateur sont affichées sur la chronologie des risques. Ces actions sont automatiquement appliquées au compte d'un utilisateur via des stratégies configurées ou vous pouvez appliquer manuellement une action spécifique.

  Pour en savoir plus : Stratégies et actions.



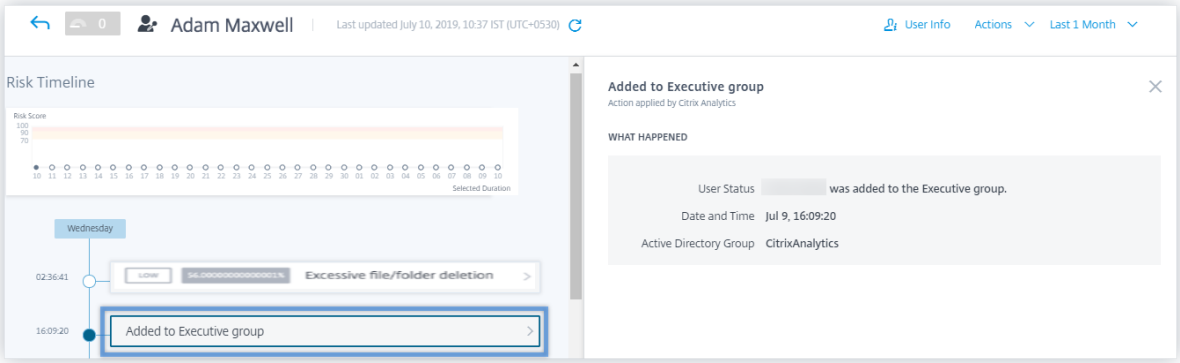
- **Événements d'utilisateurs privilégiés**. Les événements d'utilisateur privilégié sont déclenchés chaque fois qu'il y a un changement dans le statut du privilège Admin ou Executive d'un utilisateur. Lorsqu'un indicateur de risque est déclenché pour un utilisateur, vous pouvez le mettre en corrélation avec l'événement de changement de statut de privilège spécifié. Si nécessaire, vous pouvez appliquer l'action appropriée sur le profil utilisateur. Les événements de privilège Admin ou Executive affichés sur la chronologie des risques utilisateur sont les suivants :

  - Ajouté au groupe Executive
  - Supprimé du groupe Exécutif
  - Privilège élevé au rang d'administrateur
  - Privilège d'administrateur supprimé

  Prenons l'exemple de l'utilisateur Adam Maxwell qui a été ajouté au groupe de privilèges Executive **CitrixAnalytics**. L'événement du **groupe Added to Executive** est ajouté à la chronologie des risques de l'utilisateur. Maintenant, Adam commence à supprimer des fichiers et des dossiers de manière excessive et déclenche l'algorithme d'apprentissage automatique qui détecte les comportements inhabituels. L'indicateur de risque de **suppression excessive de fichiers ou de dossiers** est ajouté à la chronologie des risques de l'utilisateur. Vous pouvez comparer l'événement et l'indicateur de risque sur la chronologie des risques. Après la comparaison, vous pouvez déterminer si l'indicateur de risque a été déclenché à la suite de l'événement. Si tel est le cas, vous pouvez appliquer les actions appropriées au profil d'Adam. Pour plus d'informations sur les utilisateurs privilégiés, consultez la section Utilisateurs privilégiés.

Lorsque vous sélectionnez un événement dans la chronologie de l'utilisateur, la section des informations sur l'événement s'affiche dans le volet droit.

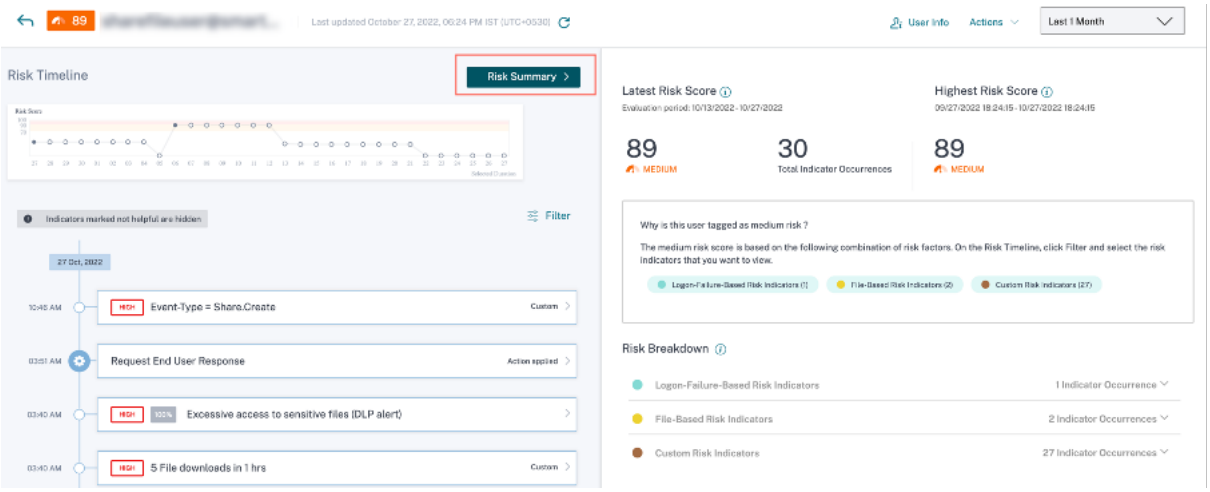
Pour un exécutif, le volet droit affiche des informations telles que le **statut de l'utilisateur**, **la date et l'heure**et le **groupe Active Directory**.



Pour un événement de privilège Admin, le volet droit affiche des informations telles que le **statut de l'utilisateur**, **la date et l'heure**et **Dans le produit**.

Résumé des risques

Affichez les facteurs de risque associés à l'utilisateur qui ont contribué à son score de risque. Vous pouvez consulter les détails du score de risque considéré comme le maximum sur la période sélectionnée, ainsi que le score le plus récent et le nombre d'indicateurs de risque correspondants. Lorsque vous accédez à la chronologie de l'utilisateur à partir de la page d'accueil principale ou de la page Utilisateurs à risque, la sélection de l'heure est conservée depuis la page source. Pour plus d'informations sur les facteurs de risque, consultez la section Indicateurs de risque utilisateur Citrix.



Cliquez sur **Résumé des risques** pour afficher les informations suivantes :

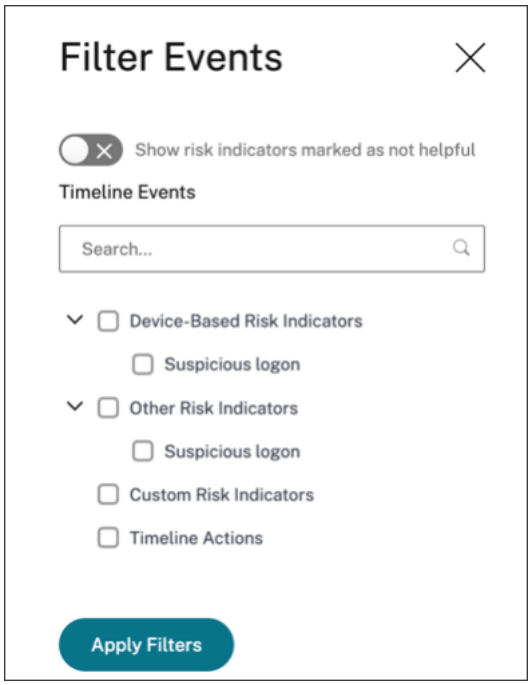
- **Dernier score de risque** : Le dernier score de risque indique le risque actuel de l'utilisateur en fonction de son comportement récent. Le score de risque détermine le niveau de risque qu'un utilisateur représente pour une organisation au cours des deux dernières semaines. La

valeur du score de risque est dynamique et varie en fonction de l'analyse du comportement des utilisateurs. Sur la base du score, un utilisateur peut appartenir à l'une des catégories suivantes : utilisateur à haut risque, utilisateur à risque moyen, utilisateur à faible risque et utilisateur ayant un score de risque nul. Pour plus d'informations sur les catégories d'utilisateurs, consultez Tableau de bord des utilisateurs.

  - **Nombre total d'occurrences d'indicateurs** : indique le nombre total d'indicateurs de risque déclenchés par l'utilisateur au cours des deux dernières semaines. Ces indicateurs de risque déclenché déterminent le score de risque de l'utilisateur.

- **Score de risque**le plus élevé : Le score de risque le plus élevé indique la valeur maximale des scores de risque calculés pour cet utilisateur pendant la durée sélectionnée. Il est représentatif du risque global pour l'utilisateur et peut ne pas toujours être égal au score de risque le plus récent.
- **Facteurs de risque** : indique une ou plusieurs combinaisons de facteurs de risque associés aux activités de l'utilisateur qui ont contribué au score de risque.
- **Répartition des risques** : indique le nombre d'indicateurs de risque déclenchés par l'utilisateur pour chaque facteur de risque. Développez la ligne pour afficher les détails.

Dans la chronologie de l'utilisateur, cliquez sur **Filtrer** et sélectionnez les facteurs de risque, les actions appliquées ou le statut d'utilisateur privilégié associé à l'utilisateur et affichez les événements correspondants.



Profil utilisateur

La page **Profil utilisateur** affiche les informations utilisateur suivantes qui proviennent de l'Active Directory de l'utilisateur :

- Intitulé du poste
- Adresse
- E-mail
- Phone
- Emplacement
- Organization

Indicateurs de risque utilisateur Citrix

April 12, 2024

> **Remarque**
>
> **Attention** : Citrix Content Collaboration et ShareFile ont atteint leur fin de vie et ne sont plus disponibles pour les utilisateurs.

Les indicateurs de risque utilisateur sont des activités utilisateur qui semblent suspectes ou qui peuvent constituer une menace pour la sécurité de votre organisation. Ces indicateurs de risque couvrent tous les produits Citrix utilisés dans votre déploiement. Les indicateurs de risque sont déclenchés lorsque le comportement de l'utilisateur s'écarte de la normale. Chaque indicateur de risque peut être associé à un ou plusieurs facteurs de risque. Ces facteurs de risque vous aident à déterminer le type d'anomalies dans les événements utilisateur. Les indicateurs de risque et les facteurs de risque associés déterminent le score de risque d'un utilisateur.

Les facteurs de risque associés aux indicateurs de risque sont les suivants :

- **Indicateurs de risque basés sur l'appareil** : se déclenche lorsqu'un utilisateur se connecte à partir d'un appareil considéré comme inhabituel en fonction de l'historique des appareils de l'utilisateur.
- **Indicateurs de risque basés sur la localisation** : se déclenche lorsqu'un utilisateur se connecte à partir d'une adresse IP associée à un emplacement considéré comme inhabituel en fonction de l'historique des positions de l'utilisateur.

- **Indicateurs de risque basés sur l'adresse IP** : se déclenche lorsqu'un utilisateur tente d'accéder à des ressources à partir d'une adresse IP identifiée comme suspecte, que l'adresse IP soit inhabituelle ou non pour l'utilisateur.
- **Indicateurs de risque basés sur les échecs de connexion** : se déclenche lorsqu'un utilisateur présente un schéma d'échecs de connexion excessifs ou inhabituels.
- **Indicateurs de risque basés sur**les données : se déclenche lorsqu'un utilisateur tente d'exfiltrer des données hors d'une session Workspace. Les comportements des utilisateurs observés incluent le copier-coller des événements, les modèles de téléchargement, etc.
- **Indicateurs de risque basés sur les fichiers** : déclenche lorsque le comportement d'un utilisateur concernant l'accès aux fichiers sur Content Collaboration est considéré comme inhabituel en fonction de son modèle d'accès historique. Les comportements des utilisateurs observés incluent les modèles de téléchargement, l'accès à du contenu sensible, les activités indiquant la présence de ransomwares, etc.
- **Indicateurs de risque personnalisés** : se déclenche lorsqu'une condition préconfigurée ou une condition définie par l'utilisateur est remplie. Pour plus d'informations, consultez les articles suivants :
  - Indicateurs de risque personnalisés
  - Indicateurs et stratégies de risque personnalisés préconfigurés
- Autres indicateurs de risque : indicateurs de risque qui n'appartiennent à aucun des facteurs de risque prédéfinis tels que les indicateurs de risque basés sur l'appareil, la localisation et les défaillances de connexion.

Les indicateurs de risque sont également regroupés en catégories de risque en fonction des risques similaires. Pour plus d'informations, consultez Catégories de risques.

Le tableau suivant montre la corrélation entre les indicateurs de risque, les facteurs de risque et les catégories de risque.

Produits	Indicateur de risque utilisateur	Facteur de risque	Catégorie de risque
Citrix Endpoint Management	Appareil avec des applications sur la liste noire détectées	Autres indicateurs de risque	Points de terminaison compromis
	Appareil jailbreaké ou rooté détecté	Autres indicateurs de risque	Points de terminaison compromis
	Périphérique non géré détecté	Autres indicateurs de risque	Points de terminaison compromis

Produits	Indicateur de risque utilisateur	Facteur de risque	Catégorie de risque
Citrix Gateway	Échec de l'analyse EPA (End Point Analysis)	Autres indicateurs de risque	Utilisateurs compromis
	Échec excessif de l'authentification	Indicateurs de risque basés sur les échecs de connexion	Utilisateurs compromis
	Voyages impossibles	Indicateurs de risque basés sur la localisation	Utilisateurs compromis
	Ouverture de session à partir d'une adresse IP suspecte	Indicateurs de risque basés sur IP	Utilisateurs compromis
	Ouverture de session suspecte	Indicateurs de risque basés sur les appareils, indicateurs de risque basés sur IP, indicateurs de risque basés sur la localisation et autres indicateurs de risque	Utilisateurs compromis
	Échec d'authentification inhabituel	Indicateurs de risque basés sur les échecs de connexion	Utilisateurs compromis
Citrix Secure Private Access	Tentative d'accès à une URL de liste noire	Autres indicateurs de risque	Menaces internes
	Téléchargement excessif de données	Autres indicateurs de risque	Menaces internes
	Accès à un site Web risqué	Autres indicateurs de risque	Menaces internes
	Volume de téléchargement inhabituel	Autres indicateurs de risque	Menaces internes

Produits	Indicateur de risque utilisateur	Facteur de risque	Catégorie de risque
Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) et Citrix Virtual Apps and Desktops sur site	Voyages impossibles	Indicateurs de risque basés sur la localisation	Utilisateurs compromis
	Exfiltration potentielle des données	Indicateurs de risque basés sur des données	Exfiltration de données
	Ouverture de session suspecte	Indicateurs de risque basés sur les appareils, indicateurs de risque basés sur IP, indicateurs de risque basés sur la localisation et autres indicateurs de risque	Utilisateurs compromis

Vous pouvez marquer manuellement les indicateurs de risque comme utiles ou inutiles. Pour plus d'informations, voir Fournir des commentaires sur les indicateurs de risque utilisateur.

Indicateurs de risque de Citrix Endpoint Management

May 6, 2022

Appareil avec des applications sur la liste noire détectées

Citrix Analytics détecte les menaces d'accès en fonction de l'activité sur un appareil doté d'applications sur liste noire et déclenche l'indicateur de risque correspondant.

L'indicateur de risque **Appareil avec des applications sur liste noire détectées** est déclenché lorsque le service Endpoint Management détecte une application sur la liste noire pendant l'inventaire des logiciels. L'alerte garantit que seules les applications autorisées sont exécutées sur les appareils qui se trouvent sur le réseau de votre organisation.

Le facteur de risque associé à l'indicateur de risque de l'appareil dont les applications sont répertoriées sur la liste noire sont les autres indicateurs de risque. Pour plus d'informations sur les facteurs de risque, consultez la section Indicateurs de risque utilisateur Citrix.

Quand l'indicateur de risque détecté de l'appareil avec des applications sur la liste noire est-il déclenché ?

L'indicateur de risque de **détection d'un appareil avec des applications** sur liste noire est signalé lorsque des applications en liste noire sont détectées sur l'appareil d'un utilisateur. Lorsque le service Endpoint Management détecte une ou plusieurs applications sur la liste noire sur un appareil lors de l'inventaire logiciel, un événement est envoyé à Citrix Analytics.

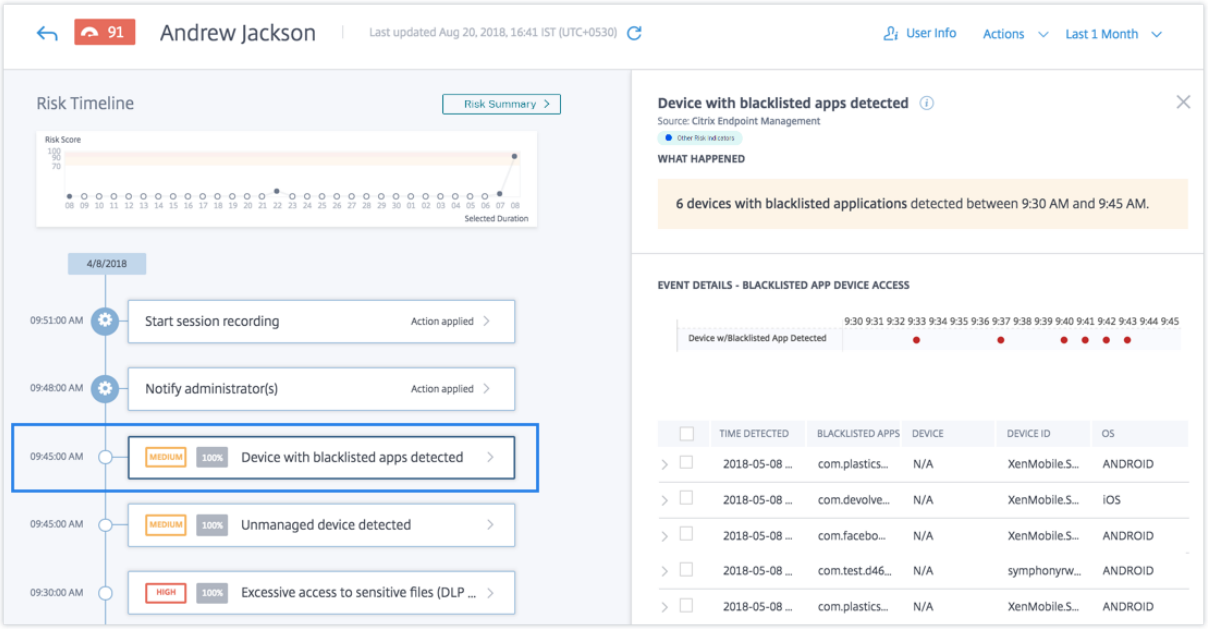
Citrix Analytics surveille ces événements et met à jour le score de risque de l'utilisateur. En outre, il ajoute une entrée d'indicateur de risque **détectée par les applications sur liste noire** à la chronologie des risques de l'utilisateur.

Comment analyser l'appareil avec des applications sur la liste noire détecté indicateur de risque ?

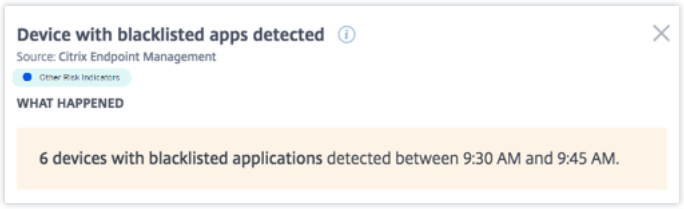
Prenons l'exemple de l'utilisateur Andrew Jackson, qui a utilisé un appareil sur lequel des applications ont été récemment installées sur la liste noire. Endpoint Management signale cette condition à Citrix Analytics, qui affecte un score de risque mis à jour à Andrew Jackson.

Dans la chronologie des risques d'Andrew Jackson, vous pouvez sélectionner l'indicateur de risque de **détection de l'appareil signalé avec les applications sur liste noire** . La raison de l'événement s'affiche avec des détails tels que la liste des applications sur la liste noire, la date à laquelle Endpoint Management a détecté l'application sur la liste noire, etc.

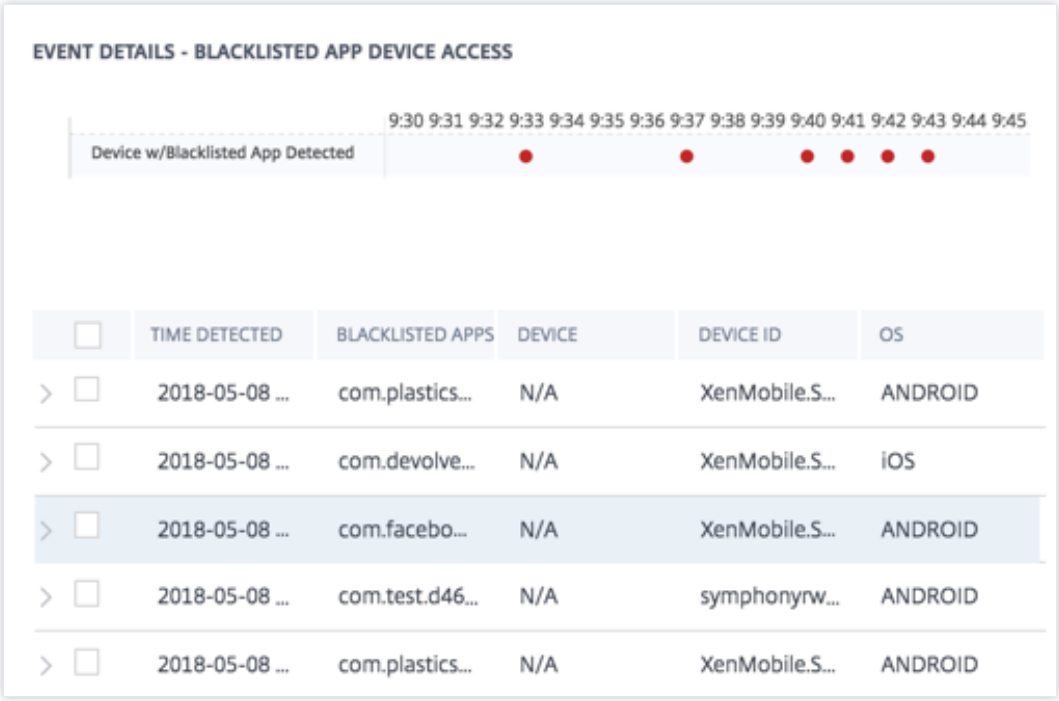
Pour afficher l'indicateur **de risque détecté** pour un utilisateur, accédez à **Sécurité > Utilisateurs**, puis sélectionnez l'utilisateur concerné.



- Dans la section **WHAT HAPPENED**, vous pouvez consulter le résumé de l'événement. Vous pouvez afficher le nombre d'appareils avec des applications sur liste noire détectés par le service Endpoint Management et l'heure à laquelle les événements se sont produits.



- Dans la section **EVENT DETAILS —BLACKLISTED APP DEVICE ACCESS**, les événements sont affichés sous forme graphique et tabulaire. Les événements sont également affichés sous forme d'entrées individuelles dans le graphique, et le tableau fournit les informations clés suivantes :
  - **Heure détectée** : lorsque la présence d'applications sur liste noire est signalée par Endpoint Management.
  - **Applications sur liste noire** : les applications de la liste noire sur l'appareil.
  - **Appareil** : appareil mobile utilisé.
  - **ID de l'appareil** : informations sur l'ID de l'appareil utilisé pour ouvrir une session.
  - **OS** : système d'exploitation de l'appareil mobile.



> **Remarque**
>
> En plus d'afficher les détails sous forme de tableau, vous pouvez cliquer sur la flèche en regard de l'instance d'une alerte pour afficher plus de détails.

Quelles actions pouvez-vous appliquer à l'utilisateur ?

Vous pouvez effectuer les actions suivantes sur le compte de l'utilisateur :

- **Ajouter à la liste de surveillance**. Lorsque vous souhaitez surveiller un utilisateur afin de détecter de futures menaces potentielles, vous pouvez les ajouter à une liste de surveillance.
- **Notifiez les administrateurs**. En cas d'activité inhabituelle ou suspecte sur le compte de l'utilisateur, une notification par e-mail est envoyée à tous les administrateurs ou à certains administrateurs.

Pour en savoir plus sur les actions et la façon de les configurer manuellement, consultez la section Stratégies et actions.

Pour appliquer manuellement les actions à l'utilisateur, accédez au profil de l'utilisateur et sélectionnez l'indicateur de risque approprié. Dans le menu **Actions**, sélectionnez une action et cliquez sur **Appliquer**.

> **Remarque**
>
> Quelle que soit la source de données qui déclenche un indicateur de risque, des mesures rela-

> tives à d'autres sources de données peuvent être appliquées.

Appareil jailbreaké ou rooté détecté

Citrix Analytics détecte les menaces d'accès en fonction de l'activité des appareils jailbreakés ou rootés et déclenche l'indicateur de risque correspondant.

L'indicateur de risque d'**appareil jailbreaké ou rooté** est déclenché lorsqu'un utilisateur utilise un appareil jailbreaké ou rooté pour se connecter au réseau. Secure Hub détecte le périphérique et signale l'incident au service Endpoint Management. L'alerte garantit que seuls les utilisateurs et appareils autorisés se trouvent sur le réseau de votre organisation.

Le facteur de risque associé à l'indicateur de risque de périphérique jailbreaké ou rooté est l'autre indicateur de risque. Pour plus d'informations sur les facteurs de risque, consultez la section Indicateurs de risque utilisateur Citrix.

Quand l'indicateur de risque détecté par l'appareil jailbreaké ou rooté est-il déclenché ?

Il est important que les responsables de la sécurité puissent s'assurer que les utilisateurs se connectent à l'aide d'appareils compatibles réseau. L'indicateur de risque **détecté par un appareil jailbreaké ou rooté** vous avertit des utilisateurs disposant d'appareils iOS jailbreakés ou d'appareils Android enracinés.

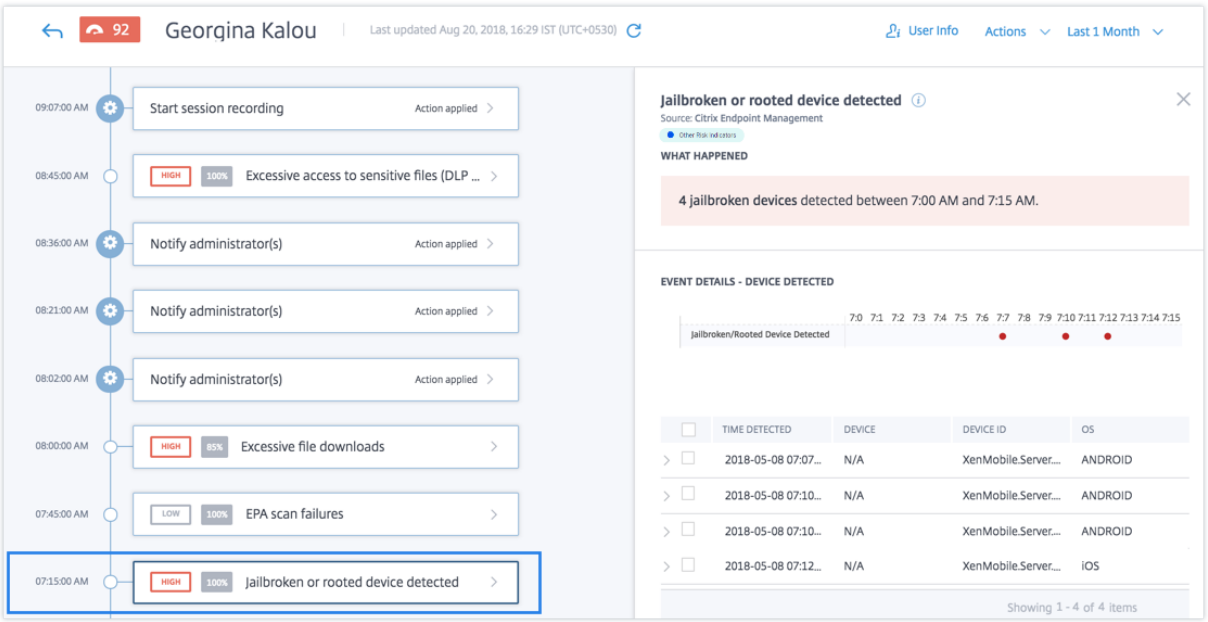
L'indicateur de risque d'**appareil jailbreaké ou rooté** est déclenché lorsqu'un appareil inscrit devient jailbreaké ou rooté. Secure Hub détecte l'événement sur l'appareil et le signale au service Endpoint Management.

Comment analyser l'indicateur de risque détecté par un appareil jailbreaké ou rooté ?

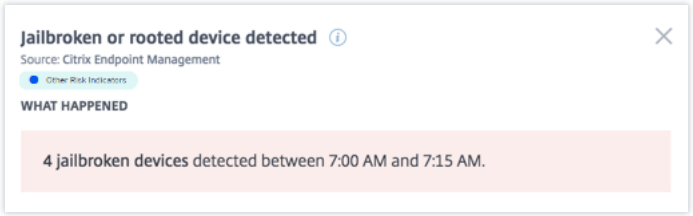
Prenons l'exemple de l'utilisateur Georgina Kalou, dont l'appareil iOS inscrit a récemment été jailbreaké. Ce comportement suspect est détecté par Citrix Analytics et un score de risque est attribué à Georgina Kalou.

Dans la chronologie des risques de Georgina Kalou, vous pouvez sélectionner l'indicateur de risque **détecté par un appareil jailbreaké ou rooté** signalé. La raison de l'événement est affichée avec les détails tels que l'heure à laquelle l'indicateur de risque a été déclenché, la description de l'événement, etc.

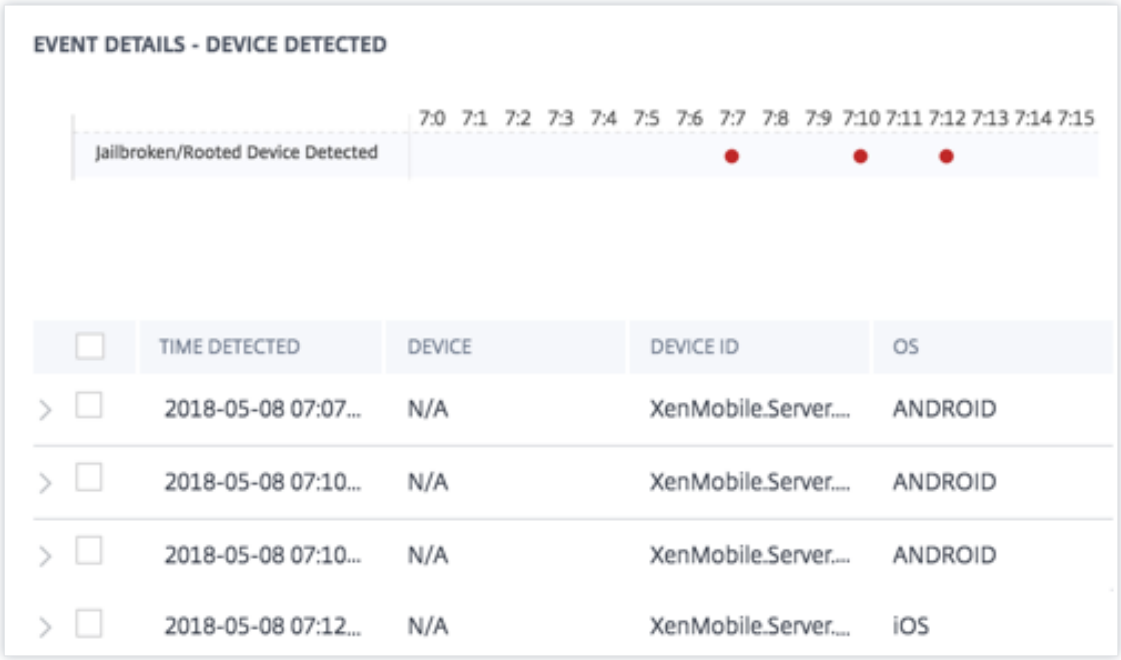
Pour afficher l'indicateur de risque **détecté par un appareil jailbreaké ou rooté** pour un utilisateur, accédez à **Sécurité > Utilisateurs**, puis sélectionnez l'utilisateur.



- Dans la section **WHAT HAPPENED**, vous pouvez consulter le résumé de l'événement. Vous pouvez afficher le nombre d'appareils jailbreakés ou rootés détectés et l'heure à laquelle les événements se sont produits.



- Dans la section **EVENT DETAILS —DEVICE DETETED**, les événements sont affichés sous forme graphique et tabulaire. Les événements sont également affichés sous forme d'entrées individuelles dans le graphique, et le tableau fournit les informations clés suivantes :
  - **Heure détectée**. Heure de détection du périphérique jailbreaké ou rooté.
  - **appareil**. L'appareil mobile utilisé.
  - **ID du périphérique**. Informations sur l'ID de l'appareil utilisé pour ouvrir une session.
  - **Système d'exploitation**. Le système d'exploitation de l'appareil mobile.



> **Remarque**
>
> Outre l'affichage des détails sous forme de tableau, cliquez sur la flèche en regard de l'instance d'une alerte pour afficher plus de détails.

Quelles actions pouvez-vous appliquer à l'utilisateur ?

Vous pouvez effectuer les actions suivantes sur le compte de l'utilisateur :

- **Ajouter à la liste de surveillance**. Lorsque vous souhaitez surveiller un utilisateur afin de détecter de futures menaces potentielles, vous pouvez les ajouter à une liste de surveillance.
- **Notifiez les administrateurs**. En cas d'activité inhabituelle ou suspecte sur le compte de l'utilisateur, une notification par e-mail est envoyée à tous les administrateurs ou à certains administrateurs.

Pour en savoir plus sur les actions et la façon de les configurer manuellement, consultez la section Stratégies et actions.

Pour appliquer manuellement les actions à l'utilisateur, accédez au profil de l'utilisateur et sélectionnez l'indicateur de risque approprié. Dans le menu **Actions**, sélectionnez une action et cliquez sur **Appliquer**.

> **Remarque**

> Quelle que soit la source de données qui déclenche un indicateur de risque, des mesures relatives à d'autres sources de données peuvent être appliquées.

Périphérique non géré détecté

Citrix Analytics détecte les menaces d'accès en fonction de l'activité des appareils non gérés et déclenche l'indicateur de risque correspondant.

L'indicateur de risque **détecté par un appareil non géré** est déclenché lorsqu'un appareil est :

- Nettoyage à distance en raison d'une action automatisée.
- Effacé manuellement par l'administrateur.
- Désinscrits par l'utilisateur.

Le facteur de risque associé à l'indicateur de risque détecté par un appareil non géré est l'autre indicateur de risque. Pour plus d'informations sur les facteurs de risque, consultez la section Indicateurs de risque utilisateur Citrix.

Quand l'indicateur de risque détecté du périphérique non géré est-il déclenché ?

L'indicateur de risque **détecté par un appareil non géré** est signalé lorsque l'appareil d'un utilisateur n'est plus géré. Un périphérique passe à un état non géré en raison de :

- Une action effectuée par l'utilisateur.
- Action effectuée par l'administrateur Endpoint Management ou le serveur.

Dans votre organisation, le service Endpoint Management vous permet de gérer les appareils et les applications qui accèdent au réseau. Pour plus d'informations, consultez la section Modes de gestion.

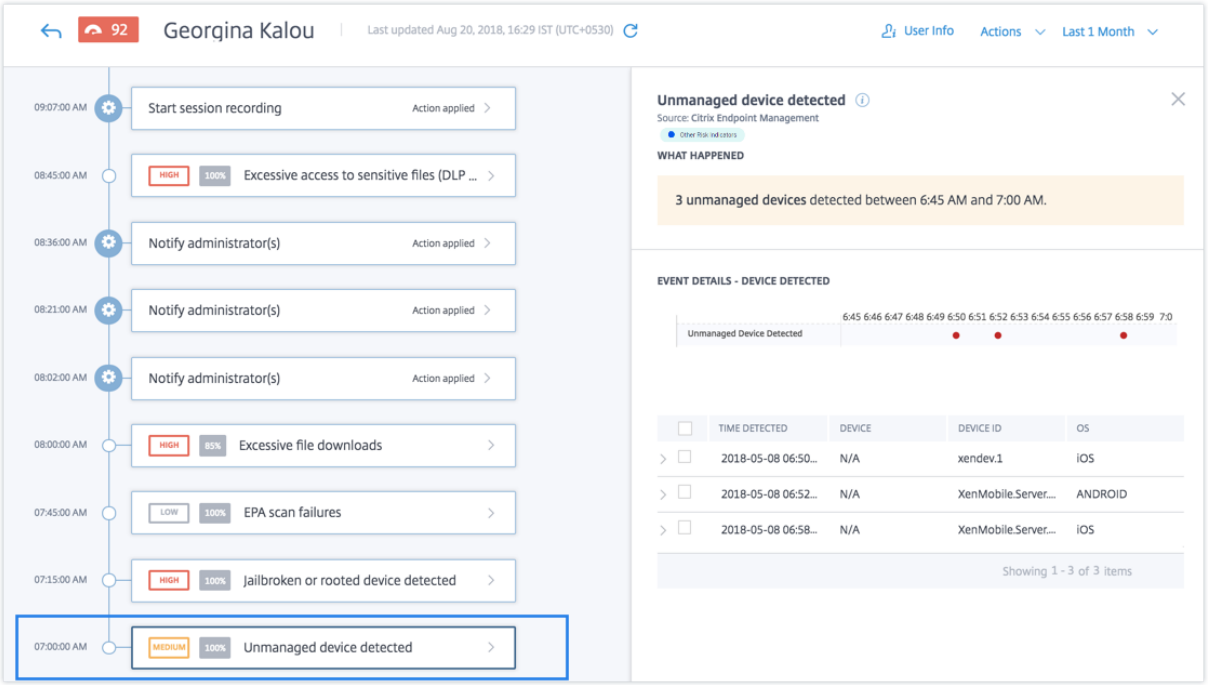
Lorsque l'appareil d'un utilisateur passe à un état non géré, le service Endpoint Management détecte cet événement et le signale à Citrix Analytics. Le score de risque de l'utilisateur est mis à jour. L'indicateur de risque **détecté par un appareil non géré** est ajouté à la chronologie des risques de l'utilisateur.

Comment analyser l'indicateur de risque détecté de périphérique non géré ?

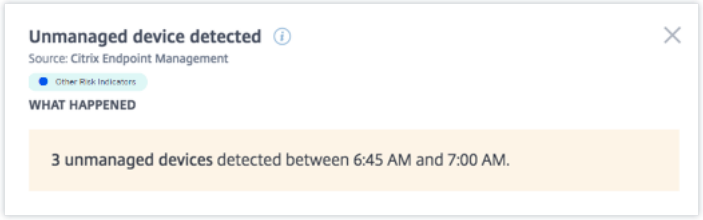
Prenons l'exemple de l'utilisateur Georgina Kalou, dont l'appareil est effacé à distance par une action automatisée sur le serveur. Endpoint Management signale cet événement à Citrix Analytics, qui attribue un score de risque mis à jour à Georgina Kalou.

Dans la chronologie des risques de Georgina Kalou, vous pouvez sélectionner l'indicateur de risque détecté par un appareil non géré signalé. La raison de l'événement est affichée avec des détails tels que l'heure à laquelle l'indicateur de risque a été déclenché, la description de l'événement, etc.

Pour afficher l'indicateur de risque **détecté par un appareil non géré** pour un utilisateur, accédez à **Sécurité > Utilisateurs**, puis sélectionnez l'utilisateur.

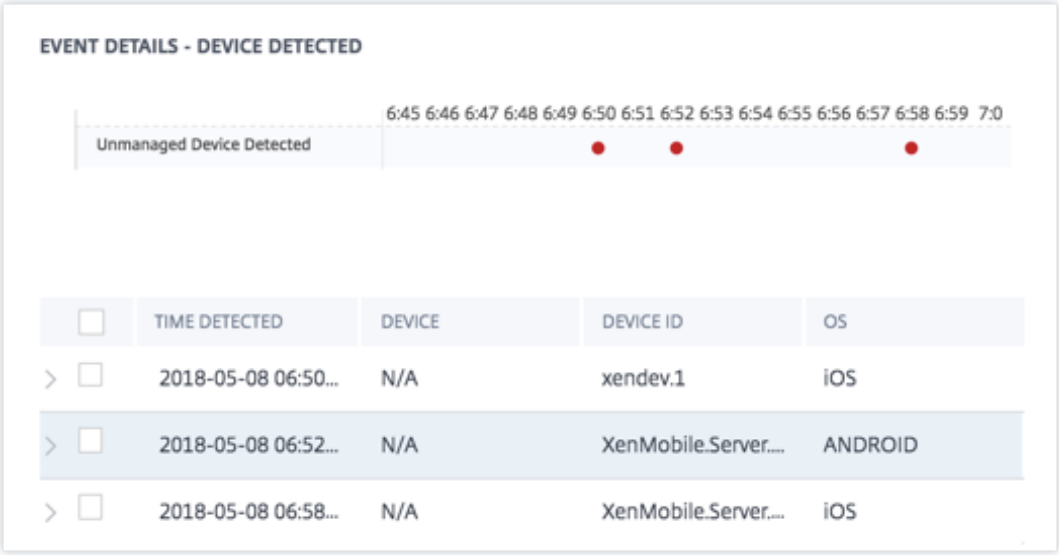


- Dans la section **WHAT HAPPENED**, vous pouvez consulter un résumé de l'événement. Vous pouvez afficher le nombre d'appareils non gérés détectés et l'heure à laquelle les événements se sont produits.



- Dans la section **EVENT DETAILS —DEVICE DETETED**, les événements sont affichés sous forme graphique et tabulaire. Les événements sont également affichés sous forme d'entrées individuelles dans le graphique, et le tableau fournit les informations clés suivantes :
  - **Heure détectée**. Heure de détection de l'événement.
  - **appareil**. L'appareil mobile utilisé.
  - **ID du périphérique**. ID d'appareil de l'appareil mobile.

- **Système d'exploitation**. Le système d'exploitation de l'appareil mobile.



Quelles actions pouvez-vous appliquer à l'utilisateur ?

Vous pouvez effectuer les actions suivantes sur le compte de l'utilisateur :

- **Ajouter à la liste de surveillance**. Lorsque vous souhaitez surveiller un utilisateur afin de détecter de futures menaces potentielles, vous pouvez les ajouter à une liste de surveillance.
- **Notifiez les administrateurs**. En cas d'activité inhabituelle ou suspecte sur le compte de l'utilisateur, une notification par e-mail est envoyée à tous les administrateurs ou à certains administrateurs.

Pour en savoir plus sur les actions et la façon de les configurer manuellement, consultez la section Stratégies et actions.

Pour appliquer manuellement les actions à l'utilisateur, accédez au profil de l'utilisateur et sélectionnez l'indicateur de risque approprié. Dans le menu **Actions**, sélectionnez une action et cliquez sur **Appliquer**.

> **Remarque**
>
> Quelle que soit la source de données qui déclenche un indicateur de risque, des mesures relatives à d'autres sources de données peuvent être appliquées.

Indicateurs de risque de Citrix Gateway

July 14, 2022

Échec de l'analyse EPA (End Point Analysis)

Citrix Analytics détecte les menaces basées sur l'accès utilisateur en fonction de l'activité des échecs d'analyse EPA et déclenche l'indicateur de risque correspondant.

Le facteur de risque associé à l'indicateur de risque d'échec de l'analyse End Point Analysis est l'autre indicateur de risque. Pour plus d'informations sur les facteurs de risque, consultez la section Indicateurs de risque utilisateur Citrix.

Quand l'indicateur de risque de défaillance du scan de l'EPA est-il déclenché ?

L'indicateur de risque d'échec de l'analyse EPA est signalé lorsqu'un utilisateur tente d'accéder au réseau à l'aide d'un appareil qui a échoué aux stratégies d'analyse EPA (End Point Analysis) de Citrix Gateway pour la pré-authentification ou la post-authentification.

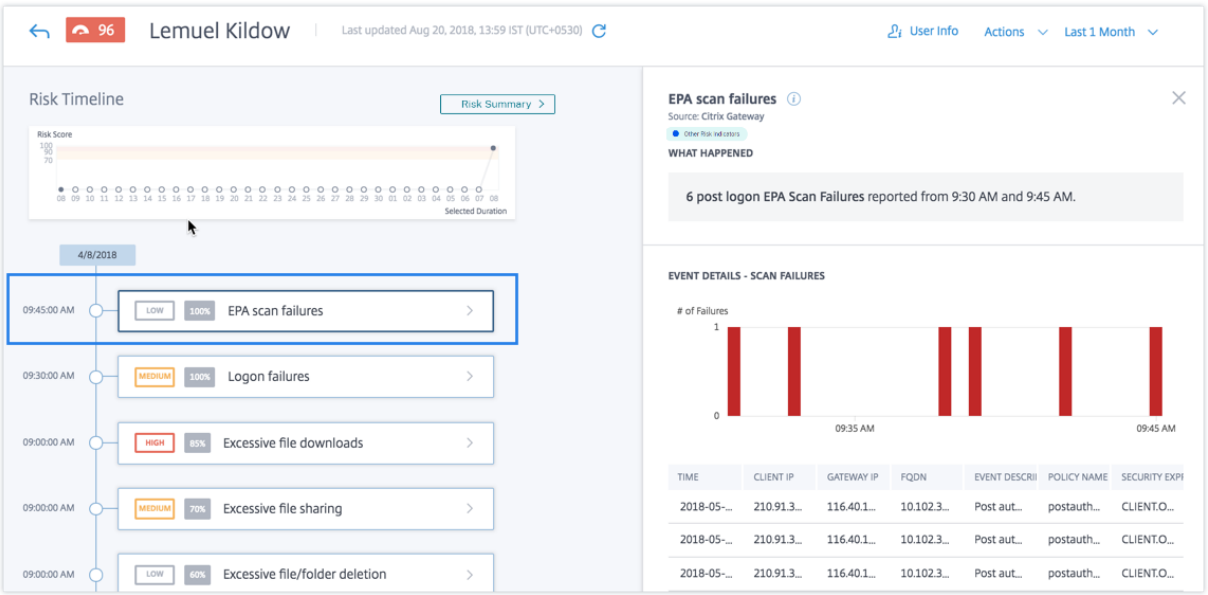
Citrix Gateway détecte ces événements et les signale à Citrix Analytics. Citrix Analytics surveille tous ces événements pour détecter si l'utilisateur a eu trop d'échecs d'analyse EPA. Lorsque Citrix Analytics détermine des échecs d'analyse EPA excessifs pour un utilisateur, il met à jour le score de risque de l'utilisateur et ajoute une entrée d'indicateur de risque d'échec de l'analyse EPA à la chronologie des risques de l'utilisateur.

Comment analyser l'indicateur de risque des échecs d'analyse EPA ?

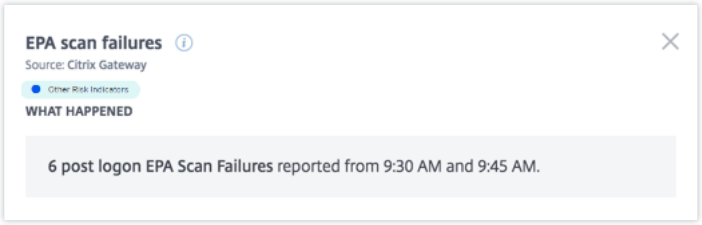
Prenons l'exemple de l'utilisateur Lemuel, qui a récemment essayé plusieurs fois d'accéder au réseau à l'aide d'un appareil qui a échoué à l'analyse EPA de Citrix Gateway. Citrix Gateway signale cet échec à Citrix Analytics, qui attribue un score de risque mis à jour à Lemuel. L'indicateur de risque de défaillance du scan de l'EPA est ajouté à la chronologie des risques de Lemuel Kildow.

Pour afficher l'entrée d'**échec de l'analyse EPA** pour un utilisateur, accédez à **Sécurité > Utilisateurs**, puis sélectionnez l'utilisateur.

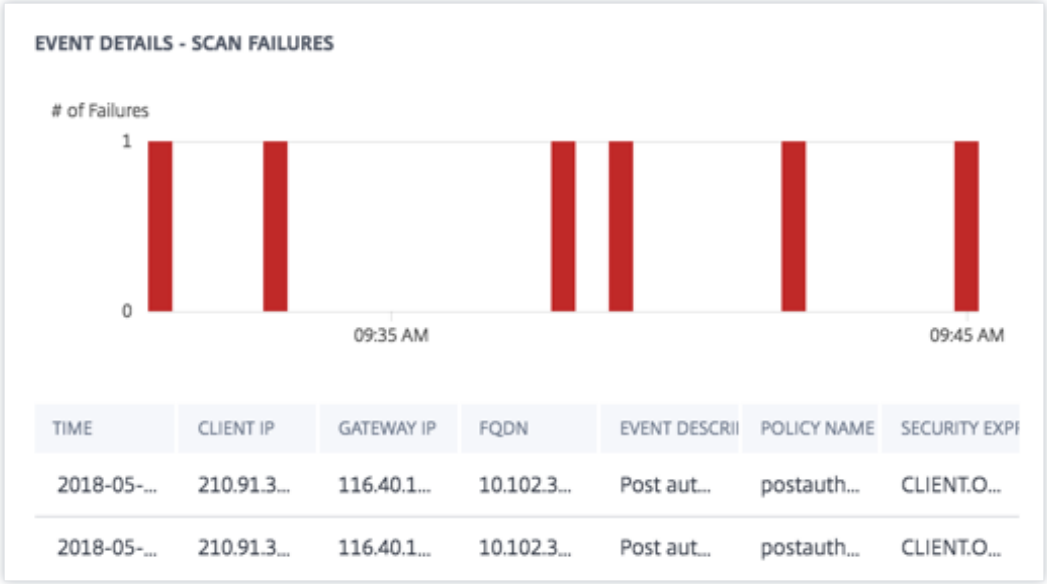
Dans la chronologie des risques de Lemuel Kildow, vous pouvez sélectionner le dernier indicateur de risque **d'échec d'analyse EPA** signalé pour l'utilisateur. Lorsque vous sélectionnez une entrée d'indicateur de risque de défaillance d'analyse EPA dans la chronologie, un panneau d'informations détaillées correspondant apparaît dans le volet droit.



- La section **WHAT HAPPENED** fournit un bref résumé de l'indicateur de risque de défaillance de l'analyse de l'EPA. Inclut également le nombre d'échecs d'analyse EPA après ouverture de session signalés au cours de la période sélectionnée.



- La section **DÉTAILS DE L'ÉVÉNEMENT —ÉCHECS DE L'ANALYSE** inclut une visualisation chronologique des événements d'échec d'analyse EPA individuels qui se sont produits pendant la période sélectionnée. Il inclut également un tableau qui fournit les informations clés suivantes concernant chaque événement :
  - **Le temps**. Heure à laquelle l'échec de l'analyse EPA s'est produit.
  - **Adresse IP du client**. Adresse IP du client à l'origine de l'échec de l'analyse EPA.
  - **IP de passerelle**. Adresse IP de Citrix Gateway qui a signalé l'échec de l'analyse EPA.
  - **FQDN**. Le nom de domaine complet de Citrix Gateway.
  - **Description de l'événement**. Brève description de la raison de l'échec de l'analyse EPA.
  - **Nom de la stratégie**. Nom de la stratégie d'analyse EPA configuré sur Citrix Gateway.
  - **Expression de sécurité**. Expression de sécurité configurée sur Citrix Gateway.



Quelles actions pouvez-vous appliquer à l'utilisateur ?

Vous pouvez effectuer les actions suivantes sur le compte de l'utilisateur :

- **Ajouter à la liste de surveillance**. Lorsque vous souhaitez surveiller un utilisateur afin de détecter de futures menaces potentielles, vous pouvez les ajouter à une liste de surveillance.
- **Notifiez les administrateurs**. En cas d'activité inhabituelle ou suspecte sur le compte de l'utilisateur, une notification par e-mail est envoyée à tous les administrateurs ou à certains administrateurs.
- **Déconnecter l'utilisateur**. Lorsqu'un utilisateur est déconnecté de son compte, il ne peut accéder à aucune ressource via Citrix Gateway tant que l'administrateur Citrix Gateway n'a pas effacé l'action Déconnecter l'utilisateur.
- **Verrouiller l'utilisateur** : lorsque le compte d'un utilisateur est verrouillé en raison d'un comportement anormal, il ne peut accéder à aucune ressource via Citrix Gateway tant que l'administrateur de la passerelle n'a pas déverrouillé le compte.

Pour en savoir plus sur les actions et la façon de les configurer manuellement, consultez la section Stratégies et actions.

Pour appliquer manuellement les actions à l'utilisateur, accédez au profil de l'utilisateur et sélectionnez l'indicateur de risque approprié. Dans le menu **Actions**, sélectionnez une action et cliquez sur **Appliquer**.

> **Remarque**
>
> Quelle que soit la source de données qui déclenche un indicateur de risque, des mesures relatives à d'autres sources de données peuvent être appliquées.

Échec excessif de l'authentification

Citrix Analytics détecte les menaces basées sur l'accès utilisateur en fonction des échecs d'authentification excessifs et déclenche l'indicateur de risque correspondant.

Le facteur de risque associé à l'indicateur de risque d'échecs d'authentification excessifs est les indicateurs de risque basés sur les échecs de connexion. Pour plus d'informations sur les facteurs de risque, consultez la section Indicateurs de risque utilisateur Citrix.

Quand l'indicateur de risque d'échecs d'authentification excessifs est-il déclenché ?

L'indicateur de risque d'échec de connexion est signalé lorsque l'utilisateur rencontre plusieurs échecs d'authentification Citrix Gateway au cours d'une période donnée. Les échecs d'authentification Citrix Gateway peuvent être des échecs d'authentification primaire, secondaire ou tertiaire, selon que l'authentification multifacteur est configurée pour l'utilisateur.

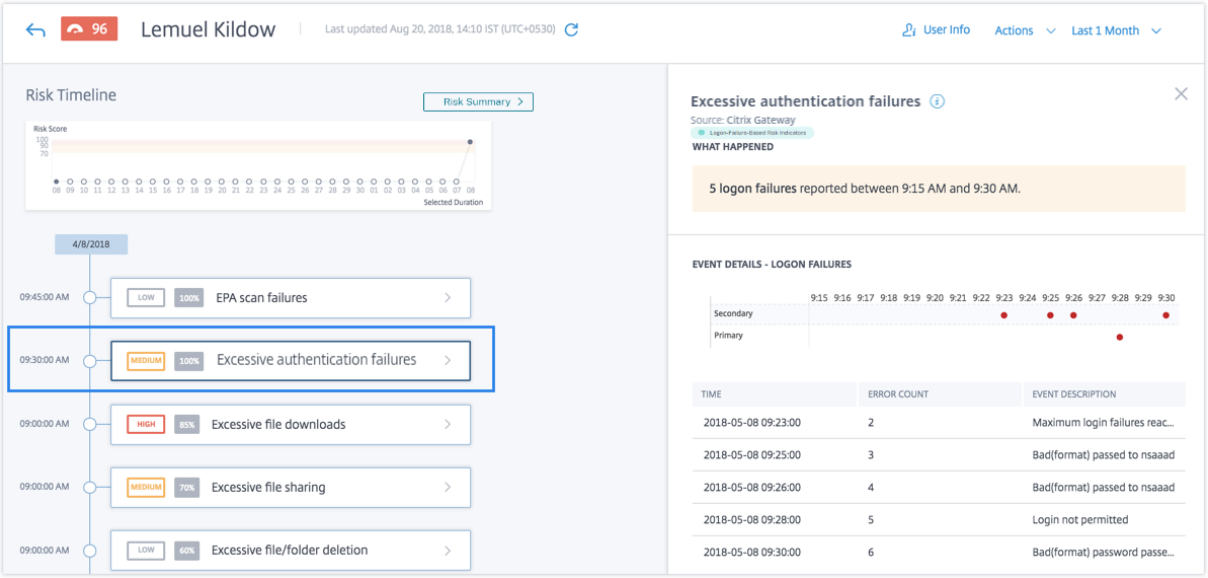
Citrix Gateway détecte tous les échecs d'authentification des utilisateurs et signale ces événements à Citrix Analytics. Citrix Analytics surveille tous ces événements pour détecter si l'utilisateur a eu trop d'échecs d'authentification. Lorsque Citrix Analytics détecte des échecs d'authentification excessifs, il met à jour le score de risque de l'utilisateur. L'indicateur de risque d'échecs d'authentification excessifs est ajouté à la chronologie des risques de l'utilisateur.

Comment analyser l'indicateur de risque d'échecs d'authentification excessifs ?

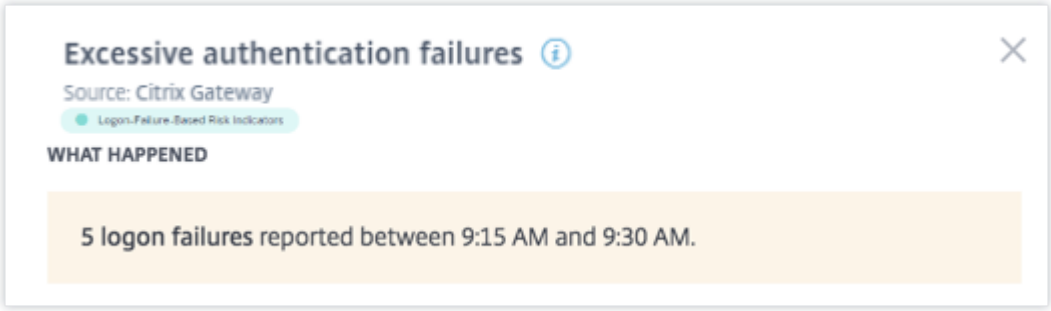
Prenons l'exemple de l'utilisateur Lemuel, qui a récemment échoué à plusieurs tentatives d'authentification du réseau. Citrix Gateway signale ces échecs à Citrix Analytics et un score de risque mis à jour est attribué à Lemuel. L'indicateur de risque **d'échecs d'authentification excessifs** est ajouté à la chronologie des risques de Lemuel Kildow.

Pour afficher l'entrée de l'indicateur de risque de **défaillances d'authentification excessives** pour un utilisateur, accédez à **Sécurité > Utilisateurs**, puis sélectionnez l'utilisateur.

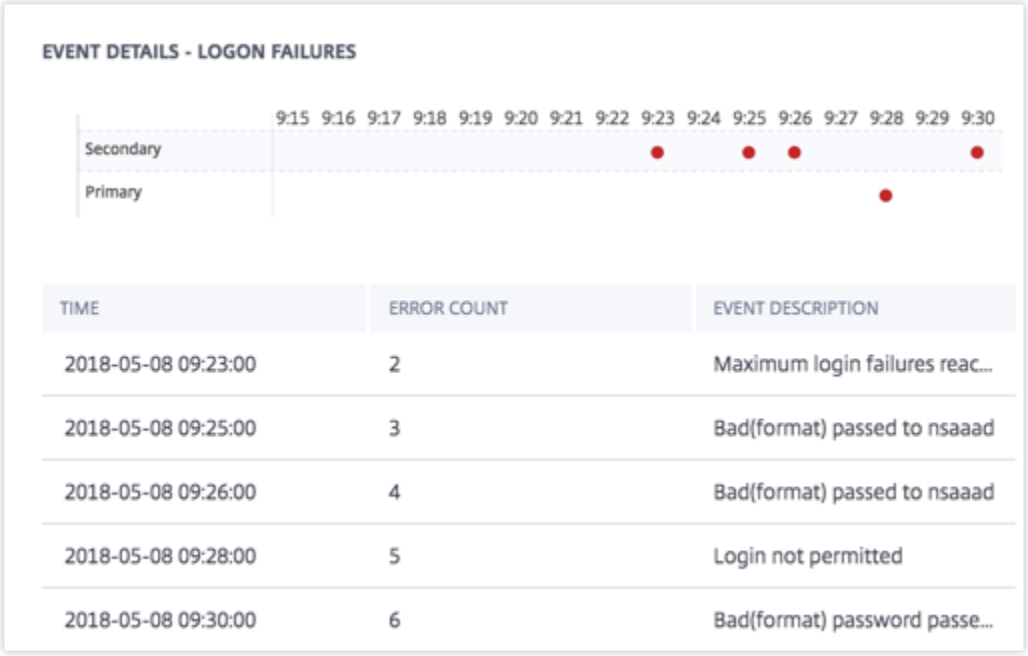
Dans la chronologie des risques de Lemuel Kildow, vous pouvez sélectionner le dernier indicateur de risque **d'échecs d'authentification excessifs** signalé pour l'utilisateur. Lorsque vous sélectionnez l'entrée de l'indicateur de risque **d'échecs d'authentification excessifs** dans la chronologie des risques, un panneau d'informations détaillées correspondant apparaît dans le volet droit.



- La section **WHAT HAPPENED** fournit un bref résumé de l'indicateur de risque, y compris le nombre d'échecs d'authentification survenus au cours de la période sélectionnée.



- La section **DÉTAILS DE L'ÉVÉNEMENT** inclut une visualisation chronologique des événements d'échec d'authentification excessif qui se sont produits pendant la période sélectionnée. En outre, vous pouvez afficher les informations clés suivantes sur chaque événement :
  - **Le temps**. Heure à laquelle l'échec d'ouverture de session s'est produit.
  - **Nombre d'erreurs**. Nombre d'échecs d'authentification détectés pour l'utilisateur au moment de l'événement et au cours des 48 heures précédentes.
  - **Description de l'événement**. Brève description de la raison de l'échec de la connexion.



Quelles actions pouvez-vous appliquer à l'utilisateur ?

Vous pouvez effectuer les actions suivantes sur le compte de l'utilisateur :

- **Ajouter à la liste de surveillance**. Lorsque vous souhaitez surveiller un utilisateur afin de détecter de futures menaces potentielles, vous pouvez les ajouter à une liste de surveillance.
- **Notifiez les administrateurs**. En cas d'activité inhabituelle ou suspecte sur le compte de l'utilisateur, une notification par e-mail est envoyée à tous les administrateurs ou à certains administrateurs.
- **Déconnecter l'utilisateur**. Lorsqu'un utilisateur est déconnecté de son compte, il ne peut accéder à aucune ressource via Citrix Gateway tant que l'administrateur Citrix Gateway n'a pas effacé l'action Déconnecter l'utilisateur.
- **Verrouiller l'utilisateur** : lorsque le compte d'un utilisateur est verrouillé en raison d'un comportement anormal, il ne peut accéder à aucune ressource via Citrix Gateway tant que l'administrateur de la passerelle n'a pas déverrouillé le compte.

Pour en savoir plus sur les actions et la façon de les configurer manuellement, consultez la section Stratégies et actions.

Pour appliquer manuellement les actions à l'utilisateur, accédez au profil de l'utilisateur et sélectionnez l'indicateur de risque approprié. Dans le menu **Actions**, sélectionnez une action et cliquez sur **Appliquer**.

> **Remarque**
>
> Quelle que soit la source de données qui déclenche un indicateur de risque, des mesures relatives à d'autres sources de données peuvent être appliquées.

Voyages impossibles

Citrix Analytics détecte les ouvertures de session d'un utilisateur comme risquées lorsque les ouvertures de session consécutives proviennent de deux pays différents au cours d'une période inférieure au temps de trajet prévu entre les pays.

Le scénario de temps de trajet impossible indique les risques suivants :

- **Informations d'identification compromises** : un attaquant distant vole les informations d'identification d'un utilisateur légitime.
- **Informations d'identification partagées** : différents utilisateurs utilisent les mêmes informations d'identification utilisateur.

Quand l'indicateur de risque de voyage impossible se déclenche-t-il ?

L'indicateur **de risque de déplacement impossible** évalue le temps et la distance estimée entre chaque paire d'ouvertures de session utilisateur consécutives, et se déclenche lorsque la distance est supérieure à ce qu'une personne peut éventuellement parcourir pendant cette période.

> **Remarque**
>
> Cet indicateur de risque contient également une logique visant à réduire les alertes de faux positifs pour les scénarios suivants qui ne reflètent pas l'emplacement réel des utilisateurs :
>
> - Lorsque les utilisateurs ouvrent une session via Citrix Gateway à partir de connexions proxy.
> - Lorsque les utilisateurs ouvrent une session via Citrix Gateway à partir de clients hébergés.

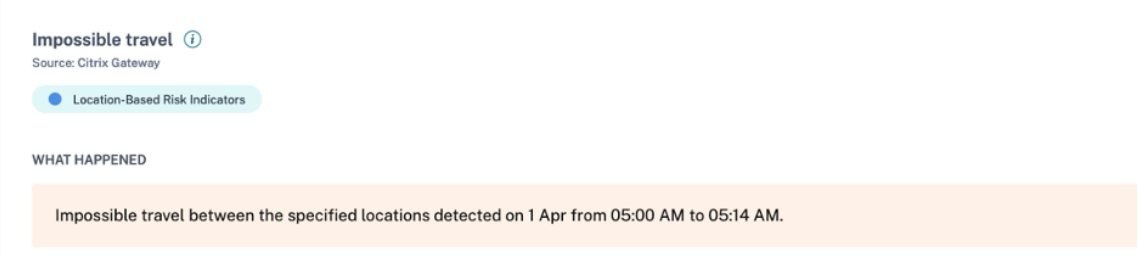
Comment analyser l'indicateur de risque impossible

Prenons l'exemple de l'utilisateur Adam Maxwell, qui se connecte à partir de deux emplacements : Bengaluru, en Inde, et Oslo, en Norvège, dans un délai d'une minute. Citrix Analytics détecte cet événement d'ouverture de session comme un scénario de voyage impossible et déclenche l'indicateur **de risque de déplacement impossible** . L'indicateur de risque est ajouté à la chronologie de risque d'Adam Maxwell et un score de risque lui est attribué.

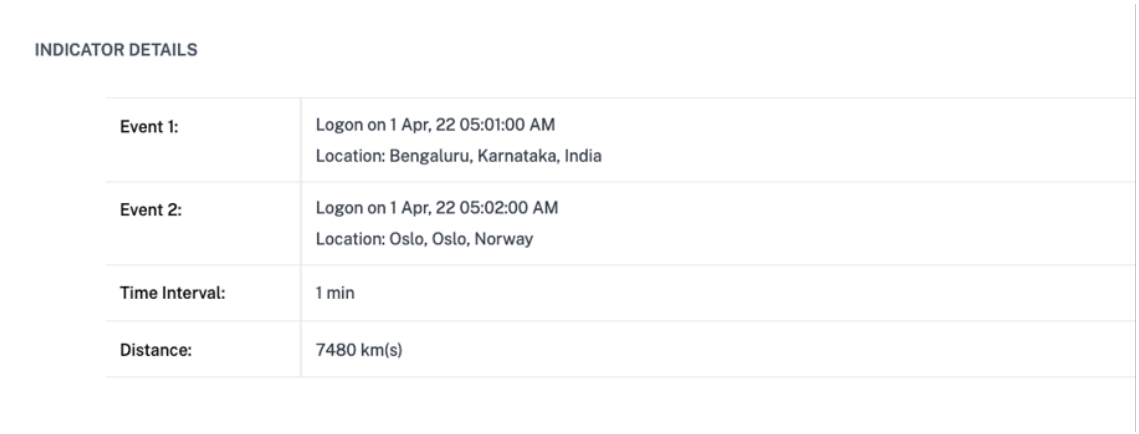
Pour consulter la chronologie des risques d'Adam Maxwell, sélectionnez **Sécurité > Utilisateurs**. Dans le volet **Utilisateurs risqués**, sélectionnez l'utilisateur Adam Maxwell.

Dans la chronologie des risques d'Adam Maxwell, sélectionnez l'indicateur **de risque de voyage impossible** . Vous pouvez consulter les informations suivantes :

- La section **WHAT HAPPENED** fournit un bref résumé de l'événement de voyage impossible.

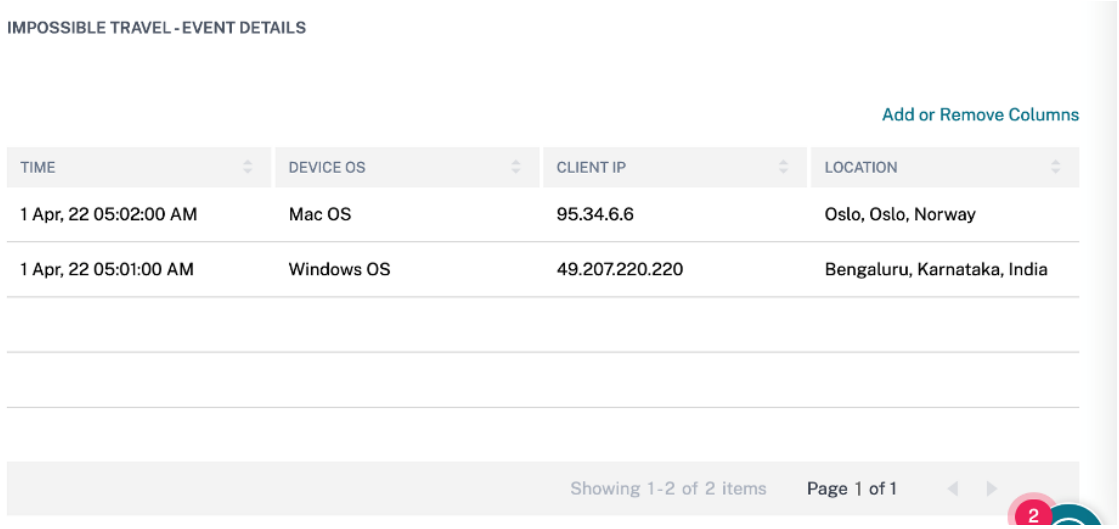


- La section **DÉTAILS DE L'INDICATEUR** fournit les emplacements à partir desquels l'utilisateur s'est connecté, la durée entre les ouvertures de session consécutives et la distance entre les deux emplacements.



- La section **EMPLACEMENT D'OUVERTURE DE SESSION - 30 DERNIERS JOURS** affiche une vue cartographique géographique des lieux de voyage impossibles et des emplacements connus de l'utilisateur. Les données de localisation sont affichées pour les 30 derniers jours. Vous pouvez survoler les pointeurs de la carte pour afficher le nombre total d'ouvertures de session de chaque emplacement.

- La section **IMPOSSIBLE TRAVEL- EVENT DETAILS** fournit les informations suivantes sur l'événement de voyage impossible :
  - **Heure** : indique la date et l'heure des ouvertures de session.
  - **Système d'exploitation de l'appareil** : indique le système d'exploitation de la machine utilisateur.
  - **IP du client** : indique l'adresse IP de la machine utilisateur.
  - **Emplacement** : indique l'emplacement depuis lequel l'utilisateur s'est connecté.



Quelles actions pouvez-vous appliquer à l'utilisateur ?

Vous pouvez effectuer les actions suivantes sur le compte de l'utilisateur :

- **Ajouter à la liste de surveillance**. Lorsque vous souhaitez surveiller un utilisateur afin de détecter de futures menaces potentielles, vous pouvez les ajouter à une liste de surveillance.
- **Notifiez les administrateurs**. En cas d'activité inhabituelle ou suspecte sur le compte de l'utilisateur, une notification par e-mail est envoyée à tous les administrateurs ou à certains d'entre eux.
- **Déconnecter l'utilisateur**. Lorsqu'un utilisateur est déconnecté de son compte, il ne peut accéder à aucune ressource via Citrix Gateway tant que l'administrateur Citrix Gateway n'a pas effacé l'action Déconnecter l'utilisateur.
- **Verrouiller l'utilisateur** : lorsque le compte d'un utilisateur est verrouillé en raison d'un comportement anormal, il ne peut accéder à aucune ressource via Citrix Gateway tant que l'administrateur de Gateway n'a pas déverrouillé le compte.

Pour en savoir plus sur les actions et la façon de les configurer manuellement, consultez la section Stratégies et actions.

Pour appliquer les actions à l'utilisateur manuellement, accédez au profil de l'utilisateur et sélectionnez l'indicateur de risque approprié. Dans le menu **Actions**, sélectionnez une action et cliquez sur **Appliquer**.

> **Remarque**
>
> Quelle que soit la source de données qui déclenche un indicateur de risque, des mesures relatives à d'autres sources de données peuvent être appliquées.

Ouverture de session à partir d'une adresse IP suspecte

Citrix Analytics détecte les menaces d'accès des utilisateurs en fonction de l'activité de connexion à partir d'une adresse IP suspecte et déclenche cet indicateur de risque.

Le facteur de risque associé à l'indicateur de risque Ouverture de session à partir d'une adresse IP suspecte est l'indicateur de risque IP. Pour plus d'informations sur les facteurs de risque, consultez la section Indicateurs de risque utilisateur Citrix.

Quand l'indicateur de risque IP suspect est-il déclenché ?

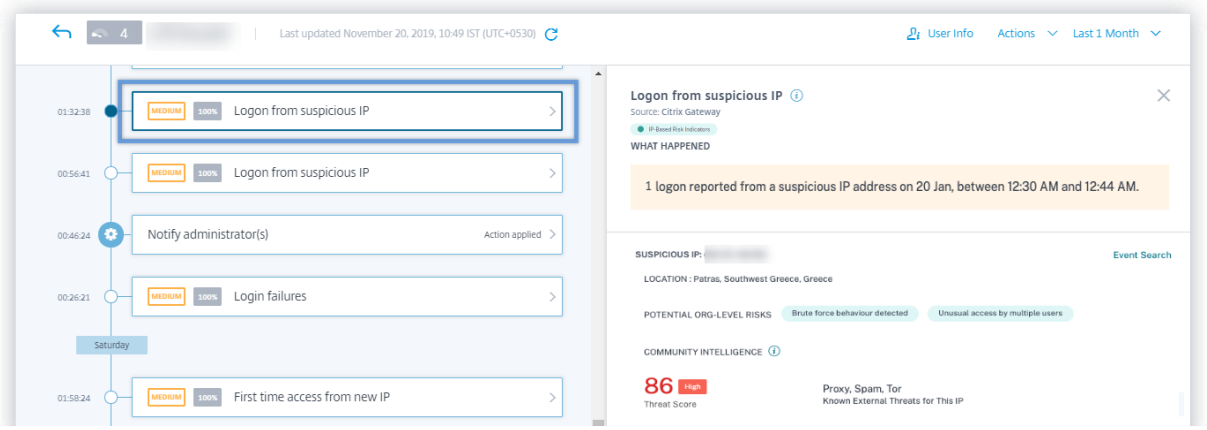
L'indicateur de risque d'ouverture de **session à partir d'une adresse IP suspecte** est déclenché lorsqu'un utilisateur tente d'accéder au réseau à partir d'une adresse IP identifiée comme suspecte par Citrix Analytics. L'adresse IP est considérée comme suspecte en raison de l'une des conditions suivantes :

- Est répertorié dans le flux externe sur la détection des menaces IP
- A plusieurs enregistrements de connexion utilisateur à partir d'un emplacement inhabituel
- Contient des tentatives de connexion excessives qui peuvent indiquer une attaque par force brute

Citrix Analytics surveille les événements de connexion reçus de Citrix Gateway et détecte si un utilisateur s'est connecté à partir d'une adresse IP suspecte. Lorsque Citrix Analytics détecte une tentative de connexion à partir d'une adresse IP suspecte, il met à jour le score de risque de l'utilisateur et ajoute une entrée d'indicateur de risque d'ouverture de **session à partir d'une adresse IP suspecte** à la chronologie des risques de l'utilisateur.

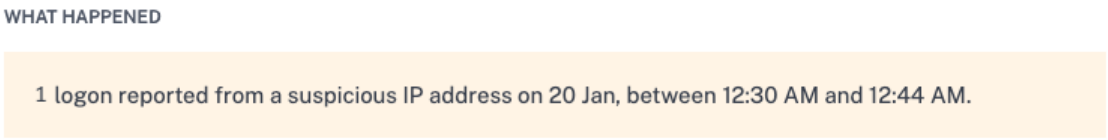
Comment analyser l'indicateur de risque IP suspect ?

Prenons l'exemple de l'utilisateur Lemuel, qui a tenté d'accéder au réseau à partir d'une adresse IP identifiée par Citrix Analytics comme suspecte. Citrix Gateway signale l'événement de connexion à Citrix Analytics, qui attribue un score de risque mis à jour à Lemuel. L'indicateur de risque **de connexion à partir d'une adresse IP suspecte** est ajouté à la chronologie des risques de Lemuel Kildow.

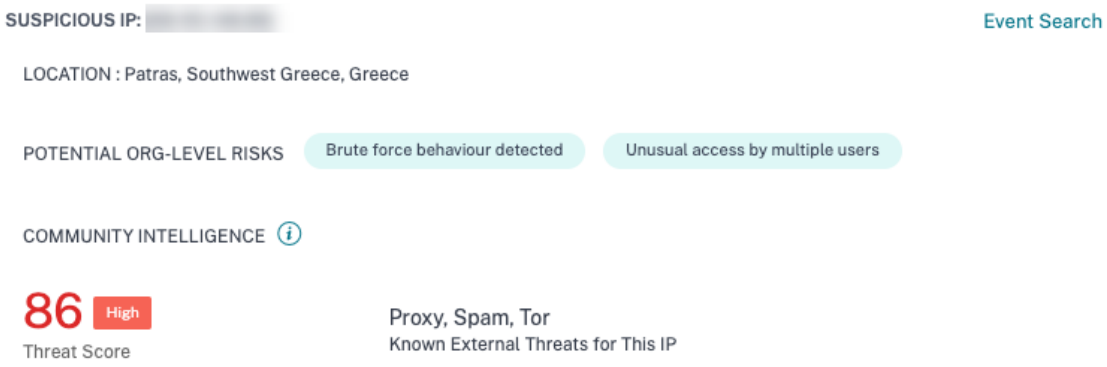


Pour afficher l'indicateur de risque IP suspect signalé pour un utilisateur, accédez à **Sécurité** > **Utilisateurs**, puis sélectionnez l'utilisateur. Dans la chronologie des risques de Lemuel Kildow, vous pouvez sélectionner la dernière **connexion à partir de l'indicateur de risque IP suspect** signalé pour l'utilisateur. Lorsque vous sélectionnez l'entrée **d'indicateur de risque IP suspect d'ouverture** de session dans la chronologie, un panneau d'informations détaillées correspondant apparaît dans le volet droit.

- La section **WHAT HAPPENED** fournit un bref résumé de l'indicateur de risque Ouverture de session à partir d'une adresse IP suspecte. De plus, inclut le nombre de connexions à partir d'une adresse IP suspecte signalée au cours de la période sélectionnée.



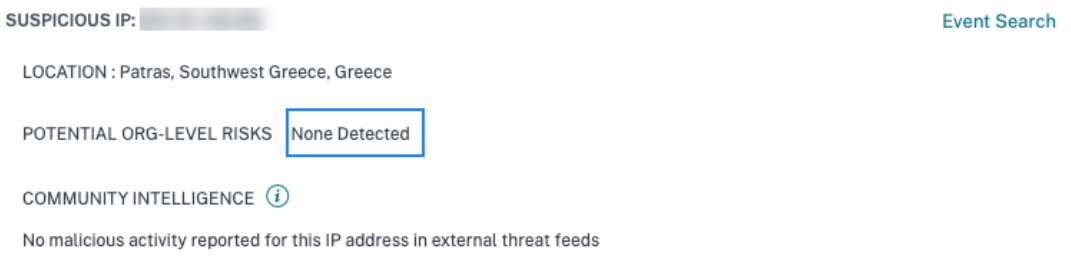
- La section **IP suspecte** fournit les informations suivantes :



  - **IP suspecte**. Adresse IP associée à une activité de connexion suspecte.

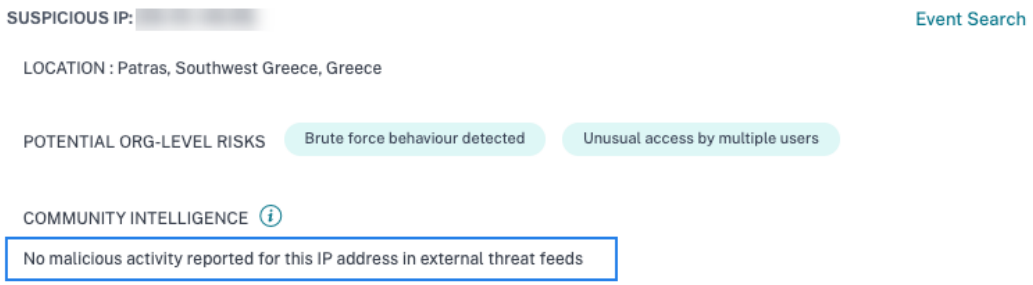
- **Emplacement**. La ville, la région et le pays de l'utilisateur. Ces emplacements sont affichés en fonction de la disponibilité des données.
- **Risque potentiel au niveau de l'organisation**. Indique tous les modèles d'activité IP suspecte que Citrix Analytics a récemment détectés dans votre organisation. Les modèles risqués incluent des échecs de connexion excessifs compatibles avec des tentatives de force brute potentielles et un accès inhabituel par plusieurs utilisateurs.

  Si aucun modèle risqué n'est détecté pour une adresse IP de votre organisation, le message suivant s'affiche.

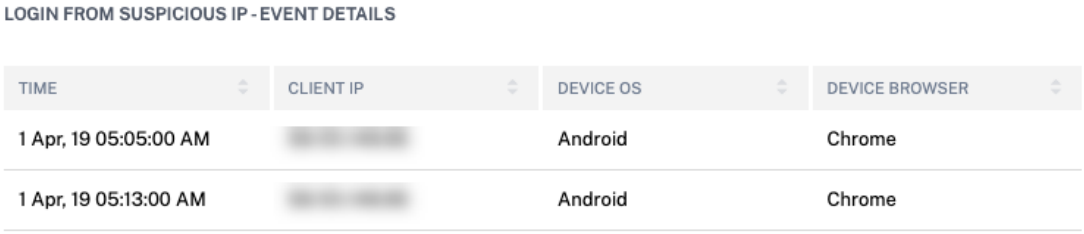


- **Intelligence communautaire**. Fournit le score de menace et les catégories de menaces d'une adresse IP identifiée comme présentant un risque élevé dans le flux externe de renseignements sur les menaces IP. Citrix Analytics attribue un score de risque à l'adresse IP à haut risque. Le score de risque commence à 80.

  Si aucune information sur les menaces n'est disponible sur une adresse IP dans le flux externe de renseignements sur les menaces IP, le message suivant s'affiche.



- La section **DÉTAILS DE L'ÉVÉNEMENT** fournit les informations suivantes sur l'activité de connexion suspecte :



- **Le temps**. Heure de l'activité de connexion suspecte.
- **Adresse IP du client**. Adresse IP de l'appareil de l'utilisateur qui a été utilisé pour l'activité de connexion suspecte.
- **Système d'exploitation de l'appareil** Le système d'exploitation du navigateur.
- **Navigateur**d'appareils. Le navigateur Web utilisé pour l'activité de connexion suspecte.

Quelles actions pouvez-vous appliquer à l'utilisateur ?

Vous pouvez effectuer les actions suivantes sur le compte de l'utilisateur :

- **Ajouter à la liste de surveillance**. Lorsque vous souhaitez surveiller un utilisateur afin de détecter de futures menaces potentielles, vous pouvez les ajouter à une liste de surveillance.
- **Notifiez les administrateurs**. En cas d'activité inhabituelle ou suspecte sur le compte de l'utilisateur, une notification par e-mail est envoyée à tous les administrateurs ou à certains administrateurs.
- **Déconnecter l'utilisateur**. Lorsqu'un utilisateur est déconnecté de son compte, il ne peut accéder à aucune ressource via Citrix Gateway tant que l'administrateur Citrix Gateway n'a pas effacé l'action Déconnecter l'utilisateur.
- **Verrouiller l'utilisateur** : lorsque le compte d'un utilisateur est verrouillé en raison d'un comportement anormal, il ne peut accéder à aucune ressource via Citrix Gateway tant que l'administrateur de la passerelle n'a pas déverrouillé le compte.

Pour en savoir plus sur les actions et la façon de les configurer manuellement, consultez la section Stratégies et actions.

Pour appliquer manuellement les actions à l'utilisateur, accédez au profil de l'utilisateur et sélectionnez l'indicateur de risque approprié. Dans le menu **Actions**, sélectionnez une action et cliquez sur **Appliquer**.

> **Remarque**
>
> Quelle que soit la source de données qui déclenche un indicateur de risque, des mesures rela-

> tives à d'autres sources de données peuvent être appliquées.

Ouverture de session suspecte

> **Remarques**
>
> - Cet indicateur de risque remplace l'indicateur de risque Accès à partir d'un emplacement inhabituel.
> - Toutes les stratégies basées sur l'indicateur de risque d'accès à partir d'un emplacement inhabituel sont automatiquement liées à l'indicateur de risque d'ouverture de session suspecte.

Citrix Analytics détecte les ouvertures de session de l'utilisateur qui semblent inhabituelles ou risquées en fonction de plusieurs facteurs contextuels, définis conjointement par l'appareil, l'emplacement et le réseau utilisés par l'utilisateur.

Quand l'indicateur de risque d'ouverture de session suspecte est-il déclenché ?

L'indicateur de risque est déclenché par la combinaison des facteurs suivants, chaque facteur étant considéré comme potentiellement suspect en fonction d'une ou de plusieurs conditions.

Facteur	Conditions
Appareil inhabituel	L'utilisateur ouvre une session à partir d'un appareil dont la signature est différente de celle des appareils utilisés au cours des 30 derniers jours. La signature de l'appareil est basée sur le système d'exploitation de l'appareil et le navigateur utilisé.
Emplacement inhabituel	Ouvrez une session à partir d'une ville ou d'un pays où l'utilisateur n'a pas ouvert de session au cours des 30 derniers jours. La ville ou le pays est géographiquement éloigné des emplacements d'ouverture de session récents (30 derniers jours). Zéro ou minimum d'utilisateurs se sont connectés depuis la ville ou le pays au cours des 30 derniers jours.

Facteur	Conditions
Réseau insolite	Ouvrez une session à partir d'une adresse IP que l'utilisateur n'a pas utilisée au cours des 30 derniers jours. Ouvrez une session à partir d'un sous-réseau IP que l'utilisateur n'a pas utilisé au cours des 30 derniers jours. Aucun ou un minimum d'utilisateurs se sont connectés depuis le sous-réseau IP au cours des 30 derniers jours.
Menace IP	L'adresse IP est identifiée comme présentant un risque élevé par le flux de renseignements sur les menaces de la communauté Webroot. Citrix Analytics a récemment détecté des activités d'ouverture de session très suspectes à partir de l'adresse IP d'autres utilisateurs.

Comment analyser l'indicateur de risque d'ouverture de session suspecte

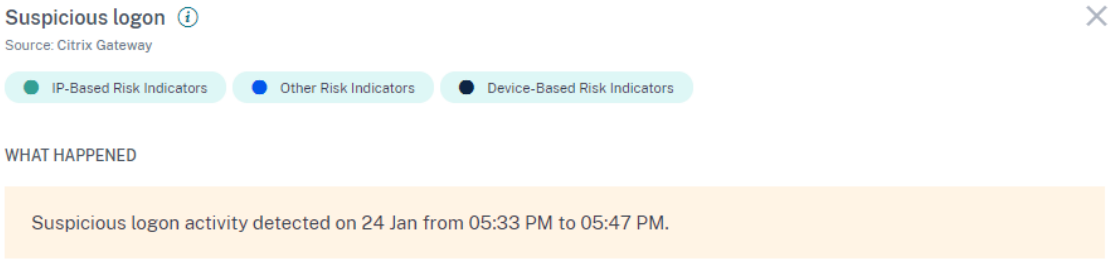
Prenons l'exemple de l'utilisateur Adam Maxwell, qui se connecte depuis l'Andhra Pradesh, en Inde, pour la première fois. Il utilise un appareil dont la signature est connue pour accéder aux ressources de l'organisation. Mais il se connecte à partir d'un réseau qu'il n'a pas utilisé depuis 30 jours.

Citrix Analytics détecte cet événement d'ouverture de session comme suspect car les facteurs tels que l'emplacement et le réseau s'écartent de son comportement habituel et déclenche l'indicateur de risque d'ouverture de session suspecte. L'indicateur de risque est ajouté à la chronologie des risques d'Adam Maxwell et un score de risque lui est attribué.

Pour afficher le temps de risque d'Adam Maxwell, sélectionnez **Sécurité > Utilisateurs**. Dans le volet **Utilisateurs risqués**, sélectionnez l'utilisateur Adam Maxwell.

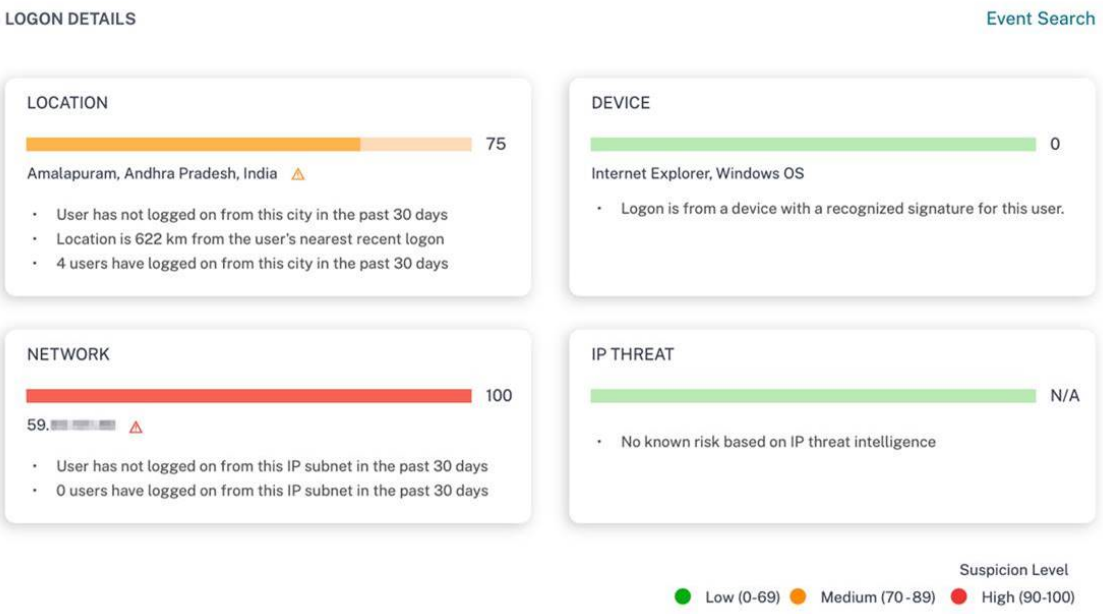
Dans la chronologie des risques d'Adam Maxwell, sélectionnez l'indicateur de risque d'**ouverture de session suspecte** . Vous affichez les informations suivantes :

- La section **WHAT HAPPENED** fournit un bref résumé des activités suspectes, y compris les facteurs de risque et le moment de l'événement.



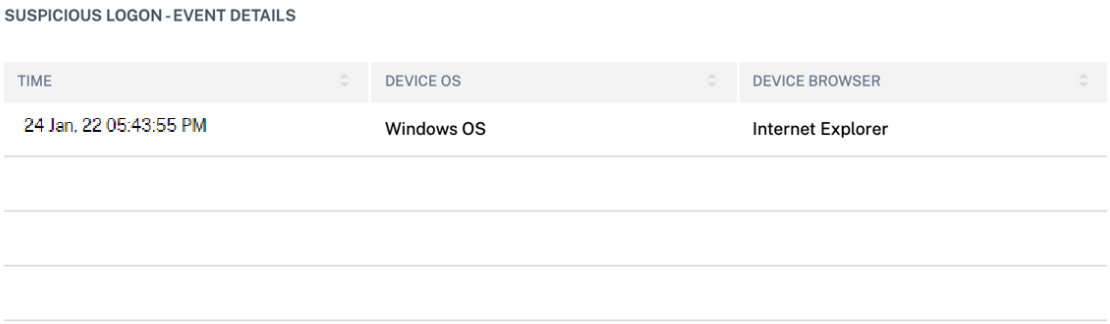
- La section **DÉTAILS DE CONNEXION** fournit un résumé détaillé des activités suspectes correspondant à chaque facteur de risque. Chaque facteur de risque se voit attribuer un score qui indique le niveau de suspicion. Un seul facteur de risque n'indique pas un risque élevé de la part d'un utilisateur. Le risque global est basé sur la corrélation entre les multiples facteurs de risque.

Niveau de suspicion	Indication
0–69	Le facteur semble normal et n'est pas considéré comme suspect.
70–89	Le facteur semble légèrement inhabituel et est considéré comme modérément suspect avec d'autres facteurs.
90–100	Le facteur est tout à fait nouveau ou inhabituel et est considéré comme très suspect par rapport à d'autres facteurs.



- L'**EMPLACEMENT D'OUVERTURE DE SESSION - 30 DERNIERS JOURS** affiche une carte géographique des derniers emplacements connus et de l'emplacement actuel de l'utilisateur. Les données de localisation sont affichées pour les 30 derniers jours. Vous pouvez survoler les pointeurs de la carte pour afficher le nombre total d'ouvertures de session de chaque emplacement.

- La section **OUVERTURE DE SESSION SUSPECTE - DÉTAILS DE L'ÉVÉNEMENT** fournit les informations suivantes sur l'événement d'ouverture de session suspect :
  - **Heure** : indique la date et l'heure de la connexion suspecte.
  - **Système d'exploitation de l'appareil** : indique le système d'exploitation de la machine utilisateur.
  - **Navigateur de l'appareil** : indique le navigateur Web utilisé pour se connecter à Citrix Gateway.



Quelles actions pouvez-vous appliquer à l'utilisateur ?

Vous pouvez effectuer les actions suivantes sur le compte de l'utilisateur :

- **Ajouter à la liste de surveillance**. Lorsque vous souhaitez surveiller un utilisateur afin de détecter de futures menaces potentielles, vous pouvez les ajouter à une liste de surveillance.
- **Notifiez les administrateurs**. En cas d'activité inhabituelle ou suspecte sur le compte de l'utilisateur, une notification par e-mail est envoyée à tous les administrateurs ou à certains administrateurs.
- **Déconnecter l'utilisateur**. Lorsqu'un utilisateur est déconnecté de son compte, il ne peut accéder à aucune ressource via Citrix Gateway tant que l'administrateur Citrix Gateway n'a pas effacé l'action Déconnecter l'utilisateur.
- **Verrouiller l'utilisateur** : lorsque le compte d'un utilisateur est verrouillé en raison d'un comportement anormal, il ne peut accéder à aucune ressource via Citrix Gateway tant que l'administrateur de la passerelle n'a pas déverrouillé le compte.

Pour en savoir plus sur les actions et la façon de les configurer manuellement, consultez la section Stratégies et actions.

Pour appliquer manuellement les actions à l'utilisateur, accédez au profil de l'utilisateur et sélectionnez l'indicateur de risque approprié. Dans le menu **Actions**, sélectionnez une action et cliquez sur **Appliquer**.

> **Remarque**
>
> Quelle que soit la source de données qui déclenche un indicateur de risque, des mesures relatives à d'autres sources de données peuvent être appliquées.

Échec d'authentification inhabituel

Citrix Analytics détecte les menaces liées à l'accès lorsqu'un utilisateur a des échecs de connexion à partir d'une adresse IP inhabituelle et déclenche l'indicateur de risque correspondant.

Le facteur de risque associé à l'indicateur de risque d'authentification inhabituel est les indicateurs de risque basés sur l'échec de la connexion. Pour plus d'informations sur les facteurs de risque, consultez la section Indicateurs de risque utilisateur Citrix.

Quand l'indicateur d'échec d'authentification inhabituel est-il déclenché ?

Vous pouvez être averti lorsqu'un utilisateur de votre organisation a des échecs de connexion à partir d'une adresse IP inhabituelle qui est contraire à son comportement habituel.

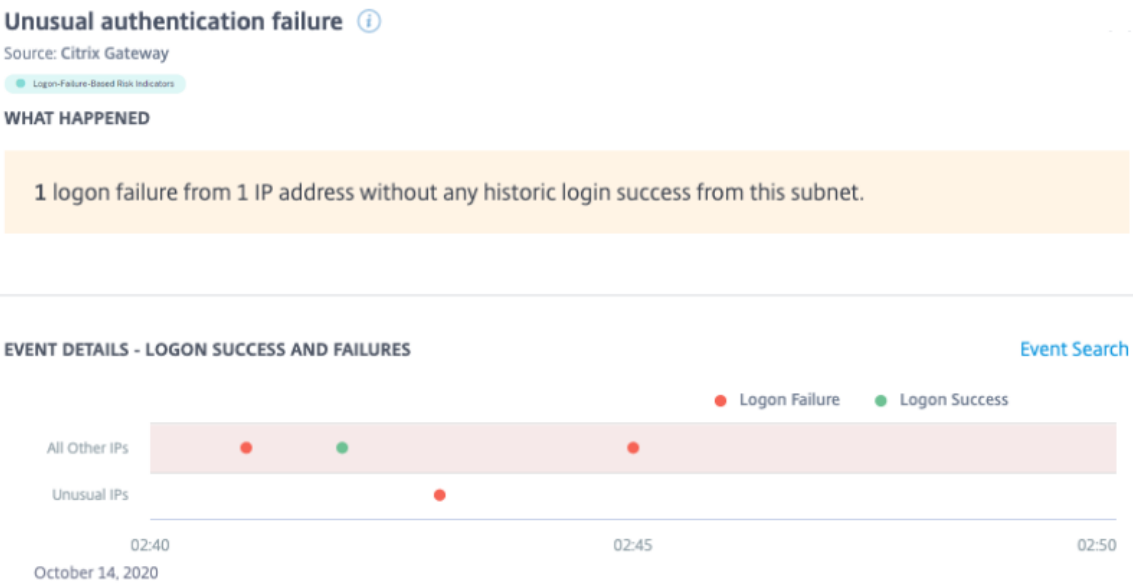
Citrix Gateway détecte ces événements et les signale à Citrix Analytics. Citrix Analytics reçoit les événements et augmente le score de risque de l'utilisateur. L'indicateur de risque **d'échec d'authentification inhabituel** est ajouté à la chronologie des risques de l'utilisateur.

Comment analyser l'indicateur d'échec d'authentification inhabituel ?

Prenons l'exemple de l'utilisateur Georgina Kalou, qui se connecte régulièrement à Citrix Gateway à partir de ses réseaux domestiques et professionnels habituels. Un attaquant distant tente d'authentifier le compte de Georgina en devinant différents mots de passe, ce qui entraîne des échecs d'authentification provenant d'un réseau inconnu.

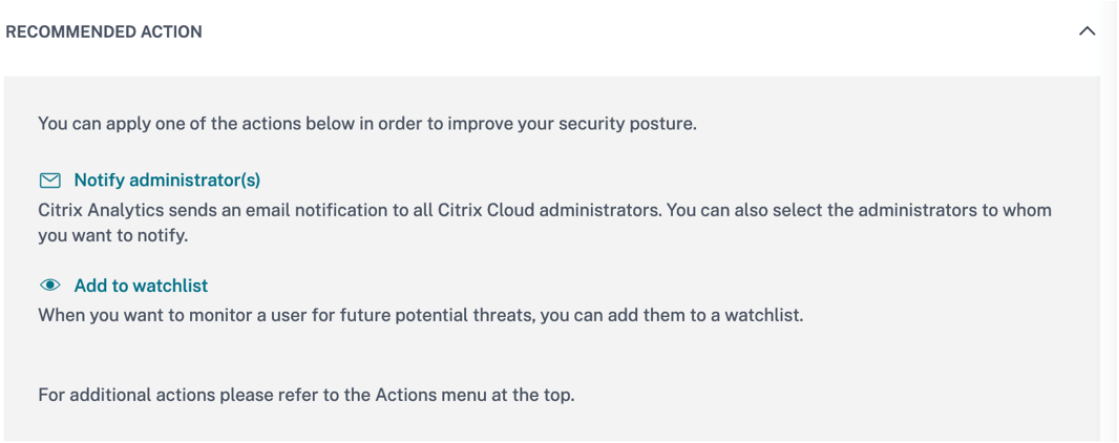
Dans ce scénario, Citrix Gateway signale ces événements à Citrix Analytics, qui attribue un score de risque mis à jour à Georgina Kalou. L'indicateur de risque d'échec d'authentification inhabituel est ajouté à la chronologie des risques de Georgina Kalou.

Dans la chronologie des risques de Georgina Kalou, vous pouvez sélectionner l'indicateur de risque d'échec d'authentification inhabituel signalé. La raison de l'événement est affichée avec des détails tels que l'heure et le lieu de l'événement.

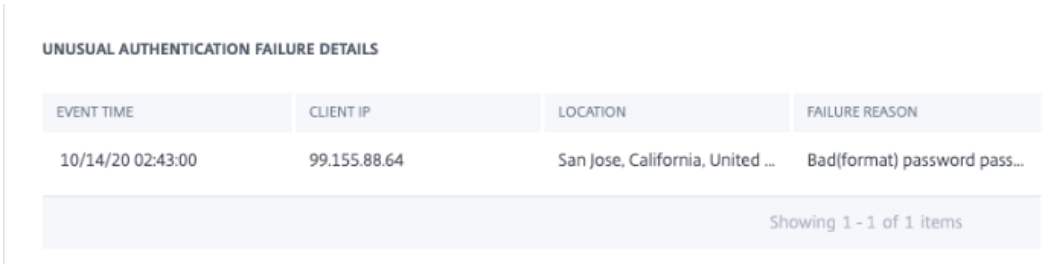


- Dans la section **WHAT HAPPENED**, vous pouvez consulter le bref résumé qui inclut le nombre total d'échecs d'authentification et l'heure de l'événement.
- Dans la section **ACTION RECOMMANDÉE**, vous trouverez les actions suggérées qui peuvent être appliquées à l'indicateur de risque. Citrix Analytics for Security recommande les actions en fonction de la gravité du risque posé par l'utilisateur. La recommandation peut être l'une des actions suivantes ou une combinaison des actions suivantes :
  - Avertir l'administrateur (s)
  - Ajouter à la liste de surveillance
  - Créer une stratégie

Vous pouvez sélectionner une action en fonction de la recommandation. Vous pouvez également sélectionner une action que vous souhaitez appliquer en fonction de votre choix dans le menu **Actions** . Pour plus d'informations, consultez Appliquer une action manuellement.

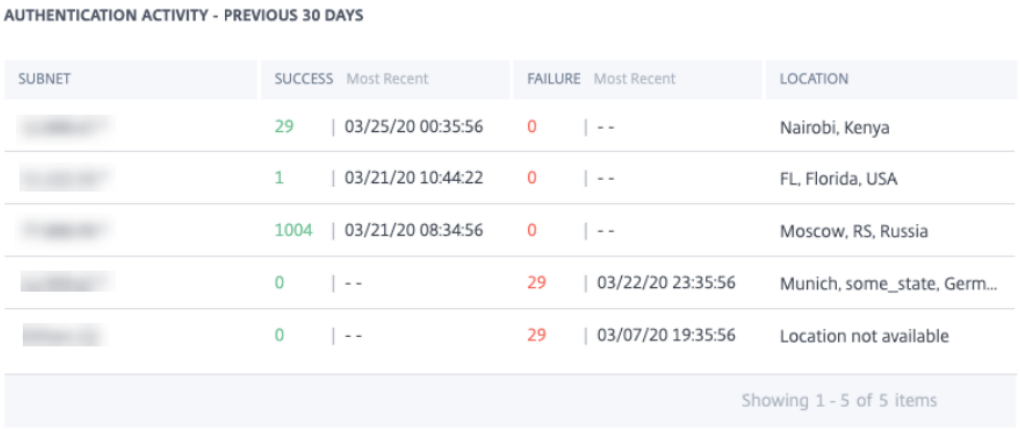


- Dans la section **DÉTAILS DE L'ÉVÉNEMENT —RÉUSSITE ET ÉCHECS DE LA CONNEXION**, vous pouvez afficher un graphique indiquant les échecs d'authentification inhabituels, ainsi que toute autre activité d'ouverture de session détectée pendant la même durée.
- Dans la section **DÉTAILS DE L'AUTHENTIFICATION INHABITUELLE**, le tableau fournit les informations suivantes sur les échecs d'authentification inhabituels :
  - **Heure de connexion** : date et heure de l'événement
  - **IP du client** : adresse IP de la machine utilisateur
  - **Lieu** : lieu à partir duquel l'événement s'est produit
  - Motif de l'**échec : raison** de l'échec de l'authentification



- Dans la section **ACTIVITÉ D'AUTHENTIFICATION DE L'UTILISATEUR —30 JOURS PRÉCÉDENTS**, le tableau fournit les informations suivantes sur les 30 derniers jours d'activité d'authentification de l'utilisateur :
  - Sous-réseau : adresse IP du réseau utilisateur.
  - Succès : nombre total d'événements d'authentification réussis et heure du dernier événement de réussite pour l'utilisateur.

- Échec : nombre total d'événements d'authentification ayant échoué et heure de l'événement échoué le plus récent pour l'utilisateur.
- Emplacement : emplacement à partir duquel l'événement d'authentification s'est produit.



Quelles actions pouvez-vous appliquer à l'utilisateur ?

Vous pouvez effectuer les actions suivantes sur le compte de l'utilisateur :

- **Ajouter à la liste de surveillance**. Lorsque vous souhaitez surveiller un utilisateur afin de détecter de futures menaces potentielles, vous pouvez les ajouter à une liste de surveillance.
- **Notifiez les administrateurs**. En cas d'activité inhabituelle ou suspecte sur le compte de l'utilisateur, une notification par e-mail est envoyée à tous les administrateurs ou à certains administrateurs.
- **Déconnecter l'utilisateur**. Lorsqu'un utilisateur est déconnecté de son compte, il ne peut accéder à aucune ressource via Citrix Gateway tant que l'administrateur Citrix Gateway n'a pas effacé l'action Déconnecter l'utilisateur.
- **Verrouiller l'utilisateur** : lorsque le compte d'un utilisateur est verrouillé en raison d'un comportement anormal, il ne peut accéder à aucune ressource via Citrix Gateway tant que l'administrateur de la passerelle n'a pas déverrouillé le compte.

Pour en savoir plus sur les actions et la façon de les configurer manuellement, consultez la section Stratégies et actions.

Pour appliquer manuellement les actions à l'utilisateur, accédez au profil de l'utilisateur et sélectionnez l'indicateur de risque approprié. Dans le menu **Actions**, sélectionnez une action et cliquez sur **Appliquer**.

> **Remarque**
>
> Quelle que soit la source de données qui déclenche un indicateur de risque, des mesures relatives à d'autres sources de données peuvent être appliquées.

Indicateurs de risque de Citrix Secure Private Access

April 12, 2024

Accès à un site Web risqué

> **Remarque**
> Les fonctionnalités suivantes de Citrix Analytics for Security sont affectées par l'abandon du filtrage Web basé sur les catégories par Secure Private Access :
>
> 1. Les champs de données tels que le groupe de catégories, la catégorie et la réputation des URL ne sont plus disponibles sur le tableau de bord Citrix Analytics for Security.
> 2. L'indicateur Risky d'accès au site Web, qui repose sur les mêmes données, est également obsolète et n'est pas déclenché pour les clients.
> 3. Les indicateurs de risque personnalisés existants utilisant les champs de données (catégorie-groupe, catégorie et réputation des URL) et les politiques associées ne sont plus déclenchés.

Pour plus de détails sur la dépréciation de Secure Private Access, consultez la section Obsolète des fonctionnalités.

Tentative d'accès à une URL de liste noire

Citrix Analytics détecte les menaces d'accès aux données en fonction des URL de liste noire auxquelles l'utilisateur accède et déclenche l'indicateur de risque correspondant.

L'indicateur de risque de **tentative d'accès à une URL sur liste noire** est signalé dans Citrix Analytics lorsqu'un utilisateur tente d'accéder à une URL sur liste noire configurée dans Secure Private Access.

Le facteur de risque associé à l'indicateur de risque **Tentative d'accès à une URL sur liste noire** est l'autre indicateur de risque. Pour plus d'informations sur les facteurs de risque, consultez la section Indicateurs de risque utilisateur Citrix.

Quand l'indicateur de risque Tentative d'accès aux URL sur liste noire est-il déclenché ?

Secure Private Access inclut une fonctionnalité de catégorisation d'URL qui fournit un contrôle basé sur des règles pour restreindre l'accès aux URL figurant sur la liste noire. Lorsqu'un utilisateur tente d'accéder à une URL sur liste noire, Secure Private Access signale cet événement à Citrix Analytics. Citrix Analytics met à jour le score de risque de l'utilisateur et ajoute une entrée **d'indicateur de risque Tentative d'accès aux URL sur liste noire** à la chronologie des risques de l'utilisateur.

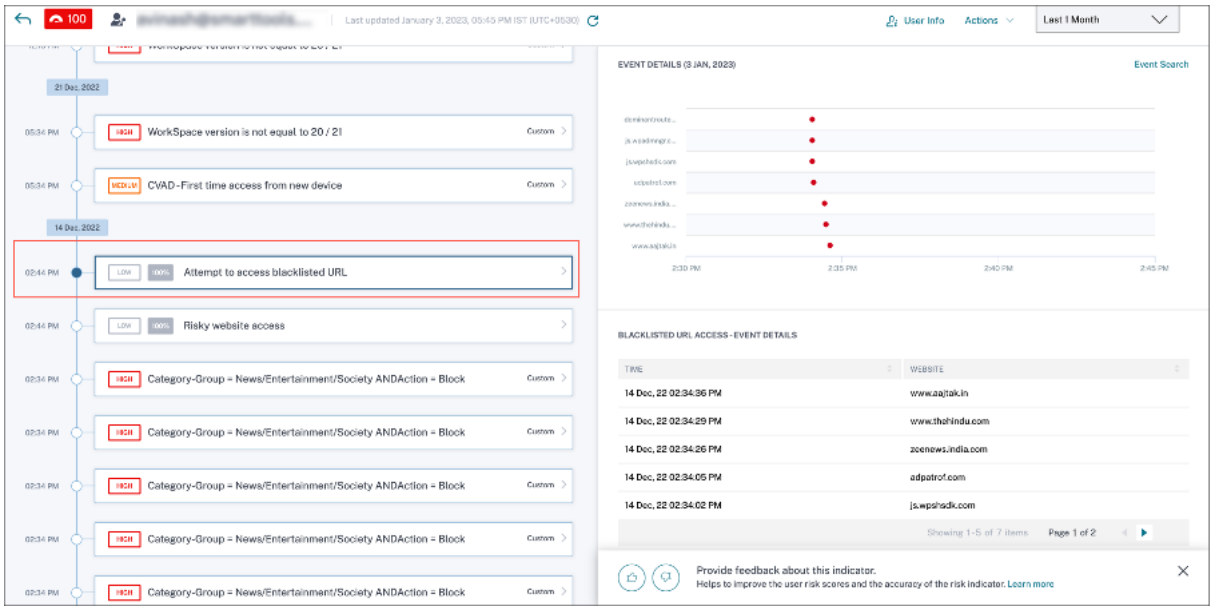
Comment analyser l'indicateur de risque d'URL sur la liste noire ?

Supposons qu'un utilisateur Georgina Kalou a accédé à une URL sur liste noire configurée dans Secure Private Access. Secure Private Access signale cet événement à Citrix Analytics, qui attribue un score de risque mis à jour à Georgina Kalou. L'indicateur de risque de **tentative d'accès aux URL sur liste noire** est ajouté à la chronologie des risques de Georgina Kalou.

Dans la chronologie des risques de Georgina Kalou, vous pouvez sélectionner l'indicateur de risque de **tentative d'accès aux URL sur liste noire** signalée. La raison de l'événement est affichée ainsi que les détails sur les événements, tels que l'heure de l'événement, les détails du site Web.

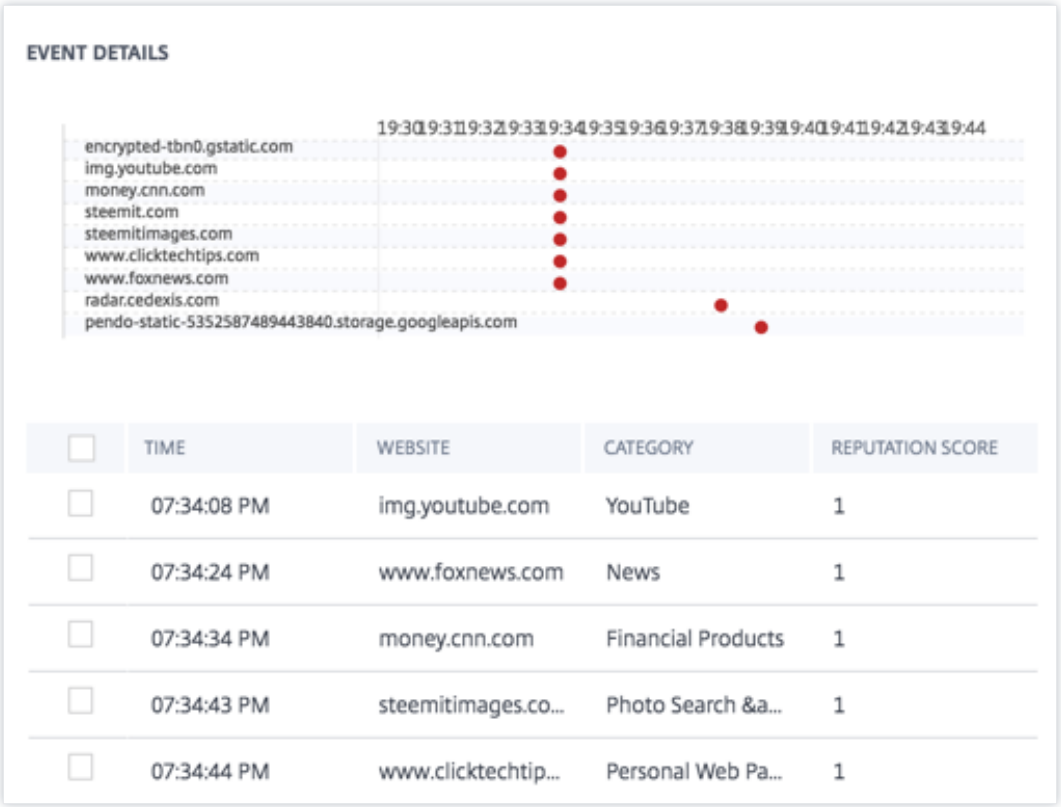
Pour afficher l'entrée **Tentative d'accès à une URL de liste noire** pour un utilisateur, accédez à **Sécurité > Utilisateurs**, puis sélectionnez l'utilisateur.

Lorsque vous sélectionnez l'entrée **Tentative d'accès à l'indicateur de risque d'URL sur liste noire** dans la chronologie, un panneau d'informations détaillées correspondant apparaît dans le volet droit.



- La section **WHAT HAPPENED** fournit un bref résumé de l'indicateur de risque. Il inclut les détails de l'URL de la liste noire à laquelle l'utilisateur a accédé pendant la période sélectionnée.

- La section **DÉTAILS DE L'ÉVÉNEMENT** inclut une visualisation chronologique des événements individuels survenus au cours de la période sélectionnée. En outre, vous pouvez afficher les informations clés suivantes sur chaque événement :
  - **Heure**. Heure à laquelle l'événement s'est produit.
  - **Site Web**. Le site Web risqué auquel l'utilisateur accède.
  - **Catégorie**. La catégorie spécifiée par Secure Private Access pour l'URL de la liste noire.
  - **Évaluation de la réputation**. L'évaluation de réputation renvoyée par Secure Private Access pour l'URL de la liste noire. Pour plus d'informations, consultez Score de réputation d'URL.



Quelles actions pouvez-vous appliquer à l'utilisateur ?

Vous pouvez effectuer les actions suivantes sur le compte de l'utilisateur :

- **Ajouter à la liste de surveillance**. Lorsque vous souhaitez surveiller un utilisateur afin de détecter de futures menaces potentielles, vous pouvez les ajouter à une liste de surveillance.
- **Notifiez les administrateurs**. En cas d'activité inhabituelle ou suspecte sur le compte de l'utilisateur, une notification par e-mail est envoyée à tous les administrateurs ou à certains administrateurs.

Pour en savoir plus sur les actions et la façon de les configurer manuellement, consultez la section Stratégies et actions.

Pour appliquer manuellement les actions à l'utilisateur, accédez au profil de l'utilisateur et sélectionnez l'indicateur de risque approprié. Dans le menu **Actions**, sélectionnez une action et cliquez sur **Appliquer**.

> **Remarque**
>
> Quelle que soit la source de données qui déclenche un indicateur de risque, des mesures relatives à d'autres sources de données peuvent être appliquées.

Volume de téléchargement inhabituel

Citrix Analytics détecte les menaces d'accès aux données en fonction de l'activité de volume de téléchargement inhabituelle et déclenche l'indicateur de risque correspondant.

L'indicateur de risque de **volume de téléchargement inhabituel** est signalé lorsqu'un utilisateur télécharge un volume de données excédentaire vers une application ou un site Web.

Le facteur de risque associé à l'indicateur de risque de volume de téléchargement inhabituel est l'autre indicateur de risque. Pour plus d'informations sur les facteurs de risque, consultez la section Indicateurs de risque utilisateur Citrix.

Quand l'indicateur de risque de volume de téléchargement inhabituel est-il déclenché ?

Vous pouvez configurer Secure Private Access pour surveiller les activités des utilisateurs, telles que les sites Web malveillants, dangereux ou inconnus visités et la bande passante consommée, ainsi que les téléchargements et les chargements risqués. Lorsqu'un utilisateur de votre organisation charge des données vers une application ou un site Web, Secure Private Access signale ces événements à Citrix Analytics.

Citrix Analytics surveille tous ces événements et s'il détermine que cette activité de l'utilisateur est contraire au comportement habituel de l'utilisateur, il met à jour le score de risque de l'utilisateur. L'

indicateur de risque de **volume de téléchargement inhabituel** est ajouté à la chronologie des risques de l'utilisateur.

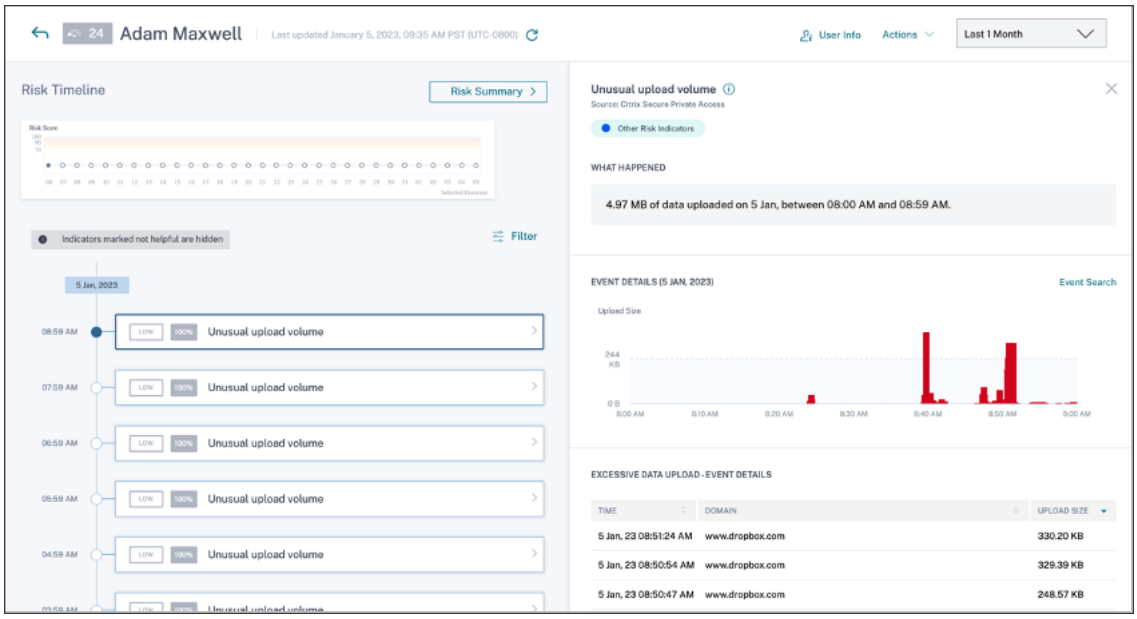
Comment analyser l'indicateur de risque de volume de téléchargement inhabituel ?

Prenons le cas d'un utilisateur Adam Maxwell, qui a téléchargé un volume excessif de données sur une application ou un site Web. Secure Private Access signale ces événements à Citrix Analytics, qui attribue un score de risque mis à jour à Adam Maxwell. L'indicateur de risque de **volume de téléchargement inhabituel** est ajouté à la chronologie des risques d'Adam Maxwell.

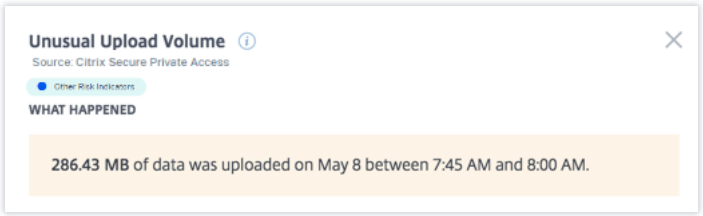
Dans la chronologie des risques d'Adam Maxwell, vous pouvez sélectionner l'indicateur de risque de **volume de téléchargement inhabituel** signalé. La raison de l'événement est affichée ainsi que les détails sur les événements, tels que l'heure de l'événement et le domaine.

Pour afficher l'indicateur de risque de **volume de chargement inhabituel**, accédez à **Sécurité > Utilisateurs**, puis sélectionnez l'utilisateur.

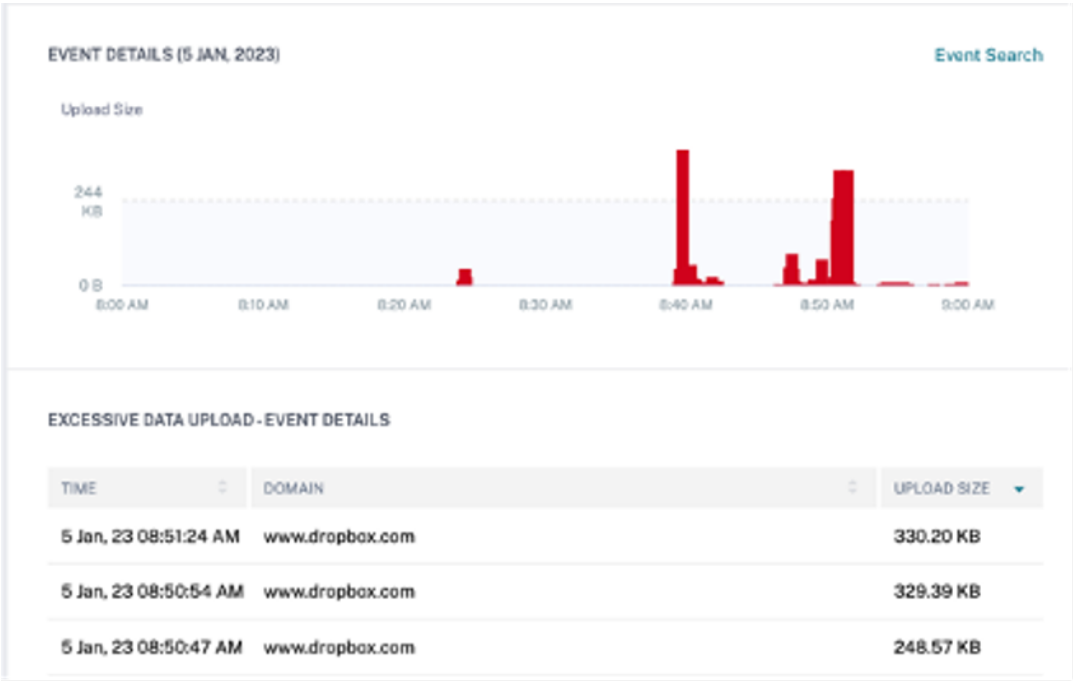
Lorsque vous sélectionnez une entrée d'indicateur de risque de **volume de chargement inhabituel** dans la chronologie, un panneau d'informations détaillées correspondant apparaît dans le volet droit.



- La section **WHAT HAPPENED** fournit un bref résumé de l'indicateur de risque, y compris le volume de données téléchargées au cours de la période sélectionnée.



- La section **DÉTAILS DE L'ÉVÉNEMENT** inclut une visualisation chronologique des événements de téléchargement de données individuels qui se sont produits pendant la période sélectionnée. En outre, vous pouvez afficher les informations clés suivantes sur chaque événement :
  - **Heure**. Heure à laquelle les données excessives ont été téléchargées sur une application ou un site Web.
  - **Domaine**. Domaine vers lequel l'utilisateur a téléchargé les données.
  - **Taille du téléchargement**. Volume de données téléchargées vers le domaine.



Quelles actions pouvez-vous appliquer à l'utilisateur ?

Vous pouvez effectuer les actions suivantes sur le compte de l'utilisateur :

- **Ajouter à la liste de surveillance**. Lorsque vous souhaitez surveiller un utilisateur afin de détecter de futures menaces potentielles, vous pouvez les ajouter à une liste de surveillance.
- **Notifiez les administrateurs**. En cas d'activité inhabituelle ou suspecte sur le compte de l'utilisateur, une notification par e-mail est envoyée à tous les administrateurs ou à certains administrateurs.

Pour en savoir plus sur les actions et la façon de les configurer manuellement, consultez la section Stratégies et actions.

Pour appliquer manuellement les actions à l'utilisateur, accédez au profil de l'utilisateur et sélectionnez l'indicateur de risque approprié. Dans le menu **Actions**, sélectionnez une action et cliquez sur **Appliquer**.

> **Remarque**
>
> Quelle que soit la source de données qui déclenche un indicateur de risque, des mesures relatives à d'autres sources de données peuvent être appliquées.

Téléchargement excessif de données

Citrix Analytics détecte les menaces d'accès aux données en fonction des données excessives téléchargées par les utilisateurs de votre réseau et déclenche l'indicateur de risque correspondant.

L'indicateur de risque est signalé lorsqu'un utilisateur de votre organisation télécharge un volume excessif de données à partir d'une application ou d'un site Web.

Quand l'indicateur de risque excessif de téléchargement de données est-il déclenché ?

Vous pouvez configurer Secure Private Access pour surveiller les activités des utilisateurs, telles que les sites Web malveillants, dangereux ou inconnus visités et la bande passante consommée, ainsi que les téléchargements et les chargements risqués. Lorsqu'un utilisateur de votre organisation télécharge des données à partir d'une application ou d'un site Web, Secure Private Access signale ces événements à Citrix Analytics.

Citrix Analytics surveille tous ces événements et s'il détermine que l'activité de l'utilisateur est contraire au comportement habituel de l'utilisateur, il met à jour le score de risque de l'utilisateur. L'indicateur de risque de téléchargement de données excessif est ajouté à la chronologie des risques de l'utilisateur.

Le facteur de risque associé à l'indicateur de risque de téléchargement excessif de données est l'autre indicateur de risque. Pour plus d'informations sur les facteurs de risque, consultez la section Indicateurs de risque utilisateur Citrix.

Comment analyser l'indicateur de risque excessif de téléchargement de données ?

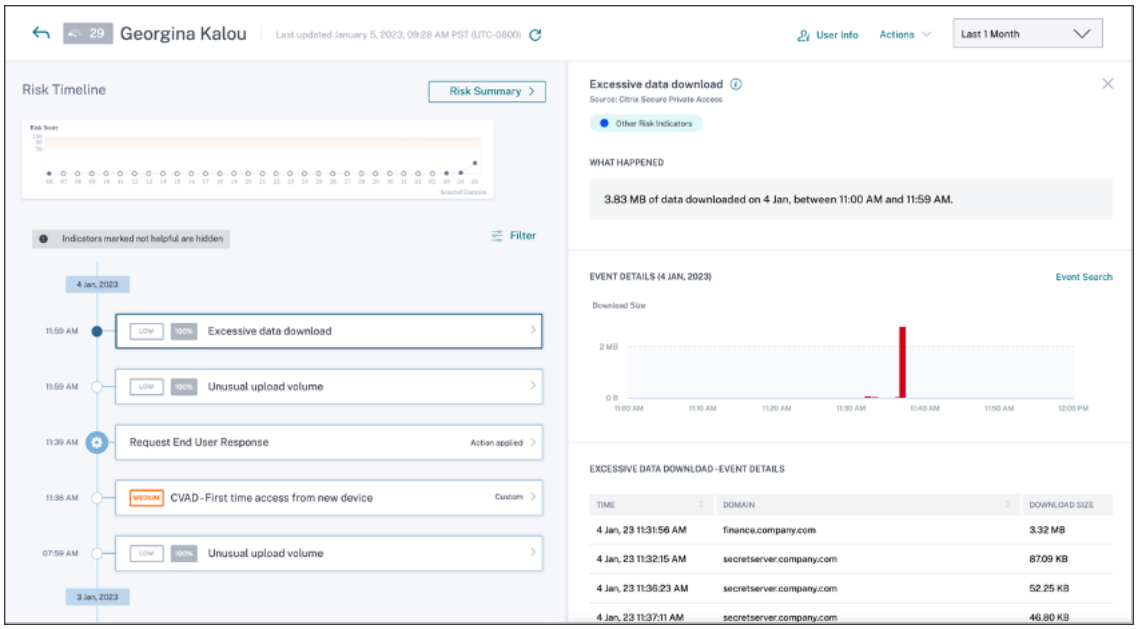
Considérez un utilisateur Georgina Kalou, téléchargé volume excédentaire de données à partir d'une application ou d'un site Web. Secure Private Access signale ces événements à Citrix Analytics, qui at-

tribue un score de risque mis à jour à Georgina Kalou et ajoute l'indicateur de risque de **téléchargement excessif de données** à la chronologie des risques de l'utilisateur.

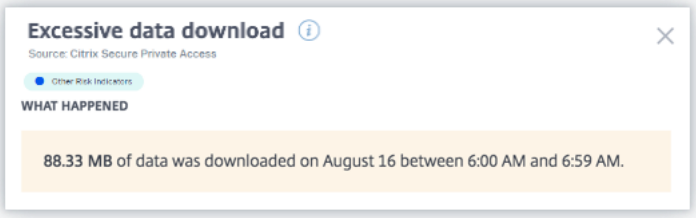
Dans la chronologie des risques de Georgina Kalou, vous pouvez sélectionner l'indicateur de risque de **téléchargement de données excessif** signalé. La raison de l'événement est affichée avec les détails sur les événements, tels que les détails de l'heure et du domaine.

Pour afficher l'indicateur de risque **excessif de téléchargement de données**, accédez à **Sécurité > Utilisateurs**, puis sélectionnez l'utilisateur.

Lorsque vous sélectionnez l'entrée de l'indicateur de risque de **téléchargement excessif de données** dans la chronologie, un panneau d'informations détaillées correspondant apparaît dans le volet droit.

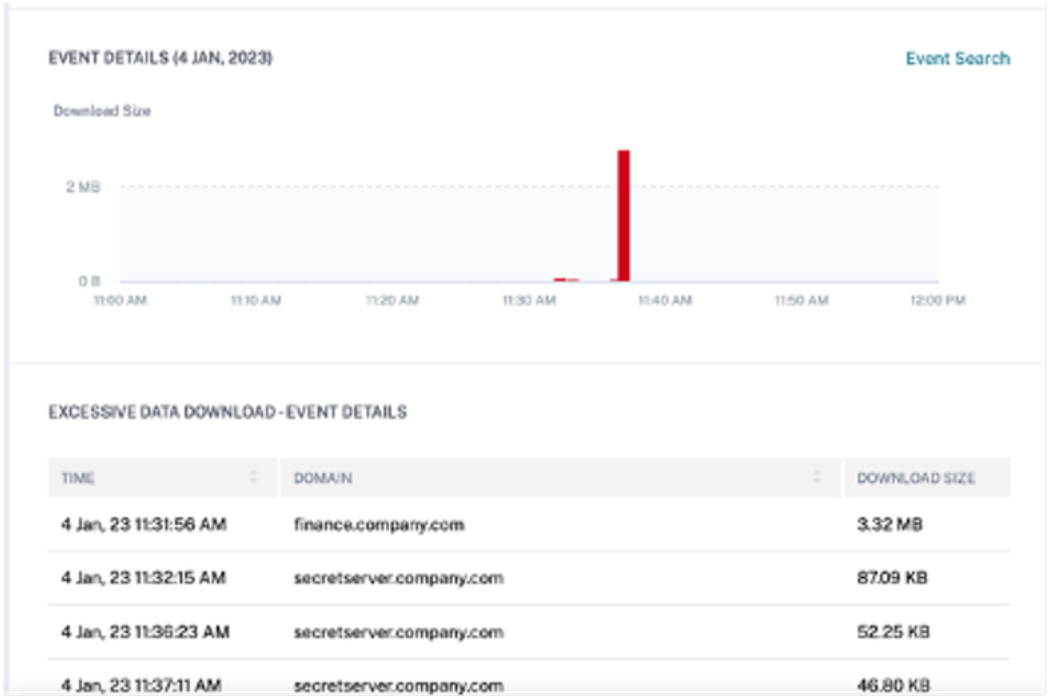


- La section **WHAT HAPPENED** fournit un bref résumé de l'indicateur de risque, y compris le volume de données téléchargées au cours de la période sélectionnée.



- La section **DÉTAILS DE L'ÉVÉNEMENT** inclut une visualisation chronologique des différents événements de téléchargement de données qui se sont produits pendant la période sélectionnée. En outre, vous pouvez afficher les informations clés suivantes sur chaque événement :

- **Heure**. Heure à laquelle les données excessives ont été téléchargées sur une application ou un site Web.
- **Domaine**. Domaine vers lequel l'utilisateur a téléchargé les données.
- **Taille du téléchargement**. Volume de données téléchargées sur le domaine.



Quelles actions pouvez-vous appliquer à l'utilisateur ?

Vous pouvez effectuer les actions suivantes sur le compte de l'utilisateur :

- **Ajouter à la liste de surveillance**. Lorsque vous souhaitez surveiller un utilisateur afin de détecter de futures menaces potentielles, vous pouvez les ajouter à une liste de surveillance.
- **Notifiez les administrateurs**. En cas d'activité inhabituelle ou suspecte sur le compte de l'utilisateur, une notification par e-mail est envoyée à tous les administrateurs ou à certains administrateurs.

Pour en savoir plus sur les actions et la façon de les configurer manuellement, consultez la section Stratégies et actions.

Pour appliquer manuellement les actions à l'utilisateur, accédez au profil de l'utilisateur et sélectionnez l'indicateur de risque approprié. Dans le menu **Actions**, sélectionnez une action et cliquez sur **Appliquer**.

> **Remarque**
>
> Quelle que soit la source de données qui déclenche un indicateur de risque, des mesures relatives à d'autres sources de données peuvent être appliquées.

Indicateurs de risque Citrix Virtual Apps and Desktops et Citrix DaaS

July 14, 2022

Voyages impossibles

Citrix Analytics détecte les ouvertures de session d'un utilisateur comme risquées lorsque les ouvertures de session consécutives proviennent de deux pays différents au cours d'une période inférieure au temps de trajet prévu entre les pays.

Le scénario de temps de trajet impossible indique les risques suivants :

- **Informations d'identification compromises** : un attaquant distant vole les informations d'identification d'un utilisateur légitime.
- **Informations d'identification partagées** : différents utilisateurs utilisent les mêmes informations d'identification utilisateur.

Quand l'indicateur de risque de voyage impossible se déclenche-t-il ?

L'indicateur **de risque de déplacement impossible** évalue le temps et la distance estimée entre chaque paire d'ouvertures de session utilisateur consécutives, et se déclenche lorsque la distance est supérieure à ce qu'une personne peut éventuellement parcourir pendant cette période.

> **Remarque**
>
> Cet indicateur de risque contient également une logique visant à réduire les alertes de faux positifs pour les scénarios suivants qui ne reflètent pas l'emplacement réel des utilisateurs :
>
> - Lorsque les utilisateurs se connectent à des applications et bureaux virtuels à partir de connexions proxy.
> - Lorsque les utilisateurs se connectent à des applications et des bureaux virtuels à partir de clients hébergés.

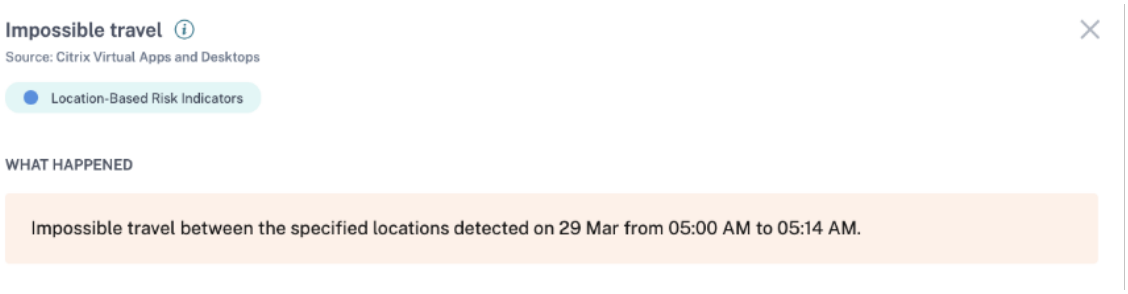
Comment analyser l'indicateur de risque impossible

Prenons l'exemple de l'utilisateur Adam Maxwell, qui se connecte à partir de deux emplacements : Moskva, en Russie, et Hohhot, en Chine, dans un délai d'une minute. Citrix Analytics détecte cet événement d'ouverture de session comme un scénario de voyage impossible et déclenche l'indicateur **de risque de déplacement impossible** . L'indicateur de risque est ajouté à la chronologie de risque d'Adam Maxwell et un score de risque lui est attribué.

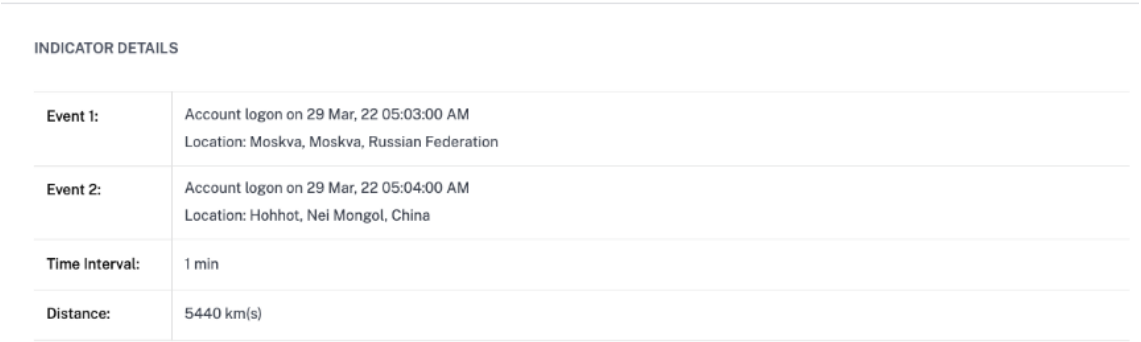
Pour consulter la chronologie des risques d'Adam Maxwell, sélectionnez **Sécurité > Utilisateurs**. Dans le volet **Utilisateurs risqués**, sélectionnez l'utilisateur Adam Maxwell.

Dans la chronologie des risques d'Adam Maxwell, sélectionnez l'indicateur **de risque de voyage impossible** . Vous pouvez consulter les informations suivantes :

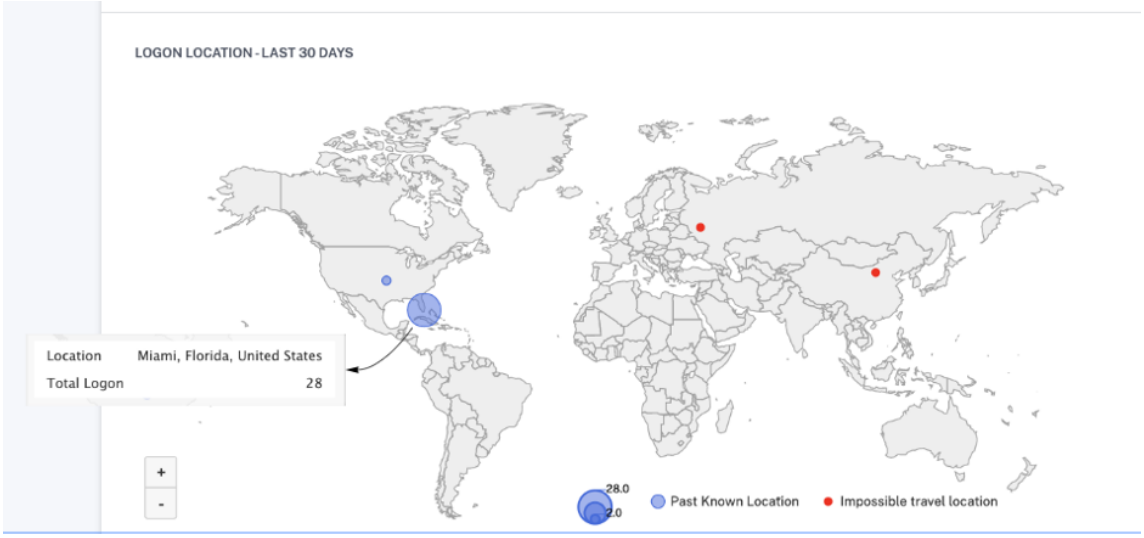
- La section **WHAT HAPPENED** fournit un bref résumé de l'événement de voyage impossible.



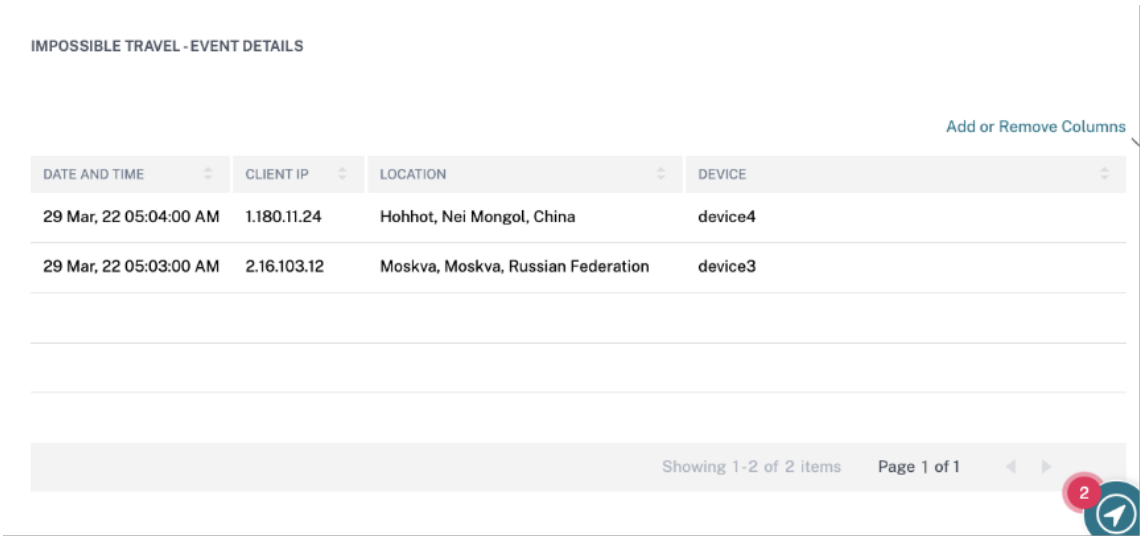
- La section **DÉTAILS DE L'INDICATEUR** fournit les emplacements à partir desquels l'utilisateur s'est connecté, la durée entre les ouvertures de session consécutives et la distance entre les deux emplacements.



- La section **EMPLACEMENT D'OUVERTURE DE SESSION - 30 DERNIERS JOURS** affiche une vue cartographique géographique des lieux de voyage impossibles et des emplacements connus de l'utilisateur. Les données de localisation sont affichées pour les 30 derniers jours. Vous pouvez survoler les pointeurs de la carte pour afficher le nombre total d'ouvertures de session de chaque emplacement.



- La section **IMPOSSIBLE TRAVEL- EVENT DETAILS** fournit les informations suivantes sur l'événement de voyage impossible :
  - **Date et heure** : indique la date et l'heure des ouvertures de session.
  - **IP du client** : indique l'adresse IP de la machine utilisateur.
  - **Emplacement** : indique l'emplacement depuis lequel l'utilisateur s'est connecté.
  - **Appareil** : indique le nom de l'appareil de l'utilisateur.
  - **Type d'ouverture**de session : indique si l'activité de l'utilisateur est l'ouverture de session ou la connexion au compte. L'événement d'ouverture de session de compte est déclenché lorsque l'authentification d'un utilisateur sur son compte réussit. Attendu que l'événement d'ouverture de session est déclenché lorsqu'un utilisateur entre ses informations d'identification et se connecte à sa session d'application ou de bureau.
  - **OS** : indique le système d'exploitation de la machine utilisateur.
  - **Navigateur** : indique le navigateur Web utilisé pour accéder à l'application.



Quelles actions pouvez-vous appliquer aux utilisateurs ?

Vous pouvez effectuer les actions suivantes sur le compte de l'utilisateur :

- **Ajouter à la liste de surveillance**. Lorsque vous souhaitez surveiller un utilisateur afin de détecter de futures menaces potentielles, vous pouvez les ajouter à une liste de surveillance.
- **Notifiez les administrateurs**. En cas d'activité inhabituelle ou suspecte sur le compte de l'utilisateur, une notification par e-mail est envoyée à tous les administrateurs ou à certains d'entre eux.
- **Déconnecter l'utilisateur**. Lorsqu'un utilisateur est déconnecté de son compte, il ne peut pas accéder à la ressource via les bureaux virtuels.
- **Démarrer l'enregistrement de la session**. En cas d'événement inhabituel sur le compte Virtual Desktops de l'utilisateur, l'administrateur peut commencer à enregistrer les activités de l'utilisateur lors des futures sessions d'ouverture de session. Toutefois, si l'utilisateur utilise Citrix Virtual Apps and Desktops 7.18 ou version ultérieure, l'administrateur peut démarrer et arrêter dynamiquement l'enregistrement de la session d'ouverture de session actuelle de l'utilisateur.

Pour en savoir plus sur les actions et la façon de les configurer manuellement, consultez la section Stratégies et actions.

Pour appliquer les actions à l'utilisateur manuellement, accédez au profil de l'utilisateur et sélectionnez l'indicateur de risque approprié. Dans le menu **Action**, sélectionnez une action et cliquez sur **Appliquer**.

> **Remarque**
>
> Quelle que soit la source de données qui déclenche un indicateur de risque, des mesures relatives à d'autres sources de données peuvent être appliquées.

Exfiltration potentielle des données

Citrix Analytics détecte les menaces liées aux données en fonction de tentatives excessives d'exfiltration des données et déclenche l'indicateur de risque correspondant.

Le facteur de risque associé à l'indicateur de risque potentiel d'exfiltration de données est l'indicateur de risque basé sur les données. Pour plus d'informations sur les facteurs de risque, consultez la section Indicateurs de risque utilisateur Citrix.

L'indicateur de risque **potentiel d'exfiltration de données** est déclenché lorsqu'un utilisateur Citrix Receiver tente de télécharger ou de transférer des fichiers vers un lecteur ou une imprimante. Ces données peuvent être un événement de téléchargement de fichier tel que le téléchargement d'un fichier sur un lecteur local, des lecteurs mappés ou un périphérique de stockage externe. Les données peuvent également être exfiltrées à l'aide du presse-papiers ou par l'action de copier-coller.

> **Remarque**
>
> Les opérations du presse-papiers sont prises en charge uniquement par les applications SaaS.

Quand l'indicateur de risque potentiel d'exfiltration de données est-il déclenché ?

Vous pouvez être averti lorsqu'un utilisateur a transféré un nombre excessif de fichiers vers un lecteur ou une imprimante au cours d'une période donnée. Cet indicateur de risque est également déclenché lorsque l'utilisateur utilise l'action copier-coller sur son ordinateur local.

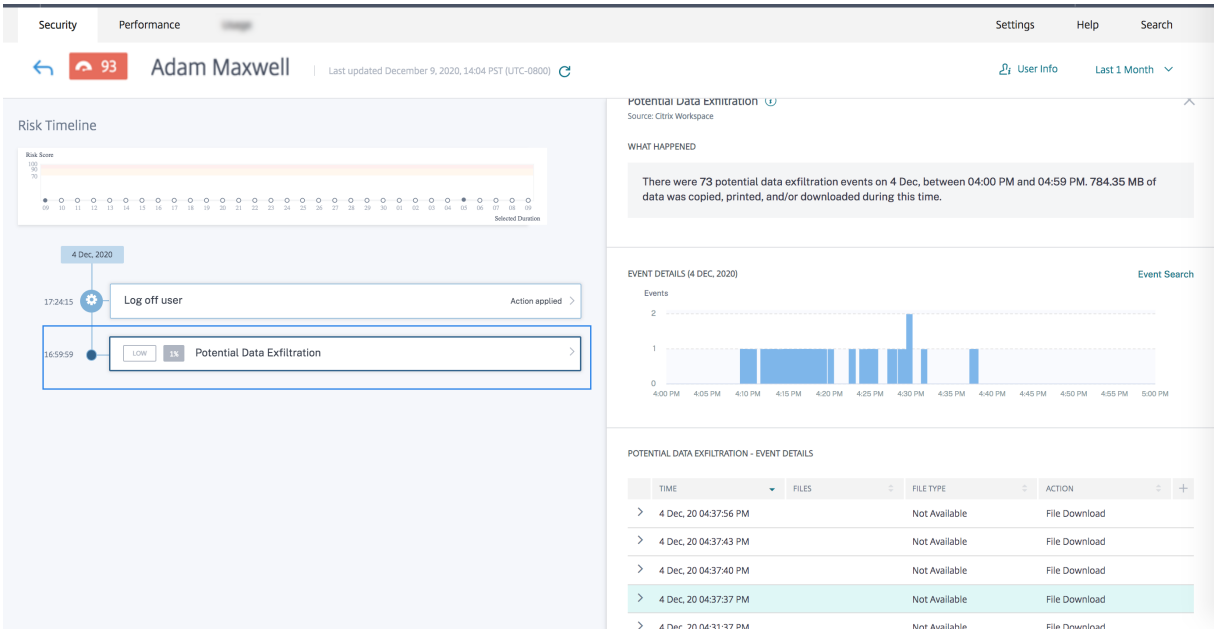
Lorsque Citrix Receiver détecte ce comportement, Citrix Analytics reçoit cet événement et attribue un score de risque à l'utilisateur concerné. L'indicateur de risque **potentiel d'exfiltration de données** est ajouté à la chronologie des risques de l'utilisateur.

Comment analyser l'indicateur de risque potentiel d'exfiltration des données ?

Prenons l'exemple de l'utilisateur Adam Maxwell, qui est connecté à une session et tente d'imprimer des fichiers dépassant la limite prédéfinie. Par cette action, Adam Maxwell avait dépassé son comportement normal de transfert de fichiers basé sur des algorithmes d'apprentissage automatique.

Dans la chronologie d'Adam Maxwell, vous pouvez sélectionner l'indicateur de risque **potentiel d'exfiltration de données** . La raison de l'événement est affichée avec les détails tels que les fichiers transférés et le périphérique utilisé pour transférer le fichier.

Pour afficher l'indicateur de risque **potentiel d'exfiltration de données** signalé pour un utilisateur, accédez à **Sécurité > Utilisateurs**, puis sélectionnez l'utilisateur.

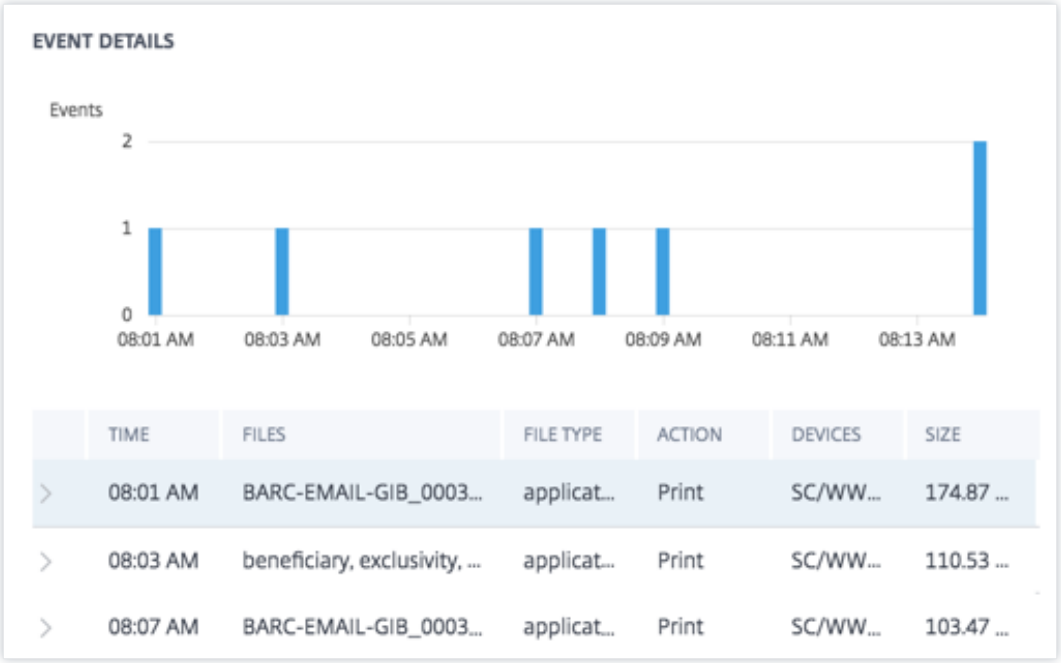


- Dans la section **WHAT HAPPENED**, vous pouvez consulter le résumé de l'événement potentiel d'exfiltration de données. Vous pouvez afficher le nombre d'événements d'exfiltration de données au cours d'une période spécifique.

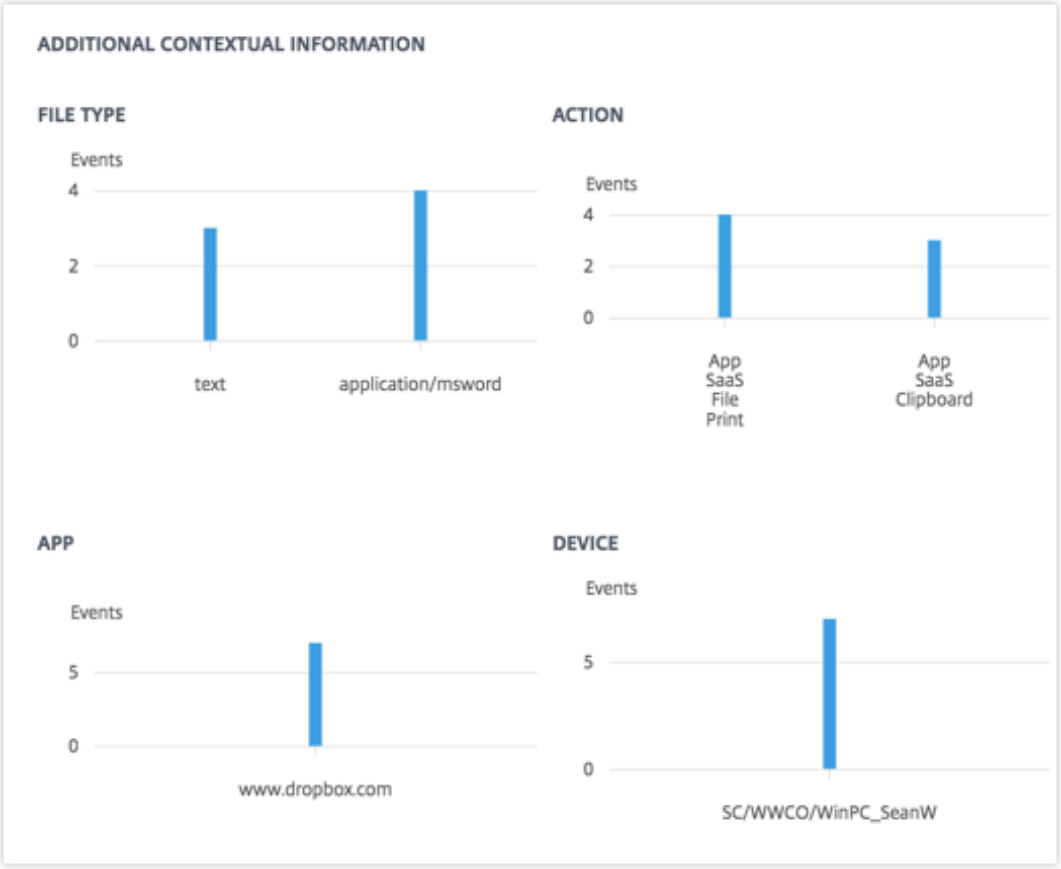
- Dans la section **DÉTAILS DE L'ÉVÉNEMENT**, les tentatives d'exfiltration de données apparaissent sous forme graphique et tabulaire. Les événements apparaissent sous forme d'entrées individuelles dans le graphique et le tableau fournit les informations clés suivantes :
  - **Le temps**. Heure à laquelle l'événement d'exfiltration de données s'est produit.
  - **Fichiers**. Le fichier qui a été téléchargé, imprimé ou copié.
  - **Type de fichier**. Type de fichier qui a été téléchargé, imprimé ou copié.

    > **Remarque**
    >
    > Le nom du fichier imprimé n'est disponible qu'à partir de l'événement d'impression des applications SaaS.

  - **Action**. Types d'événements d'exfiltration de données qui ont été effectués (impression, téléchargement ou copie).
  - **Appareils**. L'appareil utilisé.
  - **taille**. La taille du fichier qui est exfiltré.
  - **Emplacement**. Ville d'où l'utilisateur tente d'exfiltrer des données.



- La section **INFORMATIONS CONTEXTUELLES SUPPLÉMENTAIRES**, pendant la survenance de l'événement, vous permet d'afficher les éléments suivants :
  - Le nombre de dossiers qui ont été exfiltrés.
  - Les actions effectuées.
  - Les applications utilisées.
  - Appareil utilisé par l'utilisateur.



Quelles actions pouvez-vous appliquer à l'utilisateur ?

Vous pouvez effectuer les actions suivantes sur le compte de l'utilisateur :

- **Ajouter à la liste de surveillance**. Lorsque vous souhaitez surveiller un utilisateur afin de détecter de futures menaces potentielles, vous pouvez les ajouter à une liste de surveillance.
- **Notifiez les administrateurs**. En cas d'activité inhabituelle ou suspecte sur le compte de l'utilisateur, une notification par e-mail est envoyée à tous les administrateurs ou à certains administrateurs.
- **Déconnecter l'utilisateur**. Lorsqu'un utilisateur est déconnecté de son compte, il ne peut pas accéder à la ressource via les bureaux virtuels.
- **Démarrer l'enregistrement de la session**. En cas d'événement inhabituel sur le compte Virtual Desktops de l'utilisateur, l'administrateur peut commencer à enregistrer les activités de l'utilisateur lors des sessions d'ouverture de session futures. Toutefois, si l'utilisateur est sur de Citrix Virtual Apps and Desktops 7.18 ou une version ultérieure, l'administrateur peut démarrer et arrêter dynamiquement l'enregistrement de la session d'ouverture de session en cours de l'utilisateur.

Pour en savoir plus sur les actions et la façon de les configurer manuellement, consultez la section Stratégies et actions.

Pour appliquer manuellement les actions à l'utilisateur, accédez au profil de l'utilisateur et sélectionnez l'indicateur de risque approprié. Dans le menu **Action**, sélectionnez une action et cliquez sur **Appliquer**.

> **Remarque**
>
> Quelle que soit la source de données qui déclenche un indicateur de risque, des mesures relatives à d'autres sources de données peuvent être appliquées.

Ouverture de session suspecte

Citrix Analytics détecte les ouvertures de session de l'utilisateur qui semblent inhabituelles ou risquées en fonction de plusieurs facteurs contextuels, définis conjointement par l'appareil, l'emplacement et le réseau utilisés par l'utilisateur.

Quand l'indicateur de risque d'ouverture de session suspecte est-il déclenché ?

L'indicateur de risque est déclenché par la combinaison des facteurs suivants, chaque facteur étant considéré comme potentiellement suspect en fonction d'une ou de plusieurs conditions.

Facteur	Conditions
Appareil inhabituel	L'utilisateur ouvre une session à partir d'un appareil qui n'a pas été utilisé au cours des 30 derniers jours. L'utilisateur ouvre une session à partir d'un client HTML5 ou d'un client Chrome dont la signature de l'appareil n'est pas cohérente avec l'historique de l'utilisateur.
Emplacement inhabituel	Ouvrez une session à partir d'une ville ou d'un pays où l'utilisateur n'a pas ouvert de session au cours des 30 derniers jours. La ville ou le pays est géographiquement éloigné des emplacements d'ouverture de session récents (30 derniers jours).

Facteur	Conditions
	Zéro ou minimum d'utilisateurs se sont connectés depuis la ville ou le pays au cours des 30 derniers jours.
Réseau insolite	Ouvrez une session à partir d'une adresse IP que l'utilisateur n'a pas utilisée au cours des 30 derniers jours.
	Ouvrez une session à partir d'un sous-réseau IP que l'utilisateur n'a pas utilisé au cours des 30 derniers jours.
	Aucun ou un minimum d'utilisateurs se sont connectés depuis le sous-réseau IP au cours des 30 derniers jours.
Menace IP	L'adresse IP est identifiée comme présentant un risque élevé par le flux de renseignements sur les menaces de la communauté Webroot.
	Citrix Analytics a récemment détecté des activités d'ouverture de session très suspectes à partir de l'adresse IP d'autres utilisateurs.

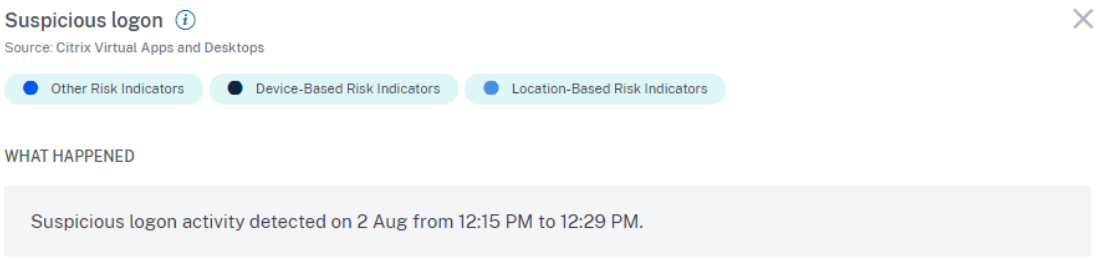
Comment analyser l'indicateur de risque d'ouverture de session suspecte

Prenons l'exemple de l'utilisateur Adam Maxwell, qui se connecte pour la première fois depuis Mumbai, en Inde. Il utilise un nouvel appareil ou un appareil qui n'a pas été utilisé au cours des 30 derniers jours pour se connecter à un nouveau réseau de Citrix Virtual Apps and Desktops et s'y connecter. Citrix Analytics détecte cet événement d'ouverture de session comme suspect car les facteurs (emplacement, appareil et réseau) s'écartent de son comportement habituel et déclenchent l'indicateur de risque d'ouverture de **session suspecte** . L'indicateur de risque est ajouté à la chronologie des risques d'Adam Maxwell et un score de risque lui est attribué.

Pour afficher le temps de risque d'Adam Maxwell, sélectionnez **Sécurité > Utilisateurs**. Dans le volet **Utilisateurs risqués**, sélectionnez l'utilisateur Adam Maxwell.

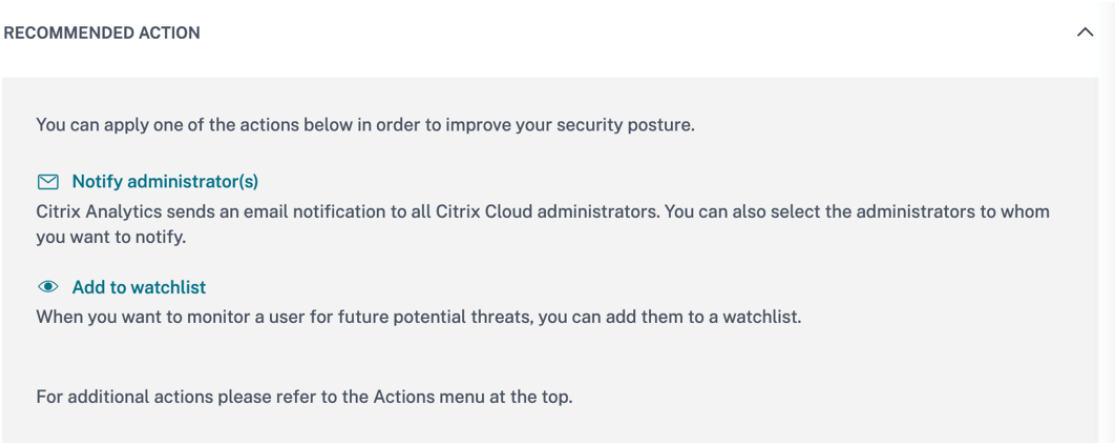
Dans la chronologie des risques d'Adam Maxwell, sélectionnez l'indicateur de risque d'ouverture de session suspecte . Vous pouvez consulter les informations suivantes :

- La section **WHAT HAPPENED** fournit un bref résumé des activités suspectes, y compris les facteurs de risque et le moment de l'événement.



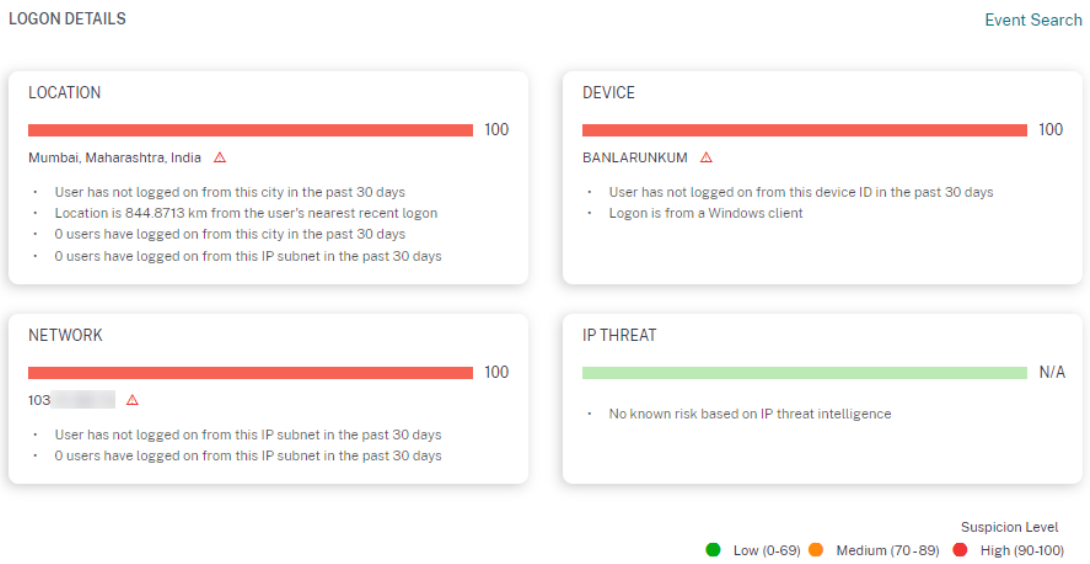
- Dans la section **ACTION RECOMMANDÉE**, vous trouverez les actions suggérées qui peuvent être appliquées à l'indicateur de risque. Citrix Analytics for Security recommande les actions en fonction de la gravité du risque posé par l'utilisateur. La recommandation peut être l'une des actions suivantes ou une combinaison des actions suivantes :
  - Avertir l'administrateur (s)
  - Ajouter à la liste de surveillance
  - Créer une stratégie

  Vous pouvez sélectionner une action en fonction de la recommandation. Vous pouvez également sélectionner une action que vous souhaitez appliquer en fonction de votre choix dans le menu **Actions** . Pour plus d'informations, consultez Appliquer une action manuellement.



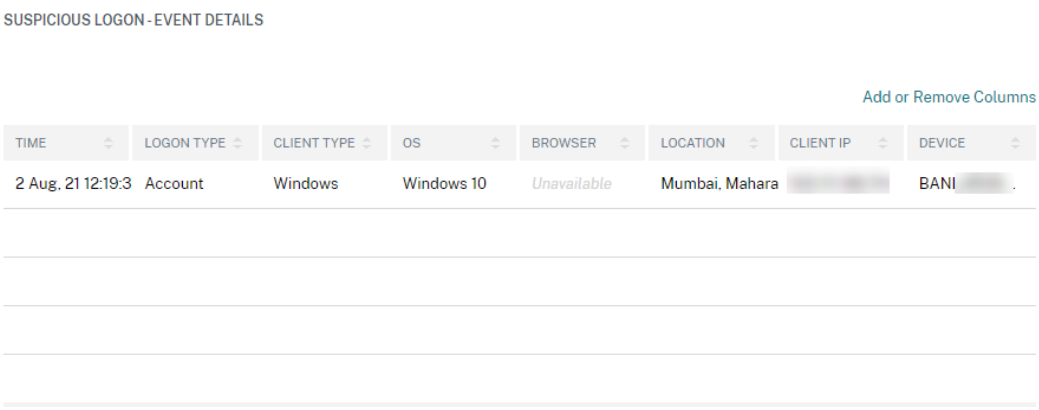
- La section **DÉTAILS DE CONNEXION** fournit un résumé détaillé des activités suspectes correspondant à chaque facteur de risque. Chaque facteur de risque se voit attribuer un score qui indique le niveau de suspicion. Un seul facteur de risque n'indique pas un risque élevé de la part d'un utilisateur. Le risque global est basé sur la corrélation entre les multiples facteurs de risque.

Niveau de suspicion	Indication
0–69	Le facteur semble normal et n'est pas considéré comme suspect.
70–89	Le facteur semble légèrement inhabituel et est considéré comme modérément suspect avec d'autres facteurs.
90–100	Le facteur est tout à fait nouveau ou inhabituel et est considéré comme très suspect par rapport à d'autres facteurs.



- La section **EMPLACEMENT D'OUVERTURE DE SESSION - 30 DERNIERS JOURS** affiche une carte géographique des derniers emplacements connus et de l'emplacement actuel de l'utilisateur. Les données de localisation sont affichées pour les 30 derniers jours. Vous pouvez survoler les pointeurs de la carte pour afficher le nombre total d'ouvertures de session de chaque emplacement.

- La section **OUVERTURE DE SESSION SUSPECTE - DÉTAILS DE L'ÉVÉNEMENT** fournit les informations suivantes sur l'événement d'ouverture de session suspect :
  - **Heure** : indique la date et l'heure de la connexion suspecte.
  - **Type d'ouverture**de session : indique si l'activité de l'utilisateur est l'ouverture de session ou la connexion au compte. L'événement de connexion au compte est déclenché lorsque l'authentification d'un utilisateur sur son compte est réussie. Attendu que l'événement d'ouverture de session est déclenché lorsqu'un utilisateur entre ses informations d'identification et se connecte à sa session d'application ou de bureau.
  - **Type de client** : indique le type d'application Citrix Workspace installée sur la machine utilisateur. Selon le système d'exploitation de la machine utilisateur, le type de client peut être Android, iOS, Windows, Linux, Mac, etc.
  - **OS** : indique le système d'exploitation de la machine utilisateur.
  - **Navigateur** : indique le navigateur Web utilisé pour accéder à l'application.
  - **Emplacement** : indique l'emplacement depuis lequel l'utilisateur s'est connecté.
  - **IP du client** : indique l'adresse IP de la machine utilisateur.
  - **Appareil** : indique le nom de l'appareil de l'utilisateur.



Quelles actions pouvez-vous appliquer aux utilisateurs ?

Vous pouvez effectuer les actions suivantes sur le compte de l'utilisateur :

- **Ajouter à la liste de surveillance**. Lorsque vous souhaitez surveiller un utilisateur afin de détecter de futures menaces potentielles, vous pouvez les ajouter à une liste de surveillance.
- **Notifiez les administrateurs**. En cas d'activité inhabituelle ou suspecte sur le compte de l'utilisateur, une notification par e-mail est envoyée à tous les administrateurs ou à certains administrateurs.
- **Déconnecter l'utilisateur**. Lorsqu'un utilisateur est déconnecté de son compte, il ne peut pas accéder à la ressource via les bureaux virtuels.
- **Démarrer l'enregistrement de la session**. En cas d'événement inhabituel sur le compte Virtual Desktops de l'utilisateur, l'administrateur peut commencer à enregistrer les activités de l'utilisateur lors des sessions d'ouverture de session futures. Toutefois, si l'utilisateur est sur de Citrix Virtual Apps and Desktops 7.18 ou une version ultérieure, l'administrateur peut démarrer et arrêter dynamiquement l'enregistrement de la session d'ouverture de session en cours de l'utilisateur.

Pour en savoir plus sur les actions et la façon de les configurer manuellement, consultez la section Stratégies et actions.

Pour appliquer manuellement les actions à l'utilisateur, accédez au profil de l'utilisateur et sélectionnez l'indicateur de risque approprié. Dans le menu **Action**, sélectionnez une action et cliquez sur **Appliquer**.

> **Remarque**
>
> Quelle que soit la source de données qui déclenche un indicateur de risque, des mesures relatives à d'autres sources de données peuvent être appliquées.

Fournir des commentaires sur les indicateurs de risque utilisateur

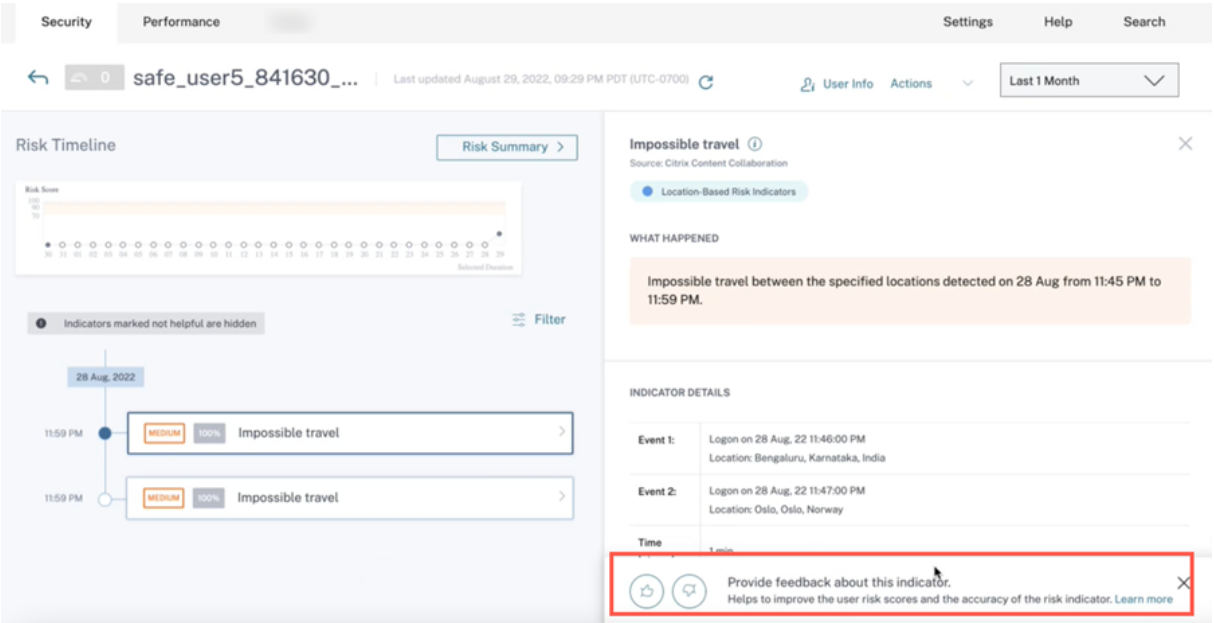
October 18, 2022

Les indicateurs de risque sont conçus pour détecter et signaler toute activité utilisateur potentiellement suspecte ou anormale, tout en augmentant automatiquement le score de risque de l'utilisateur. Dans la pratique, bien que certaines occurrences d'un indicateur de risque correspondent à une menace de sécurité sous-jacente légitime, d'autres se révèlent inoffensives.

La fonction de feedback sur les indicateurs vous permet de signaler explicitement les occurrences des indicateurs de risque :

- Aussi utile lorsque vous pensez qu'il existe un véritable risque sous-jacent pour l'utilisateur
- Ce n'est pas utile si vous avez déterminé qu'il n'y a pas de menace à la sécurité. Dans ce cas, l'occurrence de l'indicateur est masquée dans la chronologie de l'utilisateur par défaut et le score de risque de l'utilisateur est automatiquement ajusté pour exclure cette occurrence de l'indicateur dans les calculs suivants.

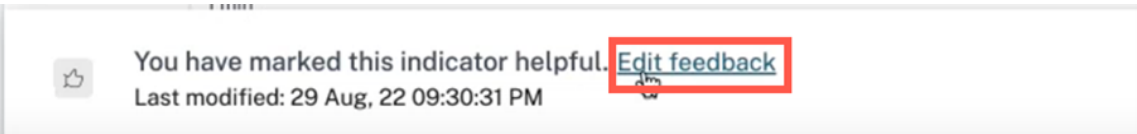
En outre, vos commentaires collectifs sont utilisés pour améliorer à l'avenir les algorithmes des indicateurs de risque.



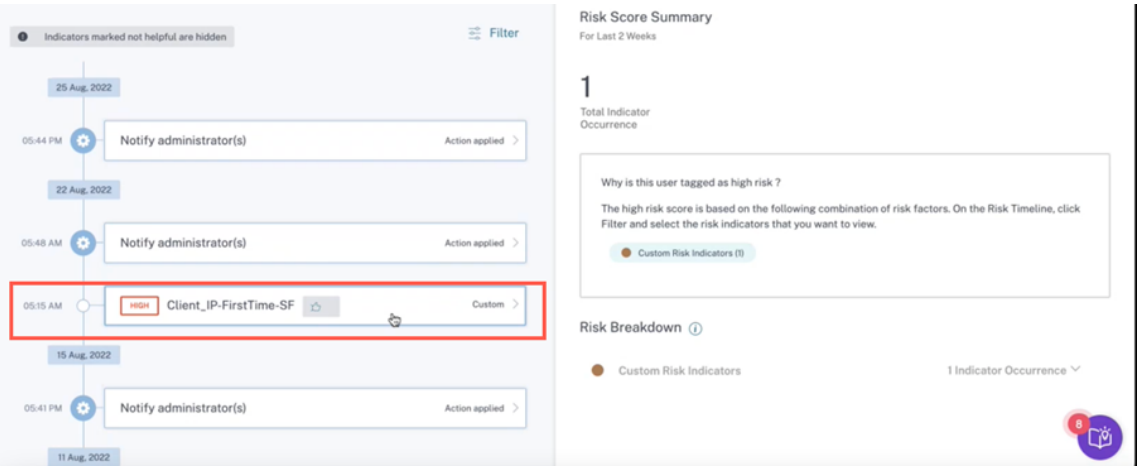
Une bannière de commentaires (avec une icône pointant vers le haut et vers le bas) s'affiche pour chaque entrée d'indicateur de risque par défaut dans le fil de l'utilisateur.

- Icône**en forme de pouce levé** - L'indicateur est utile et permet d'identifier correctement les activités à risque. Vous pouvez cliquer sur l'icône du pouce vers le haut et fournir des commentaires supplémentaires sur l'utilité de l'indicateur et ses avantages.

Vous pouvez enregistrer vos commentaires et marquer l'indicateur comme utile. Vous pouvez également modifier votre commentaire en cliquant sur Modifier le commentaire. La bannière de commentaires fournit la chronologie des derniers commentaires soumis.



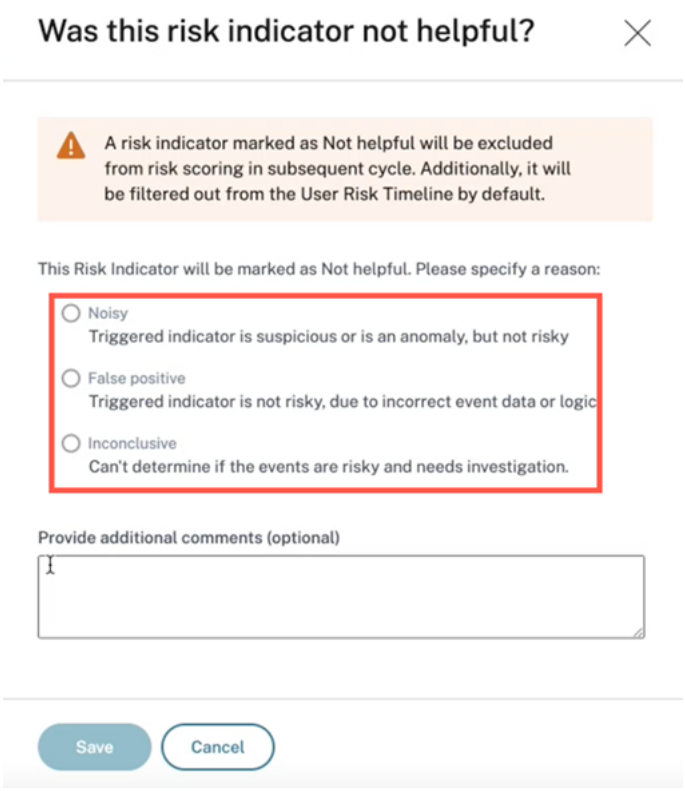
Lorsqu'un indicateur de risque est marqué comme utile, ce commentaire est affiché dans l'entrée de chronologie utilisateur correspondante et transmis à Citrix Analytics. Le score de risque de l'utilisateur n'est pas affecté.



- Icône**pointant vers le bas** - L'indicateur n'est pas utile ou se déclenche de manière incorrecte. Vous pouvez marquer l'indicateur comme étant inutile et le classer comme **bruyant**, **faux positif**ou **non concluant**. Cette occurrence de l'indicateur de risque sera exclue de toutes les mises à jour ultérieures du score de risque de l'utilisateur. Vous pouvez également fournir des commentaires supplémentaires, si nécessaire.

  - **Bruyant** —L'indicateur déclenché est suspect ou constitue une anomalie, mais il ne présente aucun risque.
  - **Faux positif** —L'indicateur déclenché n'est pas risqué, en raison de données d'événement ou d'une logique incorrectes.
  - **Non concluant** —Impossible de déterminer si les événements sont risqués et nécessitent une enquête.

    > **Remarque**
    >
    > Le recalibrage du score de risque peut prendre jusqu'à 15 minutes.

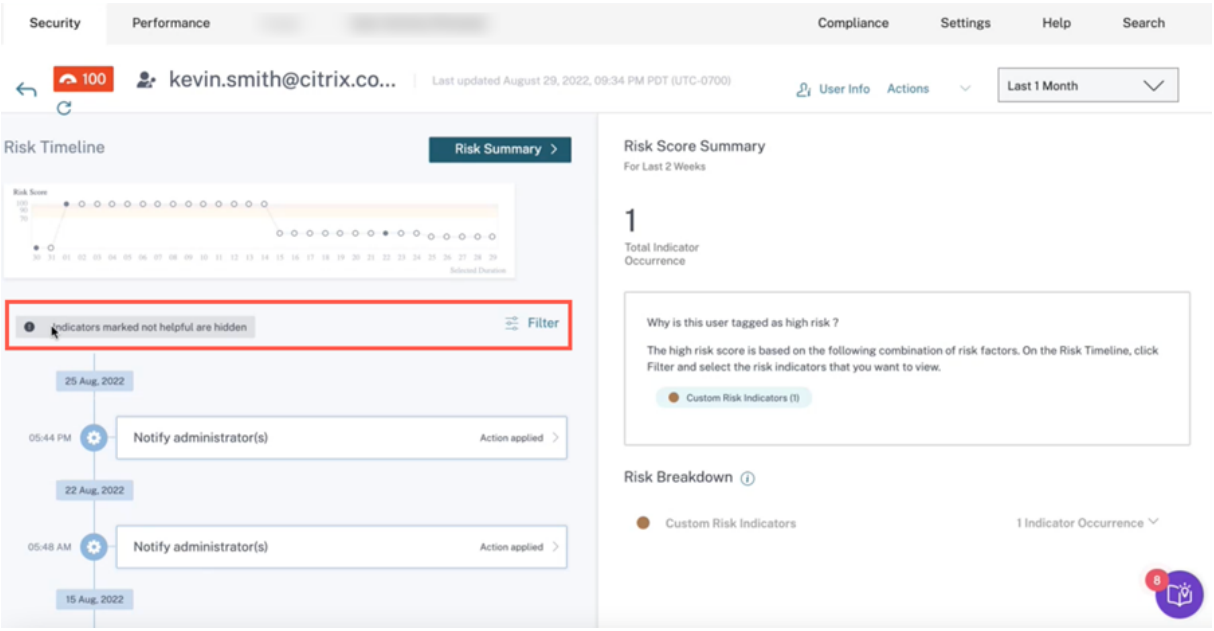


Vous pouvez consulter les résultats suivants si un indicateur est marqué comme inutile :

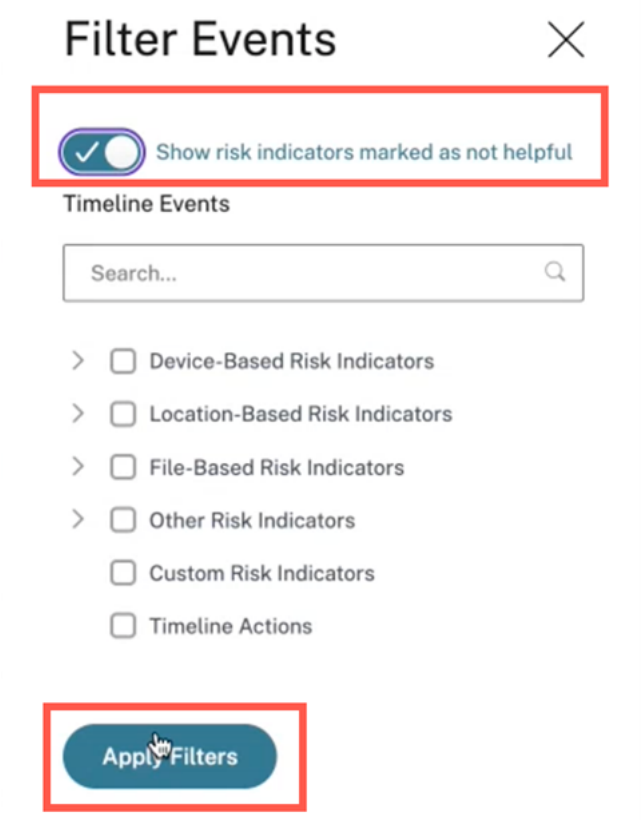
- Cet indicateur particulier est masqué dans la chronologie.
- Le score de risque est recalibré suite à l'exclusion de l'occurrence de cet indicateur du calcul du score de risque dans les mises à jour ultérieures.
- Toute information supplémentaire fournie sous forme de commentaire textuel est conservée pour référence ultérieure.

Afficher les filtres

Les indicateurs marqués comme inutiles sont masqués par défaut.

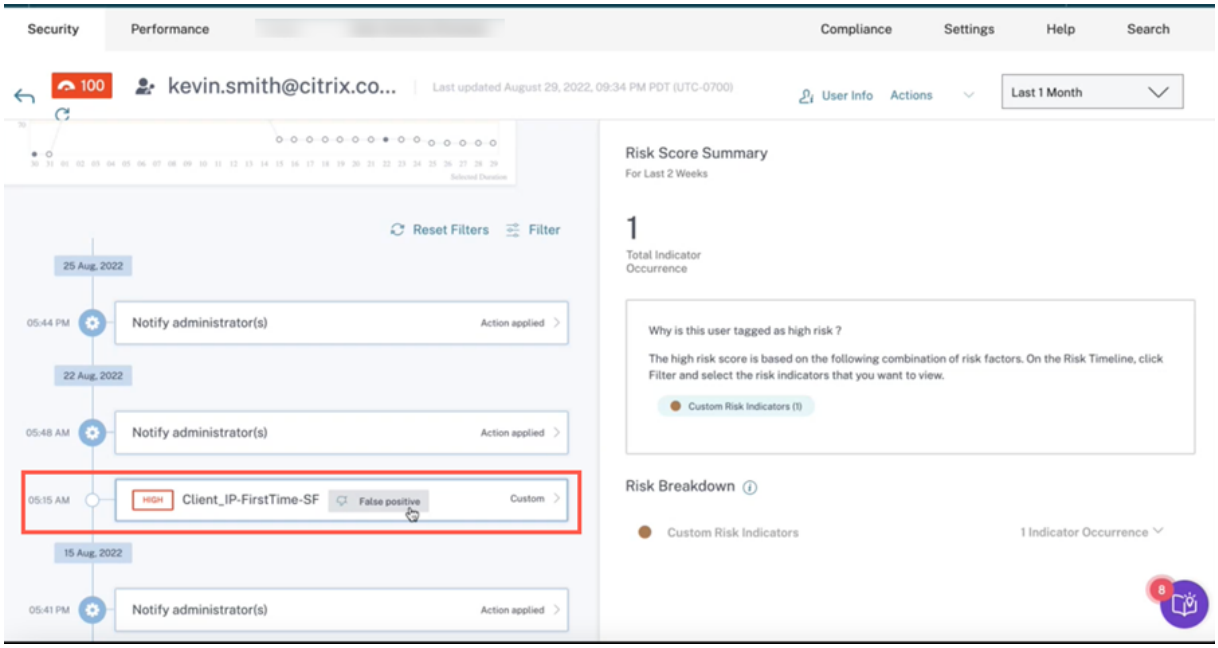


Pour afficher les indicateurs masqués, cliquez sur **Filtrer**. Dans la fenêtre **Filtrer les événements** qui apparaît, activez l'option **Afficher les indicateurs de risque marqués comme inutiles**.



Vous pouvez rechercher les indicateurs en fonction des catégories. Par exemple, pour afficher les indi-

cateurs de risque cachés basés sur la localisation, sélectionnez la catégorie et cliquez sur **Appliquer les filtres**. Vous pouvez consulter tous les indicateurs géolocalisés qui ne sont pas utiles pour les détails des commentaires.



En tant qu'administrateur, vous pouvez également effectuer les actions suivantes selon vos besoins :

- Modifier les commentaires
- Passez en revue les commentaires précédents et les métadonnées associées
- Passez en revue les commentaires fournis par un autre administrateur et les métadonnées associées

> **Remarque**
>
> - Vous pouvez fournir les commentaires par niveau d'utilisateur et non par niveau de locataire. Les commentaires relatifs à un indicateur de risque ne s'appliquent pas à toutes les instances de cet indicateur de risque en particulier.
> - Les commentaires d'un utilisateur ne s'appliquent pas aux autres utilisateurs.

Indicateurs de risque Microsoft Graph Security

September 24, 2021

Microsoft Graph Security reçoit des données des fournisseurs de sécurité **Azure AD Identity Protection** ou **Microsoft Defender for Endpoint**, et envoie les informations à Citrix Analytics.

Azure AD Identity Protection déclenche les indicateurs de risque suivants et envoie les informations à Microsoft Graph Security :

- Adresse IP anonyme
- Voyage impossible dans des lieux atypiques
- Utilisateurs avec des informations d'identification divulguées
- Connexion à partir d'appareils infectés
- Connexion à partir d'adresses IP présentant une activité suspecte
- Connexion depuis des emplacements inconnus

Pour plus d'informations sur Defender for Endpoint, consultez Microsoft Defender for Endpoint.

Le facteur de risque associé aux indicateurs de risque est les indicateurs de risque basés sur la propriété intellectuelle. Pour plus d'informations sur les facteurs de risque, consultez la section Indicateurs de risque utilisateur Citrix.

Comment analyser les indicateurs de risque de sécurité Microsoft Graph

Prenons l'exemple d'une utilisatrice Maria Brown qui présente l'un des comportements à risque mentionnés précédemment. Microsoft détecte l'incident et génère une alerte. Citrix Analytics récupère cette alerte et attribue un score de risque mis à jour à Maria Brown. De plus, l'indicateur de risque approprié est ajouté à la chronologie des risques de Maria Brown.

Pour afficher l'entrée de l'indicateur de risque de sécurité Microsoft Graph pour un utilisateur, accédez à **Sécurité** > **Utilisateurs**, puis sélectionnez l'utilisateur.

Dans la chronologie de Maria, vous pouvez sélectionner la dernière entrée d'indicateur de risque dans la chronologie des risques. Le panneau d'informations détaillées correspondant apparaît dans le volet droit. La section **CE QUI S'EST PASSÉ** fournit un bref résumé de l'indicateur de risque.

Comment obtenir plus d'informations sur les indicateurs de risque

Pour plus d'informations, consultez la section Événements de risque Azure Active Directory.

Quelles actions pouvez-vous appliquer à l'utilisateur

Actuellement, la possibilité d'effectuer les actions appropriées sur le compte de l'utilisateur via la source de données Microsoft Graph Security n'est pas disponible.

Pour plus d'informations sur l'intégration de Microsoft Graph Security, consultez la section Microsoft Graph Security.

Indicateurs de risque personnalisés

December 7, 2023

Il existe deux types d'indicateurs de risque que vous pouvez voir dans Citrix Analytics for Security :

- **Indicateurs de risque par défaut** : Ces indicateurs de risque sont basés sur l'algorithme d'apprentissage automatique. Pour plus d'informations, consultez la section Indicateurs de risque utilisateur Citrix.
- **Indicateurs de risque personnalisés** : Ces indicateurs de risque sont créés manuellement par les administrateurs.

Lorsque vous créez un indicateur de risque personnalisé, vous pouvez définir les conditions de déclenchement et les paramètres en fonction de vos cas d'utilisation. Si les événements utilisateur correspondent à vos critères définis, Citrix Analytics déclenche l'indicateur de risque personnalisé et l'affiche sur la chronologie des risques de l'utilisateur.

Créez des indicateurs de risque personnalisés pour les sources de données suivantes :

- Citrix Gateway
- Citrix Secure Private Access
- Citrix Virtual Apps and Desktops sur site
- Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service)
- Citrix Secure Browser

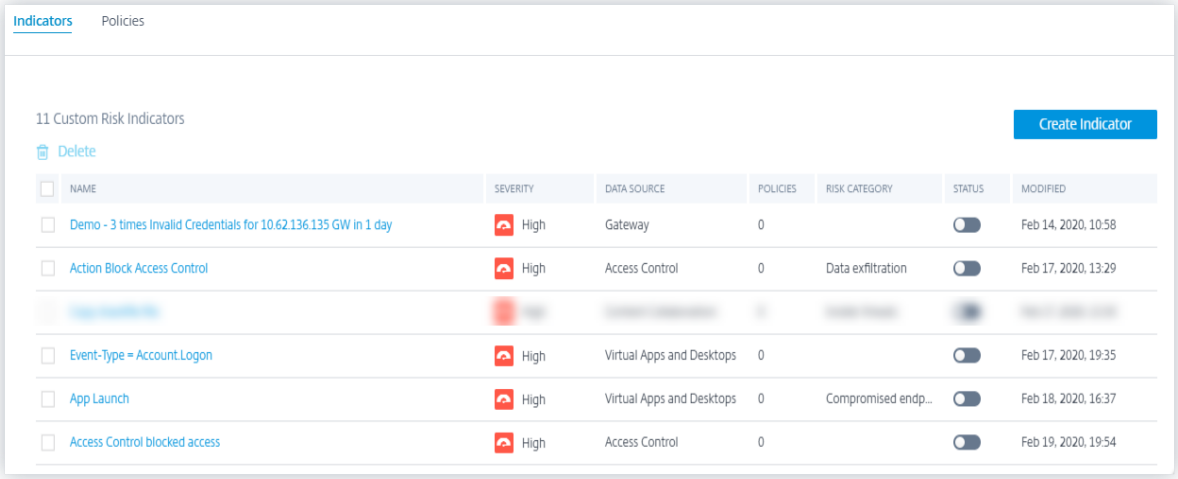
Indicateurs de risque personnalisés préconfigurés

Citrix fournit également quelques indicateurs de risque personnalisés avec des conditions préconfigurées pour vous aider à surveiller la sécurité de votre infrastructure Citrix. Vous pouvez modifier les conditions préconfigurées en fonction de vos cas d'utilisation. Pour plus d'informations, consultez la section Indicateurs de risque personnalisés préconfigurés.

Page des indicateurs de risque personnalisés

La page **Indicateurs de risque personnalisés** fournit des informations sur tous les indicateurs de risque personnalisés générés pour un utilisateur, la gravité, la source de données, le nombre de stratégies, la catégorie de risque, le statut et la date et l'heure de dernière modification de l'indicateur.

Pour créer un indicateur de risque personnalisé, reportez-vous à la section Création d'un indicateur de risque personnalisé.



Lorsque vous sélectionnez l'indicateur de risque, vous êtes redirigé vers la page **Modifier l'indicateur de risque** . Pour plus d'informations, consultez la section Modification d'un indicateur de risque personnalisé.

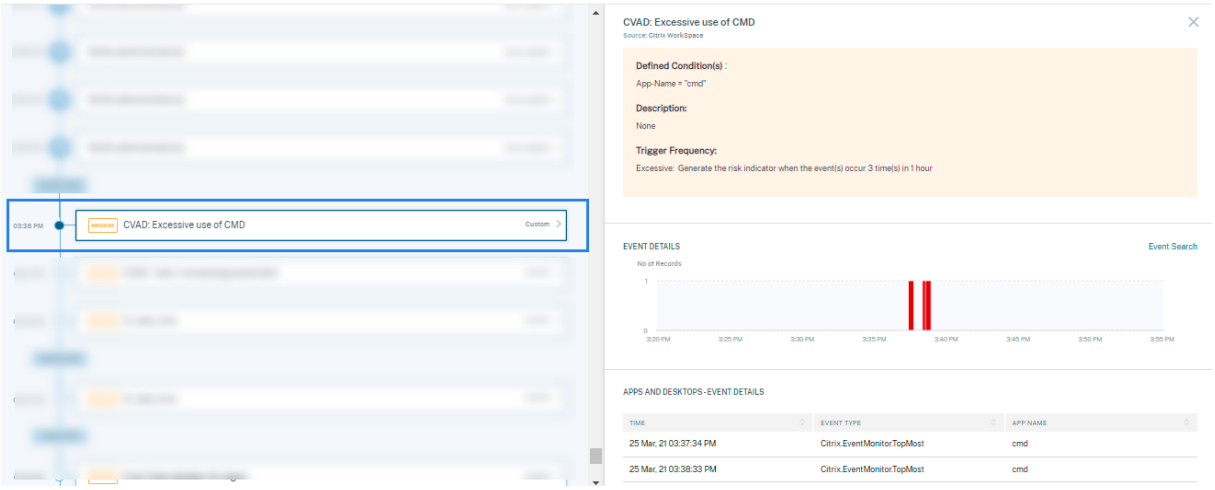
Analyse d'un indicateur de risque personnalisé

Prenons l'exemple d'un utilisateur dont l'action a déclenché un indicateur de risque personnalisé que vous avez défini. Citrix Analytics affiche l'indicateur de risque personnalisé sur la chronologie des risques de l'utilisateur.

Lorsque vous sélectionnez l'indicateur de risque personnalisé sur la chronologie des risques de l'utilisateur, le volet droit affiche les informations suivantes :

- **Condition (s) définie (s)** : affiche un résumé des conditions que vous avez définies lors de la création d'un indicateur de risque personnalisé.
- **Description** : fournit un résumé de la description que vous fournissez lors de la création de l'indicateur de risque personnalisé. Si aucune description n'est fournie lors de la création de l'indicateur de risque personnalisé, cette section indique **Aucun**.
- **Fréquence de déclenchement** : affiche l'option que vous sélectionnez dans la section **Options avancées**lors de la création de l'indicateur de risque personnalisé.
- **Détails de l'événement** : affiche la chronologie et les détails des événements utilisateur qui ont déclenché l'indicateur de risque personnalisé. Vous pouvez cliquer sur **Recherche d'événements** pour afficher les événements utilisateur sur la page de recherche en libre-service. La page de recherche en libre-service affiche les événements associés à l'utilisateur et l'indicateur

de risque personnalisé. La requête de recherche affiche les conditions définies pour l'indicateur de risque personnalisé.



> **Remarque**
>
> Les indicateurs de risque personnalisés sont représentés par une étiquette sur la chronologie des risques utilisateur.

Actions que vous pouvez appliquer à l'utilisateur

Lorsqu'un indicateur de risque personnalisé est déclenché pour un utilisateur, vous pouvez appliquer une action manuellement ou créer une stratégie pour appliquer une action automatiquement. Pour plus d'informations, consultez la section Stratégies et actions.

Modèles d'indicateurs de risque personnalisés

Vous pouvez créer un indicateur de risque personnalisé à l'aide de l'un des modèles prédéfinis ou continuer sans utiliser de modèle.

Les modèles servent de point de départ à la création d'un indicateur de risque personnalisé. Il vous aide à créer un indicateur de risque personnalisé en fournissant des requêtes et des paramètres prédéfinis que vous pouvez sélectionner en fonction de vos cas d'utilisation.

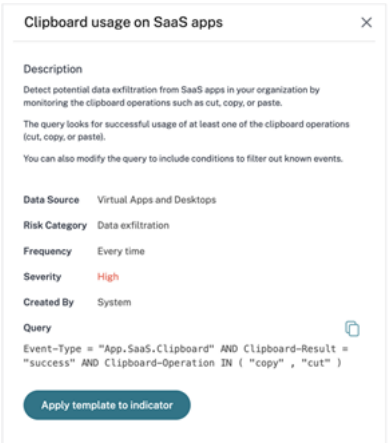
Vous pouvez utiliser un modèle tel quel ou le modifier pour répondre à vos besoins. À l'aide des modèles, les administrateurs peuvent créer des indicateurs de risque intéressants sans formation supplémentaire.

Un modèle comprend les informations suivantes :

- **Description** : Indique l'objectif de la requête définie dans le modèle.
- **Source de données** : indique la source de données à laquelle le modèle s'applique.

- **Catégorie de risque** : indique la catégorie de risque associée aux événements recherchés par la requête. Il existe quatre catégories d'événements à risque : l'exfiltration de données, les menaces internes, les utilisateurs compromis et les points finaux de compromission. Pour plus d'informations, voir Catégories de risques.
- **Fréquence** : indique la fréquence à laquelle la requête se déclenche.
- **Gravité** : indique la gravité du risque associé à l'événement. Le risque peut être élevé, moyen ou faible.
- **Créé par** : indique le créateur du modèle. Les modèles sont toujours définis par le système.
- **Requête** : indique les conditions définies dans le modèle. La requête récupère les événements utilisateur qui répondent aux conditions.

L'image suivante montre le modèle pour l'utilisation du cas d'utilisation du presse-papiers sur les applications SaaS.

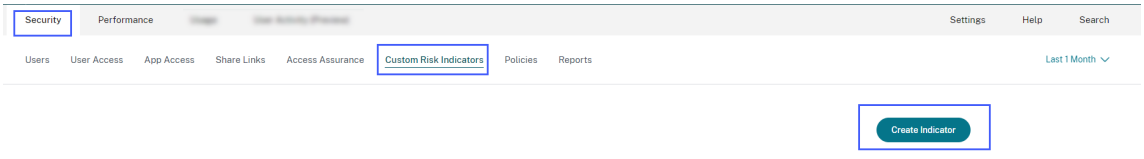


Si vous ne trouvez pas de modèle pour votre cas d'utilisation ou si vous souhaitez définir votre propre requête, vous pouvez continuer sans modèle.

Création d'un indicateur de risque personnalisé

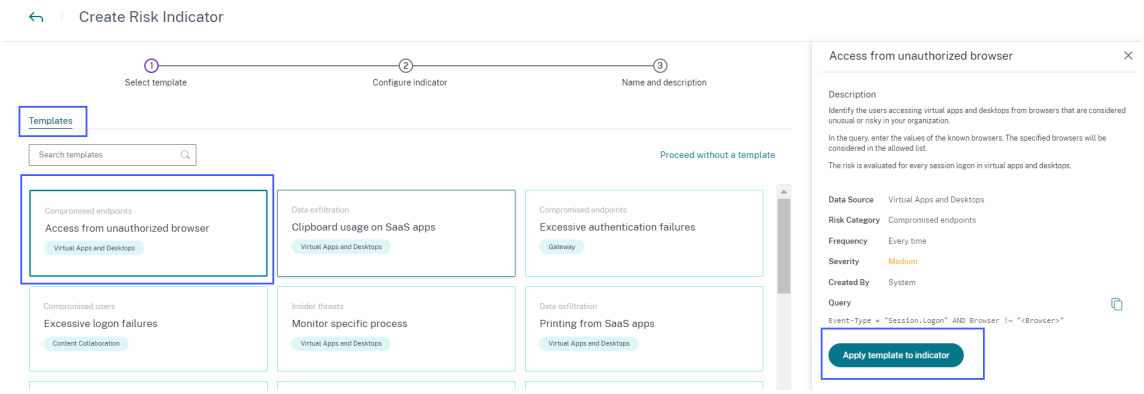
Pour créer un indicateur de risque personnalisé :

1. Accédez à **Sécurité > Indicateurs de risque personnalisés > Créer un indicateur**.

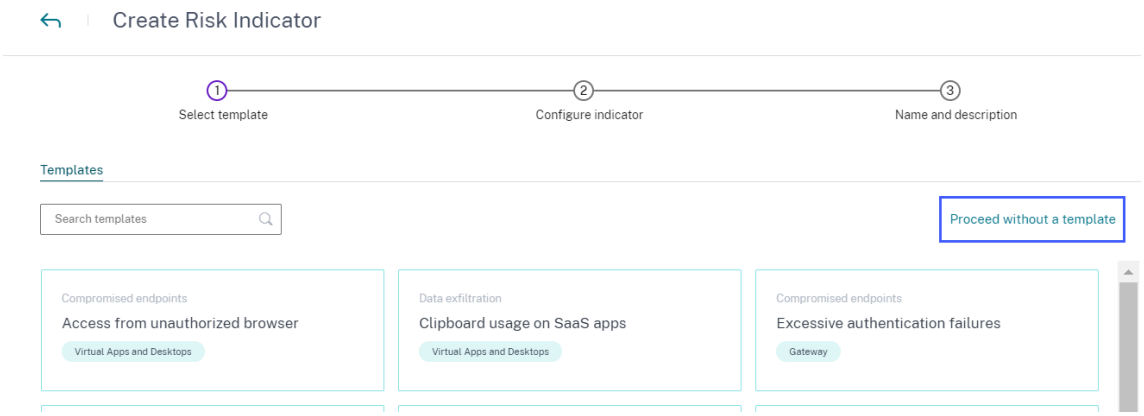


2. Sélectionnez un modèle pour afficher le cas d'utilisation. S'il répond à vos besoins, sélectionnez **Appliquer le modèle à l'indicateur**.

> **Remarque**
>
> Vous pouvez également modifier les conditions prédéfinies et les paramètres d'un modèle.



3. Si vous ne trouvez pas le modèle souhaité ou si vous souhaitez créer votre propre condition, sélectionnez **Poursuivre sans modèle**.



4. Suivez les instructions à l'écran pour créer un indicateur.

> **Remarques**
>
> - Vous pouvez créer des indicateurs de risque personnalisés jusqu'à une limite maximale de 50. Si vous atteignez cette limite maximale, vous devez supprimer ou modifier tout indicateur de risque personnalisé existant pour créer un indicateur de risque personnalisé.
> - Lorsqu'un indicateur de risque personnalisé est déclenché, il s'affiche immédiatement sur la chronologie de l'utilisateur . Toutefois, le résumé des risques et le score de risque de l'utilisateur sont mis à jour après quelques minutes (environ 15 à 20 minutes).

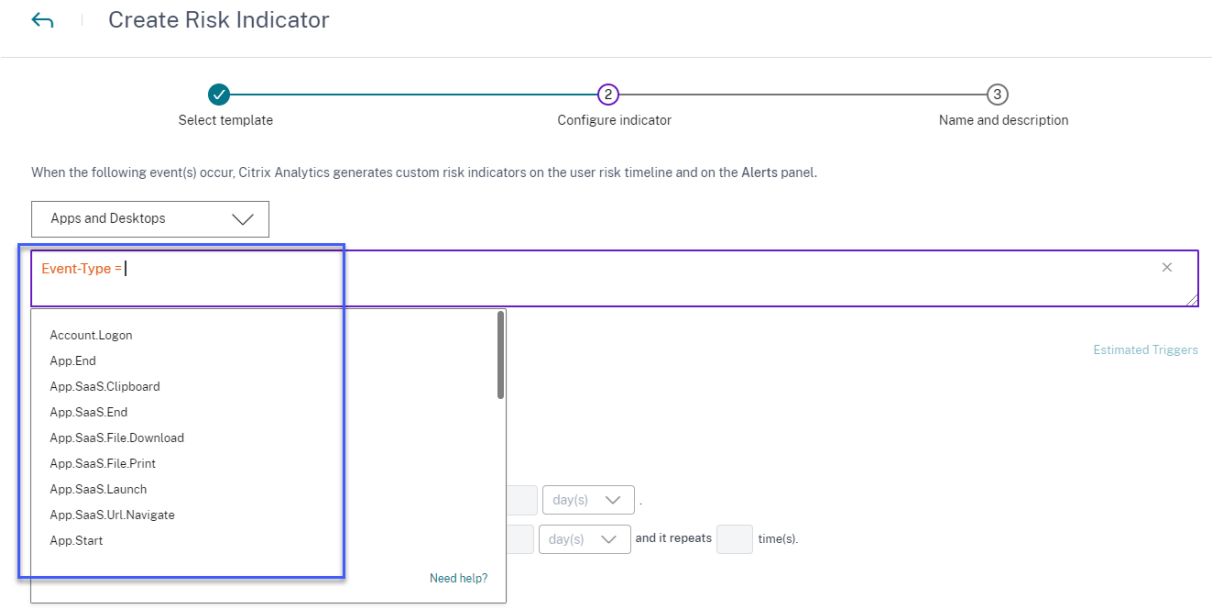
Définition d'une condition pour un indicateur de risque personnalisé

Utilisez la zone de requête pour définir les conditions de l'indicateur de risque personnalisé. Selon la source de données sélectionnée, vous obtenez les dimensions correspondantes et les opérateurs

valides pour définir vos conditions.

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.

L'image suivante montre les valeurs suggérées pour la dimension `Event-Type`.



Si vous utilisez un modèle, la condition est prédéfinie. Toutefois, vous pouvez ajouter ou modifier la condition prédéfinie en fonction de votre cas d'utilisation.

En dessous de la zone de requête, vous pouvez voir le lien **Déclencheurs estimés** . Cliquez sur le lien pour prédire les instances approximatives de l'indicateur de risque personnalisé qui serait déclenché pour les conditions définies. Ces instances sont calculées sur la base des données historiques que Citrix Analytics conserve et répondent aux conditions définies.

Assurez-vous de cliquer sur **Déclencheurs estimés** pour prédire le nombre d'occurrences d'indicateurs de risque personnalisés pour la dernière condition définie.

Utilisation des options avancées

Dans la section **Options avancées**, sélectionnez la fréquence de l'événement pour déclencher l'indicateur de risque personnalisé. Lorsque vous ne sélectionnez aucune option, Citrix Analytics considère **Chaque fois : Générer l'indicateur de risque chaque fois que le ou les événements se produisent** en tant qu'option par défaut et génère l'indicateur de risque personnalisé. Vous pouvez choisir parmi les options suivantes :

- **À chaque fois** : l'indicateur de risque est déclenché chaque fois que les événements répondent aux conditions définies.
- **Première fois** : l'indicateur de risque est déclenché lorsque les événements remplissent les conditions définies pour la première fois.
  - **Première fois pour une nouvelle**entité : activez cette option pour détecter les événements reçus d'une nouvelle entité pour la première fois. Voici quelques exemples d'entités : Client IP, Country, City et Device-ID. Vous ne pouvez sélectionner qu'une seule entité en fonction de la source de données. Cette option vous permet de créer un indicateur de risque sans spécifier de valeur explicite pour les entités. Par exemple, lorsque vous sélectionnez l'entité comme « Ville », il n'est pas nécessaire de spécifier le nom de la ville. L'indicateur de risque est déclenché lorsque des événements sont reçus d'une nouvelle ville pour la première fois.

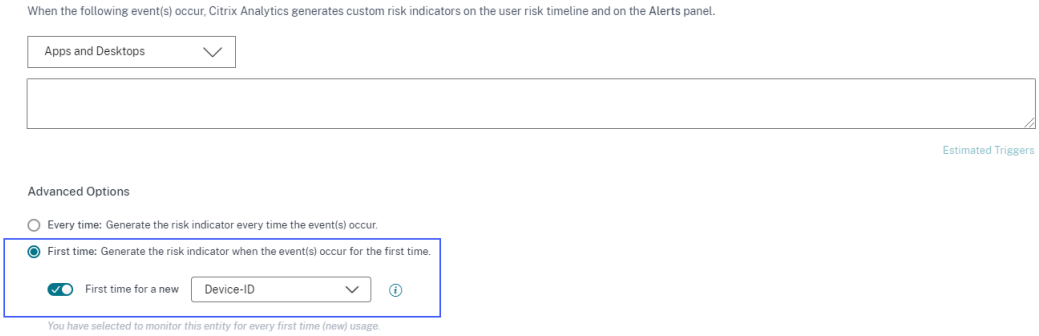
    Le tableau suivant répertorie les entités correspondant à chaque source de données et décrit les conditions du déclencheur.

Source de données	Entité	condition de déclenchement
Secure Private Access	City	Lorsqu'un utilisateur ouvre une session depuis une nouvelle ville pour la première fois.
	Client-IP	Lorsqu'un utilisateur ouvre une session à partir d'une nouvelle adresse IP pour la première fois.
	Pays	Lorsqu'un utilisateur ouvre une session depuis un nouveau pays pour la première fois.
Applications et bureaux	Nom de l'application	Lorsqu'un utilisateur ouvre une nouvelle application virtuelle ou une application SaaS pour la première fois.
	URL de l'application	Lorsqu'un utilisateur saisit une nouvelle URL d'application dans un navigateur de son bureau virtuel pour la première fois.

Source de données	Entité	condition de déclenchement
	City	Lorsqu'un utilisateur lance des applications ou des bureaux depuis une nouvelle ville pour la première fois.
	Client-IP	Lorsqu'un utilisateur ouvre une session à partir d'une nouvelle adresse IP pour la première fois.
	Pays	Lorsqu'un utilisateur lance des applications ou des bureaux depuis un nouveau pays pour la première fois.
	ID de l'appareil	Lorsqu'un utilisateur lance pour la première fois des applications ou des bureaux virtuels à partir d'un nouvel appareil tel qu'un mobile, un ordinateur portable ou un ordinateur de bureau.
	Type de périphérique de téléchargement	Lorsqu'un utilisateur utilise un nouveau support de stockage tel qu'une clé USB pour la première fois.
	Format de fichier d'impression	Format du fichier imprimé.
	Taille du fichier d'impression	Taille du fichier imprimé en octets.
	Nom du fichier d'impression	Nom du fichier imprimé.
	Printer-Name	Nom de l'imprimante utilisée.
	Nombre total de copies imprimées	Nombre total de copies imprimées par l'utilisateur.
	Nombre total de pages imprimées	Nombre total de pages du document imprimées par l'utilisateur.
Gateway	Client-IP	Lorsqu'un utilisateur ouvre une session à partir d'une nouvelle adresse IP pour la première fois.

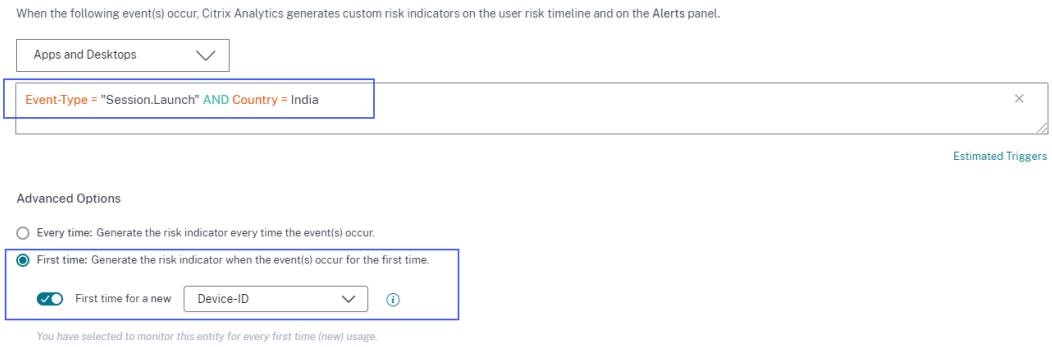
Source de données	Entité	condition de déclenchement
Secure Browser	Nom d'utilisateur	Le nom de l'utilisateur qui a initié l'événement.
	Accès autorisé	Indique si l'utilisateur est autorisé ou non à accéder au service hôte.
	Client-IP	L'adresse IP de la machine utilisateur.
	Nom d'hôte consulté	Service hôte auquel l'utilisateur accède via le réseau.
	ID de session	Le numéro unique attribué à la session utilisateur.

L'exemple suivant montre un indicateur de risque personnalisé créé pour la source de données Apps and Desktops. L'indicateur de risque est déclenché lorsqu'un utilisateur lance pour la première fois un bureau virtuel ou une application virtuelle à partir d'un nouvel appareil.



Vous pouvez également ajouter une condition en même temps que la **première fois pour une nouvelle** option. Dans ce cas, l'indicateur de risque est déclenché lorsqu'il détecte les événements de la nouvelle entité pour la première fois et lorsque les événements répondent à la condition définie.

L'exemple suivant montre une condition définie pour l'indicateur de risque personnalisé et l'option **Première fois pour un nouvel ID de périphérique** activée. L'indicateur de risque est déclenché lorsqu'un utilisateur situé en Inde lance pour la première fois une session de bureau virtuel à partir d'un nouvel appareil.



- **Excessif** : L'indicateur de risque est déclenché lorsque les conditions suivantes sont remplies :
  - Les événements répondent aux conditions définies.
  - Les événements se produisent un certain nombre de fois au cours de la période spécifiée.
- **Fréquents** : L'indicateur de risque est déclenché lorsque les conditions suivantes sont remplies :
  - Les événements répondent aux conditions définies.
  - Les événements se produisent le nombre de fois spécifié au cours de la période spécifiée.
  - Le modèle d'événement se répète le nombre de fois spécifié.

Sélection de la catégorie de risque

Sélectionnez la catégorie de risque pour votre indicateur de risque personnalisé.

Les indicateurs de risque sont regroupés en fonction du type d'exposition au risque de l'indicateur de risque personnalisé. Pour obtenir de l'aide sur la sélection des catégories de risques, voir Catégories de risques.

Sélection de la gravité

La gravité indique le niveau de gravité d'un événement à risque, détecté par l'indicateur de risque. Lorsque vous créez un indicateur de risque personnalisé, sélectionnez un niveau de gravité élevé, moyen ou faible.

Si vous appliquez un modèle, l'option de gravité est présélectionnée. Vous pouvez modifier cette présélection en fonction de votre cas d'utilisation.

Opérateurs pris en charge pour définir une condition

Vous pouvez utiliser les opérateurs suivants lorsque vous définissez une condition.

Opérateur	Description	Exemple	Sortie
	Attribuez une valeur à la requête de recherche.	User-Name : John	Affiche les événements de l'utilisateur John.
=	Attribuez une valeur à la requête de recherche.	User-Name = John	Affiche les événements de l'utilisateur John.
~	Recherchez 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	Valeurs de recherche pour lesquelles les deux conditions 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.
*	Valeurs de recherche qui correspondent au caractère zéro fois ou plus.	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.
		User-Name = *Smith	Affiche les événements pour tous les noms d'utilisateurs qui se terminent par Smith.

Opérateur	Description	Exemple	Sortie
!~	Vérifie dans les événements utilisateur 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 la chaîne exacte que vous spécifiez dans les événements utilisateur. 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.
IN	Attribuez plusieurs valeurs à une dimension pour obtenir les événements liés à une ou plusieurs valeurs.	User-Name IN (John, Kevin)	Retrouvez tous les événements liés à John ou Kevin.
NOT IN	Attribuez plusieurs valeurs à une dimension et recherchez les événements qui ne contiennent pas les valeurs spécifiées.	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
OU	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 condition, 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.

Modification d'un indicateur de risque personnalisé

1. Accédez à **Sécurité > Indicateurs de risque personnalisés**.
2. Sélectionnez l'indicateur de risque personnalisé que vous souhaitez modifier.
3. Sur la page **Modifier l'indicateur**, modifiez les informations si nécessaire.
4. Cliquez sur **Enregistrer**.

> **Remarque**
>
> Si vous modifiez les attributs tels que la condition, la catégorie de risque, la gravité et le nom d'un indicateur de risque personnalisé existant, sur la chronologie de l'utilisateur, vous pouvez toujours afficher les occurrences précédentes de l'indicateur de risque personnalisé (avec les anciens attributs) qui ont été déclenchées pour l'utilisateur.
>
> Par exemple, vous avez créé un indicateur de risque personnalisé avec la condition *Country ! = Inde*. Ainsi, cet indicateur de risque personnalisé est déclenché lorsqu'un utilisateur ouvre une session depuis l'extérieur de l'Inde. Maintenant, vous modifiez l'état de l'indicateur de risque personnalisé en *Pays ! = « États-Unis »*. Dans ce cas, vous pouvez toujours afficher les occurrences précédentes de l'indicateur de risque personnalisé avec la condition *Country ! = Inde* sur les chronologies des utilisateurs qui ont déclenché l'indicateur de risque.

Supprimer un indicateur de risque personnalisé

1. Accédez à **Sécurité > Indicateurs de risque personnalisés**.

2. Sélectionnez l'indicateur de risque personnalisé que vous souhaitez supprimer.
3. Cliquez sur **Delete**.
4. Dans la boîte de dialogue, confirmez votre demande de suppression de l'indicateur de risque personnalisé.

> **Remarque**
>
> Si vous supprimez un indicateur de risque personnalisé, sur la chronologie de l'utilisateur, vous pouvez toujours afficher les occurrences précédentes de l'indicateur de risque personnalisé qui ont été déclenchées pour l'utilisateur.
>
> Par exemple, vous supprimez un indicateur de risque personnalisé existant avec la condition *Country ! = Inde*. Dans ce cas, vous pouvez toujours afficher les occurrences précédentes de l'indicateur de risque personnalisé avec la condition *Country ! = Inde* sur les chronologies des utilisateurs qui ont déclenché l'indicateur de risque.

Évaluation continue des risques

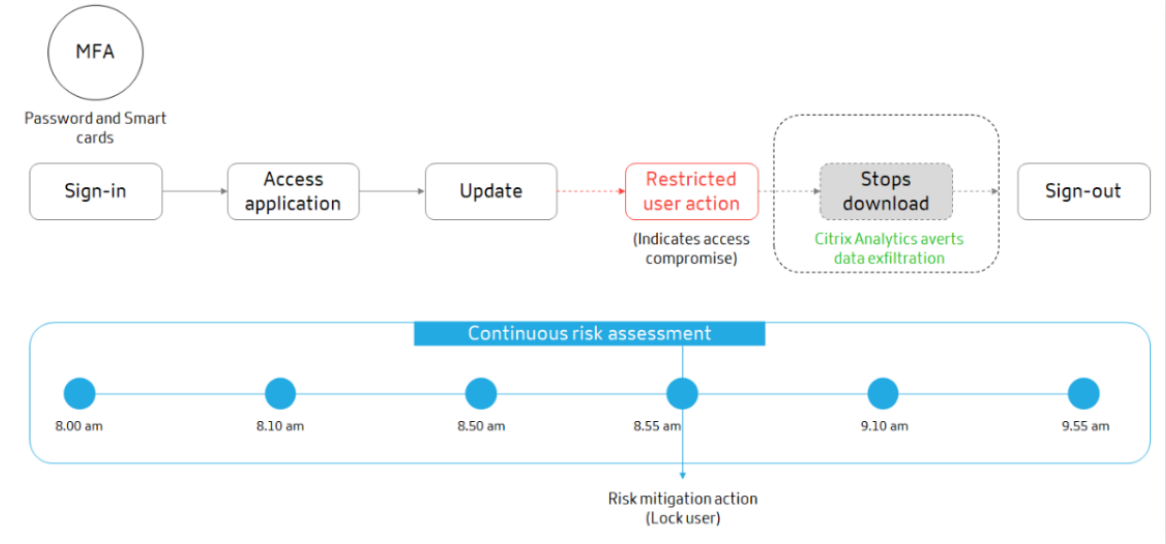
December 7, 2023

L'utilisation accrue des appareils informatiques portables et d'Internet permet aux utilisateurs de Citrix Workspace de travailler depuis presque n'importe quel endroit et sur n'importe quel appareil. Le défi de cette flexibilité réside dans le fait que l'accès à distance expose les données sensibles à des risques de sécurité par le biais d'activités cybercriminelles telles que l'exfiltration de données, le vol, le vandalisme et les interruptions de service. Les employés au sein des organisations sont également susceptibles de contribuer à ces dommages.

Certains moyens conventionnels de remédier à ces risques sont d'implémenter une authentification multifacteur, des sessions de connexion courtes, etc. Bien que ces méthodes d'évaluation des risques garantissent un niveau de sécurité plus élevé, elles ne fournissent pas une sécurité complète après la validation initiale des utilisateurs. Si un utilisateur malveillant parvient à accéder au réseau, il utilise à mauvais escient des données sensibles qui nuisent à une organisation.

Pour améliorer l'aspect sécurité et garantir une meilleure expérience utilisateur, Citrix Analytics introduit la solution d'évaluation continue des risques. Cette solution protège vos données à la fois contre les cybercriminels externes et les personnes internes malintentionnées en garantissant que l'exposition aux risques des utilisateurs qui utilisent Citrix Virtual Apps and Desktops ou Citrix DaaS (anciennement Citrix Virtual Apps and Desktops service) reste la même que lors de la vérification initiale, sans que l'utilisateur ait à le prouver à chaque fois. Cette solution est obtenue en évaluant en

permanence un événement à risque au cours d'une session et en appliquant automatiquement des mesures pour empêcher toute utilisation abusive des ressources de l'organisation.



Cas d'utilisation

Prenons l'exemple d'un utilisateur Adam Maxwell, qui a pu accéder à un réseau pour la première fois après plusieurs tentatives de connexion infructueuses à partir d'un emplacement inhabituel qui est contraire à son comportement habituel. De plus, l'emplacement a fait ses preuves en matière de cyberattaques. Dans ce scénario, vous devez prendre des mesures immédiates pour éviter que le compte d'Adam ne soit davantage utilisé à mauvais escient. Vous pouvez verrouiller le compte d'Adam et l'informer de l'action entreprise. Cette action peut entraîner temporairement des interruptions de service sur le compte de l'utilisateur. L'utilisateur peut contacter l'administrateur pour obtenir de l'aide pour restaurer le compte.

Imaginons un autre scénario dans lequel Adam accède pour la première fois à un réseau à partir d'un nouvel appareil et d'une nouvelle adresse IP. Vous pouvez contacter Adam pour lui demander de confirmer s'il identifie cette activité. Si c'est le cas, il se peut qu'Adam ait changé d'appareil de travail et qu'il travaille depuis son réseau domestique. Cette activité ne nuit pas à la sécurité de votre organisation et peut être ignorée. Toutefois, si l'utilisateur n'a pas effectué cette activité, il est probable que le compte ait été compromis. Dans ce scénario, vous pouvez verrouiller le compte de l'utilisateur pour éviter tout dommage supplémentaire.

Fonctionnalités principales

L'évaluation continue des risques automatise certaines des fonctionnalités associées aux stratégies et aux tableaux de bord de visibilité :

Prise en charge de plusieurs conditions

Lorsque vous créez ou modifiez une stratégie, vous pouvez ajouter jusqu'à quatre conditions. Les conditions peuvent contenir des combinaisons d'indicateurs de risque par défaut et d'indicateurs de risque personnalisés, de scores de risque utilisateur, ou les deux.

Pour plus d'informations, consultez la section Que sont les stratégies.

Informer les utilisateurs avant d'appliquer des actions

Avant d'appliquer une action appropriée sur le compte d'un utilisateur, vous pouvez informer l'utilisateur et évaluer la nature d'une activité inhabituelle détectée.

Pour plus d'informations, consultez Demander une réponse de l'utilisateur final.

Informer les utilisateurs après avoir appliqué des actions

Pour certaines activités, attendre la réponse de l'utilisateur avant d'appliquer une action peut mettre en danger le compte de l'utilisateur et la sécurité de votre organisation. Dans de tels scénarios, vous pouvez appliquer une action perturbatrice lorsque vous détectez une activité inhabituelle et que vous en informez l'utilisateur.

Pour plus d'informations, consultez la section Notifier l'utilisateur après avoir appliqué une action perturbatrice.

Modes d'application et de surveillance

Vous pouvez définir des stratégies sur des modes d'application ou de surveillance en fonction de vos besoins. Les stratégies en mode d'application ont un impact direct sur les comptes des utilisateurs. Toutefois, si vous souhaitez évaluer l'impact ou le résultat de vos stratégies avant de les implémenter, vous pouvez définir vos stratégies en mode de surveillance.

Pour plus d'informations, consultez la section Modes pris en charge.

Visibilité des tableaux de bord d'accès et de stratégie

À l'aide du tableau de bord **Access Summary**, vous pouvez obtenir des informations sur le nombre de tentatives d'accès effectuées par les utilisateurs. Pour plus d'informations, consultez la section Résumé des accès.

À l'aide du tableau de bord **Stratégies et actions**, vous pouvez obtenir des informations sur les stratégies et les actions appliquées aux comptes d'utilisateurs. Pour plus d'informations, consultez la section Stratégies et actions.

Stratégies par défaut

Citrix Analytics introduit des stratégies prédéfinies qui sont activées par défaut dans le tableau de bord **Stratégies** . Ces stratégies sont créées en utilisant des indicateurs de risque et des scores de risque utilisateur comme conditions prédéfinies. Une action globale est attribuée à chaque stratégie par défaut.

> **Remarque**
>
> Les stratégies répertoriées dans votre environnement peuvent varier selon la date à laquelle vous avez commencé à utiliser Citrix Analytics et selon que vous avez apporté des modifications locales.

Pour plus d'informations, consultez la section Que sont les stratégies.

Vous pouvez utiliser les stratégies par défaut suivantes ou les modifier en fonction de vos besoins :

Nom de la stratégie	Condition	Source de données	Action
Exploitation réussie des informations d'identification	Lorsque les indicateurs de risque d'échec d'authentification excessif et d'ouverture de session suspecte sont déclenchés	Citrix Gateway	Verrouiller l'utilisateur
Exfiltration potentielle des données	Lorsque l'indicateur de risque potentiel d'exfiltration de données est déclenché	Citrix Virtual Apps and Desktops et Citrix DaaS	Fermer la session utilisateur
Accès inhabituel à partir d'une adresse IP suspecte	Lorsque les indicateurs de risque d'ouverture de session et d'ouverture de session suspects sont déclenchés	Citrix Gateway	Verrouiller l'utilisateur
Premier accès à partir de l'appareil	Lorsque l'indicateur de risque CVAD - Premier accès à partir d'un nouvel appareil est déclenché	Citrix Virtual Apps and Desktops et Citrix DaaS	Demander une réponse de l'utilisateur final
Déplacement impossible lors de l'accès	Lorsque l'indicateur de risque Impossible Travel est déclenché.	Citrix Virtual Apps and Desktops et Citrix DaaS	Demander une réponse de l'utilisateur final

Nom de la stratégie	Condition	Source de données	Action
Déplacement impossible lors de l'authentification	Lorsque l'indicateur de risque Impossible Travel est déclenché.	Citrix Gateway	Demander une réponse de l'utilisateur final

Stratégies et actions

December 7, 2023

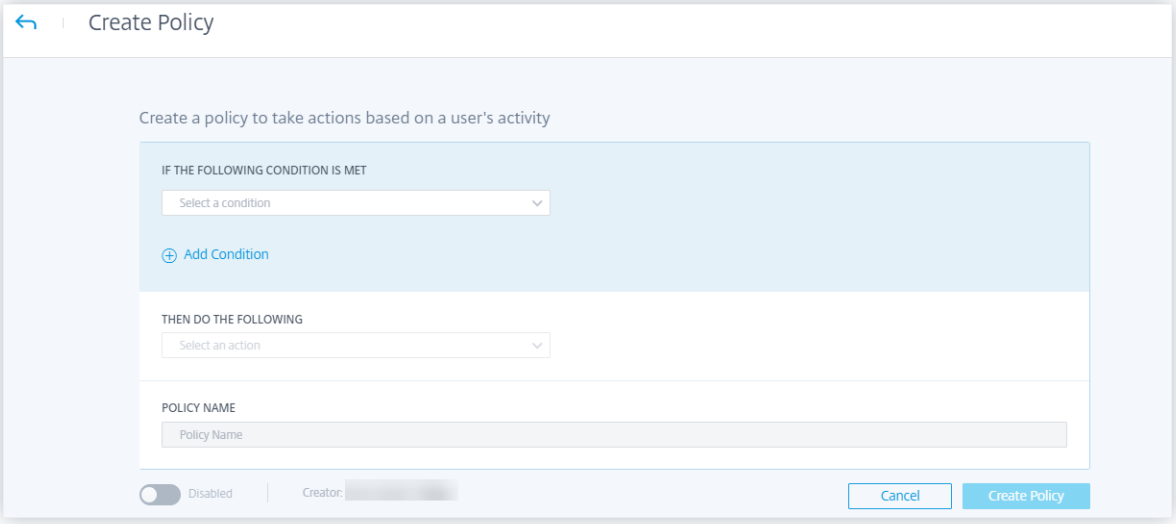
> **Remarque**
>
> **Attention** : Citrix Content Collaboration et ShareFile ont atteint leur fin de vie et ne sont plus disponibles pour les utilisateurs.

Vous pouvez créer des stratégies sur Citrix Analytics pour vous aider à effectuer des actions sur les comptes d'utilisateurs en cas d'activités inhabituelles ou suspectes. Les stratégies vous permettent d'automatiser le processus d'application d'actions telles que la désactivation d'un utilisateur et l'ajout d'utilisateurs à une liste de suivi. Lorsque vous activez les stratégies, une action correspondante est appliquée immédiatement après qu'un événement anormal se produit et que la condition de stratégie est remplie. Vous pouvez également appliquer manuellement des actions sur les comptes d'utilisateurs présentant des activités anormales.

Quelles sont les stratégies ?

Une stratégie est un ensemble de conditions qui doivent être remplies pour appliquer une action. Une stratégie contient une ou plusieurs conditions et une seule action. Vous pouvez créer une stratégie comportant plusieurs conditions et une action qui peut être appliquée au compte d'un utilisateur.

Le **score de risque** est une condition globale. Des conditions globales peuvent être appliquées à un utilisateur spécifique pour une source de données spécifique. Vous pouvez surveiller les comptes d'utilisateurs qui affichent des activités inhabituelles. D'autres conditions sont spécifiques aux sources de données et à leurs indicateurs de risque. Les conditions contiennent des combinaisons de scores de risque, d'indicateurs de risque par défaut et d'indicateurs de risque personnalisés. Vous pouvez ajouter jusqu'à 4 conditions lors de la création d'une stratégie.



Par exemple, si votre organisation utilise des données sensibles, vous pouvez limiter la quantité de données partagées ou accessibles par les utilisateurs en interne. Mais si vous avez une grande organisation, il ne serait pas possible pour un seul administrateur de gérer et de surveiller de nombreux utilisateurs. Vous pouvez créer une stratégie dans laquelle toute personne qui partage des données sensibles de manière excessive peut être ajoutée à une liste de suivi ou avoir son compte désactivé immédiatement.

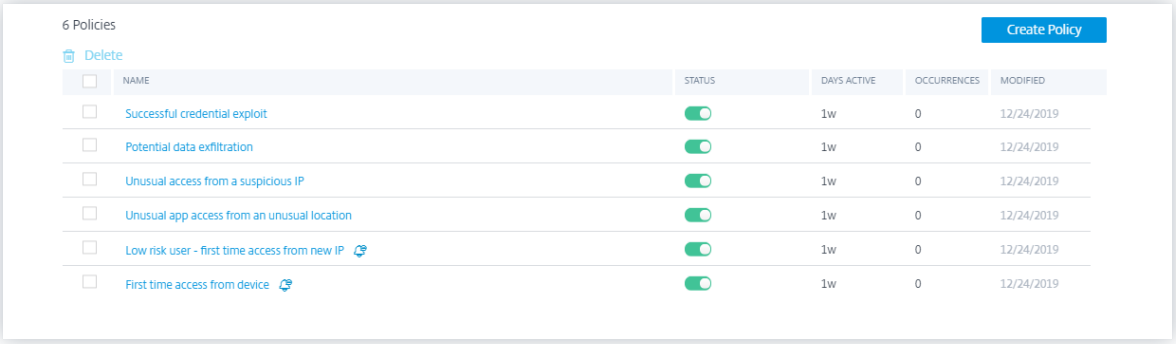
Stratégies par défaut

Les stratégies par défaut sont prédéfinies et activées sur le tableau de bord **Stratégies**. Ils sont créés en fonction de conditions prédéfinies et une action correspondante est affectée à chaque stratégie par défaut. Vous pouvez utiliser une stratégie par défaut ou la modifier en fonction de vos besoins.

Citrix Analytics prend en charge les stratégies par défaut suivantes :

- Exploitation réussie des identifiants
- Exfiltration potentielle des données
- Accès inhabituel à partir d'une adresse IP suspecte
- Premier accès à partir de l'appareil
- Virtual Apps and Desktops et Citrix DaaS : impossibilité de se déplacer en cas d'accès
- Gateway - Impossible de se déplacer lors de l'authentification

Pour plus d'informations sur les conditions prédéfinies et les actions concernant les stratégies par défaut précédentes, consultez la section Évaluation continue des risques.



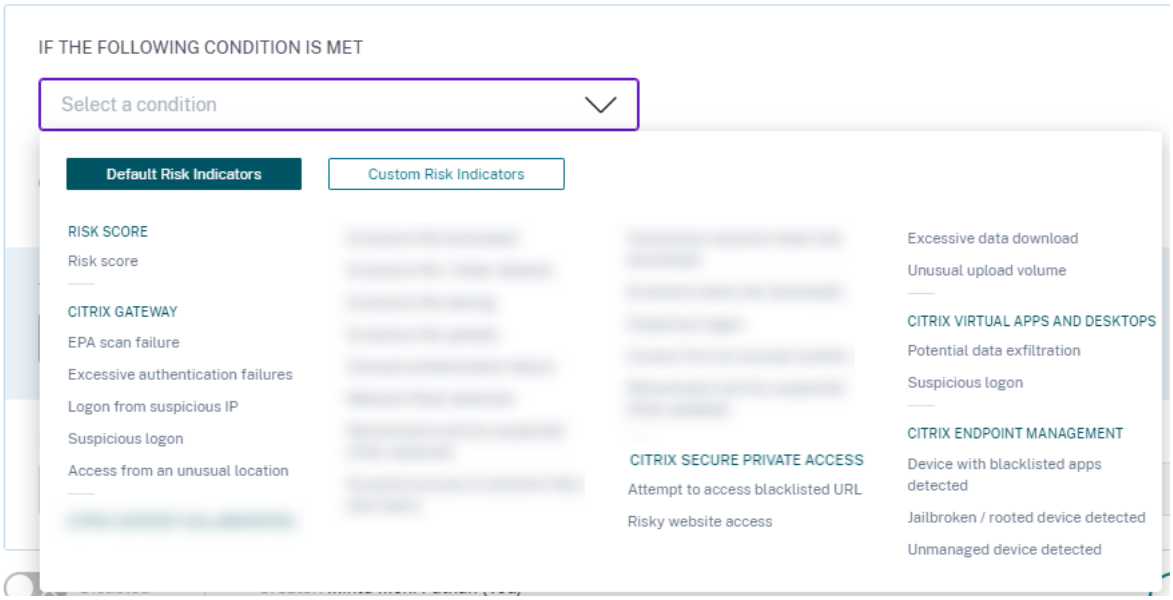
Pour plus d'informations sur la stratégie prédéfinie pour le cas d'utilisation du géorepérage, consultez la section Stratégie préconfigurée.

Comment ajouter ou supprimer des conditions ?

Pour ajouter d'autres conditions, sélectionnez **Ajouter une condition** dans la section **SI LA CONDITION SUIVANTE EST REMPLIE** de la page **Créer une stratégie** . Pour supprimer une condition, sélectionnez l'icône **-** qui s'affiche en regard de la condition.

Indicateurs de risque par défaut et personnalisés

Le menu des conditions est séparé en fonction des onglets **Indicateurs de risque par défaut** et **Indicateurs de risque personnalisés** de la page **Créer une stratégie** . À l'aide de ces onglets, vous pouvez facilement identifier le type d'indicateur de risque que vous souhaitez choisir lors de la sélection d'une condition pour la configuration de la stratégie.



Quelles sont les mesures à prendre ?

Les actions sont des réponses à des événements suspects qui empêchent de futurs événements anormaux de se produire. Vous pouvez appliquer des actions sur les comptes d'utilisateurs qui affichent un comportement inhabituel ou suspect. Vous pouvez configurer des stratégies pour appliquer automatiquement une action sur le compte de l'utilisateur ou appliquer manuellement une action spécifique à partir de la chronologie des risques de l'utilisateur.

Vous pouvez afficher les actions globales ou les actions pour chaque source de données Citrix. Vous pouvez également désactiver les actions précédemment appliquées pour un utilisateur à tout moment.

> **Remarque**
>
> Quelle que soit la source de données qui déclenche un indicateur de risque, des mesures relatives à d'autres sources de données peuvent être appliquées.

Le tableau suivant décrit les actions que vous pouvez effectuer.

Nom de l'action	Description	Sources de données applicables
Actions mondiales		

Nom de l'action	Description	Sources de données applicables
Ajouter à la liste de surveillance	Lorsque vous souhaitez surveiller un utilisateur afin de détecter de futures menaces potentielles, vous pouvez les ajouter à une liste de surveillance. Le volet **Utilisateurs de la Liste de surveillance** affiche tous les utilisateurs que vous souhaitez surveiller pour détecter les menaces potentielles en fonction de l'activité inhabituelle de leur compte. En fonction de la stratégie de votre organisation, vous pouvez ajouter un utilisateur à la liste de suivi à l'aide de l'action Ajouter à la liste de suivi. Pour ajouter un utilisateur à la liste de suivi, accédez au profil de l'utilisateur, dans le menu **Actions**, sélectionnez **Ajouter à la liste de suivi**. Cliquez sur **Appliquer** pour appliquer l'action.	Toutes les sources de données

Nom de l'action	Description	Sources de données applicables
Avertir l'administrateur (s)	Lorsqu'un indicateur de risque est déclenché pour un utilisateur, vous pouvez le notifier manuellement aux administrateurs ou créer une stratégie de notification automatique. Vous pouvez sélectionner les administrateurs à partir du domaine Citrix Cloud et d'autres domaines non Citrix Cloud de votre organisation. Si vous êtes un administrateur Citrix Cloud avec des autorisations d'accès complet, par défaut, les notifications par e-mail sont désactivées pour votre compte Citrix Cloud. Pour recevoir des notifications par e-mail, activez-le sur votre compte Citrix Cloud. Pour plus d'informations, consultez la section Recevoir des notifications par e-mail. Si vous êtes un administrateur Citrix Cloud avec des autorisations d'accès personnalisées (accès en lecture seule et complet) pour gérer Security Analytics, les notifications par e-mail sont activées pour votre compte Citrix Cloud. Pour ne plus recevoir de notifications par e-mail de Citrix Analytics, demandez à votre administrateur d'accès complet Citrix Cloud de supprimer votre nom de la liste de distribution Notifier les administrateurs. Pour plus d'informations sur, voir Liste de distribution des e-mails.	

Nom de l'action	Description	Sources de données applicables
Demander une réponse de l'utilisateur final	En cas d'activité inhabituelle ou suspecte sur le compte de l'utilisateur, vous pouvez en informer l'utilisateur pour confirmer si l'utilisateur identifie l'activité. En fonction de l'activité, vous pouvez déterminer le plan d'action suivant à prendre sur le compte de l'utilisateur. Pour plus d'informations, consultez Demander une réponse de l'utilisateur final.	
Avertir l'utilisateur final	Lorsqu'une activité inhabituelle ou suspecte se produit sur le compte de l'utilisateur, vous pouvez en informer l'utilisateur final par le biais d'une notification par e-mail. Pour plus d'informations, voir Notifier l'utilisateur final.	
Actions Citrix Gateway		
Déconnecter les sessions actives	Lorsque l'action est appliquée, elle ferme la session utilisateur actuellement active. Il ne bloque aucune session utilisateur future.	Citrix Gateway sur site et Citrix Application Delivery Management
Verrouiller le compte utilisateur	Lorsque le compte d'un utilisateur est verrouillé en raison d'un comportement anormal, il ne peut accéder à aucune ressource via Citrix Gateway tant que l'administrateur Gateway n'a pas déverrouillé le compte.	Citrix Gateway sur site

Nom de l'action	Description	Sources de données applicables
Déverrouiller le compte utilisateur **Citrix Virtual Apps and Desktops et actions Citrix DaaS**	Lorsque le compte d'un utilisateur est verrouillé accidentellement bien que le comportement anormal n'ait pas été détecté, vous pouvez appliquer cette action pour le déverrouiller et restaurer l'accès au compte.	Citrix Gateway sur site
Déconnecter les sessions actives	Lorsque l'action est appliquée, elle ferme la session utilisateur actuellement active. Il ne bloque aucune session utilisateur future.	Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service)
Démarrer l'enregistrement de session	En cas d'événement inhabituel sur le compte Virtual Desktops de l'utilisateur, l'administrateur peut commencer à enregistrer les sessions actives actuelles de l'utilisateur. Si l'utilisateur utilise Citrix Virtual Apps and Desktops 7.18 ou une version ultérieure et qu'il est connecté à la session virtuelle, un administrateur peut déclencher dynamiquement une action de démarrage de l'enregistrement de session à partir de Citrix Analytics for Security qui lance l'enregistrement de la session active en cours de l'utilisateur.	Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service)

Remarques

- Vous pouvez appliquer n'importe quelle action à un indicateur de risque, quelles que soient les sources de données.
- Les administrateurs peuvent désormais exécuter des actions d'enregistrement de session dynamique sur les sites Citrix DaaS et enregistrer de manière dynamique les sessions virtuelles des utilisateurs.
- Les actions **Demander une réponse à l'utilisateur final**et **Notifier l'utilisateur final** ne peuvent pas être appliquées à des utilisateurs anonymes car ils n'ont pas d'adresse e-mail dans **Active Directory**. Par conséquent, assurez-vous que les adresses e-mail de vos utilisateurs sont disponibles dans **Active Directory** avec une connexion établie entre votre Active Directory et Citrix Cloud.

Partage en lecture seule

Avant d'appliquer l'action **Modifier les liens au partage en lecture seule** sur le compte d'un utilisateur, assurez-vous que les conditions suivantes sont remplies :

Conditions préalables

- L'administrateur doit disposer d'un compte Enterprise dans Content Collaboration pour pouvoir utiliser l'action **Modifier les liens vers le partage en lecture seule** .
- Le partage en lecture seule est une fonctionnalité disponible sur demande dans les comptes d'entreprise de Citrix Content Collaboration. Avant d'appliquer l'action **Modifier les liens au partage en lecture seule** dans Citrix Analytics, assurez-vous que la fonctionnalité de partage en lecture seule est déjà activée dans les comptes Content Collaboration Enterprise de l'utilisateur et de l'administrateur. Pour plus d'informations, consultez l'article de support Citrix CTX208601.

Types de fichiers pris en charge L'action de partage en lecture seule s'applique uniquement aux types de fichiers suivants :

- Fichiers Microsoft Office
- PDF
- Fichiers image (nécessite SZC v3.4.1 ou une version ultérieure) :
  - BMP
  - GIF

  - JPG
  - JPEG
  - PNG
  - TIF
  - TIFF

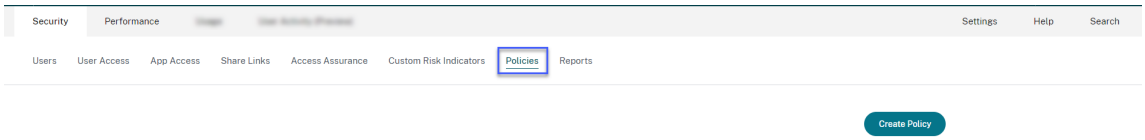
- Fichiers audio et vidéo stockés sur une zone de stockage gérée par Citrix.

Configurer les stratégies et les actions

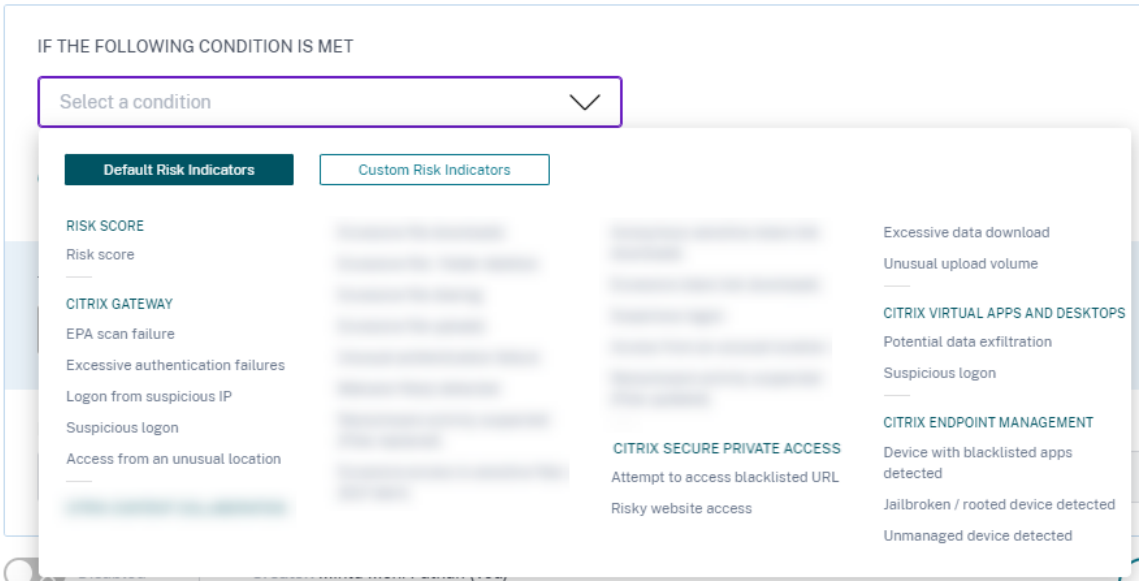
Par exemple, en suivant les étapes ci-dessous, vous pouvez créer une stratégie de partage de fichiers excessif. À l'aide de cette stratégie, lorsqu'un utilisateur de votre organisation partage une quantité exceptionnellement importante de données, les liens de partage expirent automatiquement. Vous êtes averti lorsqu'un utilisateur partage des données qui dépassent le comportement normal de cet utilisateur. En appliquant la stratégie de partage de fichiers excessif et en prenant des mesures immédiates, vous pouvez empêcher l'exfiltration de données depuis le compte de n'importe quel utilisateur.

Pour créer une stratégie, procédez comme suit :

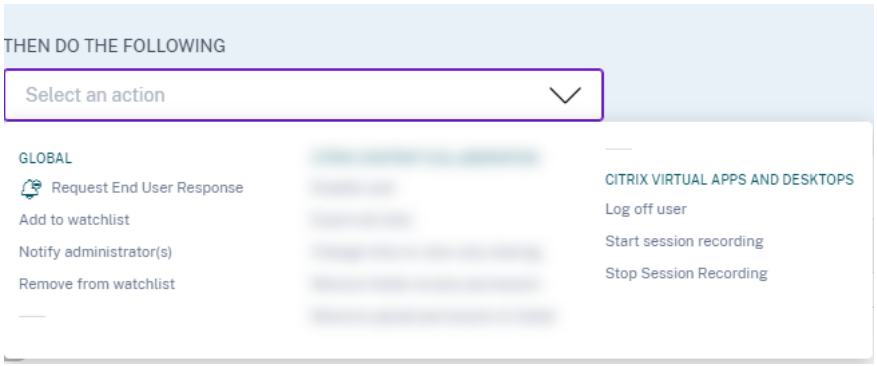
1. Après vous être connecté à Citrix Analytics, accédez à **Sécurité > Stratégies > Créer une stratégie**.



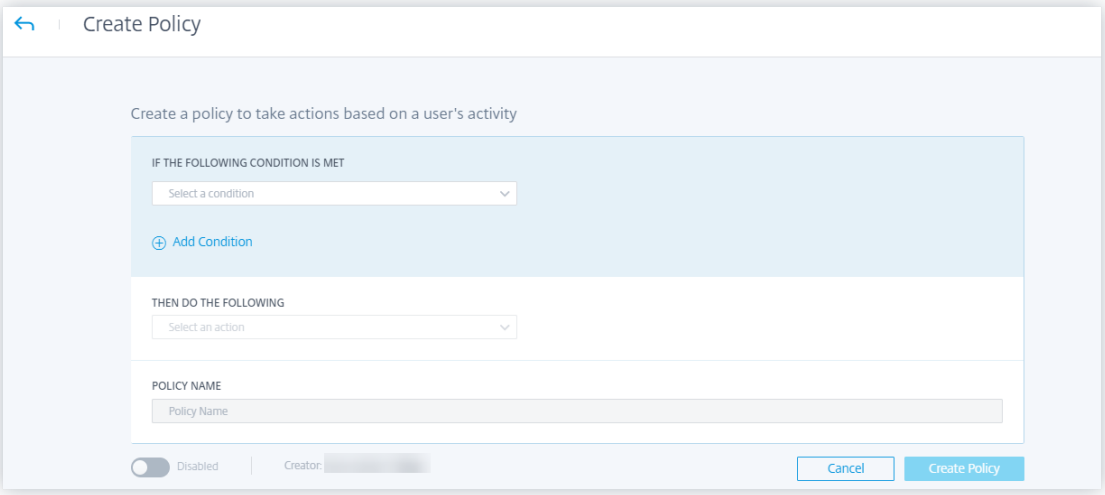
2. Dans la zone de liste **SI LA CONDITION SUIVANTE EST REMPLIE**, sélectionnez les conditions de l'indicateur de risque par défaut ou personnalisé auxquelles vous souhaitez appliquer une action.



3. Dans la liste **PUIS PROCÉDER COMME SUIT**, sélectionnez une action.



4. Dans la zone **de texte Nom de la stratégie**, indiquez un nom et activez la stratégie à l'aide du bouton bascule fourni.



5. Cliquez sur **Créer une stratégie**.

Après avoir créé une stratégie, celle-ci apparaît dans le tableau **de bord Stratégies** .

Le tableau de bord **Stratégies** affiche les stratégies associées aux sources de données qui ont été découvertes et connectées à Citrix Analytics. Le tableau de bord n'affiche pas les stratégies pour lesquelles des conditions sont définies pour les sources de données non découvertes.

Toutefois, la désactivation du traitement des données pour une source de données déjà connectée n' affecte pas les stratégies existantes dans le tableau **de bord Stratégies** .

Demander une réponse de l'utilisateur final

Demander une réponse de l'utilisateur final est une action globale qui vous permet d'alerter un utilisateur immédiatement après avoir détecté une activité inhabituelle dans son compte Citrix. Lorsque vous appliquez l'action, une notification par e-mail est envoyée à l'utilisateur. L'utilisateur doit répondre par e-mail à propos de la légitimité de son activité.

Déterminez l'action que vous souhaitez appliquer à vos utilisateurs :

En fonction de la réponse de l'utilisateur, vous pouvez déterminer le prochain plan d'action que vous souhaitez entreprendre. Vous pouvez appliquer une action globale telle que Ajouter à la liste de suivi, Notifier les administrateurs. Vous pouvez également appliquer une action spécifique à la source de données, telle que Citrix Gateway- Lock user.

Si vous recevez une réponse indiquant que l'utilisateur a effectué l'activité signalée, l'activité n'est pas suspecte et vous n'avez pas besoin d'agir sur le compte de l'utilisateur. La limite quotidienne pour envoyer des alertes de sécurité à l'utilisateur est de trois e-mails.

Considérez un utilisateur Citrix Content Collaboration dont le score de risque a dépassé 80 en une durée de 80 minutes. Vous pouvez avertir l'utilisateur de ce comportement inhabituel en appliquant l'action **Demander une réponse de l'utilisateur final** . Une alerte de sécurité est envoyée à l'utilisateur à partir de l'ID de messagerie `security-analytics@cloud.com`.

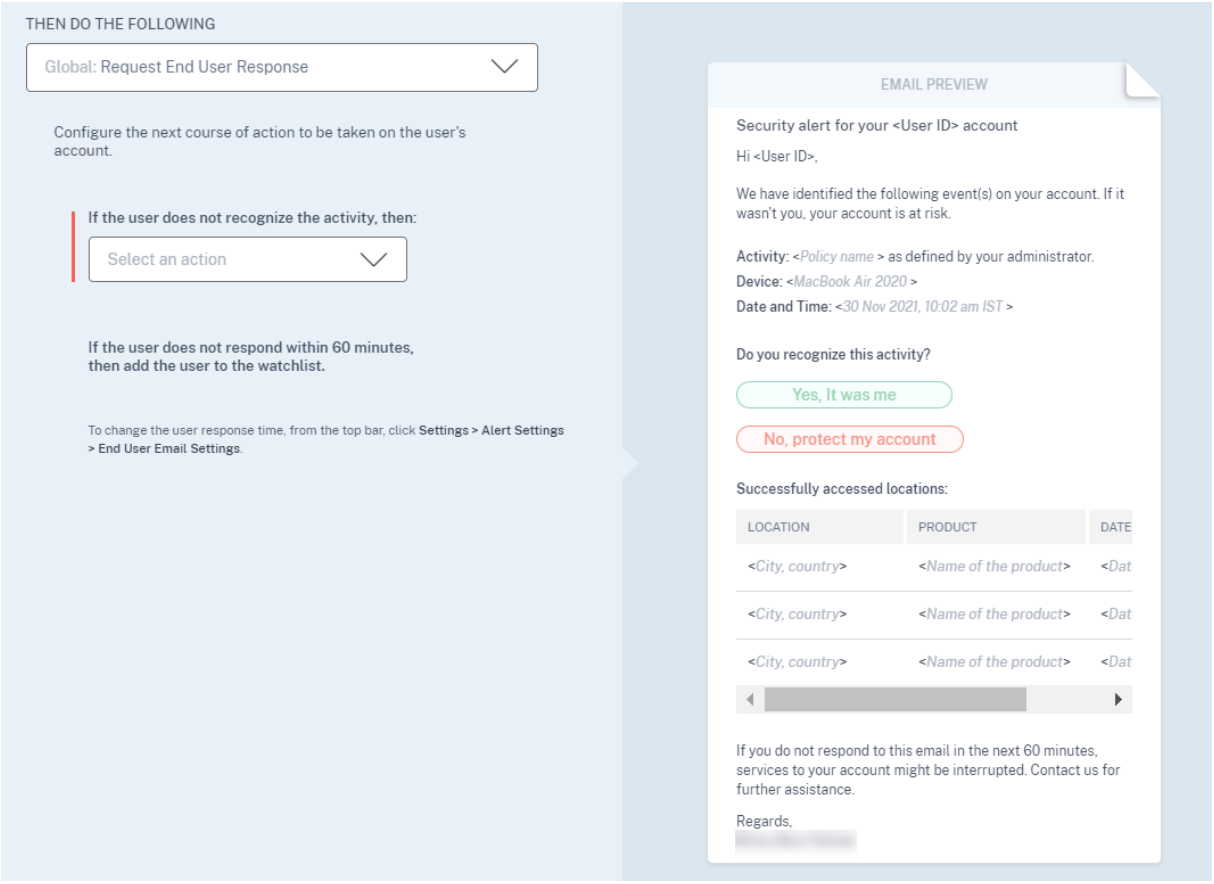
L'e-mail contient les informations suivantes :

- Activité de l'utilisateur qui a déclenché l'indicateur de risque
- Appareil de l'utilisateur
- Date et heure de l'activité de l'utilisateur
- Emplacements (villes et pays) à partir desquels les produits ou services sont accessibles avec succès. Si la ville ou le pays n'est pas disponible, la valeur correspondante est affichée comme « Inconnu »

L'action **Demander une réponse de l'utilisateur final** est ajoutée à la chronologie des risques de l' utilisateur.

Si l'utilisateur ne reconnaît pas l'activité détectée dans son compte Citrix, Citrix Analytics applique l'action que vous avez définie.

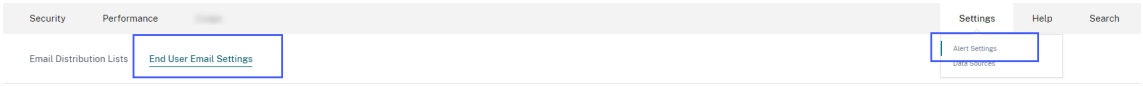
Si l'utilisateur ne parvient pas à envoyer sa réponse dans l'heure suivant la réception de l'e-mail, Citrix Analytics l'ajoute à la liste de surveillance. Vous pouvez surveiller l'utilisateur et son compte pour détecter toute activité suspecte et prendre les mesures nécessaires.



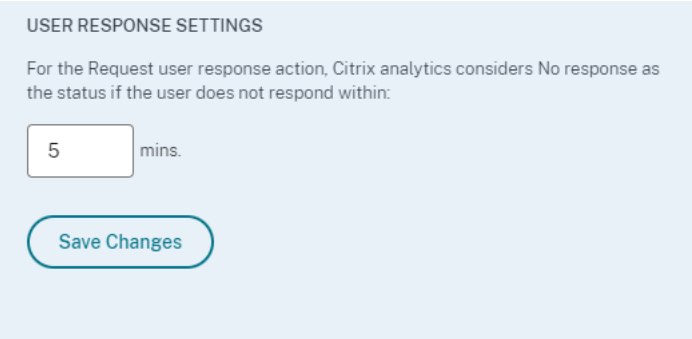
Comment définir le temps de réponse de l'utilisateur ? Vous pouvez configurer le temps de réponse de l'utilisateur à votre e-mail d'alerte de sécurité. Si l'utilisateur ne répond pas à l'activité signalée dans le délai spécifié, il est ajouté à la liste de suivi à des fins de surveillance.

Suivez les étapes pour configurer le temps de réponse de l'utilisateur :

1. Cliquez sur **Paramètres > Paramètres d'alerte > Paramètres de messagerie de l'utilisateur final**.



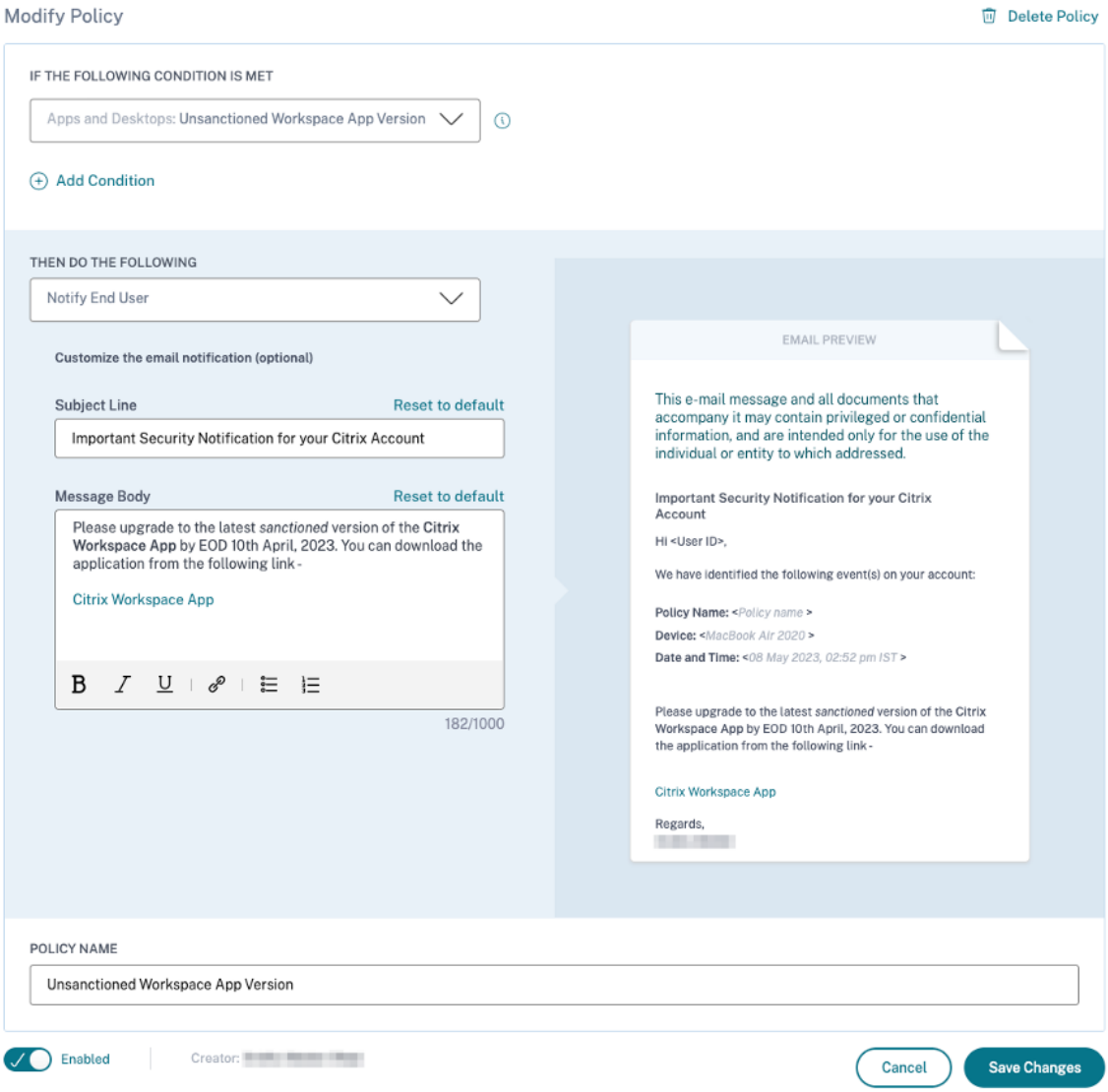
2. Sur la page **Paramètres de messagerie de l'utilisateur final**, saisissez le nombre de minutes dans la zone de texte.



3. Cliquez sur **Enregistrer**.

Vous pouvez également ajouter une bannière, un texte d'en-tête et un texte de pied de page dans l'e-mail d'alerte de sécurité pour le rendre légitime, attirer l'attention des utilisateurs et augmenter le temps de réponse. Pour plus d'informations, consultez la section Paramètres de messagerie de l'utilisateur final.

Avertir l'utilisateur final **Notifier l'utilisateur final** est une action globale qui vous permet d'envoyer des notifications par e-mail aux utilisateurs finaux lorsqu'un comportement inhabituel ou suspect est détecté sur leurs comptes Citrix. La ligne d'objet de l'e-mail et le corps du message sont personnalisables. Lorsque l'action est appliquée après le déclenchement d'une stratégie, une notification par e-mail est envoyée à l'utilisateur. Aucune réponse n'est demandée à l'utilisateur final et aucune action perturbatrice n'est effectuée sur le compte de l'utilisateur.



Cette action peut aider à répondre à divers cas d'utilisation en matière de conformité en fonction d'un ou de plusieurs déclencheurs d'indicateurs de risque intégrés ou personnalisés. Avec la ligne d'objet et le corps du message personnalisables, il est également suffisamment flexible pour répondre à de nombreux cas d'utilisation génériques de notifications aux utilisateurs finaux, qui ne nécessitent pas de réponse ou d'action perturbatrice sur le compte de l'utilisateur.

L'e-mail contient les informations suivantes :

- Nom de la stratégie associé à l'action.
- Appareil de l'utilisateur (si disponible)
- Date et heure de l'activité de l'utilisateur

La notification par e-mail de l'utilisateur final est envoyée à partir de l'identifiant e-mail `security`

-analytics@cloud.com.

> **Remarque**
>
> La limite quotidienne pour toutes les stratégies est de **trois** e-mails par utilisateur. Une fois ce seuil franchi, l'action n'est pas appliquée et aucune notification par e-mail n'est envoyée à l'utilisateur final. L'action est visible sur la chronologie de l'utilisateur avec le message **Limite quotidienne d'e-mails atteinte pour l'utilisateur**.

L'action est ajoutée à la chronologie des risques de l'utilisateur. Toutefois, il ne s'agit pas d'une action manuelle et ne peut pas être appliquée à un utilisateur depuis la vue chronologique.

Personnalisation du contenu des e-mails des utilisateurs finaux Auparavant, les administrateurs de Citrix Analytics contactaient manuellement les utilisateurs finaux pour leur fournir des instructions de correction concernant la détection d'une activité suspecte, processus fastidieux pour clôturer un incident.

La fonctionnalité **de personnalisation du contenu des e-mails des utilisateurs finaux** est introduite pour demander une réponse à l'utilisateur final, avertir les utilisateurs finaux et envoyer des e-mails d'information. L'e-mail de réponse de l'utilisateur final demande la validation/la réponse de l'utilisateur, mais un e-mail d'information indique le type d'activité suspecte et le type de mesures correctives déjà prises. L'e-mail de notification à l'utilisateur final informe l'utilisateur final des violations de conformité ou des activités suspectes sur son compte Citrix sans lui demander de réponse.

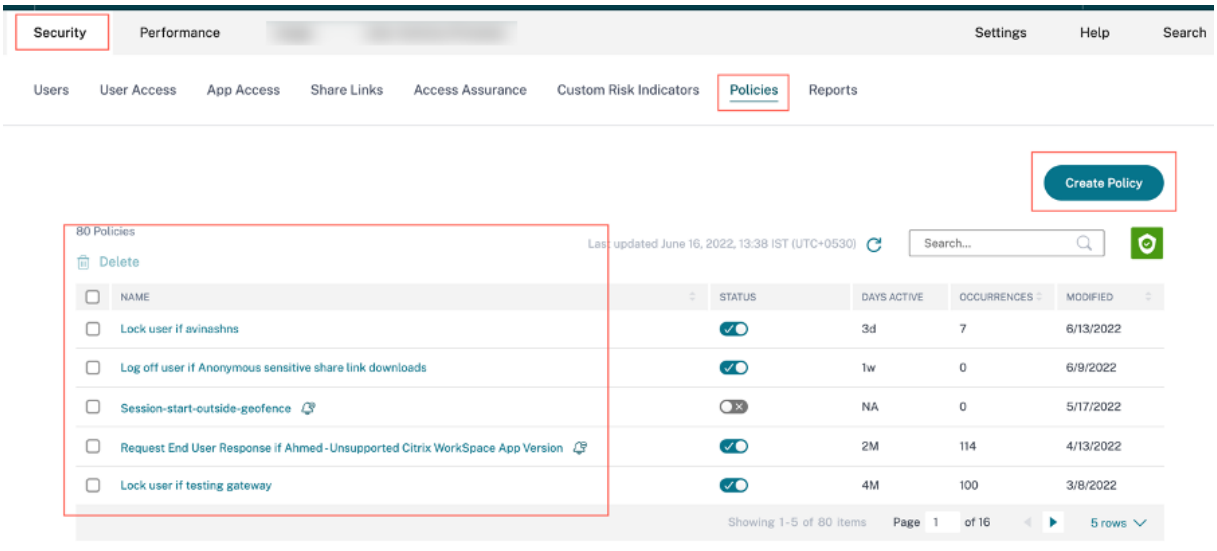
Grâce à la fonctionnalité **de personnalisation du contenu des e-mails de l'utilisateur final**, les administrateurs de Citrix Analytics peuvent ajouter un message personnalisé dans le modèle de corps de l'e-mail de demande de réponse/de notification à l'utilisateur final/d'information. À l'aide de l'éditeur de zone de texte enrichi, un administrateur peut modifier le contenu par stratégie à l'aide de divers outils d'édition tels que le gras, l'italique, le lien hypertexte, etc.

> **Remarque**
>
> La fonctionnalité Personnalisation du contenu des e-mails de l'utilisateur final n'est disponible que pour les actions basées sur des stratégies et non pour les actions manuelles.

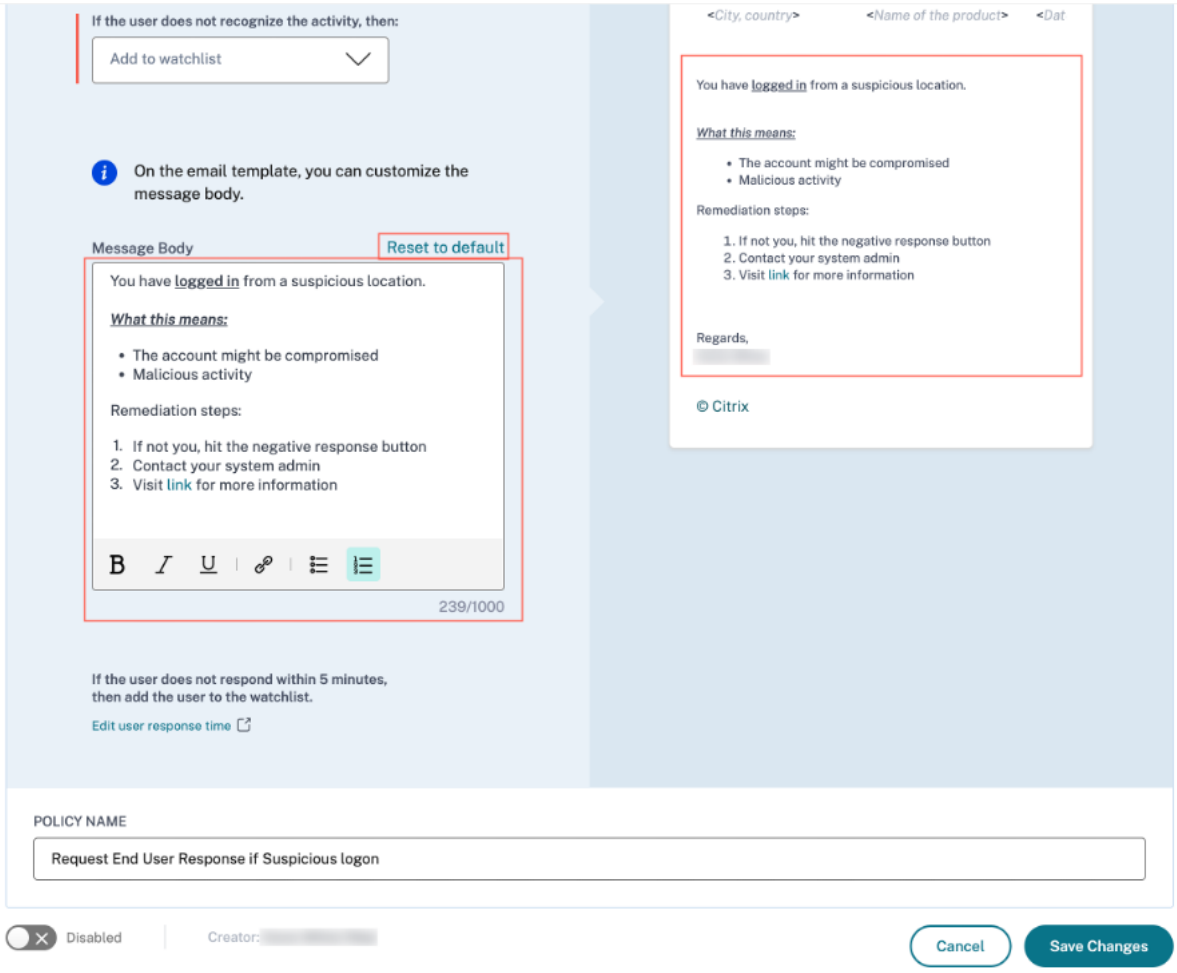
Vous pouvez personnaliser le contenu pour trois types d'e-mails :

- Demander un e-mail de réponse à l'utilisateur final.
- Envoyer un e-mail à l'utilisateur final
- E-mail envoyé lorsque l'une des actions suivantes de l'utilisateur final est effectuée :
  - Action de fermeture de session sous **Citrix Apps and Desktop**
  - Déconnexion et verrouillage de l'utilisateur sous **Citrix Gateway**

Vous pouvez consulter la liste des stratégies dans l'onglet **Sécurité > Stratégies** .



Vous pouvez consulter le corps personnalisé de l'e-mail en cliquant sur la stratégie existante ou lors de la création d'une nouvelle stratégie. Dans le volet de droite, vous pouvez obtenir un aperçu du contenu mis à jour de l'e-mail.



Remarque

- L'administrateur peut définir le contenu selon le modèle par défaut en cliquant sur le lien **Rétablir les paramètres par défaut** . La limite de caractères pour le corps personnalisé est de 1 000.
- Pour l'action **Notifier l'utilisateur final**, le **champ Objet** est également personnalisable par l'administrateur. Il peut être rétabli par défaut en cliquant sur le lien **Rétablir les paramètres par défaut** . La limite de caractères pour l'objet de l'e-mail personnalisé est de 500.

Cliquez sur **Enregistrer les modifications** pour créer/mettre à jour la stratégie. Lorsque la stratégie est déclenchée, la notification par e-mail suivante est envoyée à l'utilisateur final :

- **Demander un e-mail de réponse à l'utilisateur final** : action de stratégie qui envoie un e-mail demandant une réponse à l'utilisateur.
- **E-mail de notification à l'utilisateur final** : notification par e-mail envoyée aux utilisateurs finaux pour les informer de problèmes de conformité, d'activités suspectes, etc. sur leur compte Citrix.

- **E-mail d'information** : e-mail d'information envoyé après une action de l'utilisateur final.

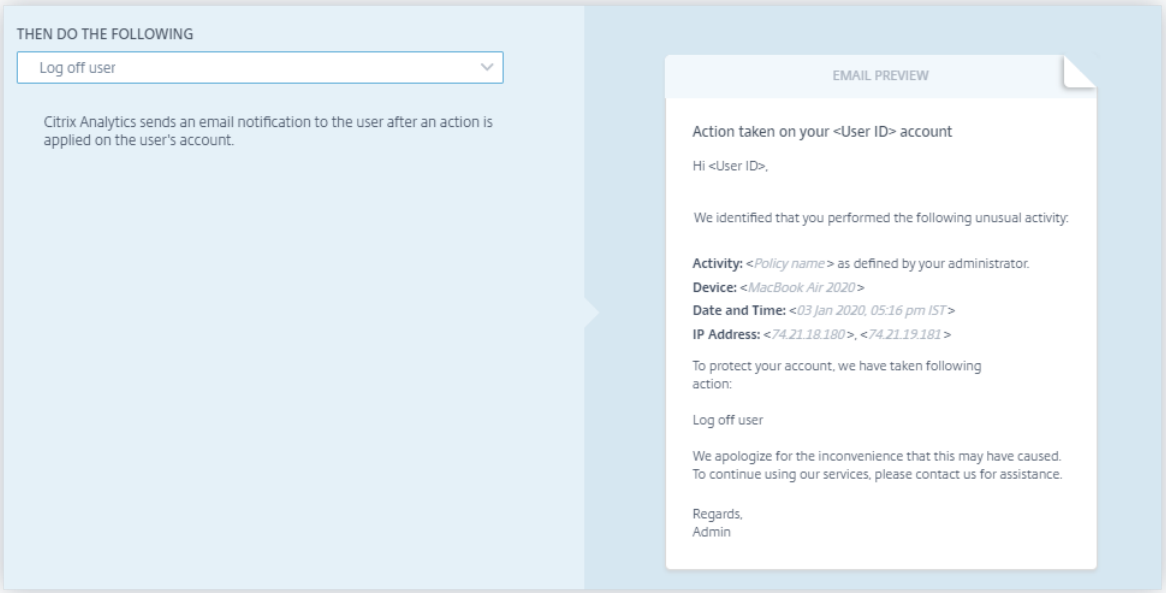
L'utilisateur final peut lire l'e-mail et effectuer les actions correctives demandées par l'administrateur.

> **Remarque**
>
> L'administrateur disposant d'un accès en lecture seule ne peut pas modifier/ajouter le corps du message.

Notifier l'utilisateur après avoir appliqué une action perturbatrice

Dans ce type d'action, vous pouvez appliquer une action perturbatrice telle que Fermer la **session de l'utilisateur** et **Verrouiller l'utilisateur** sur le compte de l'utilisateur lorsqu'une activité inhabituelle est détectée. Lorsqu'une action est appliquée au compte de l'utilisateur, les services liés à son compte peuvent être interrompus. Dans de tels cas, l'utilisateur doit contacter l'administrateur pour pouvoir accéder à son compte comme auparavant.

Considérez un utilisateur Citrix Content Collaboration dont le score de risque a dépassé 80 en une durée de 80 minutes. Vous pouvez fermer la session de l'utilisateur. Une fois cette tâche effectuée, l'utilisateur ne peut pas accéder à son compte et une notification par e-mail lui est envoyée à partir de l'ID de messagerie `security-analytics@cloud.com`. L'e-mail contient des détails sur l'événement, tels que l'activité, l'appareil, la date et l'heure et l'adresse IP. L'utilisateur doit contacter l'administrateur pour accéder à son compte comme auparavant.

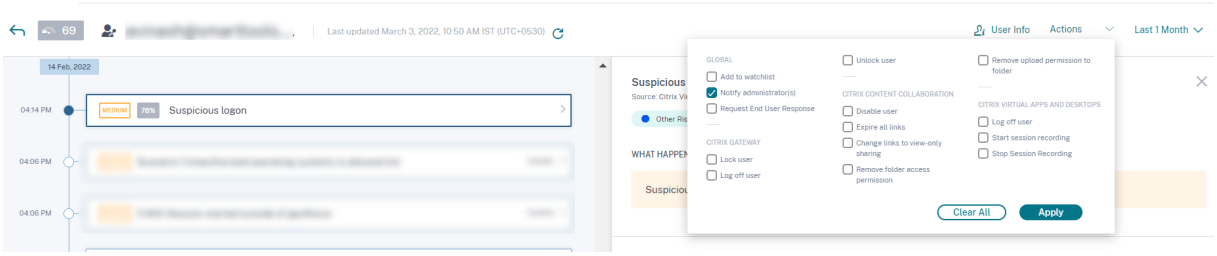


Appliquer une action manuellement

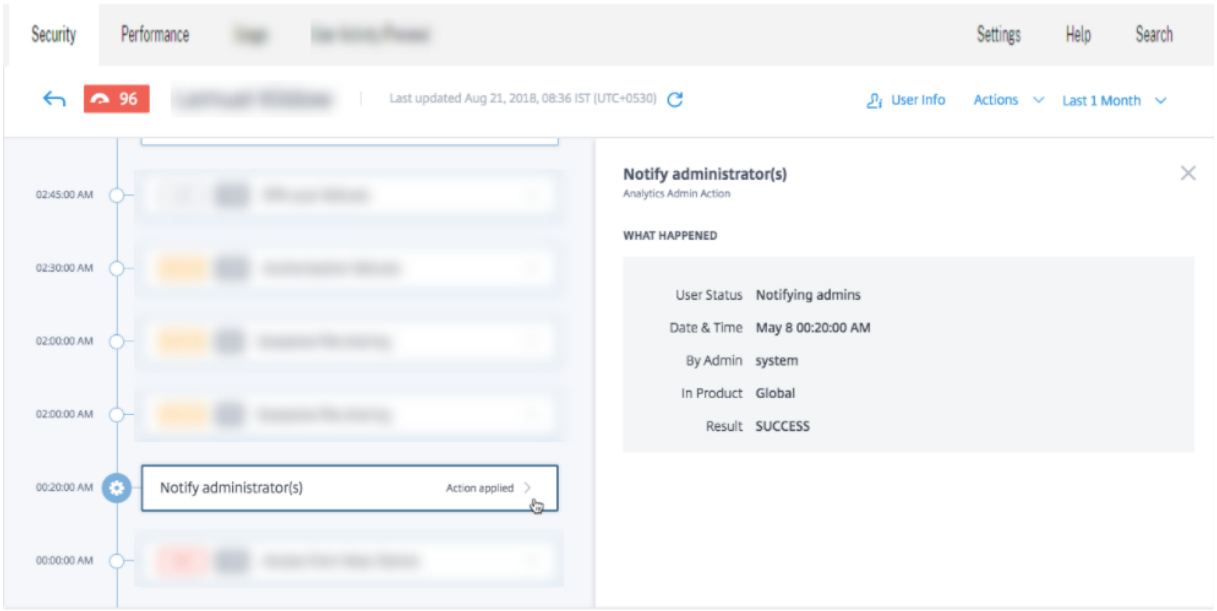
Prenons l'exemple d'un utilisateur, Lemuel, qui se connecte à un réseau en utilisant un nouvel appareil pour la première fois. Pour surveiller son compte car son comportement est inhabituel, vous pouvez utiliser l'action **Notifier l'administrateur (s)** .

Pour appliquer manuellement l'action à l'utilisateur, vous devez :

Accédez au profil d'un utilisateur et sélectionnez l'indicateur de risque approprié. Dans le menu **Actions**, sélectionnez l'action **Notifier les administrateurs** et cliquez sur **Appliquer**.



Une notification par e-mail est envoyée à tous les administrateurs ou à certains administrateurs pour surveiller son compte. L'action appliquée est ajoutée à sa chronologie de risque et les détails de l'action sont affichés dans le volet droit de la page de chronologie de risque.



Remarques

- Si vous êtes un administrateur Citrix Cloud avec des autorisations d'accès complet, par défaut, les notifications par e-mail sont désactivées pour votre compte Citrix Cloud. Pour recevoir des notifications par e-mail, activez-le sur votre compte Citrix Cloud. Pour plus d'informations, consultez la section Recevoir des notifications par e-mail.

> - Si vous êtes un administrateur Citrix Cloud avec des autorisations d'accès personnalisées (accès en lecture seule et complet) pour gérer Security Analytics, les notifications par e-mail sont activées pour votre compte Citrix Cloud. Pour ne plus recevoir de notifications par e-mail de Citrix Analytics, demandez à votre administrateur d'accès complet Citrix Cloud de supprimer votre nom de la liste de distribution Notifier les administrateurs. Pour plus d'informations sur, voir Liste de distribution des e-mails.

Gérer les stratégies

Vous pouvez consulter le tableau de bord Stratégies pour gérer toutes les stratégies créées sur Citrix Analytics afin de surveiller et d'identifier les incohérences sur votre réseau. Dans le tableau de bord des stratégies, vous pouvez :

1. Afficher la liste des stratégies
2. Détails de la stratégie
    - Nom de la stratégie
    - État : activé ou désactivé.
    - Durée de la stratégie : nombre de jours pendant lesquels la stratégie a été active ou inactive.
    - Occurrences : nombre de fois que la stratégie est déclenchée.
    - Modifié : horodatage, uniquement si la stratégie a été modifiée.
3. Supprimer la stratégie
    - Pour supprimer une stratégie, vous pouvez sélectionner la stratégie que vous souhaitez supprimer, puis cliquer sur **Supprimer**.
    - Vous pouvez également cliquer sur le nom de la stratégie pour être redirigé vers la page Modifier la stratégie. Cliquez sur **Supprimer la stratégie**. Dans la boîte de dialogue, confirmez votre demande de suppression de la stratégie.
4. Créer une stratégie
5. Cliquez sur le nom d'une stratégie pour afficher plus de détails. Vous pouvez également modifier la stratégie lorsque vous cliquez sur son nom. Les autres modifications qui peuvent être apportées sont les suivantes :
    - Modifiez le nom de la stratégie.
    - Conditions de la stratégie.
    - Les actions à appliquer.

- Activez ou désactivez la stratégie.
- Supprimez la stratégie.

> **Remarque**
>
> - Si vous ne souhaitez pas supprimer votre stratégie, vous pouvez choisir de la désactiver.
> - Pour réactiver la stratégie dans le tableau de bord Stratégies, procédez comme suit :
>   - On the Policies dashboard, click the **Status** slider button and refresh the page. The **Status** slider button turns green.
>   - On the Modify Policy page, click the **Enabled** slider button on the bottom of the page.

Modes pris en charge

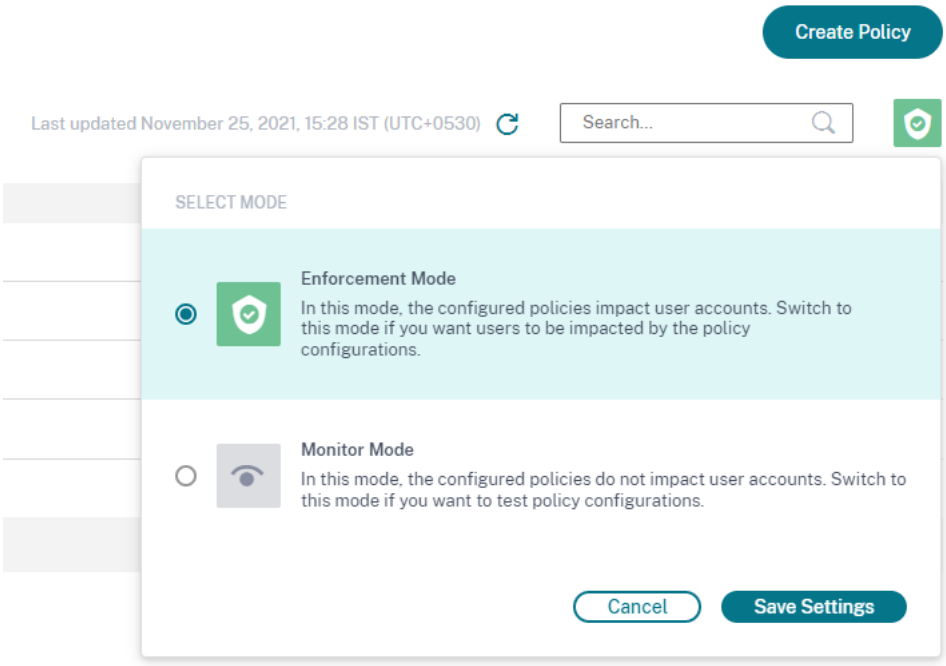
Citrix Analytics prend en charge les modes de stratégie suivants :

- **Mode d'application** - Dans ce mode, les stratégies configurées ont un impact sur les comptes d'utilisateurs.
- **Mode de surveillance** - Dans ce mode, les stratégies configurées n'affectent pas les comptes d'utilisateurs. Vous pouvez définir des stratégies sur ce mode si vous souhaitez tester des configurations de stratégie.

Suivez les instructions suivantes pour configurer les modes sur les stratégies :

1. Accédez à **Sécurité** > **Stratégies**.
2. Sur la page **Stratégies**, sélectionnez l'icône en haut à droite qui s'affiche à côté de la barre **de recherche** . La fenêtre **SELECT MODE** s'affiche.
3. Sélectionnez le mode de votre choix et cliquez sur **Enregistrer les paramètres**.

> **Remarque**
>
> Les stratégies par défaut créées par Analytics sont définies en mode de surveillance. Par conséquent, les stratégies existantes héritent également de ce mode. Vous pouvez évaluer l'impact de toutes les stratégies ensemble, puis les passer en mode d'application.



Recherche en libre-service pour les stratégies

Sur la page de recherche en libre-service, vous pouvez afficher les événements utilisateur qui ont satisfait aux conditions définies dans les stratégies. La page affiche également les actions appliquées à ces événements utilisateur. Filtrez les événements utilisateur en fonction des actions appliquées.

Indicateurs et stratégies de risque personnalisés préconfigurés

December 7, 2023

Citrix Analytics for Security fournit une liste d'indicateurs de risque personnalisés préconfigurés et une stratégie pour vous aider à surveiller la sécurité de votre infrastructure Citrix. Les conditions de ces indicateurs de risque personnalisés préconfigurés et de la stratégie sont déjà définies en fonction de scénarios de risque de sécurité spécifiques tels que les utilisateurs compromis, les menaces internes et l'exfiltration de données. Vous pouvez également modifier ces conditions préconfigurées ou ajouter vos propres conditions en fonction de vos exigences de sécurité et utiliser les indicateurs de risque personnalisés pour atténuer les risques.

Actuellement, les indicateurs de risque personnalisés préconfigurés sont disponibles pour les scénarios suivants :

- Géofencing

- Premier accès

Indicateurs de risque personnalisés préconfigurés pour le scénario de géorepérage

Utilisez les indicateurs de risque personnalisés préconfigurés suivants pour détecter les événements utilisateur provenant de l'extérieur des zones géo-clôturées.

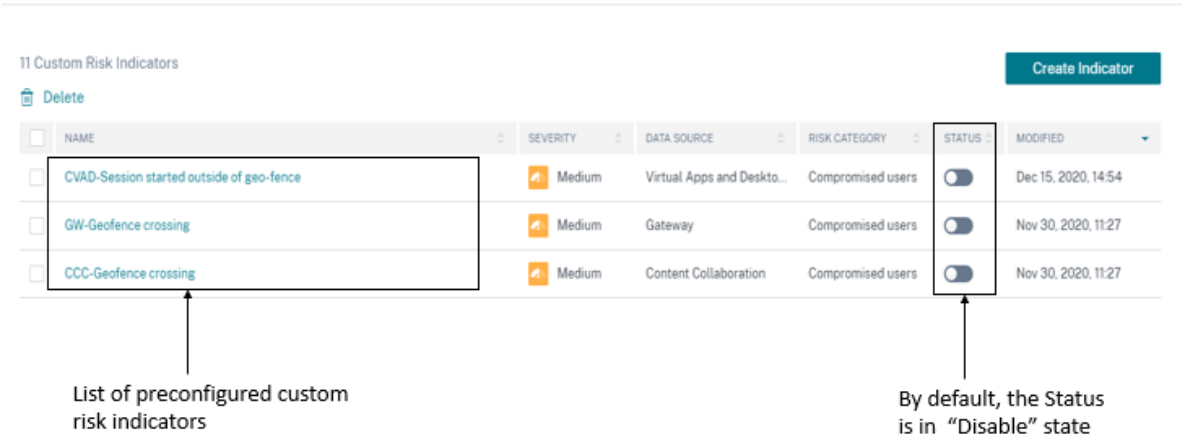
- La session CVAD débute en dehors du périmètre de géofencing
- GW-Geofence crossing

Les indicateurs de risque personnalisés préconfigurés sont déclenchés chaque fois que les utilisateurs accèdent aux produits Citrix en dehors de leur pays d'exploitation habituel ou de la géofence. Par défaut, la géofence est définie sur « États-Unis ». Vous pouvez définir le pays de votre choix en tant que géofence.

> **Remarque**
>
> La *session CVAD démarrée en dehors de l'indicateur de risque de géofence* est liée aux **paramètres de géolocalisation** de la fonctionnalité Access Assurance Location. Vous ne pouvez donc pas modifier directement les pays géoréférencés dans l'état de l'indicateur de risque. Pour mettre à jour les pays géoréférencés dans l'indicateur de risque, sélectionnez les pays dans les **paramètres de Geofence** du tableau de bord Access Assurance Location. Pour plus d'informations, consultez le tableau de bord de l'emplacement Access Assurance.

Pour afficher les indicateurs de risque personnalisés préconfigurés, sélectionnez **Sécurité > Indicateurs de risque personnalisés**.

Par défaut, les indicateurs de risque personnalisés préconfigurés sont désactivés. Utilisez le bouton **STATUS** pour les activer.



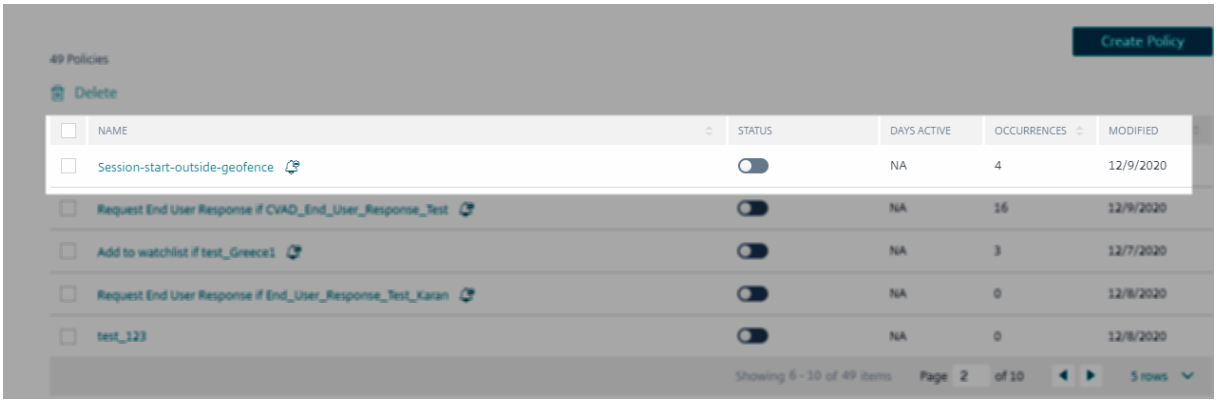
Le tableau suivant décrit les différents indicateurs de risque personnalisés préconfigurés pour le géorepérage.

Nom de l'indicateur de risque personnalisé	Scénario	Conditions de l'indicateur personnalisé	Source de données	Catégorie de risque
La session CVAD débute en dehors du périmètre de géofencing	L'utilisateur a démarré une session virtuelle en dehors de son pays d'exploitation	Event-Type = Session.logon Country != "United States"	Application Citrix Workspace	Utilisateurs compromis
GW-Geofence crossing	L'utilisateur a réussi l'authentification depuis l'extérieur de son pays d'opération	Event-Type = "VPN_AI"AND Country != "United States"	Citrix Gateway (local)	Utilisateurs compromis

Stratégie préconfigurée pour le scénario de géofencing

Citrix fournit une stratégie préconfigurée qui applique l'action **Demander une réponse à l'utilisateur final** à un compte utilisateur chaque fois que celui-ci démarre une session virtuelle depuis un autre pays que son pays d'opération. L'utilisateur reçoit un e-mail et, en fonction de la réponse de l'utilisateur, une action appropriée est entreprise, telle que l'ajout de l'utilisateur à la liste de suivi ou la notification de l'administrateur pour une action ultérieure. Pour plus d'informations, consultez Demander une réponse de l'utilisateur final.

Pour afficher la stratégie préconfigurée, sélectionnez **Sécurité > Stratégies**.



Le tableau suivant décrit la stratégie préconfigurée de géorepérage.

Nom de la stratégie	Scénario	Condition de stratégie	Action appliquée
Début de la session en dehors de la clôture géographique	Possibilité pour un administrateur de valider la légitimité de l'utilisateur via l'action « Demander une réponse de l'utilisateur final » lorsque l'utilisateur démarre la session virtuelle en dehors de son pays d'opération	À utiliser avec un indicateur de risque personnalisé préconfiguré - « Session CVAD démarrée en dehors de la géofence »	Demande de réponse de l'utilisateur final En fonction de la réponse de l'utilisateur suivante, l'action correspondante est appliquée Si l'utilisateur ne reconnaît pas l'activité : **Ajouter à la liste de suivi** Si l'utilisateur reconnaît l'activité : **aucune action n'est requise** Si l'utilisateur ne répond pas dans les 60 minutes suivant la réception de l'e-mail : **Ajouter l'utilisateur à la liste de suivi**

> **Remarque**
>
> L'action **Demander une réponse de l'utilisateur final** est prise en charge uniquement dans la région États-Unis. Par conséquent, si votre organisation est intégrée dans la région de l'Union européenne dans Citrix Cloud, la stratégie préconfigurée n'est pas appliquée à votre compte. Pour utiliser la stratégie préconfigurée, modifiez la stratégie et sélectionnez une autre action de

> votre choix.

Créez votre propre stratégie avec des indicateurs de risque personnalisés préconfigurés pour le géorepérage

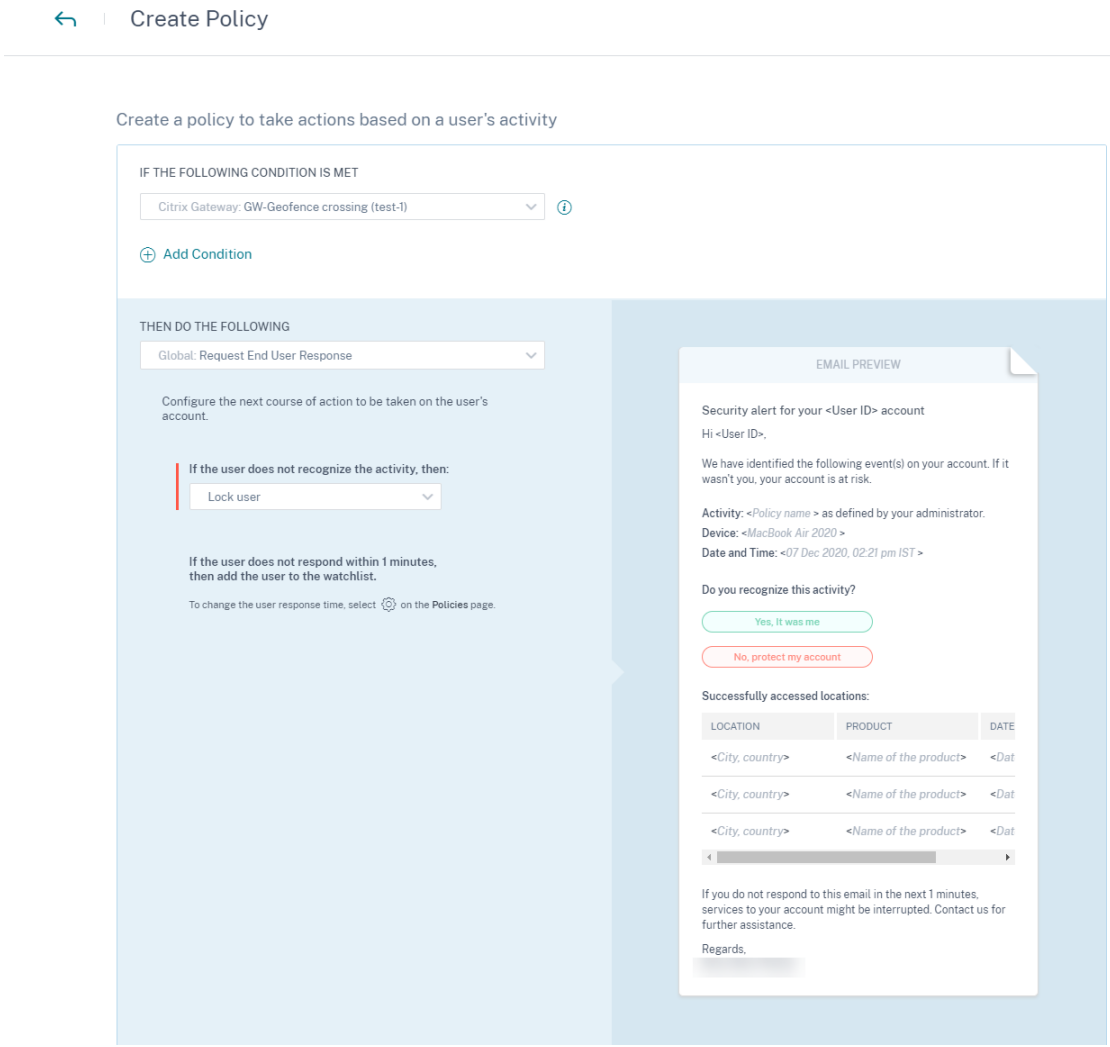
Vous pouvez également créer vos propres stratégies avec ces indicateurs de risque personnalisés préconfigurés et appliquer des actions telles que verrouiller des utilisateurs ou déconnecter des utilisateurs chaque fois que les indicateurs sont déclenchés. Pour plus d'informations sur la création de stratégies, consultez la section Configurer des stratégies et des actions.

L'exemple suivant illustre une stratégie qui bloque les utilisateurs qui tentent d'accéder aux services Citrix depuis l'extérieur des États-Unis. L'accès utilisateur est verrouillé si l'utilisateur ne reconnaît pas son activité d'accès.

Condition : passage à niveau GW-Geofence

Action : demande de réponse de l'utilisateur final

Action suivante : Verrouiller l'utilisateur s'il ne reconnaît pas l'activité



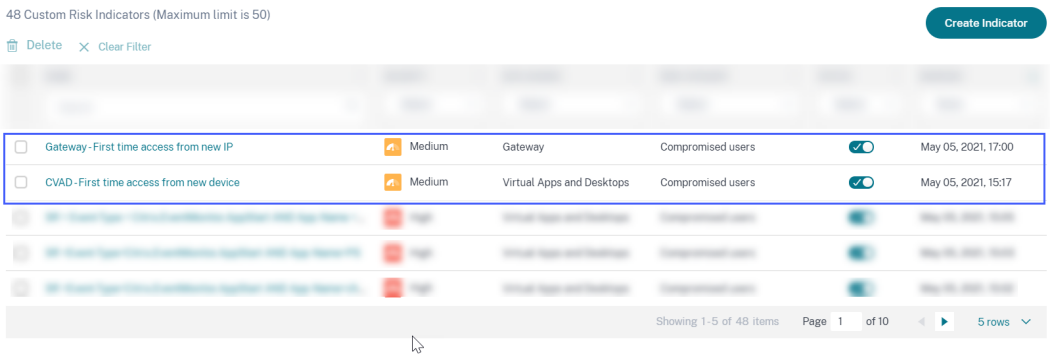
> **Remarque**
>
> L'action **Demander une réponse de l'utilisateur final** est prise en charge uniquement dans la région États-Unis. Par conséquent, si votre organisation est intégré à la région Union européenne, sélectionnez une autre action de votre choix au lieu de l'action **Demander une réponse de l'utilisateur final**.

Indicateurs de risque personnalisés préconfigurés pour le premier scénario d'accès

Utilisez les indicateurs de risque personnalisés suivants pour détecter les événements liés aux utilisateurs dans les scénarios de premier accès :

- Accès au CVAD pour la première fois depuis un nouvel appareil
- Accès Gateway pour la première fois à partir d'une nouvelle adresse IP

Par défaut, ces indicateurs de risque personnalisés préconfigurés sont dans l'état activé. Utilisez le bouton **STATUS** si vous souhaitez les désactiver.



Le tableau suivant décrit les indicateurs de risque personnalisés préconfigurés pour un premier accès.

Nom de l'indicateur personnalisé	Scénario	Conditions préconfigurées	Source de données	Catégorie de risque
Accès au CVAD pour la première fois depuis un nouvel appareil	Lorsqu'un utilisateur de l'application Citrix Workspace se connecte à partir de l'un des éléments suivants Un nouvel appareil	Les conditions suivantes sont activées par défaut La première fois pour un nouvel identifiant d'appareil.	Citrix Virtual Apps and Desktops sur site et Citrix DaaS (anciennement le Citrix Virtual Apps and Desktops Service)	Utilisateurs compromis

Nom de l'indicateur personnalisé	Scénario	Conditions préconfigurées	Source de données	Catégorie de risque
	Un appareil existant qui n'a pas été utilisé au cours des 90 derniers jours.	`Event-Type = "Session.Logon"AND Client-Type IN ("XA.Receiver.Windows", "XA.Receiver.Mac", "XA.Receiver.Chrome", "XA.Receiver.Android", "XA.Receiver.Linux", "XA.Receiver.iOS")`		
Accès Gateway pour la première fois à partir d'une nouvelle adresse IP	Lorsqu'un utilisateur Citrix Gateway se connecte correctement à partir de l'un des éléments suivants Une nouvelle adresse IP publique	Les conditions suivantes sont activées par défaut La première fois pour un nouveau client IP	Citrix Gateway	Utilisateurs compromis

Nom de l'indicateur personnalisé	Scénario	Conditions préconfigurées	Source de données	Catégorie de risque
	Une adresse IP publique existante qui n'a pas été utilisée au cours des 90 derniers jours.	`Event-Type = "Authentication"AND Status-Code = "Successful login"AND Client-IP-Type != "private"AND Access-Insight-Flags = 1`		

Dans la barre de conditions, vous pouvez également ajouter vos propres conditions en plus des conditions préconfigurées pour identifier les menaces en fonction de vos besoins.

Par exemple, si vous souhaitez identifier les événements utilisateur d'un pays particulier, vous pouvez ajouter la dimension pays avec la condition préconfigurée :

- `Event-Type = "Session.Logon"AND Client-Type IN ("XA.Receiver.Windows", "XA.Receiver.Mac", "XA.Receiver.Chrome", "XA.Receiver.Android", "XA.Receiver.Linux", "XA.Receiver.iOS")AND Country = “United States”`
- `Event-Type = "Authentication"AND Status-Code = "Successful login" AND Client-IP-Type != "private"AND Access-Insight-Flags = 1 AND Country = “United States”`

Paramètres de messagerie de l'utilisateur final

December 7, 2023

Les paramètres de courrier électronique de l'utilisateur final contrôlent le modèle d'e-mail associé à l'action globale Demander une réponse de l'utilisateur final. Vous appliquez cette action pour obtenir

une réponse des utilisateurs pour toute activité inhabituelle détectée sur leur compte. Les utilisateurs répondent par le biais des e-mails qu'ils reçoivent de Citrix Analytics for Security.

Vous pouvez utiliser les paramètres de messagerie pour :

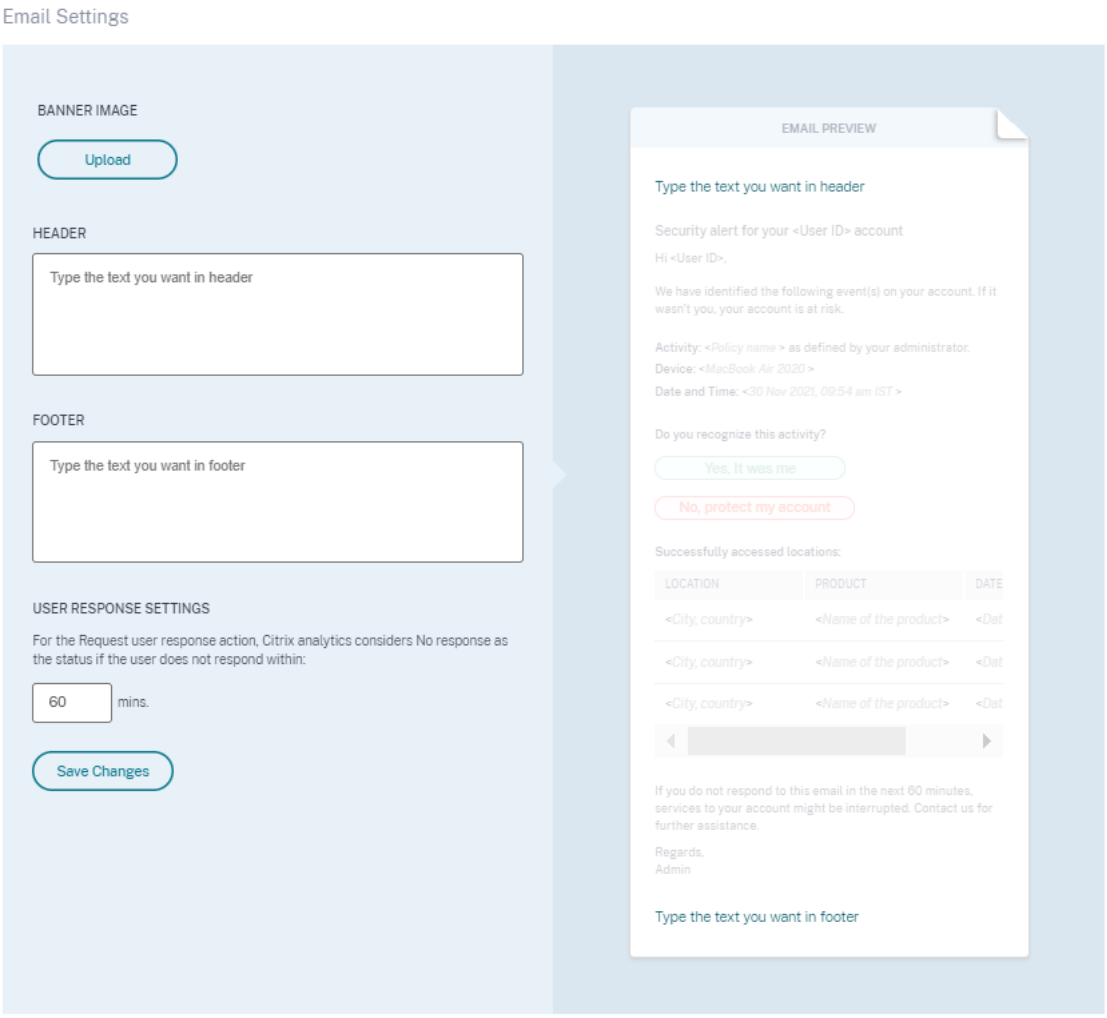
- Ajoutez une bannière, un texte d'en-tête et un texte de pied de page appropriés pour attirer l'attention de l'utilisateur et obtenir sa réponse. Cela donne également à votre e-mail un aspect plus légitime.
- Ajoutez la durée (en minutes) pendant laquelle l'utilisateur doit répondre à votre e-mail. Si l'utilisateur ne répond pas dans le délai de réponse, Citrix Analytics applique l'action spécifiée à l'utilisateur.

Modifier les paramètres d'e-mail

Pour modifier les paramètres d'e-mail :

1. Dans la barre supérieure, cliquez sur **Paramètres > Paramètres d'alerte > Paramètres de messagerie de l'utilisateur final**.

2. Cliquez sur Modifier pour télécharger ou parcourir une image de bannière. Lorsque vous téléchargez un fichier image, assurez-vous que l'image répond aux exigences suivantes :
   - Formats pris en charge : JPEG ou PNG
   - Dimensions maximales : 400* 100 pixels
   - Taille de fichier maximale : 5 Mo
3. Saisissez vos textes dans les champs **EN-TÊTE** et **PIED** DE PAGE. Ces champs sont facultatifs.
4. Entrez l'heure dans les paramètres de réponse de l'utilisateur.
5. Prévisualisez l'e-mail et cliquez sur **Enregistrer les modifications**.



Paramètres de messagerie de l'administrateur

December 7, 2023

La page **Paramètres de messagerie de l'administrateur** vous permet de configurer les destinataires de la liste de distribution personnalisée pour les alertes système. Cela garantit que les administrateurs reçoivent des alertes système qui leur sont utiles.

La fonctionnalité **Paramètres de messagerie de l'administrateur** offre les fonctionnalités suivantes :

Consultez les alertes système, les listes de distribution par e-mail qui reçoivent l'alerte, le dernier utilisateur qui a modifié les paramètres de l'alerte et la dernière date à laquelle l'alerte a été modifiée. Modifiez les paramètres d'alerte. Modifiez la liste de distribution cible pour différentes alertes sys-

tème.

Modifier les paramètres d'alerte

Pour modifier les paramètres d'alerte, procédez comme suit :

1. Dans la barre supérieure, cliquez sur **Paramètres > Paramètres d'alerte > Paramètres de messagerie de l'administrateur**.

2. Cliquez sur l'alerte dont vous souhaitez modifier la liste de diffusion par e-mail.
3. Sélectionnez les listes de distribution qui doivent recevoir l'alerte dans la **liste déroulante Choisissez la liste de distribution par e-mail** .
   Vous pouvez également créer votre propre liste de distribution en cliquant sur **Créer une liste de distribution par e-mail**. Pour plus d'informations, voir Création d'une liste de distribution par e-mail.
4. Cliquez sur **Enregistrer**.

Watchlist

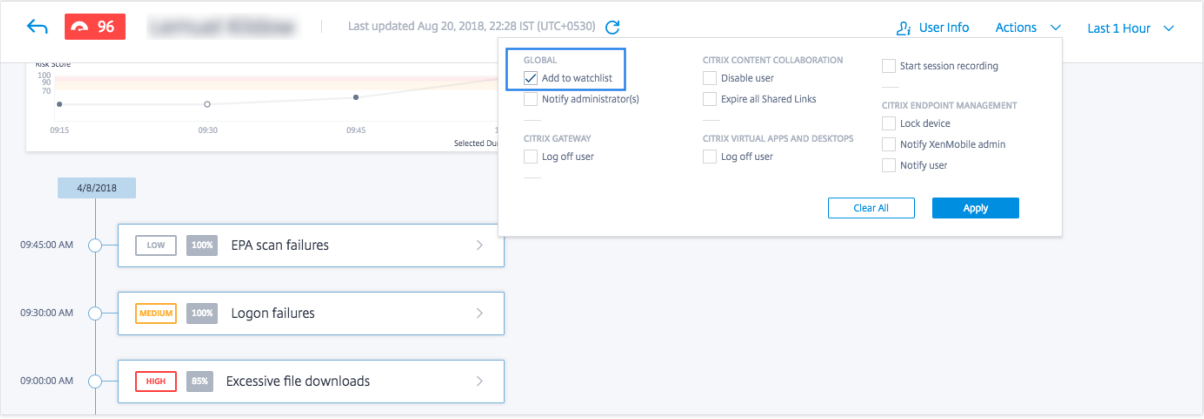
February 13, 2023

Utilisez des listes de surveillance pour surveiller l'activité de certains utilisateurs afin de détecter d'éventuelles menaces. Par exemple, vous pouvez surveiller les utilisateurs qui ne sont pas des employés à plein temps de votre organisation ou ceux qui déclenchent fréquemment un indicateur de risque spécifique.

Comment ajouter un utilisateur à la liste de suivi

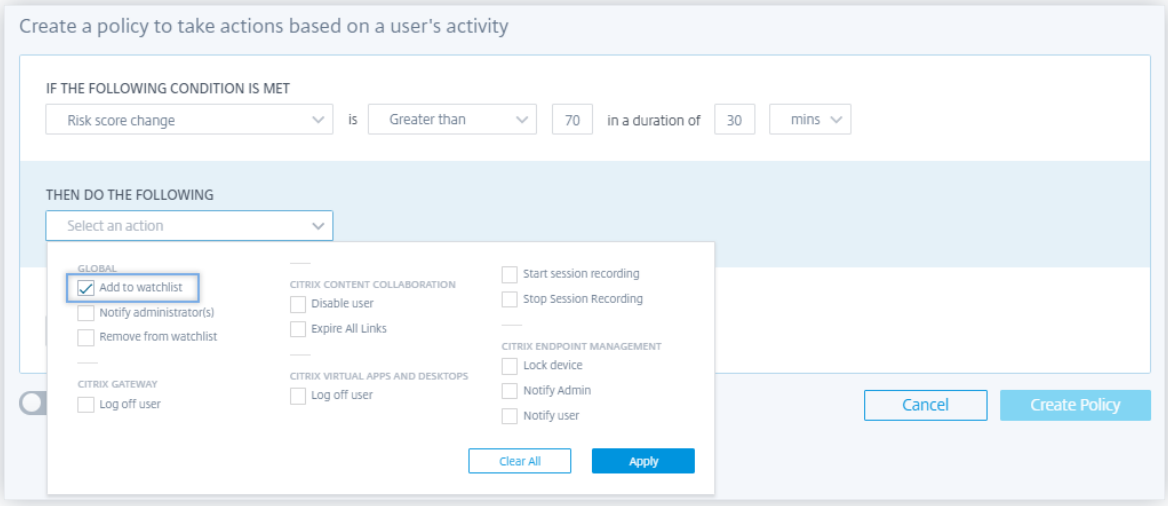
Vous pouvez soit ajouter un utilisateur à la liste de surveillance manuellement, soit définir des politiques qui, lorsqu'elles sont déclenchées, ajoutent un utilisateur à la liste de surveillance.

Pour ajouter manuellement un utilisateur à la liste de surveillance, accédez au profil de l'utilisateur dans la chronologie des risques. Ensuite, dans le menu **Actions**, sélectionnez **Ajouter à la liste de suivi**. Cliquez sur **Appliquer** et suivez les instructions pour appliquer l'action.



Pour ajouter un utilisateur à la liste de surveillance à l'aide de politiques, créez une politique avec un ensemble de conditions qui doivent être remplies. Sélectionnez l'action **Ajouter à la liste** de suivi. Lorsque les conditions sont remplies, l'utilisateur est ajouté à la liste de suivi. Par exemple, vous souhaiterez peut-être ajouter un utilisateur à la liste de surveillance si la modification de son score de risque est supérieure à 70 en 30 minutes.

Pour plus d'informations sur la création de politiques, voir Configurer des stratégies et des actions.

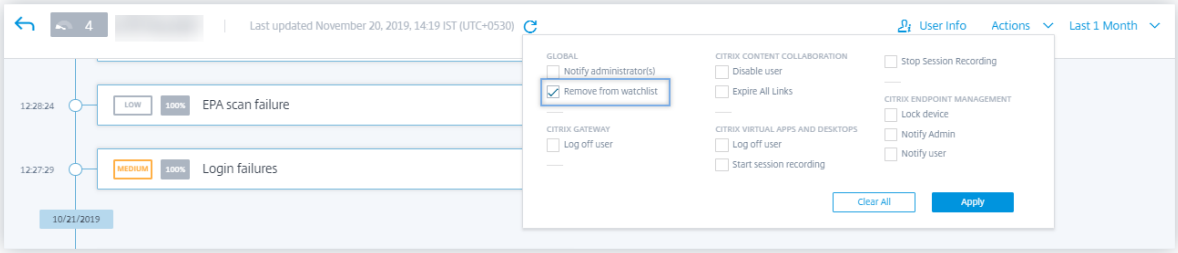


Comment supprimer un utilisateur de la liste de suivi

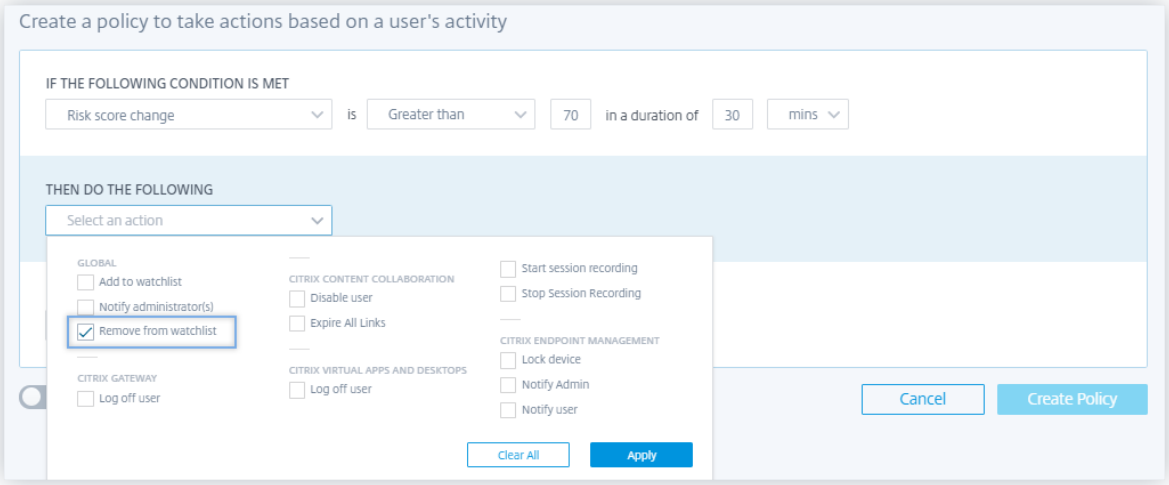
Vous pouvez soit supprimer un utilisateur de la liste de surveillance manuellement, soit définir des politiques qui, lorsqu'elles sont déclenchées, suppriment un utilisateur de la liste de surveillance.

Pour supprimer manuellement un utilisateur de la liste de surveillance, accédez au profil de l'utilisateur dans la chronologie des risques. Ensuite, dans le menu **Actions**, sélectionnez **Supprimer de la liste de suivi**. Cliquez sur **Appliquer** et suivez les instructions pour appliquer l'action.

> **Remarque**
>
> Lorsqu'un utilisateur figure sur la liste de suivi et que vous souhaitez le supprimer, l'option **Supprimer de la liste de suivi** apparaît dans le menu **Actions** .



Pour supprimer un utilisateur de la liste de surveillance à l'aide de politiques, créez une politique avec un ensemble de conditions qui doivent être remplies. Sélectionnez l'action **Supprimer de la liste** de suivi. Lorsque les conditions sont remplies, l'utilisateur est supprimé de la liste de suivi. Par exemple, vous souhaiterez peut-être supprimer un utilisateur de la liste de surveillance si la modification de son score de risque est inférieure à 70 en 60 minutes. Pour en savoir plus sur la création de politiques, voir Configurer des politiques et des actions.



Comment surveiller les utilisateurs dans une liste de suivi

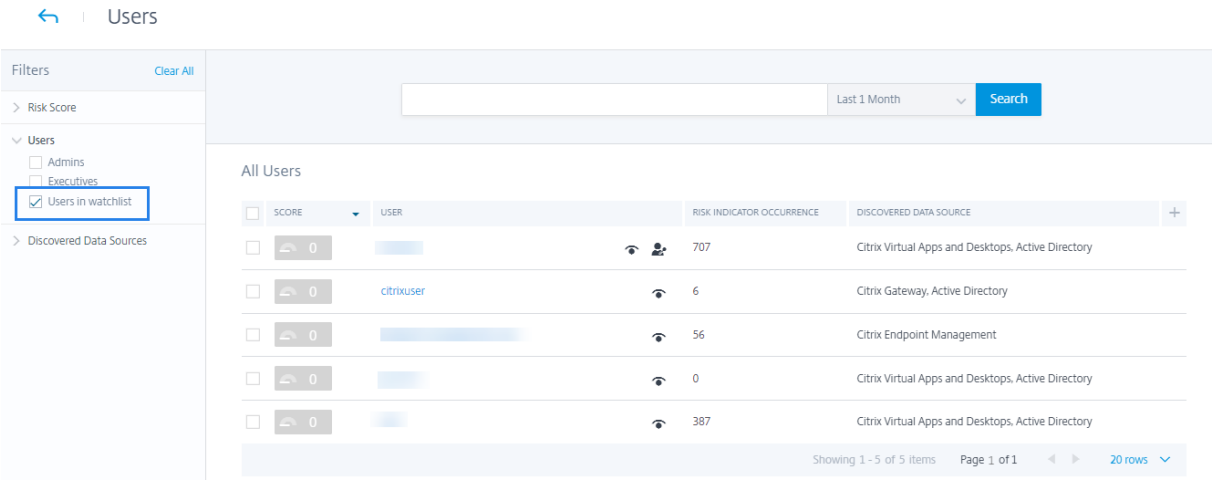
Dans le tableau de bord **Sécurité > Utilisateurs**, consultez les informations suivantes :

- Résumé du nombre d'utilisateurs figurant dans la liste de surveillance au cours des 13 derniers mois. Cliquez sur la case pour afficher la liste de tous les utilisateurs de la liste de surveillance **dans le volet Utilisateurs de la liste de surveillance** .

- Les cinq principaux utilisateurs de la liste de surveillance sont répertoriés en fonction du score de risque. Dans le volet **Utilisateurs dans la liste de surveillance**, consultez le score de risque et les occurrences des indicateurs de risque ainsi que le nom de l'utilisateur. Cliquez sur **Afficher plus** pour afficher la liste de tous les utilisateurs figurant dans la liste de suivi sur la page **Utilisateurs** .
- Les utilisateurs les plus risqués figurant sur la liste de surveillance. Dans le volet **Utilisateurs à risque**, l'icône en forme d'œil située à côté d'un utilisateur indique que celui-ci figure dans la liste de suivi.

Sur la page **Utilisateurs**, consultez la liste de tous les utilisateurs figurant dans la liste de suivi. Affichez des détails tels que le score de risque, le nombre d'indicateurs de risque déclenchés et les sources de données associées à un utilisateur.

Utilisez le champ de recherche pour trouver les utilisateurs et les détails de leurs événements. Sélectionnez la période pour afficher les occurrences des indicateurs de risque pour la période spécifique.



Notification hebdomadaire par e-mail

December 7, 2023

Citrix Analytics envoie des notifications hebdomadaires par e-mail résumant les risques de sécurité auxquels est exposée l'infrastructure informatique de votre entreprise. La notification hebdomadaire vous tient au courant des événements risqués et de leur survenance au cours de la semaine précédente. Vous pouvez savoir si des événements nécessitent votre attention ou des actions sans vous connecter à Citrix Analytics. Ces informations vous tiennent au courant de ce qui se passe dans votre domaine de sécurité informatique.

Activer les notifications par e-mail

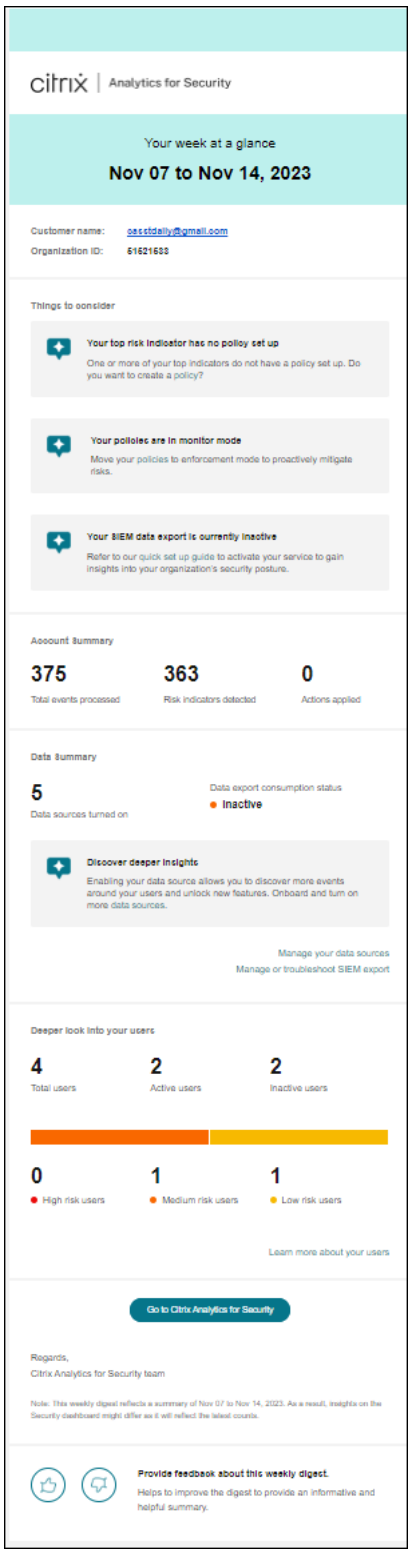
- Si vous êtes administrateur Citrix Cloud et que vous disposez d'une autorisation d'accès complète ou personnalisée, les notifications par e-mail sont désactivées par défaut sur votre compte Citrix Cloud. Pour recevoir des notifications par e-mail de la part de tout service Citrix Cloud tel que Citrix Analytics, activez l'option de notification dans votre Citrix Cloud. Pour plus d'informations, consultez la section Recevoir des notifications par e-mail. Les préférences de notification ne sont pas disponibles pour les administrateurs ajoutés via Active Directory/Azure AD Groups.
- Par défaut, les notifications par e-mail sont envoyées à la liste par défaut des administrateurs de sécurité Citrix. Vous pouvez modifier cela en configurant les destinataires de la liste de distribution personnalisée pour les alertes hebdomadaires. Pour plus d'informations, consultez la section Paramètres de messagerie de l'administrateur.

Quand recevrez-vous un e-mail de Citrix Analytics ?

Chaque mardi, une notification par e-mail vous est envoyée depuis Citrix Cloud donotreplynotifications@citrix.com.

La notification par e-mail fournit les informations suivantes :

- Résumé du nombre total d'événements traités, des indicateurs de risque détectés et des actions appliquées
- Résumé du nombre total de sources de données actives et de l'état de consommation des données exportées
- Les trois principaux indicateurs de risque
- Les trois principales mesures prises en fonction des indicateurs de risque
- Nombre total d'utilisateurs actifs et nombre total d'utilisateurs à risque
- Tous les événements ou actions qui requièrent votre attention

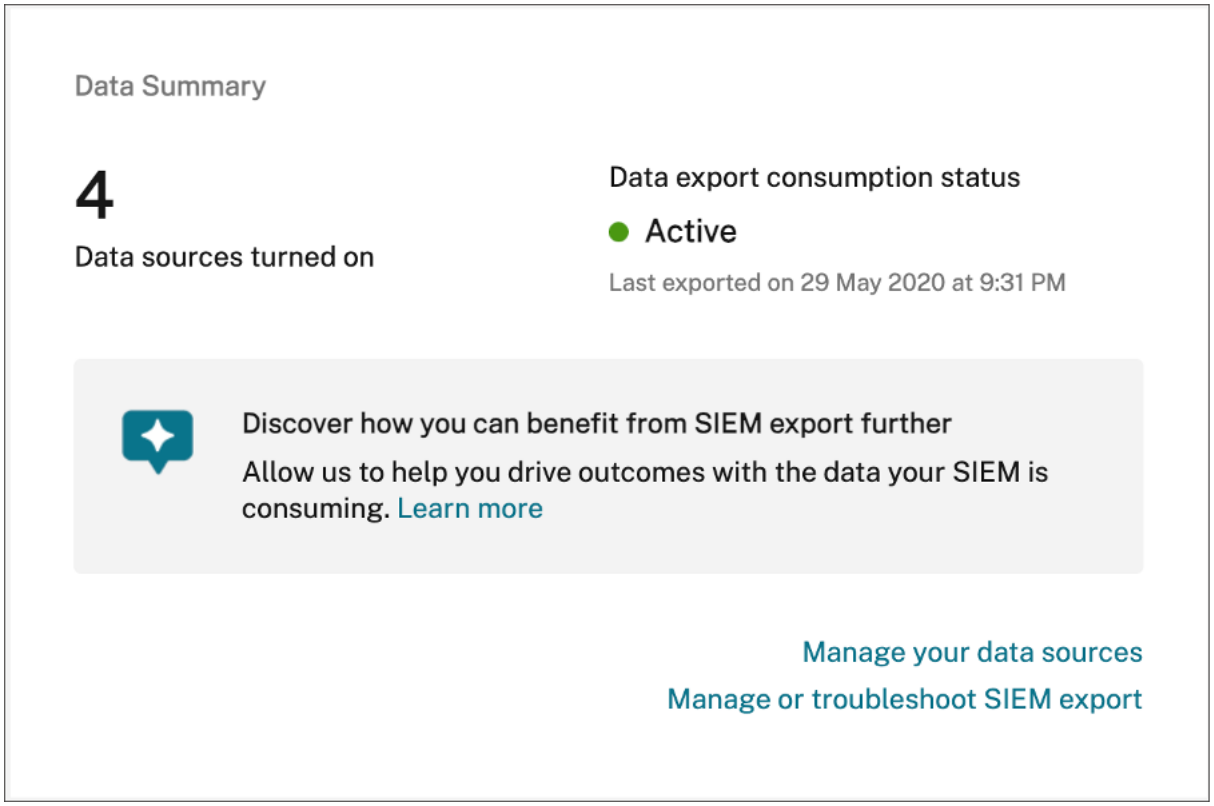


Récapitulatif du compte

L'e-mail hebdomadaire fournit un résumé du nombre total d'événements traités, des indicateurs de risque détectés et des actions appliquées.

Résumé des données

L'e-mail hebdomadaire fournit également des informations sur les sources de données qui ont été activées ainsi que sur l'état de consommation des exportations de données.



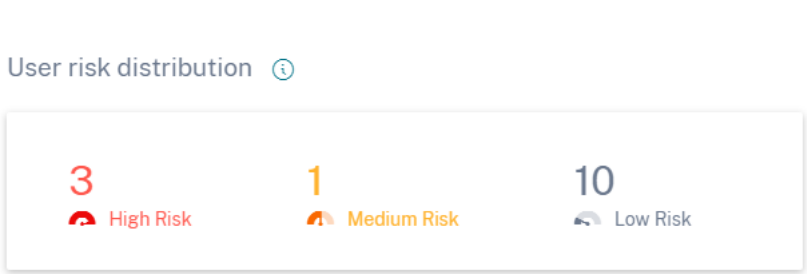
Cliquez sur **Gérer vos sources de données** dans l'e-mail pour afficher la page **Sources de données** dans Citrix Analytics. Vous pouvez intégrer la source de données et activer le traitement des données pour permettre à Citrix Analytics d'autoriser le traitement des données. Pour plus d'informations sur l'activation des analyses, consultez la section Activer les analyses sur les sources de données.

Cliquez sur **Gérer ou résoudre les problèmes liés à l'exportation SIEM** pour afficher la page Exportations de données dans Citrix Analytics afin de résoudre les problèmes liés à votre environnement et de gérer vos paramètres d'exportation de données.

Informations sur les utilisateurs

L'e-mail hebdomadaire donne un aperçu du nombre total d'utilisateurs et d'utilisateurs qui ont agi de manière risquée.

- **Nombre d'utilisateurs à haut risque** : identifiés en rouge. Ils constituent une menace immédiate pour l'organisation.
- **Numéro de risque moyen** —Identifié en orange. Ils ont enregistré plusieurs violations graves sur leur compte au cours de la semaine sélectionnée et doivent être surveillés de près.
- **Nombre d'utilisateurs à faible risque** : identifiés en jaune. Ils ont commis quelques violations graves, mais elles ne sont potentiellement pas considérées comme une menace.

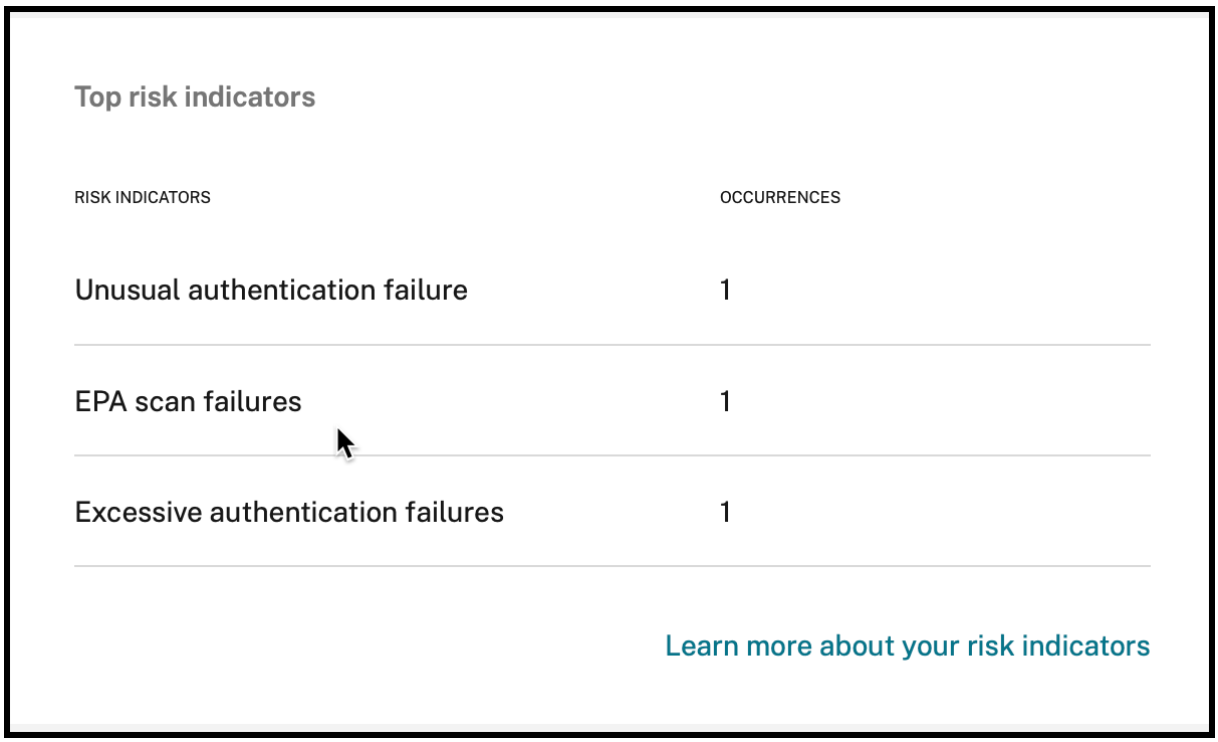


Pour plus d'informations, consultez la section Utilisateurs à risque.

Cliquez sur **En savoir plus sur vos utilisateurs** pour afficher la page **Utilisateurs à risque** dans Citrix Analytics. Vous pouvez obtenir des informations plus détaillées sur les utilisateurs actifs et la catégorisation des risques.

Principaux indicateurs de risque

L'e-mail hebdomadaire fournit des informations sur les trois principaux indicateurs de risque et le nombre d'occurrences pour la semaine sélectionnée. En fonction du nombre d'occurrences, les indicateurs de risque par défaut et personnalisés pour la semaine sélectionnée s'affichent.

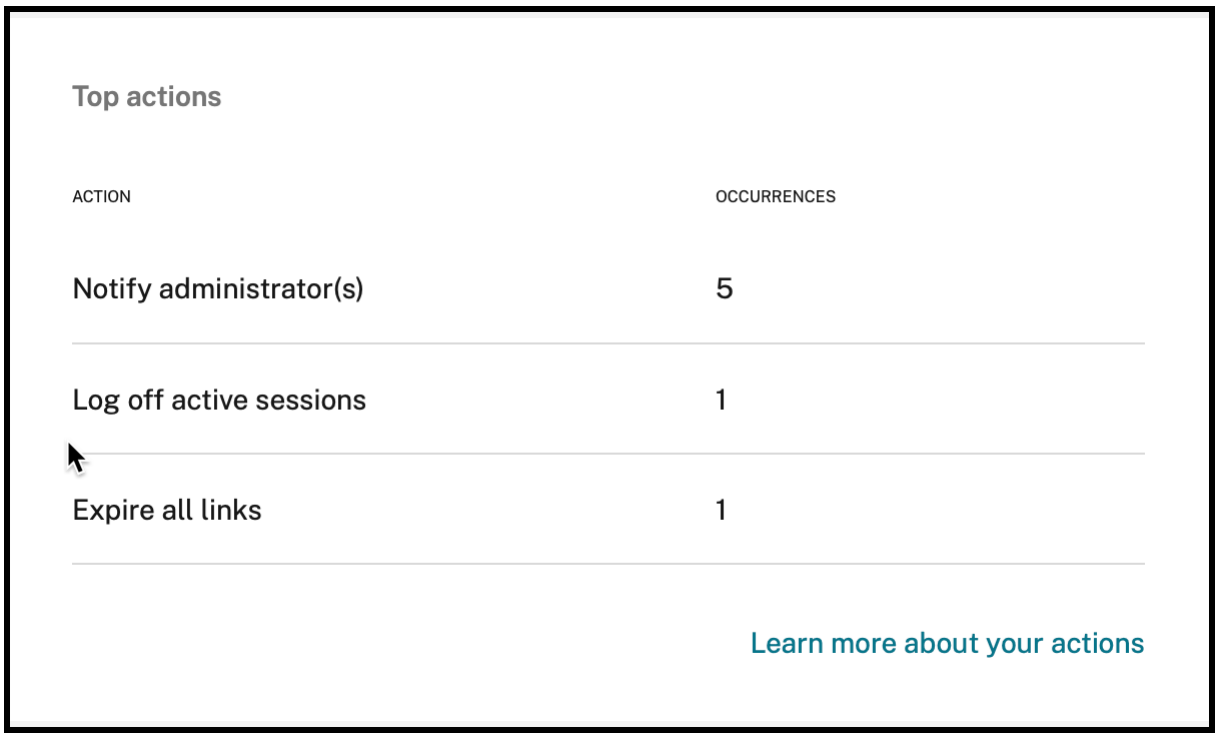


Pour plus d'informations, consultez la section Indicateurs de risque.

Cliquez sur **En savoir plus sur vos indicateurs de risque** dans l'e-mail pour consulter la page de **présentation des indicateurs de risque** dans Citrix Analytics.

Principales actions

L'e-mail hebdomadaire fournit des informations sur les trois principales mesures prises en réponse aux menaces suspectes et anormales survenues la semaine dernière. En fonction du nombre d'occurrences, les actions globales et les actions Citrix Gateway pour la semaine sélectionnée sont affichées.



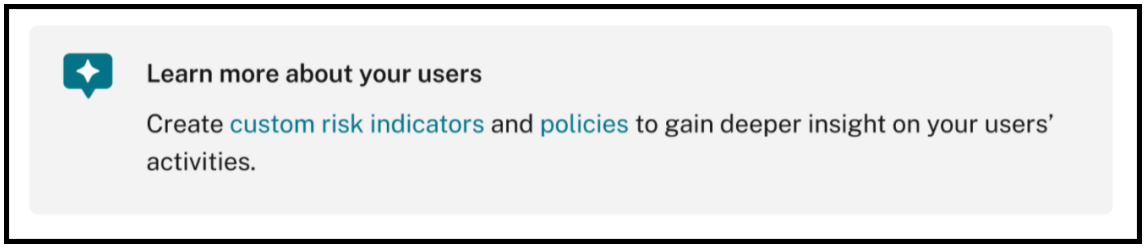
Pour plus d'informations sur les actions et la configuration d'une action, consultez la section Stratégies et actions.

Cliquez sur **En savoir plus sur vos actions** dans l'e-mail pour afficher la page **des principales actions** dans Citrix Analytics.

Quelles mesures devez-vous prendre après avoir reçu l'e-mail ?

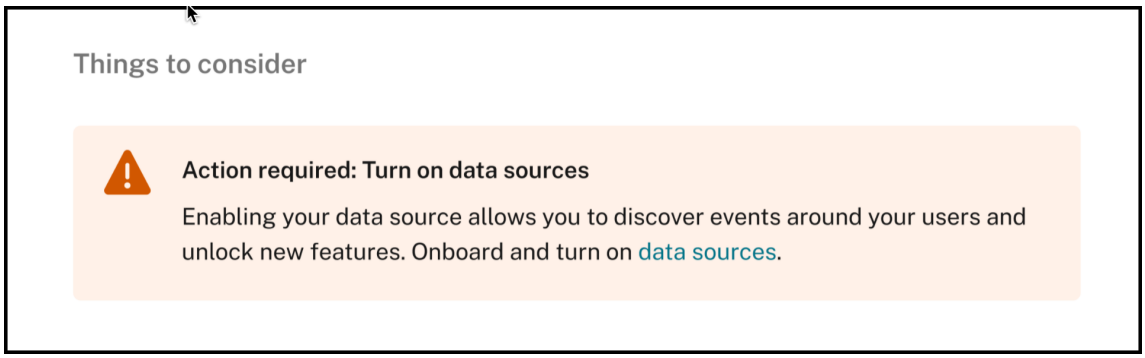
Les e-mails hebdomadaires vous permettent de savoir si des événements ou des actions requièrent votre attention.

- Si aucun indicateur de risque n'est détecté pour la semaine, le message suivant vous invite à créer d'autres indicateurs de risque personnalisés.

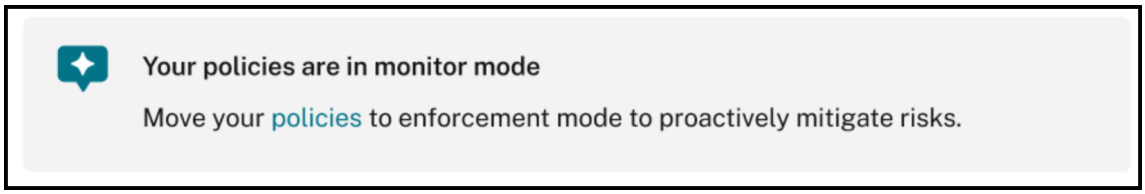


Vous pouvez vous connecter à Citrix Analytics pour créer davantage d'indicateurs de risque personnalisés.

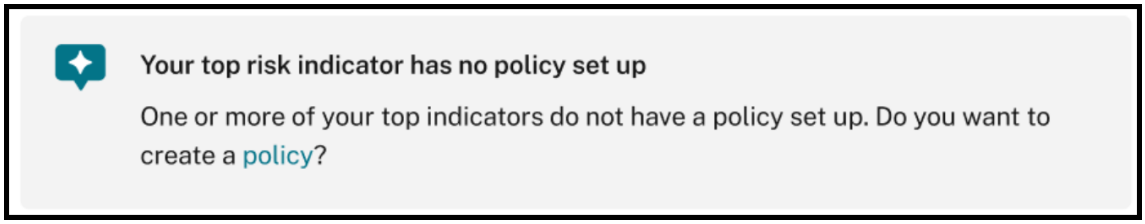
- Si aucune des sources de données n'est activée dans Security Analytics, le message suivant s'affiche qui vous invite à activer le traitement des données pour les sources de données.



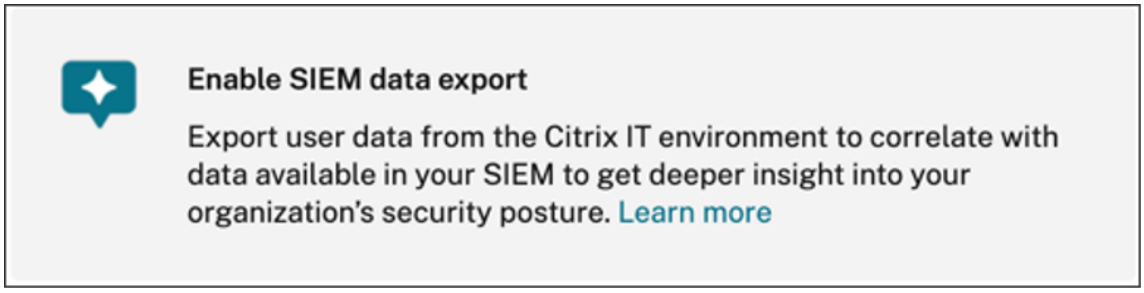
- Si aucune des stratégies n'est en mode surveillance, le message suivant s'affiche, qui vous invite à faire passer les stratégies en mode d'application.



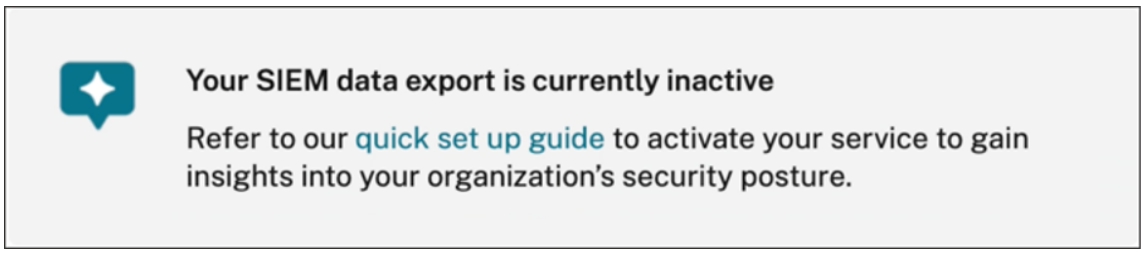
- Si aucune stratégie n'est définie pour l'un des trois principaux indicateurs de risque de la semaine, le message suivant vous invite à créer une stratégie.



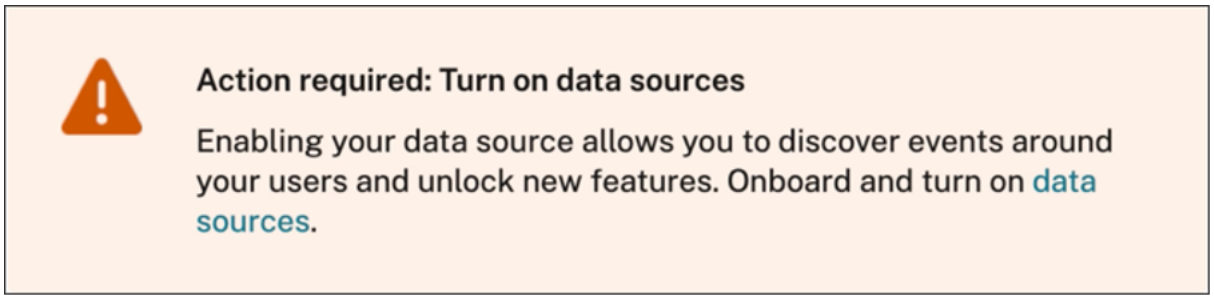
- Si vous n'avez pas activé les **exportations de données** pour votre client Citrix Analytics, les recommandations suivantes vous indiquent plus de détails sur nos options d'**exportation de données** qui vous permettent d'exporter vos données Citrix vers un environnement SIEM.



- Si le statut de consommation d'exportation de données est inactif, le message suivant vous invite à activer votre service.



> **Remarque**
>
> La transmission de données n'est activée que lorsque le traitement des données est activé pour au moins une source de données. Si le traitement des données est désactivé pour toutes les sources de données, le message d'avertissement suivant s'affiche pour activer votre source de données.



Journaux d'audit

February 22, 2021

Un journal d'audit décrit les informations d'audit relatives aux événements générés sur Citrix Analytics. Il peut s'agir d'événements système tels que des erreurs, ou d'une piste d'audit des actions de configuration effectuées par l'administrateur Citrix Analytics.

Chaque fois qu'une configuration est ajoutée, supprimée ou mise à jour, les informations d'événement sont écrites dans le journal d'audit. Ces informations concernent ce qui a été modifié, le moment où il a été modifié et les personnes qui l'ont modifié.

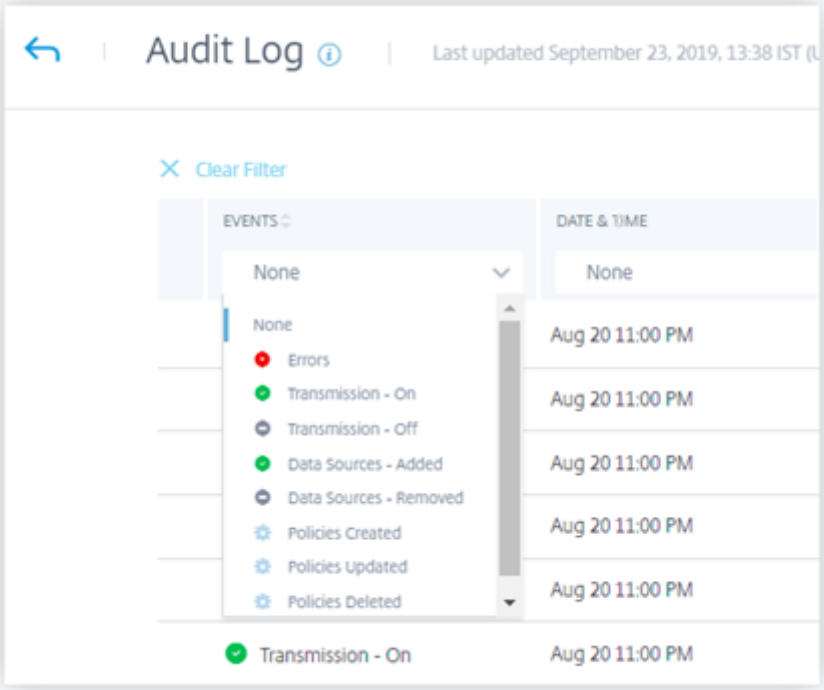
Vous pouvez afficher les informations du journal d'audit des trois derniers mois.

Activités qui génèrent des événements d'audit

Les événements suivants sont enregistrés sur Citrix Analytics :

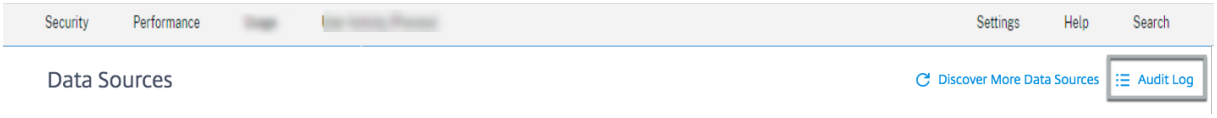
- Erreurs générées

- Transmission activée
- Transmission désactivée
- Sources de données ajoutées
- Sources de données supprimées
- Stratégies créées
- Politiques mises à jour
- Stratégies supprimées



Comment afficher le journal d'audit

Pour afficher les journaux d'audit, connectez-vous à Citrix Analytics. Accédez à **Paramètres > Sources de données**. Dans la page **Sources de données**, cliquez sur **Journal d'audit** dans le coin supérieur droit.

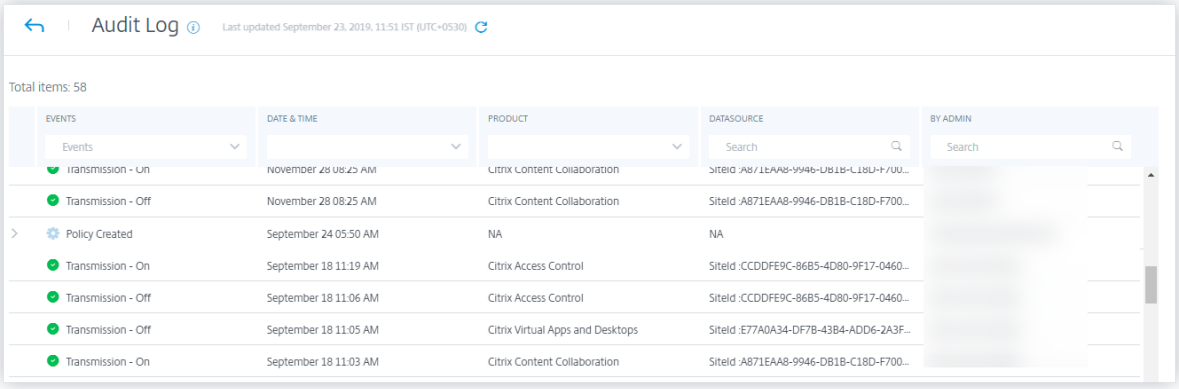


Comment utiliser le journal d'audit

Vous pouvez utiliser le journal d'audit pour consulter et connaître tout événement sur Citrix Analytics. Actualisez la page **Journal d'audit** pour récupérer les dernières données d'audit. La page affiche la date et l'heure de la dernière mise à jour des données d'audit.

Vous pouvez afficher les informations d'audit suivantes sur la page **Journal d'audit** . Vous pouvez également filtrer les données d'audit en fonction de ces champs.

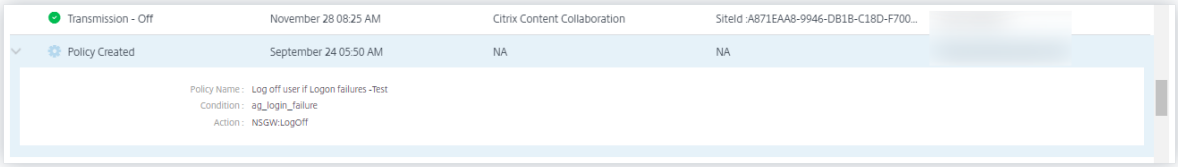
- **Événements**. Les événements peuvent être générés par le système ou des configurations appliquées par l'administrateur sur Citrix Analytics. Les événements peuvent également représenter des erreurs telles que l'échec d'application d'actions ou une source de données. Par défaut, les journaux de tous les événements sont affichés. Vous pouvez filtrer en fonction du type d'événement que vous souhaitez afficher.
- **Date et heure**. Les données et l'heure à laquelle l'événement s'est produit. Vous pouvez filtrer en fonction de la période pour laquelle vous souhaitez afficher le journal. Vous pouvez afficher les événements pour le jour en cours, les sept derniers jours, les 15 derniers jours, le mois dernier et les trois derniers mois.
- **Produit**. Produit pour lequel l'événement a été généré. Les événements sont générés sur le produit et agrégés sur Citrix Analytics où ils sont affichés. Vous pouvez filtrer le journal en fonction d'un ou plusieurs produits.
- **Source de données**. Nom de l'instance de produit associée à l'entrée d'audit. Vous pouvez rechercher n'importe quelle source de données spécifique pour afficher ses données d'audit.
- **Par Admin**. Administrateur Citrix Analytics qui a effectué les activités d'administration. Vous pouvez rechercher les activités effectuées par n'importe quel administrateur spécifique.



Si votre événement enregistré était basé sur une stratégie, vous pouvez cliquer sur l'icône de flèche pour afficher plus de détails tels que :

- Nom de la stratégie

- La condition spécifiée
- L'action résultante



Rapports personnalisés

June 18, 2024

Vous pouvez créer et planifier des rapports personnalisés à l'aide des événements et des informations disponibles dans Citrix Analytics for Security. Les rapports personnalisés vous aident à extraire des informations présentant un intérêt spécifique et à organiser les données graphiquement. Il permet d'analyser la sécurité de la source de données de votre choix au fil du temps.

Les rapports personnalisés prennent en charge les sources de données suivantes :

- Applications et bureaux
- Gateway
- Secure Private Access
- Secure Browser
- Stratégies
- Indicateurs de risque
- Score de risque

Champs pris en charge dans les rapports personnalisés

Certaines sources de données sont également disponibles dans la recherche en libre-service. Pour afficher ces types d'événements et les champs pris en charge, cliquez sur les sources de données suivantes.

- Applications et bureaux
- Gateway
- Secure Private Access
- Secure Browser
- Stratégies

Les sources de données suivantes ne sont disponibles que dans les rapports personnalisés. Le tableau suivant répertorie les champs pris en charge dans les rapports personnalisés pour les sources de données suivantes :

- Indicateurs de risque
- Score de risque

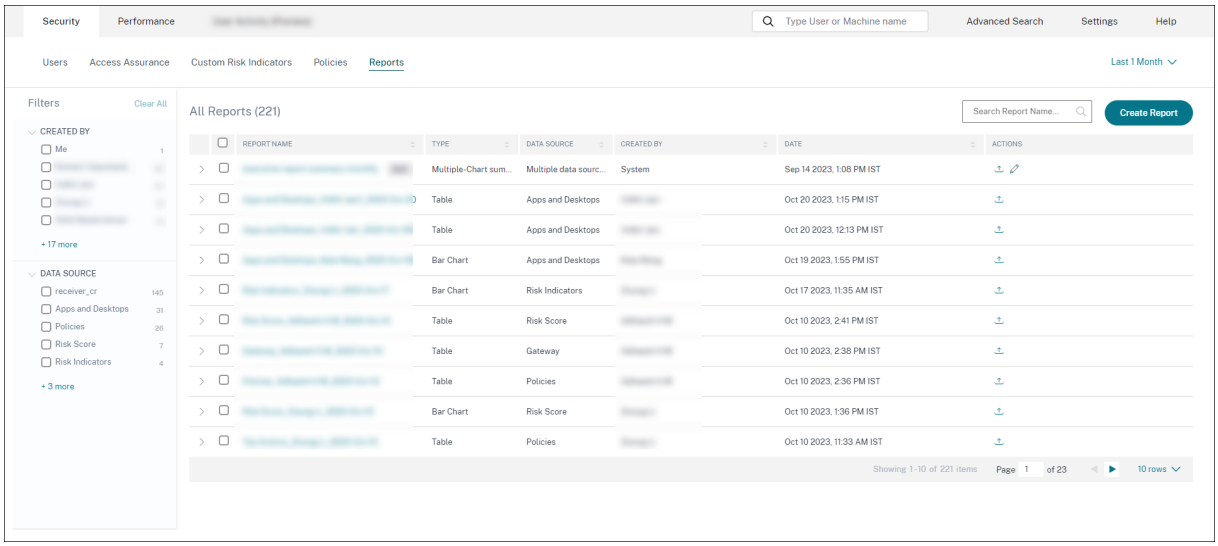
Source de données	Dimension	Description
Indicateurs de risque	Catégorie	Indique la catégorie des indicateurs de risque. Les indicateurs de risque sont regroupés dans l'une des quatre catégories suivantes : terminaux compromis, utilisateurs compromis, exfiltration de données ou menaces internes.
	Nom de l'indicateur de risque	Le nom de l'indicateur de risque. Pour un indicateur de risque personnalisé, le nom est défini par l'administrateur lors de la création de l'indicateur.
	Gravité	Indique la gravité du risque. Il peut être faible, moyen ou élevé.
	Nom d'utilisateur	Le nom d'utilisateur ou domaine\nom d'utilisateur utilisé pour la connexion.
Score de risque	Score de risque	Le score de risque attribué à l'utilisateur. Le score de risque varie de 0 à 100 en fonction de la gravité de la menace associée à l'activité de l'utilisateur.
	Nom d'utilisateur	Le nom d'utilisateur ou domaine\nom d'utilisateur utilisé pour la connexion.

Source de données	Dimension	Description
	Catégorie de score de risque	Sur la base du score de risque, un utilisateur à risque peut appartenir à l'une des catégories suivantes : risque élevé, risque moyen et risque faible.

Rapports

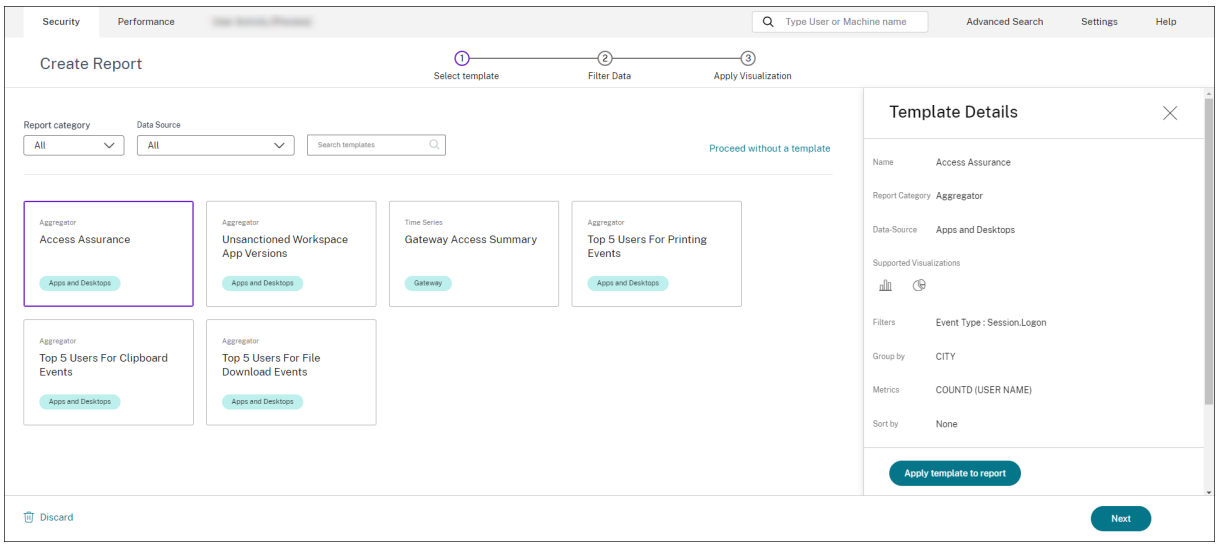
Vous pouvez effectuer les actions suivantes sur les rapports à l'aide de cette vue :

- Cliquez sur **Créer un rapport** pour créer un rapport personnalisé.
- Agrandissez une ligne pour afficher l'aperçu d'un rapport personnalisé existant.
- Cliquez sur le nom du rapport pour voir la visualisation détaillée du rapport.
- Cliquez sur l'icône d'exportation pour exporter un rapport personnalisé existant au format PDF.
- Cliquez sur l'icône de modification pour modifier les rapports que vous avez créés.
- Cliquez sur l'icône de suppression pour supprimer les rapports que vous avez créés.



Création d'un rapport personnalisé

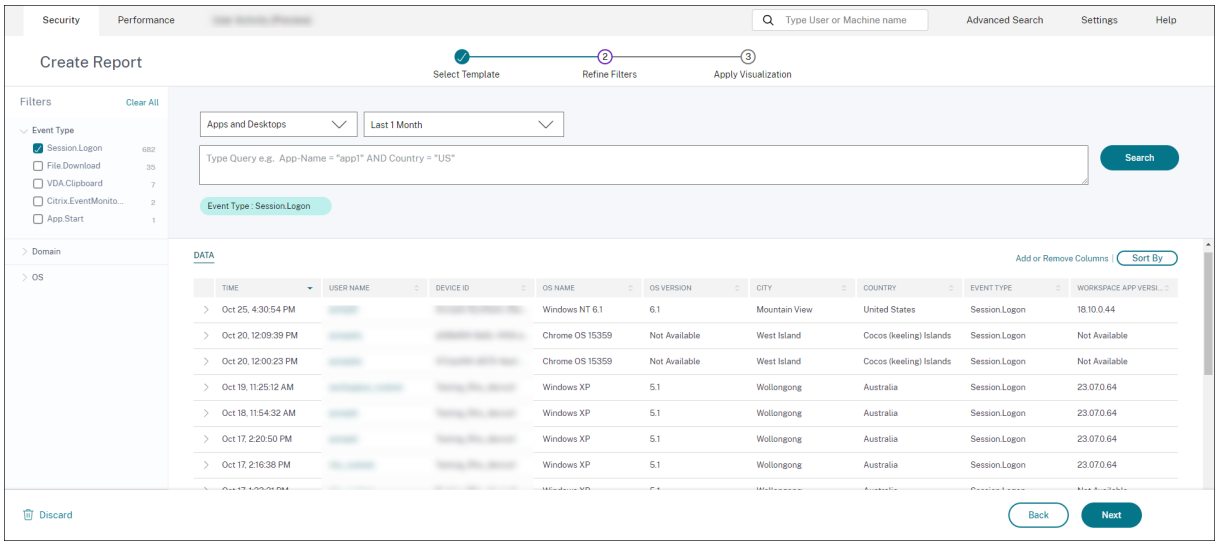
Pour créer un rapport personnalisé, cliquez sur **Créer des rapports**. Sur la page **Créer un rapport**, vous pouvez choisir de créer un rapport personnalisé avec ou sans modèles.



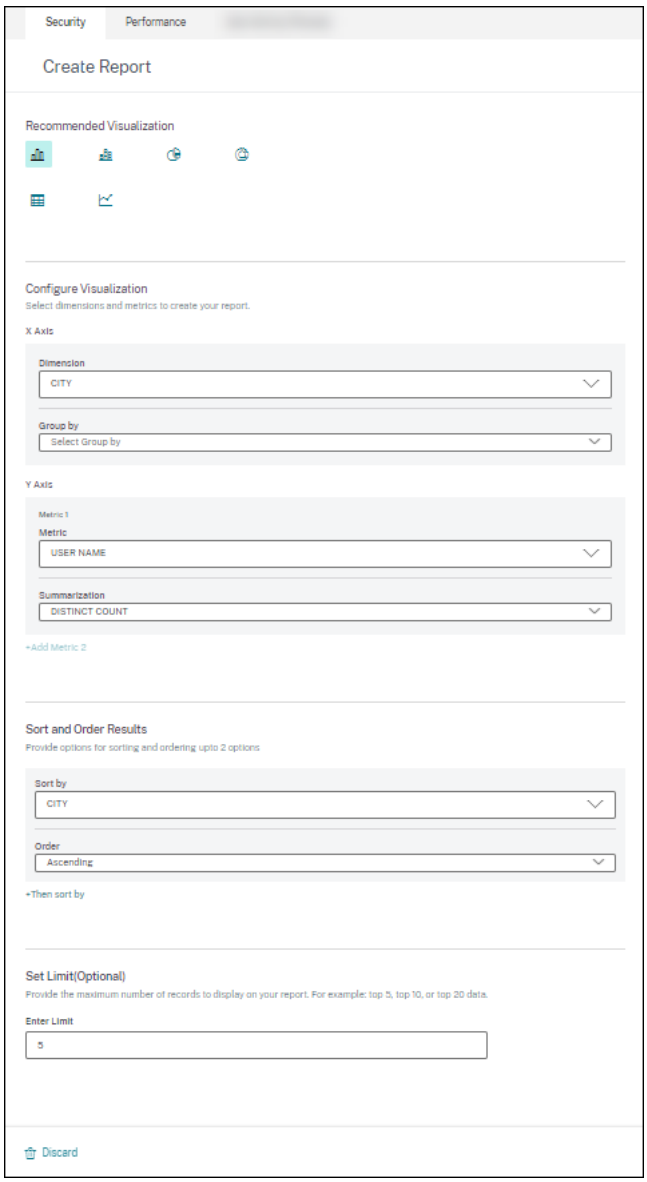
Création d'un rapport personnalisé à l'aide de modèles

Pour créer un rapport personnalisé à l'aide d'un modèle :

1. **Sélectionnez un modèle** : une fois que vous avez cliqué sur un modèle, les détails du modèle sont répertoriés sur la droite. Cliquez sur **Appliquer le modèle au rapport** pour permettre au rapport d'utiliser le modèle sélectionné.
2. **Affiner les filtres** : la page **Affiner les filtres** affiche les filtres prédéfinis pour le modèle que vous avez sélectionné. Apportez les modifications nécessaires, puis cliquez sur **Suivant**.



1. **Appliquer la visualisation** : sélectionnez l'une des visualisations disponibles pour afficher le rapport.

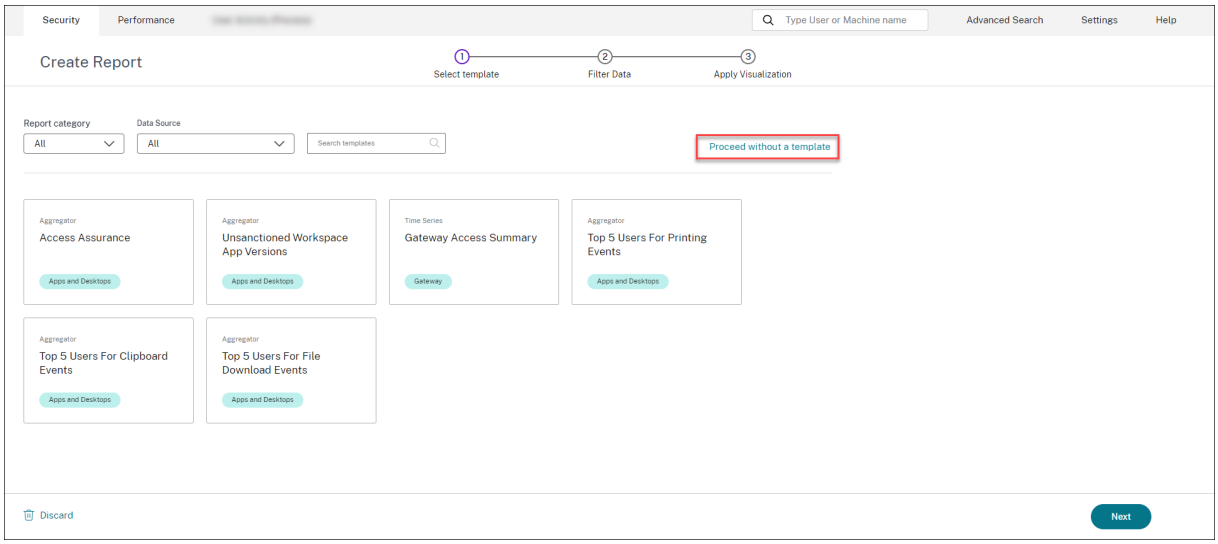


- **Diagramme à barres** : présente les données avec des barres rectangulaires verticales dont la hauteur est proportionnelle aux valeurs. Utilisé pour comparer des événements.
- **Graphique à colonnes empilées** : présente les données sous forme de barres empilées les unes sur les autres. Utilisé pour visualiser la somme totale des données sur plusieurs sous-catégories.
- **Diagramme à secteurs** : présente les données sous la forme d'un diagramme circulaire. Utilisé pour visualiser la taille relative des données ou des pourcentages.
- **Diagramme en anneau** : présente les données sous la forme d'un anneau. Utilisé pour visualiser la taille relative des données ou des pourcentages. - **Tableau** : présente les données sous forme de tableau. Utilisé pour visualiser autant de dimensions que nécessaire.
- **Graphique linéaire** : présente les données sous forme de points reliés par des segments de ligne droite. Utilisé pour visualiser les tendances des données sur une période donnée.

1. Configurez maintenant la visualisation avec les paramètres suivants :
    - Dimension pour l'axe X
    - Métriques à tracer sur l'axe Y
    - Synthèse ou agrégations, telles que la moyenne ou le nombre, à appliquer à la métrique
    - Options de tri et de commande
    - Limite facultative du nombre maximum d'enregistrements à afficher dans le rapport.

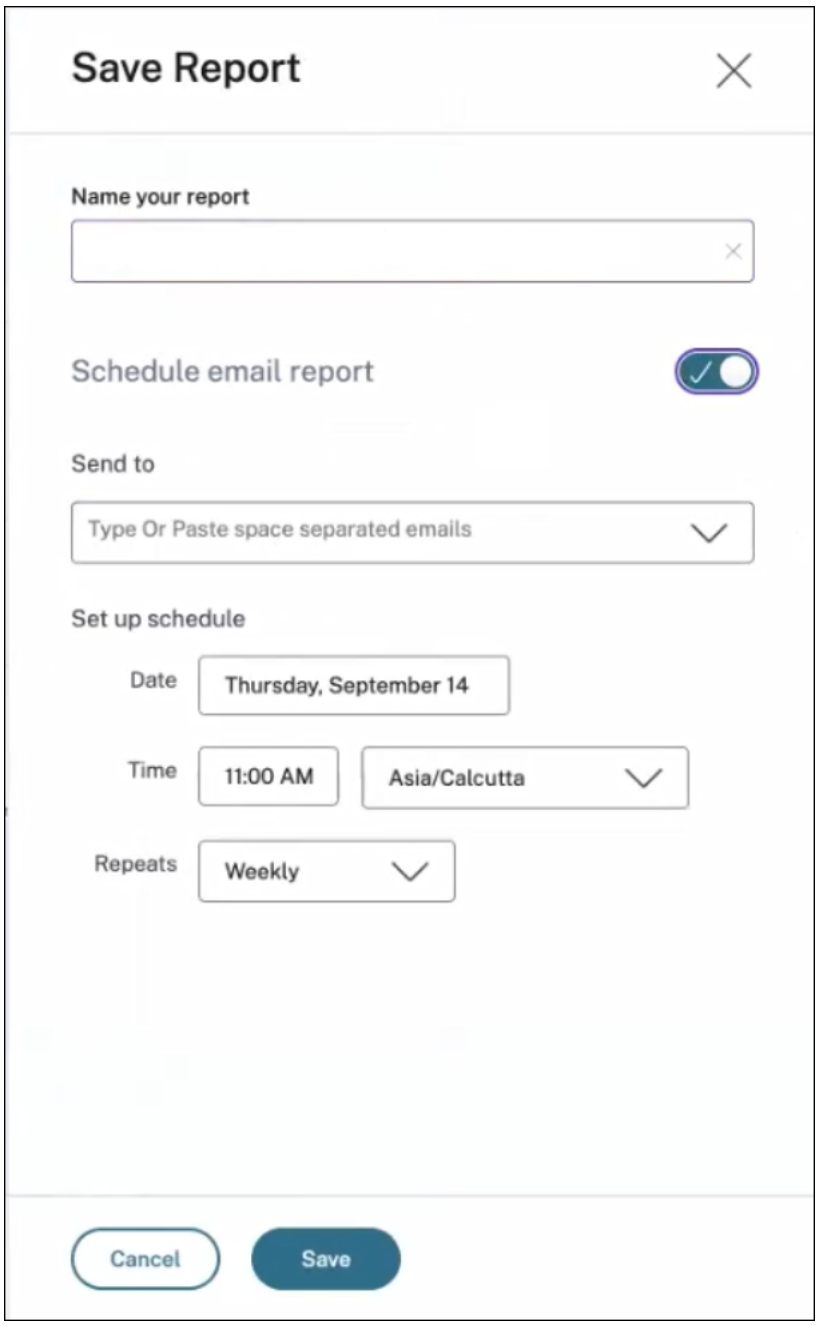
Création d'un rapport personnalisé sans modèles

Vous pouvez également créer un rapport personnalisé sans modèle prédéfini. Cliquez sur **Créer un rapport personnalisé sans modèle**. Sélectionnez une source de données dans la liste déroulante. Suivez les étapes pour définir les filtres, appliquer la visualisation, enregistrer et planifier le rapport.



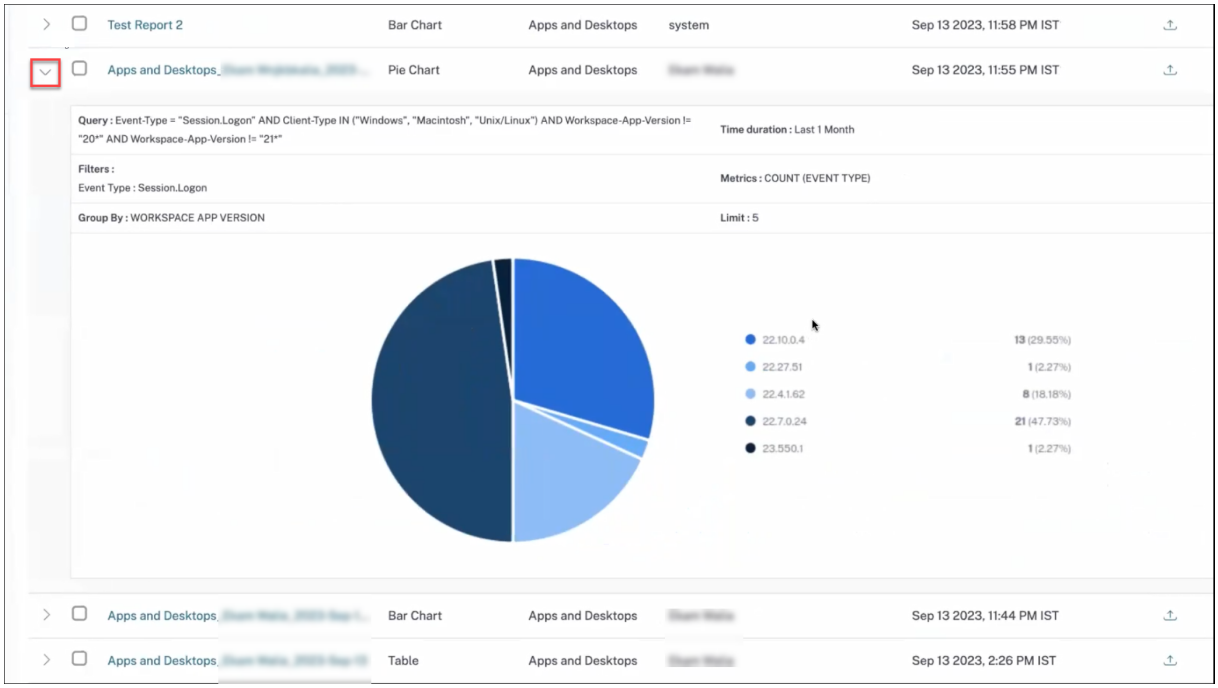
Enregistrer un rapport

1. Pour enregistrer le rapport, cliquez sur **Enregistrer**. Indiquez un titre pour votre rapport.
2. Vous pouvez planifier l'envoi du rapport par e-mail aux adresses e-mail et aux listes de distribution spécifiées à une date et une heure spécifiques ou selon un calendrier récurrent.



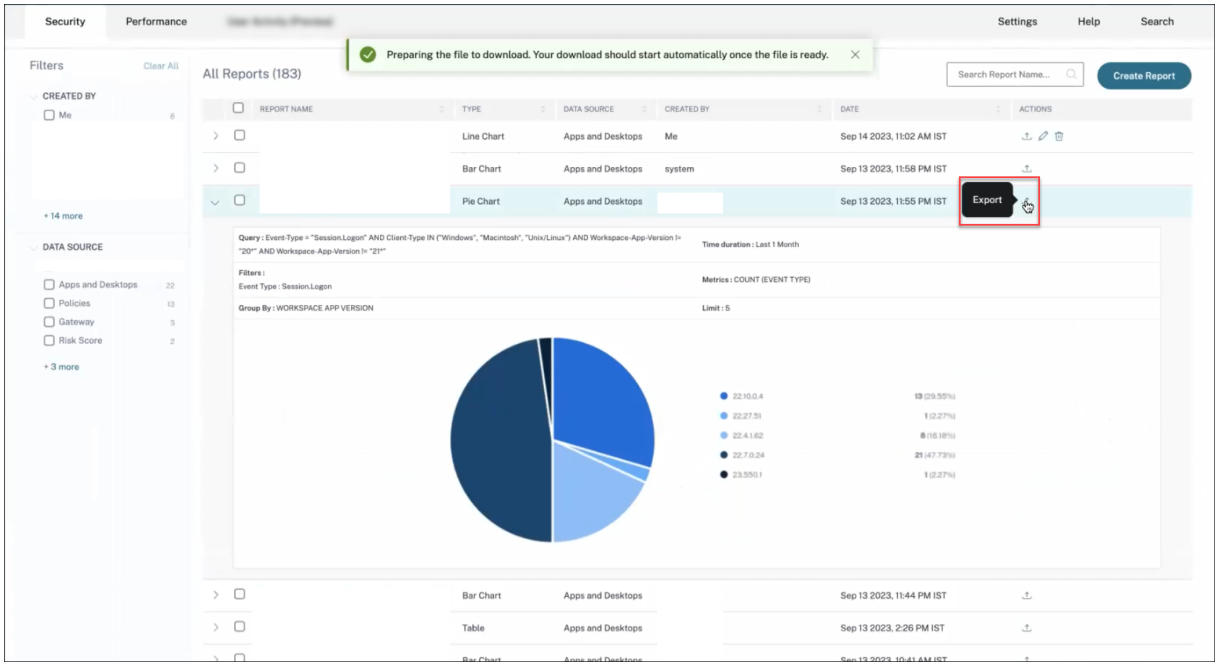
Afficher un rapport

1. Après avoir créé et enregistré un rapport, vous pouvez le consulter sur la page **Rapports** . Vous pouvez également modifier ou supprimer un rapport enregistré.
2. Cliquez sur le bouton déroulant pour prévisualiser le rapport.



Exporter un rapport

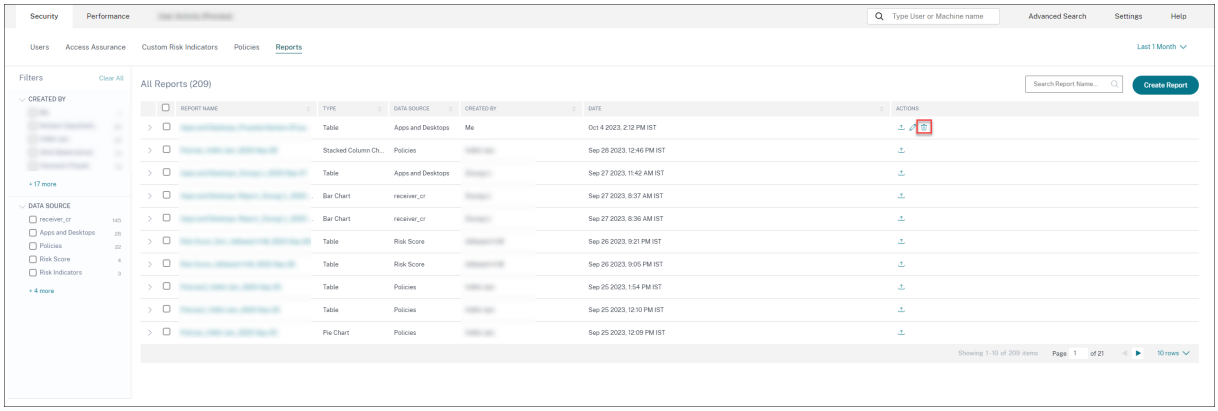
Cliquez sur l'icône d'exportation pour exporter le rapport.



Supprimer un rapport

Cliquez sur l'icône de suppression pour supprimer le rapport.

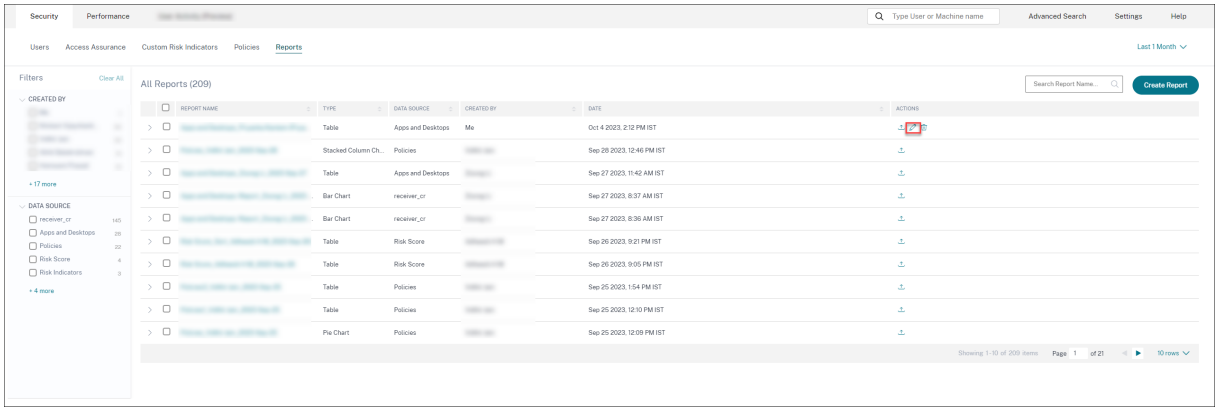
> Remarque :
>
> Seul l'utilisateur qui crée le rapport peut le supprimer.



Modifier un rapport

Cliquez sur l'icône de modification pour modifier le rapport.

> Remarque :
>
> Seul l'utilisateur qui crée le rapport peut le modifier.

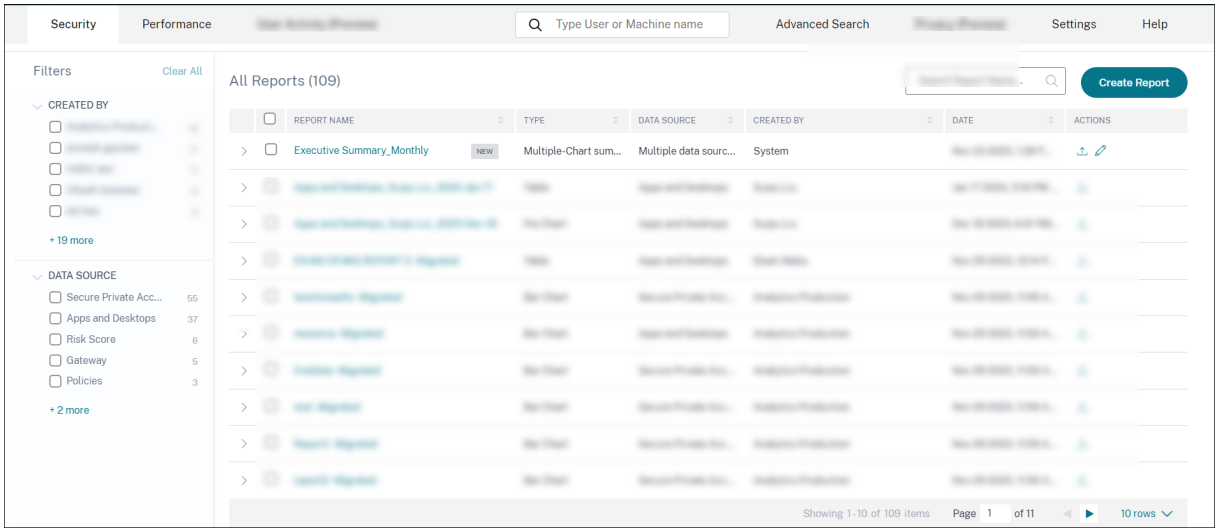


Rapport de synthèse

Vous pouvez planifier une exportation automatique par e-mail contenant un PDF d'un rapport de synthèse pré-créé. Le rapport de synthèse est un ensemble de rapports décrivant la posture de sécurité de votre entreprise en un seul coup d'œil pour la période sélectionnée et destinés au public de votre choix.

Vous pouvez créer le rapport pour les données pour les durées suivantes :

- Dernière heure
- 12 dernières heures
- Dernier jour
- Dernière semaine
- Dernier mois



Quels rapports contient-il ?

Le rapport de synthèse contient les rapports suivants :

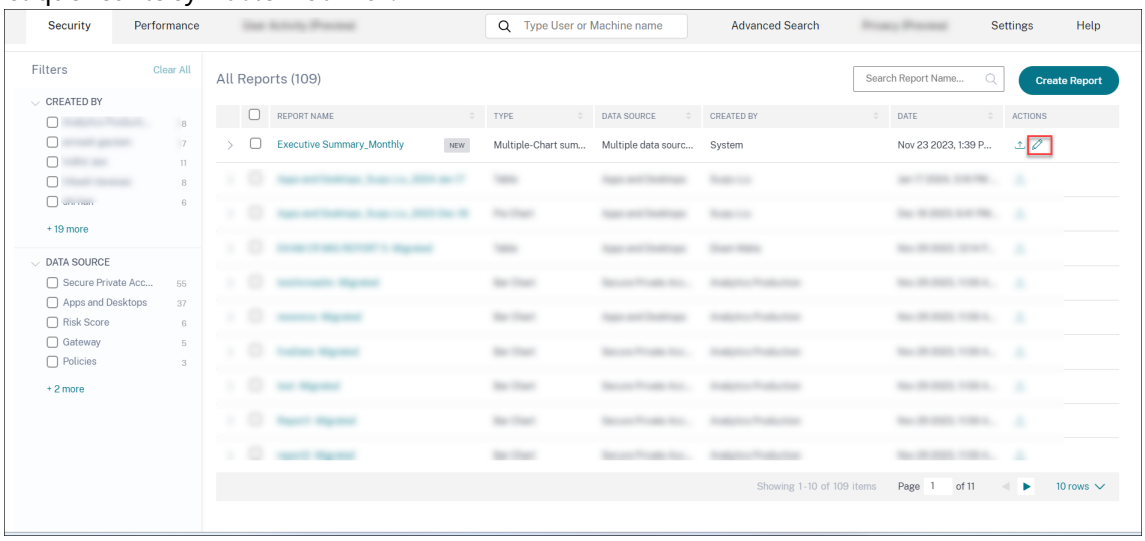
- **Distribution des risques pour les utilisateurs** : distribution des profils à risque élevé, moyen et faible en fonction de leur score de risque calculé le plus élevé au cours de la période sélectionnée.
- Utilisateurs les plus risqués : utilisateurs les plus risqués parmi tous les utilisateurs, triés selon les scores de risque les plus élevés pour la période sélectionnée.
- **Occurrences de risques par catégories** : vue complète des types d'expositions aux risques et des risques critiques fournis par les catégories de risques nécessitant une action immédiate. Les indicateurs de risque sont regroupés dans les catégories suivantes :
  - Utilisateurs compromis
  - Points de terminaison compromis
  - Exfiltration de données
  - Menaces internes
- **Indicateurs de risque** : indicateurs de risque déclenchés pour les utilisateurs pendant la période sélectionnée.
- **Actions** : actions appliquées aux indicateurs de risque déclenchés pour les utilisateurs pendant la période sélectionnée.

- **Principales stratégies** : les cinq stratégies les plus déclenchées au cours de la période sélectionnée.
- **Principales actions** : les cinq actions les plus déclenchées au cours de la période sélectionnée.
- **Indicateurs de risque par gravité** : indicateurs de risque par défaut et personnalisés déclenchés par les utilisateurs, triés en fonction de la gravité.
- **Indicateurs de risque par nombre total d'occurrences** : indicateurs de risque par défaut et personnalisés déclenchés par les utilisateurs, triés en fonction des occurrences.

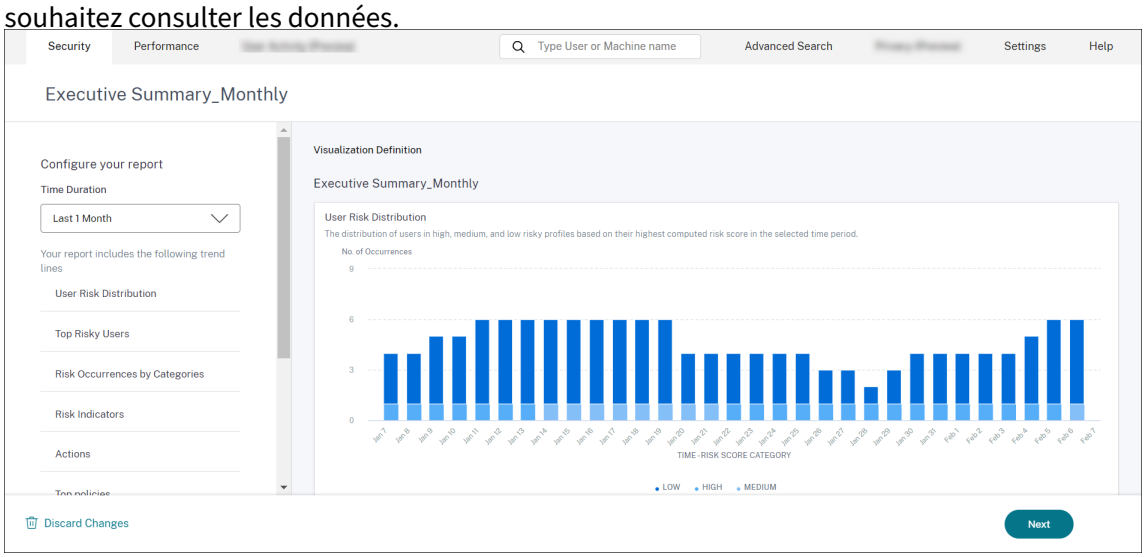
Modifier un rapport de synthèse

Pour modifier un rapport de synthèse, procédez comme suit :

1. Cliquez sur le symbole **Modifier**.



2. Dans le panneau **Configurer votre rapport**, sélectionnez la durée pendant laquelle vous souhaitez consulter les données.



3. Cliquez sur **Suivant**. Le panneau **Enregistrer le rapport** apparaît.

   > **Remarque :**
   >
   > Pour annuler les modifications, cliquez sur **Ignorer les modifications**.

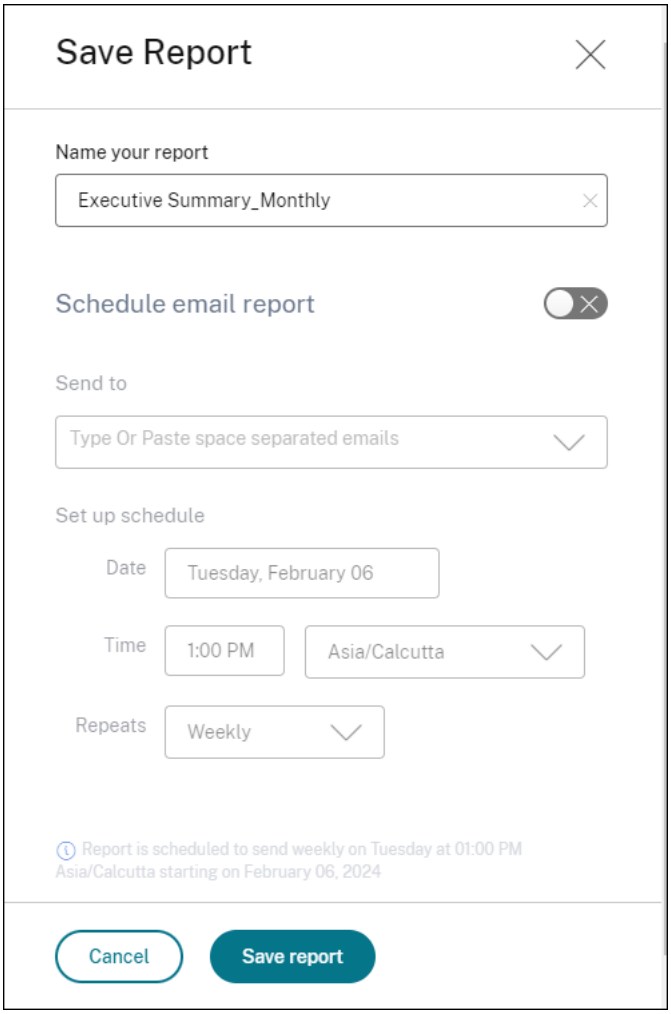
4. Dans le panneau **Enregistrer le rapport**, entrez les informations suivantes :

   a) **Donner un nom à votre rapport** : nom du rapport de synthèse.

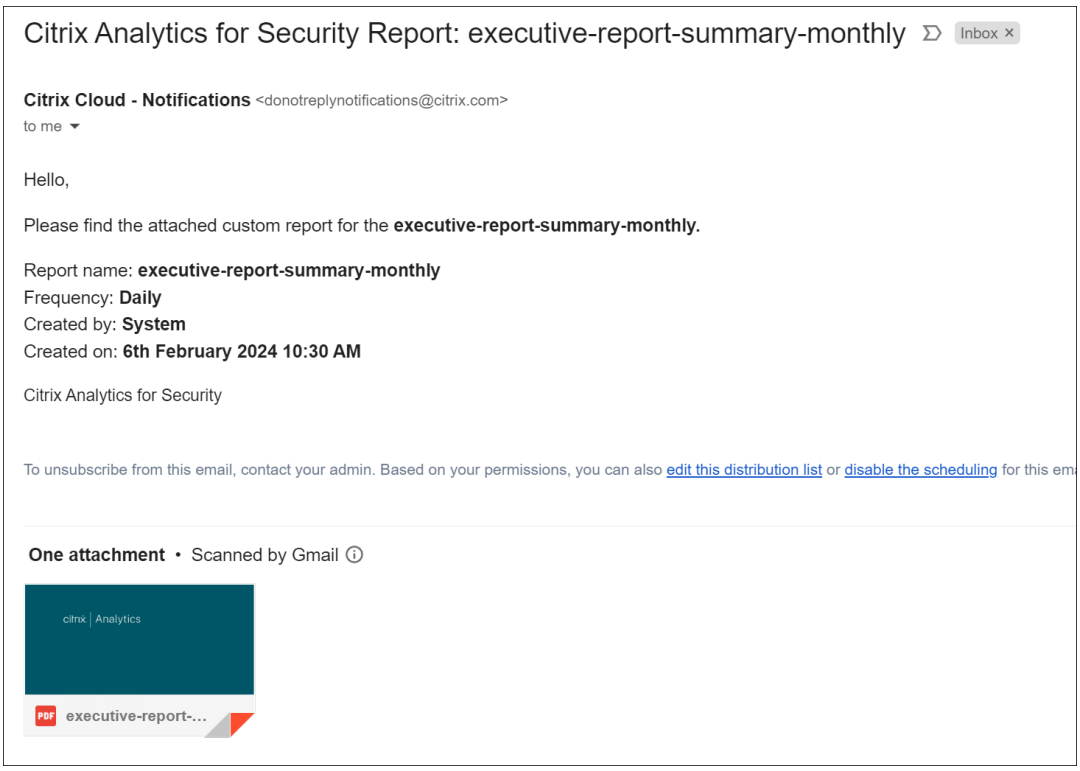
   b) **Planifier un rapport par e-mail** : activez cette option pour planifier le rapport. L'option est désactivée par défaut.

   c) **Envoyer à** : sélectionnez une liste de distribution dans la liste déroulante. Vous pouvez également ajouter une combinaison de listes de distribution et d'adresses e-mail individuelles. Pour créer une liste de distribution personnalisée, consultez la section Paramètres de messagerie de l'administrateur.

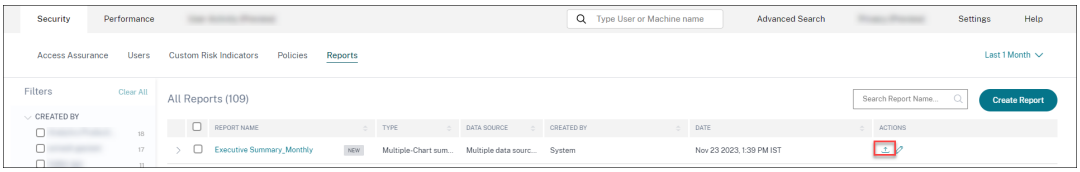
   d) **Configurer le calendrier** : sélectionnez l'heure à laquelle le rapport est envoyé pour la première fois au public sélectionné et l'heure à laquelle il se répète.



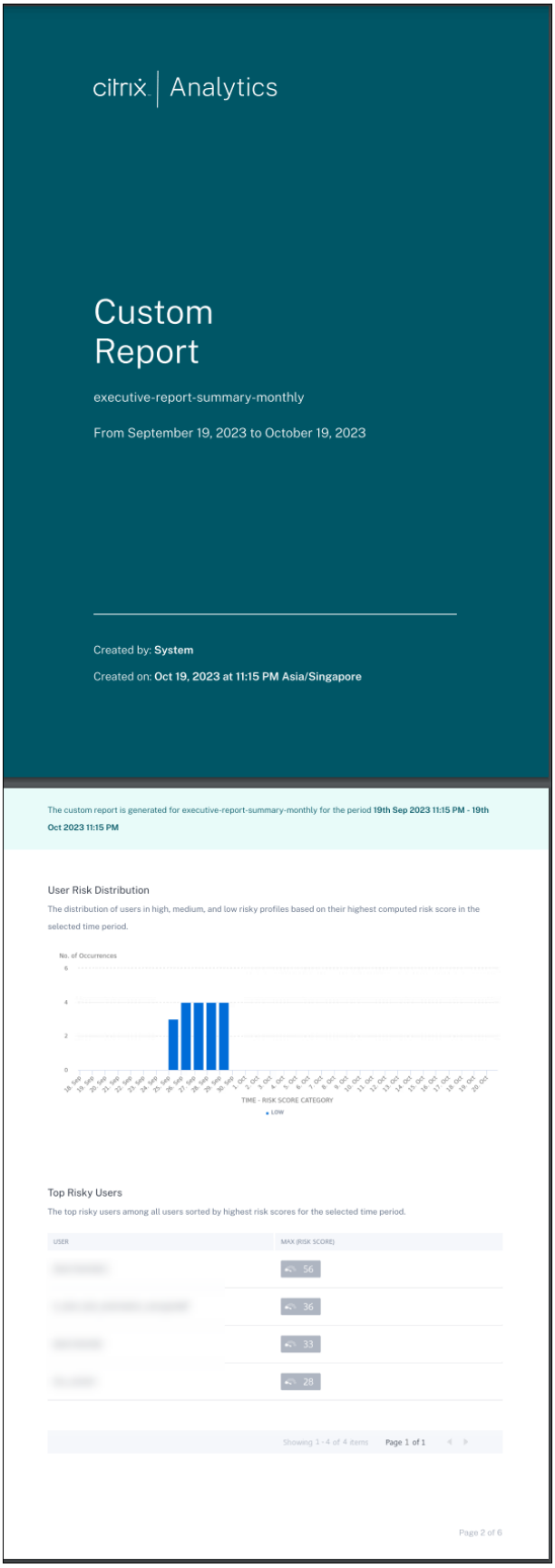
e) Cliquez sur **Enregistrer le rapport**. Le rapport est ensuite envoyé sous forme de courrier électronique aux destinataires répertoriés.



Vous pouvez également exporter le rapport exécutif au format PDF à l'aide du symbole **Exporter**.



La capture d'écran suivante montre un exemple de sortie PDF :



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

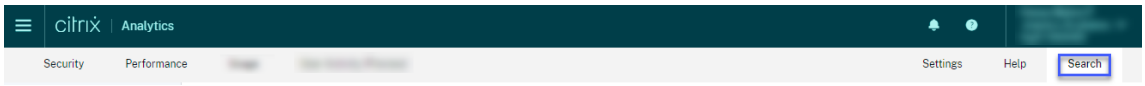
Vous pouvez accéder à la recherche en libre-service en utilisant les options suivantes :

- **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.

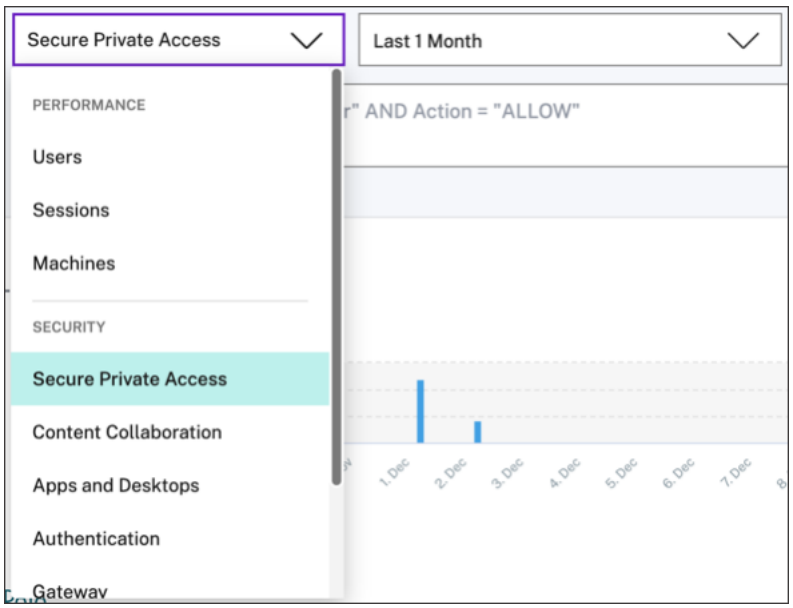
Recherche en libre-service depuis la barre supérieure

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.



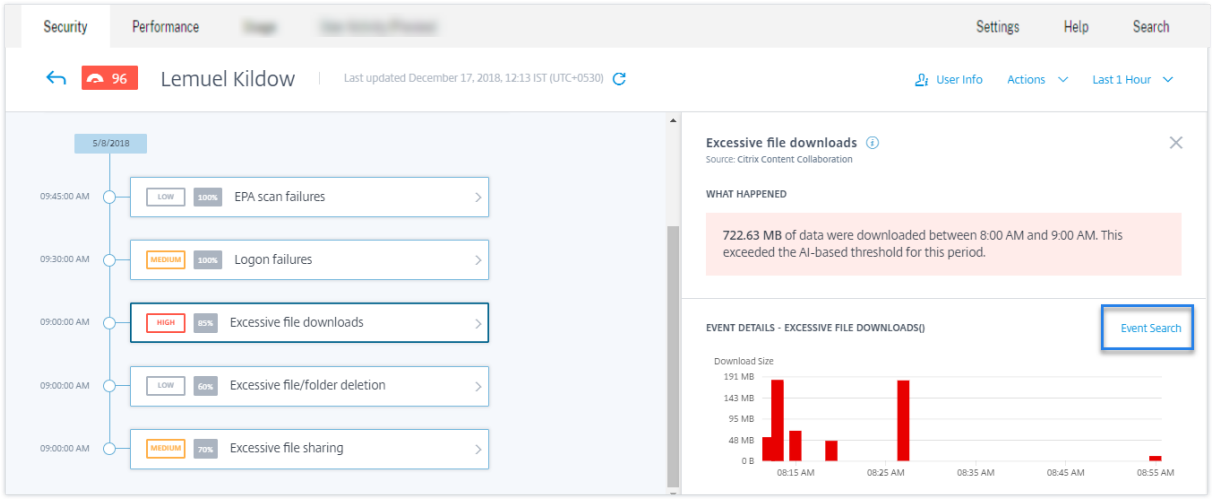
2. Sélectionnez la source de données et la période pour afficher les événements correspondants.



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.

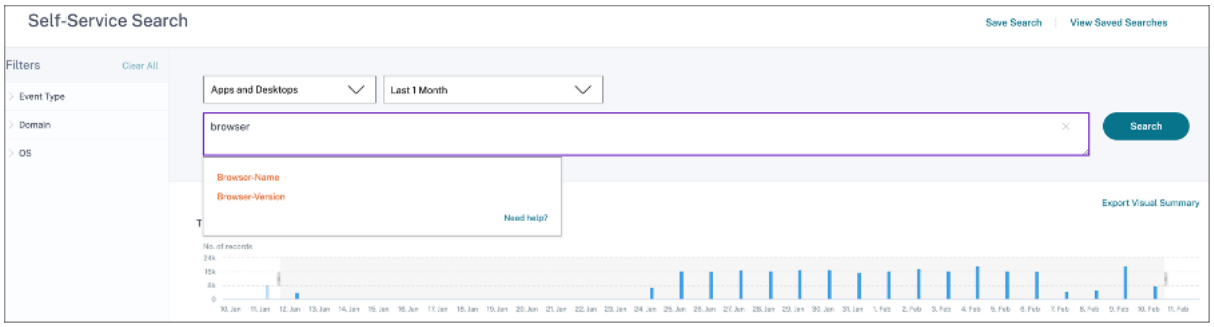
Sélectionnez les facettes pour filtrer les résultats de votre recherche. Les facettes sélectionnées sont affichées sous forme de jetons.

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.

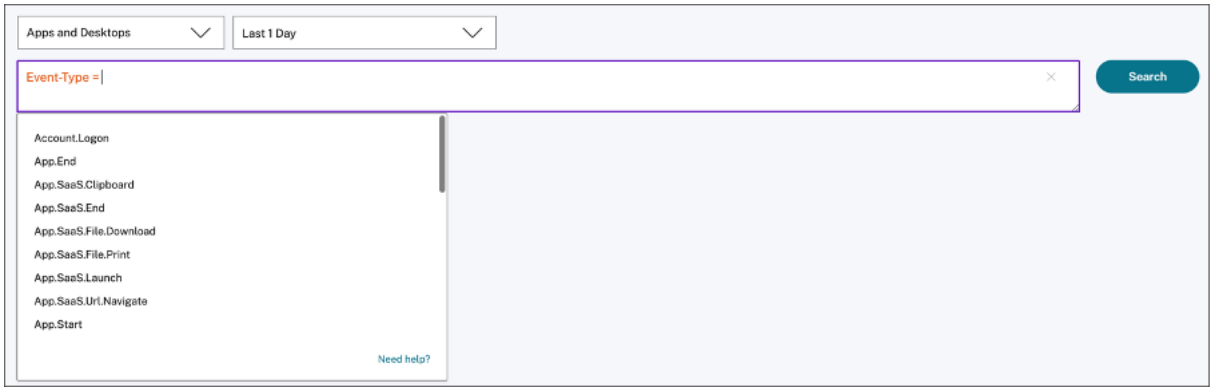
Utiliser la requête de recherche dans la zone de recherche pour filtrer les événements

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.
! ~	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 ».

Opérateur	Description	Exemple	Sortie
! =	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.
		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.

Opérateur	Description	Exemple	Sortie
		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.
`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.

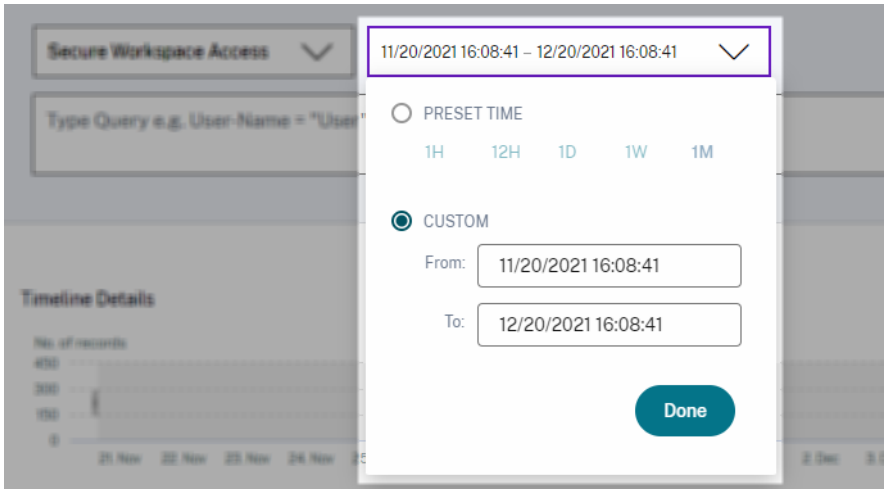
Opérateur	Description	Exemple	Sortie
OR	Recherche des valeurs pour lesquelles l'une ou les deux conditions sont vraies.	(User-Name = John* OU User-Name = *Smith) ET Event-Type = "Session.Logon"	Affiche les événements Session.Logon pour tous les noms d'utilisateur commençant par John ou se terminant par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

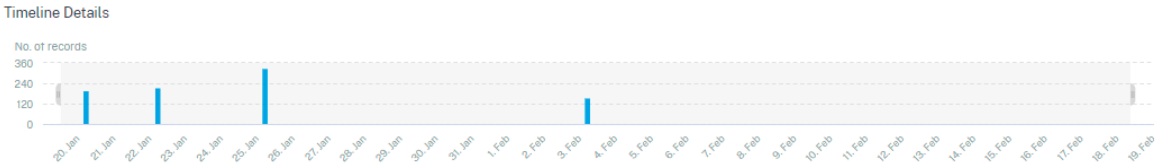


Afficher les détails de la chronologie

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.

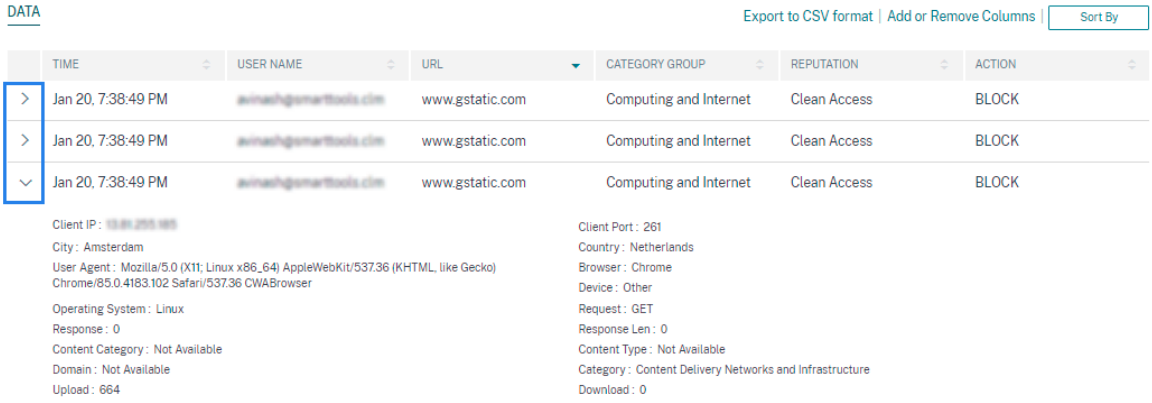
La figure montre les détails de la chronologie des données d'accès.



Voir l'événement

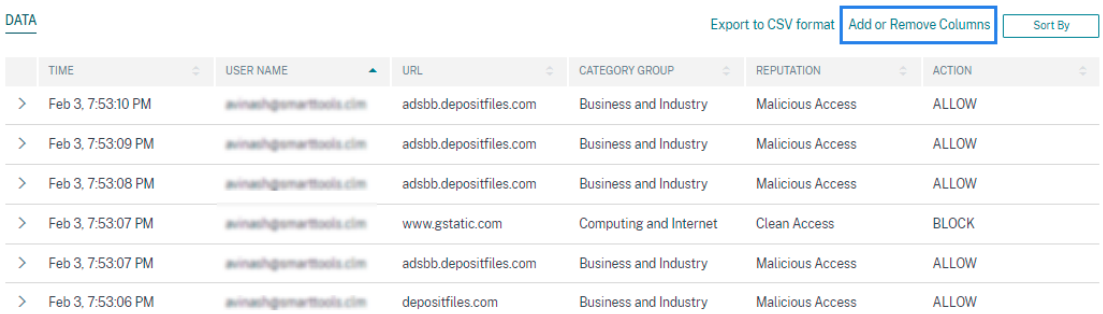
Vous pouvez consulter les informations détaillées sur l'événement utilisateur. Dans le tableau **DATA**, cliquez sur la flèche de chaque colonne pour afficher les détails de l'événement utilisateur.

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

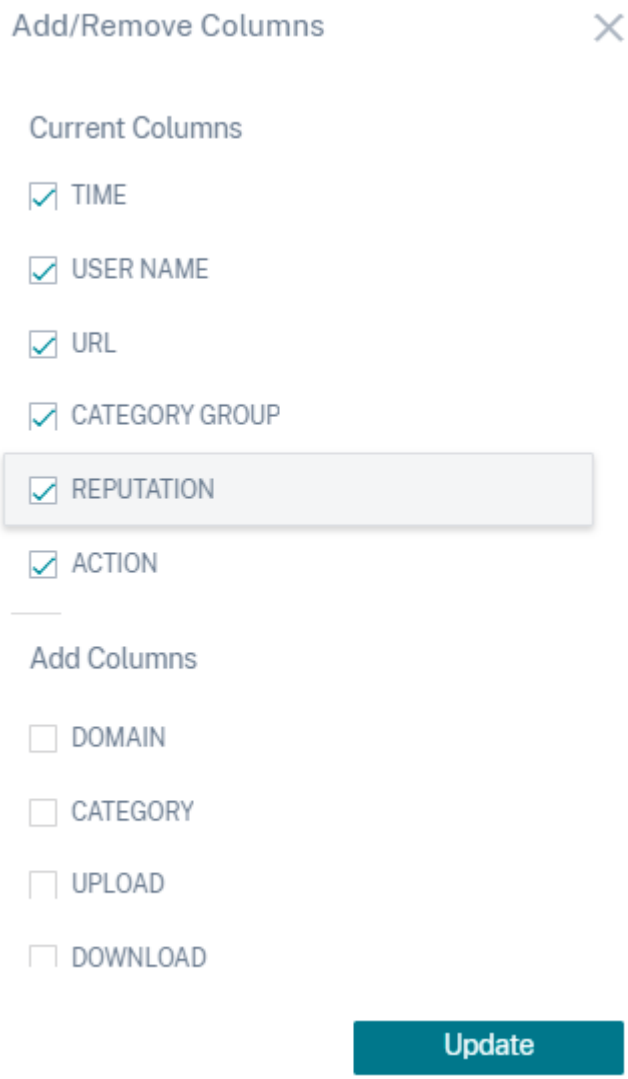


Ajouter ou supprimer des colonnes Vous pouvez ajouter ou supprimer des colonnes de la table d'événements pour afficher ou masquer les points de données correspondants. Procédez comme suit :

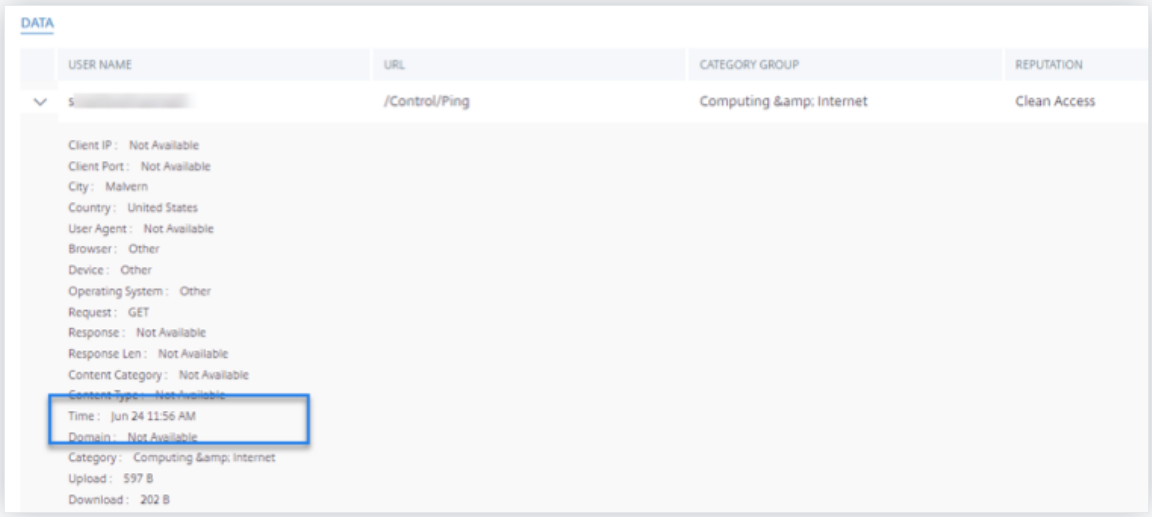
1. Cliquez sur **Ajouter ou supprimer des colonnes**.



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

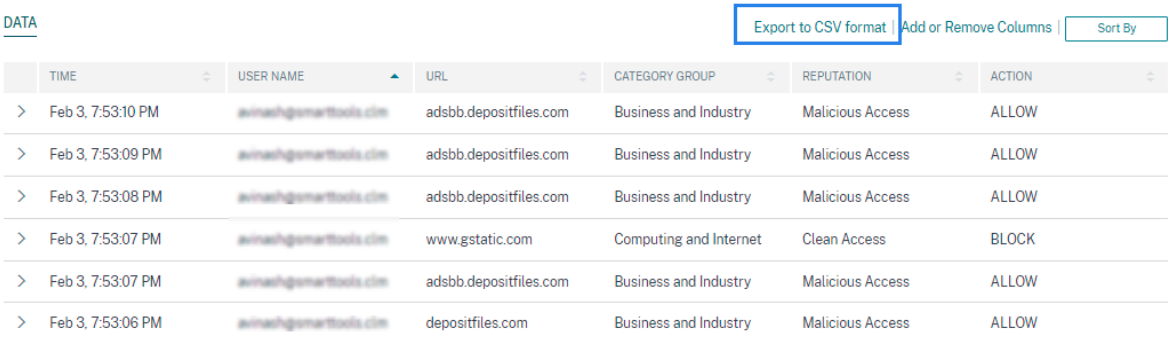


Si vous désélectionnez un point de données de la liste, la colonne correspondante est supprimée de la table des événements. Toutefois, vous pouvez afficher ce point de données en développant la ligne d'événement pour un utilisateur. Par exemple, lorsque vous désélectionnez le point de données **TIME**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

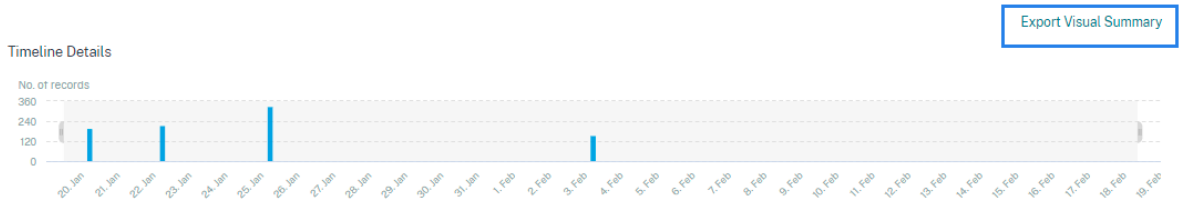
Vous pouvez télécharger le rapport de synthèse visuel de votre requête de recherche et en partager une copie avec d'autres utilisateurs, administrateurs ou votre équipe de direction.

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.

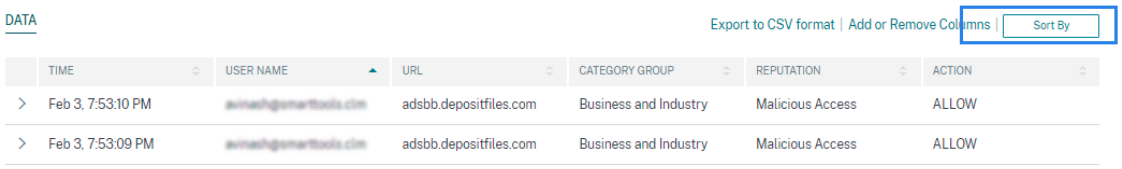


Tri multi-colonnes

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**.

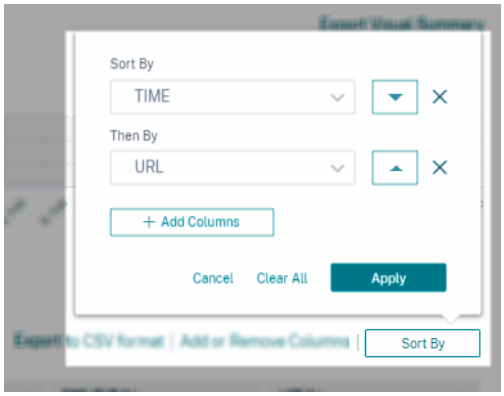


2. Sélectionnez une colonne dans la liste **Trier par** .
3. Sélectionnez l'ordre de tri : croissant (flèche vers le haut) ou décroissant (flèche vers le bas) pour trier les événements de la colonne.
4. Cliquez **sur+Ajouter des colonnes**.
5. Sélectionnez une autre colonne dans la liste **Then By**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

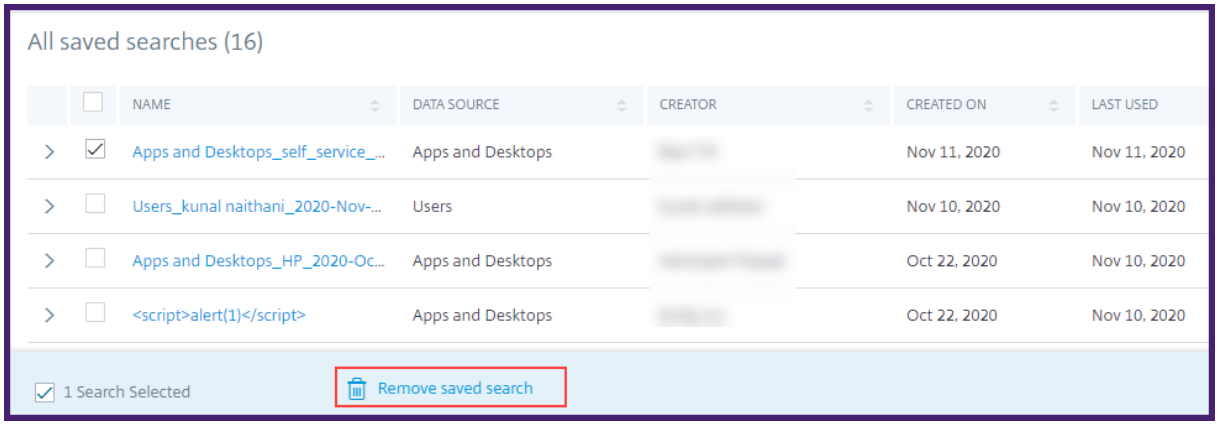
6. Activez le bouton **Planifier le rapport par e-mail** si vous souhaitez envoyer une copie du rapport de requête de recherche à vous-même et à d'autres utilisateurs à intervalles réguliers. Pour plus d'informations, consultez la rubrique Planifier un e-mail pour une requête de recherche.
7. Cliquez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

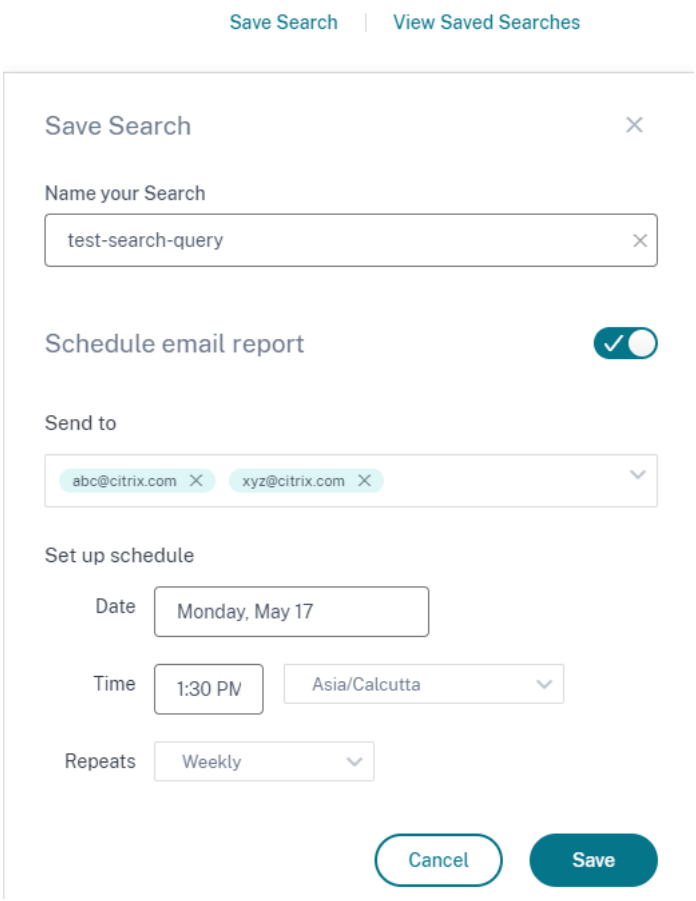
Vous pouvez envoyer une copie du rapport de requête de recherche à vous et à d'autres utilisateurs à intervalles réguliers en configurant un calendrier de remise des e-mails.

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.

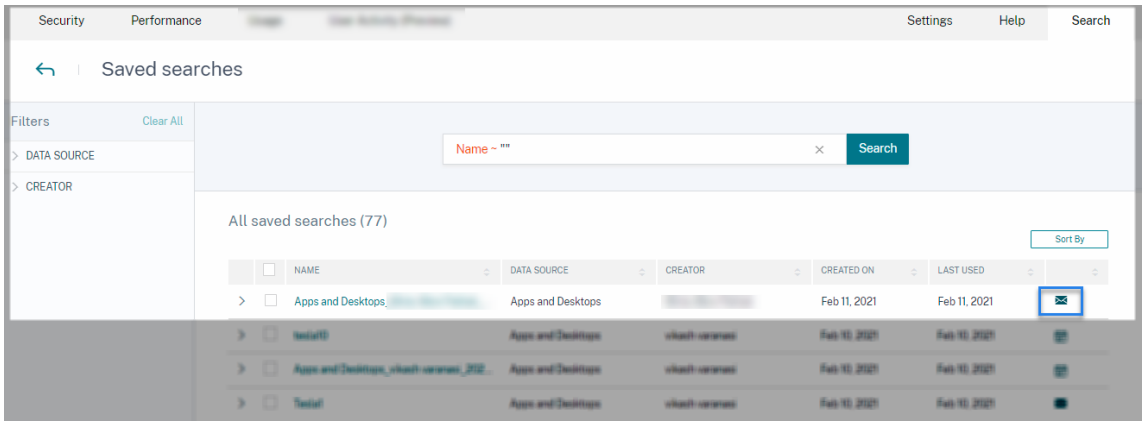
3. Définissez la date et l'heure de la livraison de l'e-mail.
4. Sélectionnez la fréquence de livraison : quotidienne, hebdomadaire ou mensuelle.
5. Cliquez sur **Enregistrer**.

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.

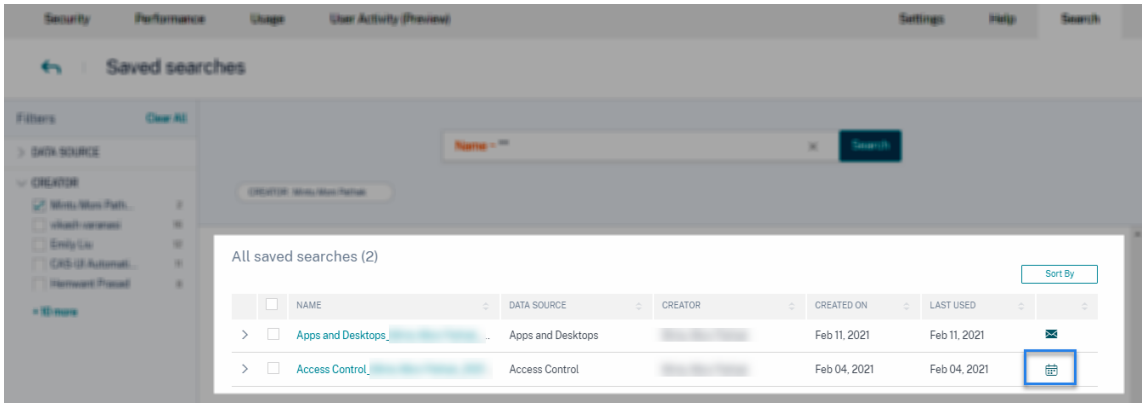
> **Remarque**
>
> Les groupes de messagerie ne sont pas pris en charge.

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.

Recherche en libre-service pour l'authentification

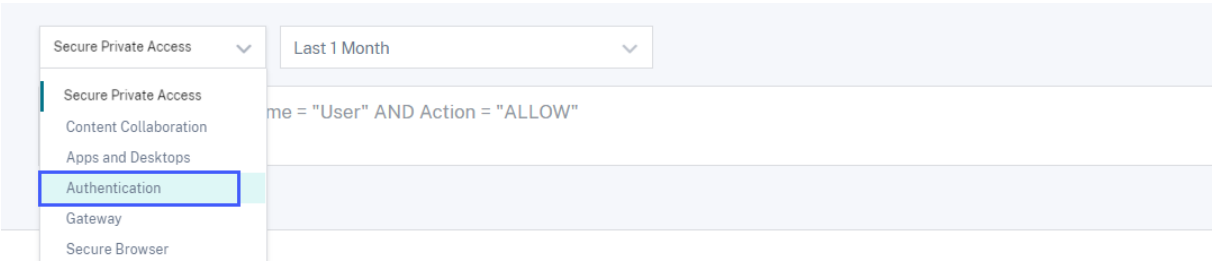
September 24, 2021

Utilisez la recherche en libre-service pour obtenir des informations sur les détails d'authentification des utilisateurs Citrix Cloud de votre entreprise. Citrix Analytics for Security reçoit les événements d'authentification des utilisateurs du service Identity and Access Management de Citrix Cloud. Les événements d'authentification tels que la connexion utilisateur, la fermeture de session utilisateur et la mise à jour du client sont affichés sur la page de recherche en libre-service.

Pour plus d'informations sur les fonctionnalités de recherche, consultez la rubrique **Recherche en libre-service**.

Sélectionnez la source de données d'authentification

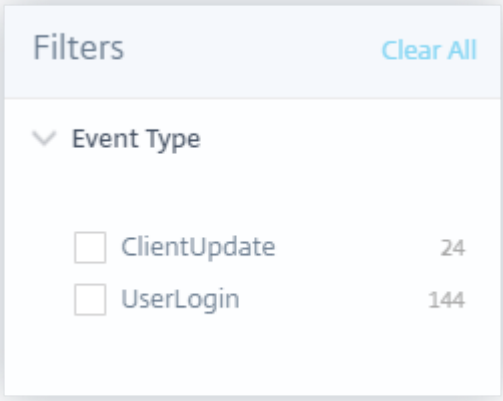
Pour afficher les événements d'authentification, sélectionnez **Authentification** dans la liste. Par défaut, la page en libre-service affiche les événements du dernier jour. Vous pouvez également sélectionner la période pendant laquelle vous souhaitez afficher les événements.



Sélectionnez les facettes pour filtrer les événements

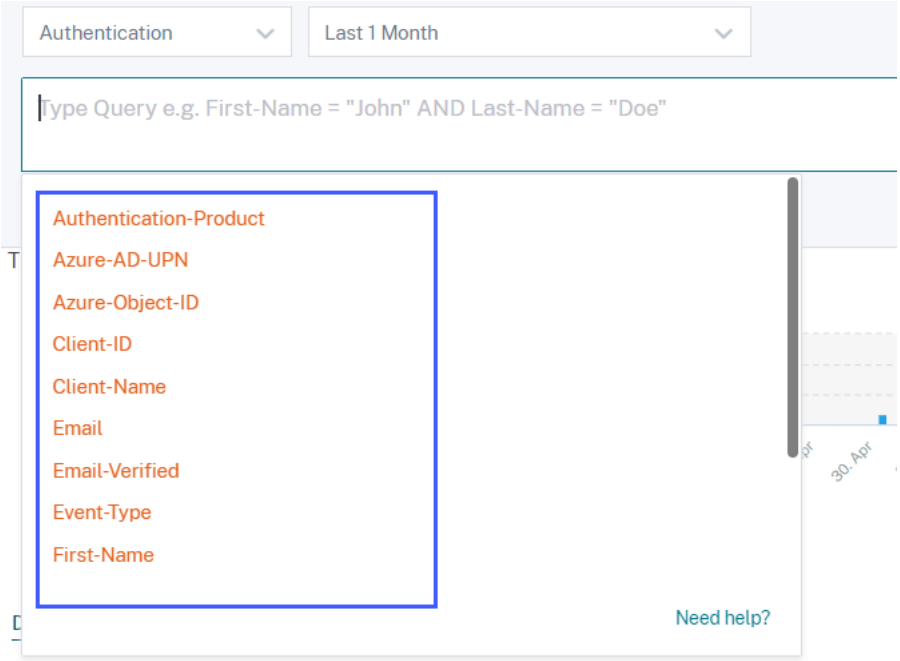
Utilisez le filtre suivant pour les événements d'authentification :

- **Type d'événement :**recherchez les événements en fonction des types d'événements utilisateur tels que la connexion utilisateur, la fermeture de session utilisateur et la mise à jour du client.



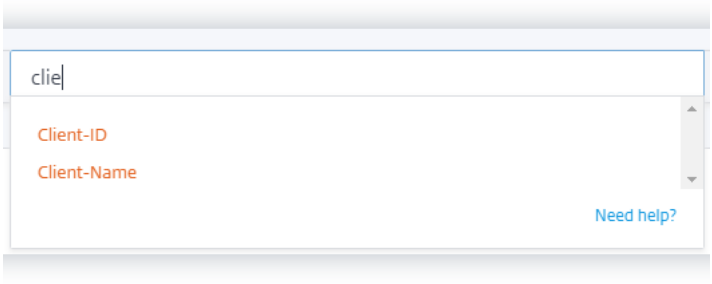
Spécifier la requête de recherche pour filtrer les événements

Placez le curseur dans la zone de recherche pour afficher la liste des dimensions des événements d'authentification. Utilisez les dimensions et les opérateurs pour spécifier votre requête et rechercher les événements requis.

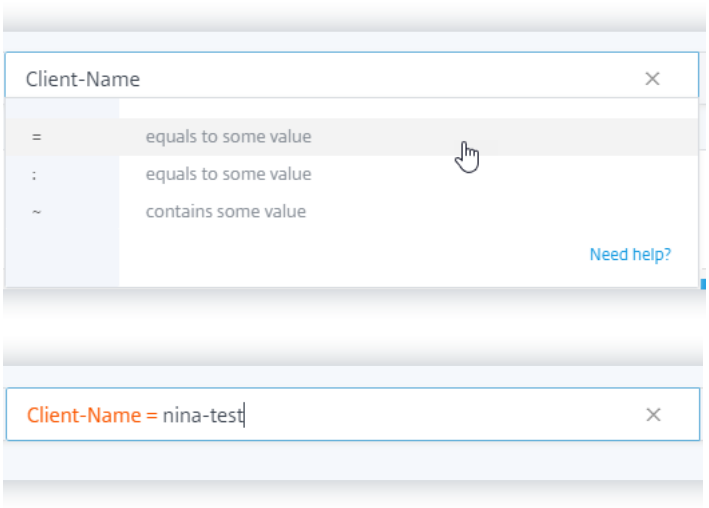


Par exemple, vous souhaitez afficher les événements d'authentification d'un client « nina-test » avec l'état de l'e-mail vérifié.

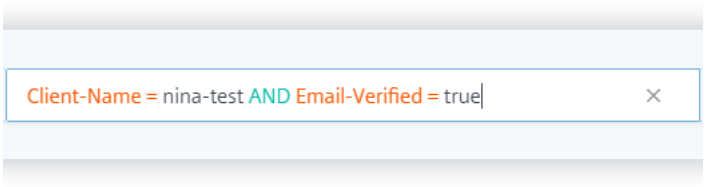
1. Entrez « client » dans la zone de recherche pour obtenir les dimensions associées.



2. Sélectionnez **Client-Name**, puis spécifiez la valeur « nina-test » à l'aide de l'opérateur égal.



3. Sélectionnez l'opérateur **AND**, puis sélectionnez la dimension **Email-Verified** . Attribuez la valeur « true » à **Email-Verified** à l'aide de l'opérateur égal. La valeur « true » indique que l'e-mail de l'utilisateur est vérifié.



4. Sélectionnez la période et cliquez sur **Rechercher** pour afficher les événements dans la table **DATA**.

Recherche en libre-service pour Gateway

September 24, 2021

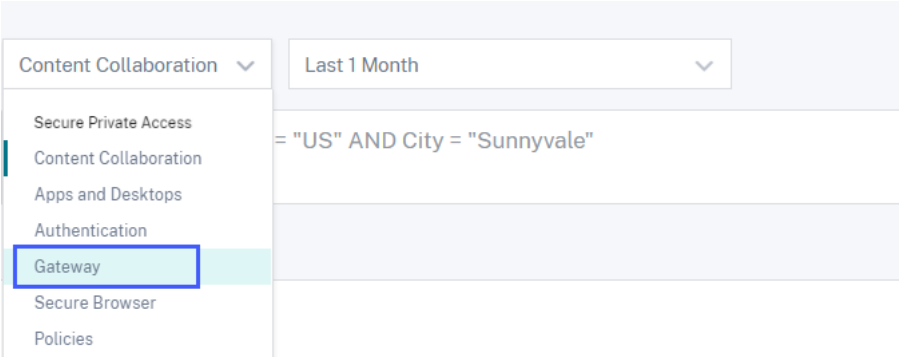
Utilisez la fonction de recherche en libre-service pour obtenir des informations sur les événements utilisateur reçus de la source de données Citrix Gateway. Lorsque les utilisateurs accèdent à leurs

ressources réseau telles que les serveurs de fichiers, les applications et les sites Web via Citrix Gateway, des événements sont générés pour chaque connexion utilisateur. Certains exemples d'événements utilisateur sont tels que la phase d'authentification, le type d'autorisation et le code de session VPN. Citrix Analytics for Security reçoit ces événements et les affiche sur la page de recherche en libre-service. Vous pouvez consulter les utilisateurs et leurs détails d'accès.

Pour plus d'informations sur les fonctionnalités de recherche, consultez la rubrique **Recherche en libre-service**.

Sélectionnez la source de données Gateway

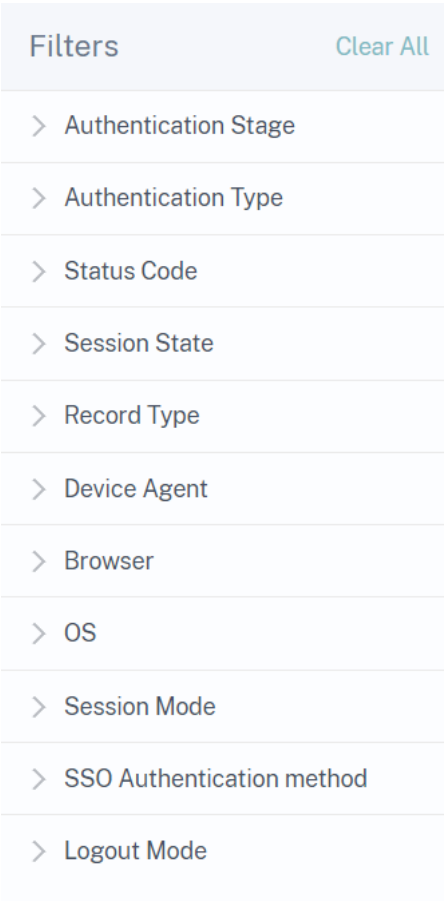
Pour afficher les événements Gateway, sélectionnez **Gateway** dans la liste. Par défaut, la page en libre-service affiche les événements du dernier jour. Vous pouvez également sélectionner la période pendant laquelle vous souhaitez afficher les événements.



> **Remarque**
>
> Vous pouvez également accéder à la page Recherche en libre-service de passerelle à partir du tableau de bord **Sécurité** > **Utilisateurs** > **Résumé des accès** . Dans les scénarios de connexion réussis, vous pouvez accéder aux données par le code d'état. Pour plus d'informations, consultez le tableau de bord Access Summary .

Utilisez les facettes pour filtrer les événements

Les facettes sont classées en fonction des événements reçus de votre source de données. Utilisez les facettes suivantes pour filtrer vos événements :



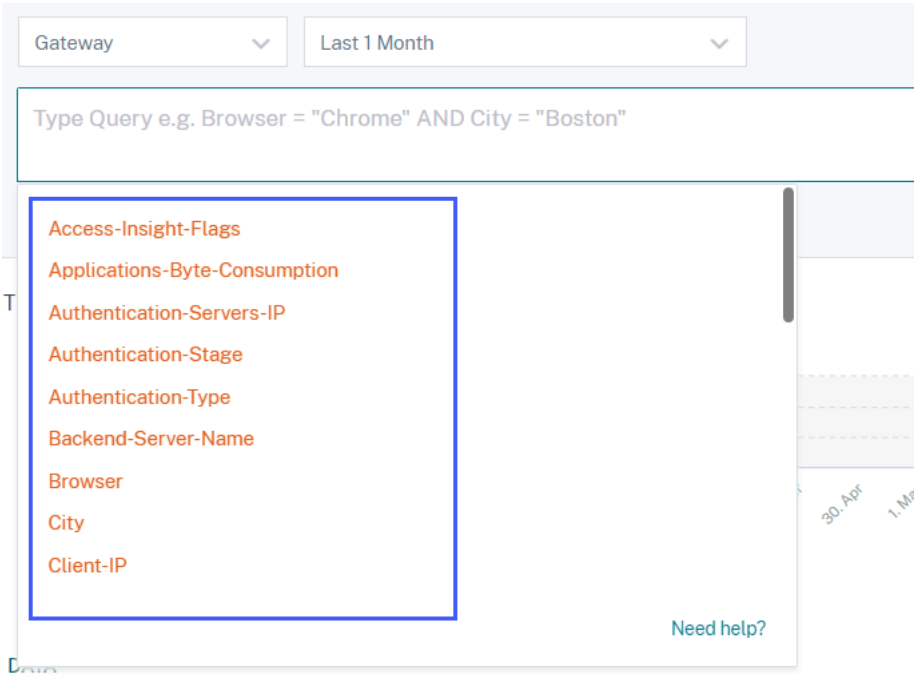
- **Étape d'authentification** : recherchez des événements en fonction des différentes étapes de l'authentification du client, telles que primaire, secondaire et tertiaire.
- **Type d'authentification :**recherchez les événements en fonction des types d'authentification client tels que Local, RADIUS, LDAP, TACACS, l'authentification par certificat client, y compris l'authentification par carte à puce.
- **Agent de périphériques**- Recherchez des événements basés sur les périphériques clients tels que iPhone, iPad, Windows Mobile.
- **Type d'enregistrement :**recherchez des événements en fonction des types d'enregistrements VPN. Les types d'enregistrements VPN suivants sont disponibles :

Type d'enregistrement	Description
VPN_AI	Filtre les événements utilisateur liés à l'authentification.
VPN_IF	Filtre les événements utilisateur liés au fichier ICA.
VPN_ST	Filtre les événements utilisateur liés à la déconnexion de session.

- **Navigateur**- Rechercher des événements basés sur les navigateurs tels que Internet Explorer, Chrome, Firefox, Safari.
- **OS**- Recherchez des événements en fonction des systèmes d'exploitation clients tels que Windows, Mac, Linux, Android, iOS.
- **Code d'état**- Recherchez des événements en fonction des codes d'état VPN tels que l'échec de la réponse de redirection SSL, l'échec d'autorisation, l'échec de l'authentification unique.
- **État de la session** : recherchez les événements en fonction des états de session VPN tels que l'état du client, l'état d'autorisation, l'état SSO, la mise à jour de la bande passante de l'application.
- **Mode session**- Recherchez des événements en fonction des modes de session VPN tels que Tunnel complet, ICA Proxy, Clientless.
- **Méthode d'authentification SSO**- Recherchez des événements en fonction de différentes méthodes d'authentification unique telles que basic, digest, NTLM, Kerberos, AG basic, SSO basée sur des formulaires.
- **Mode de déconnexion**- Rechercher des événements basés sur les modes de déconnexion VPN tels que la déconnexion d'erreur interne, le délai de déconnexion de session, la déconnexion initiée par l'utilisateur, la session terminée par l'administrateur.

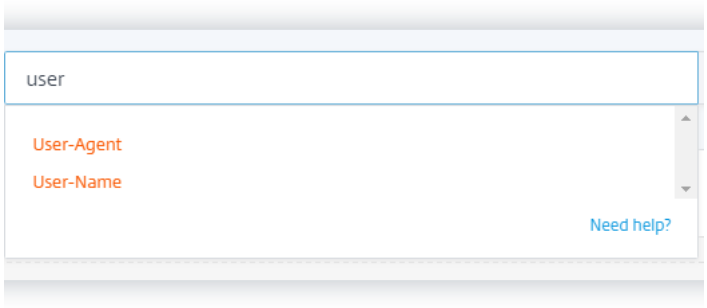
Spécifier la requête de recherche pour filtrer les événements

Placez le curseur dans la zone de recherche pour afficher la liste des dimensions des événements Gateway. Utilisez les dimensions et les opérateurs pour spécifier votre requête et rechercher les événements requis.

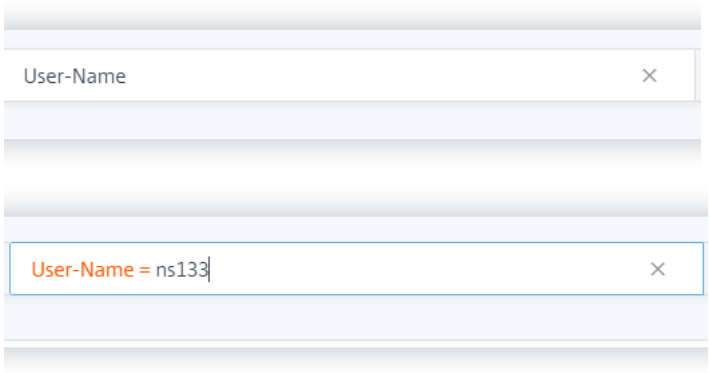


Par exemple, vous souhaitez afficher les événements d'un utilisateur « ns133 » dont le code d'état VPN est « connexion réussie ».

1. Saisissez « utilisateur » dans la zone de recherche pour choisir la dimension associée.

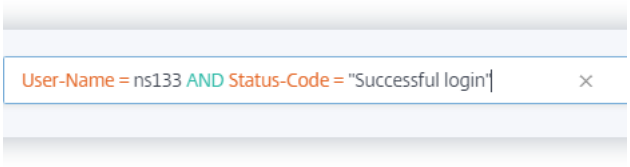


2. Sélectionnez **Nom d'utilisateur** et saisissez la valeur « ns133 » à l'aide de l'opérateur égal.

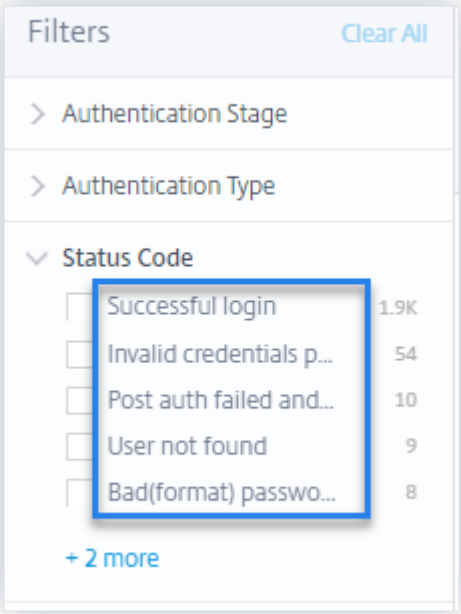


3. Sélectionnez l'opérateur **AND**, puis la dimension **Code d'état** . Entrez la chaîne « Connexion

réussie » pour le **code d'état** à l'aide de l'opérateur égal.



Pour identifier les valeurs de chaîne possibles pour le **code d'état**, développez la liste de filtres **Code d'état** et utilisez le nom du filtre comme chaîne dans votre requête de recherche.



4. Sélectionnez la période et cliquez sur **Rechercher** pour afficher les événements dans la table **DATA**.

Valeurs prises en charge pour votre requête de recherche

Entrez les valeurs suivantes pour les dimensions afin de définir votre requête de recherche.

Indicateurs d'accès Insight

Indique les états de session VPN. Entrez l'une des valeurs d'indicateur suivantes :

État de la session VPN	Valeur du drapeau
Pré-authentification	2

État de la session VPN	Valeur du drapeau
Dernier ou dernier état de l'authentification nFactor (multi-facteurs)	1
Post-authentification	4

> **Remarque**
>
> Cet indicateur s'applique uniquement aux états de session VPN précédents pour les événements d'authentification. Pour tous les autres événements, la valeur de l'indicateur est nulle.

Consommation d'octets d'applications

Pour la `Applications-Byte-Consumption` dimension, saisissez la valeur suivante :

Valeur	Type	Description
Exemples : `40`, `100`	Nombre	Données (en octets) consommées par l'application que vous utilisez.

Serveurs d'authentification IP

Pour la `Authentication-Servers-IP` dimension, saisissez la valeur suivante :

Valeur	Type	Description
Exemple : `10.xxx.xx.xx`	Chaîne	Adresse IP du serveur d'authentification.

Étape d'authentification

Pour la `Authentication-Stage` dimension, saisissez la valeur suivante :

Valeur	Type	Description
`PrimarySecondary`, ou `Tertiary`	Chaîne	Différentes étapes de l'authentification du client.

Type d'authentification

Pour la `Authentication-Type` dimension, saisissez la valeur suivante :

Valeur	Type	Description
`LDAP`,`SAML`, `Local`, `RadiusTACACS`, `SAMLIDP`, ou `OTP`.	Chaîne	Authentifiez vos utilisateurs via l'une des méthodes disponibles.

Nom du serveur principal

Pour la `Backend-Server-Name` dimension, saisissez la valeur suivante :

Valeur	Type	Description
Exemple : `10.xxx.xxx.xx`	Chaîne	Adresse IP du serveur principal.

Browser

Pour la `Browser` dimension, saisissez la valeur suivante :

Valeur	Type	Description
`PN Agent`, `EdgeFirefox`, `Chrome`, ou `Safari`.	Chaîne	Navigateur utilisé.

Ville

Pour la `City` dimension, saisissez la valeur suivante :

Valeur	Type	Description
Exemples : `Boston`, `Beijing`	Chaîne	Ville à partir de laquelle l'utilisateur s'est connecté.

Client-IP

Pour la `Client-IP` dimension, saisissez la valeur suivante :

Valeur	Type	Description
Exemple : `10.xxx.xxx.xx`	Chaîne	Adresse IP de la machine utilisateur.

Type IP client

Pour la `Client-IP-Type` dimension, saisissez la valeur suivante :

Valeur	Type	Description
public, privé	Chaîne	Indique si l'adresse IP de l'utilisateur est publique ou privée.

> **Remarque**
>
> Les valeurs sont sensibles à la casse. Entrez les valeurs en minuscules.

Port client

Pour la `Client-Port` dimension, saisissez la valeur suivante :

Valeur	Type	Description
Exemple : `45334`	Nombre	Numéro de port de la machine utilisateur.

Pays

Pour la `Country` dimension, saisissez la valeur suivante :

Valeur	Type	Description
Exemples : `United States`, `India`	Chaîne	Pays depuis lequel l'utilisateur s'est connecté.

> **Remarque**
>
> Enclenchez la valeur dans « » si la valeur contient des espaces. **Exemple** : Country = « États-Unis ».

Type d'événement

Pour la `Event-Type` dimension, saisissez la valeur suivante :

Valeur	Type	Description
Authentification, fichier ICA, déconnexion de session	Chaîne	Type d'événements utilisateur.

FQDN de passerelle

Pour la `Gateway-FQDN` dimension, saisissez la valeur suivante :

Valeur	Type	Description
Exemple : `Gateway-test`	Chaîne	Nom de domaine de votre Citrix Gateway.

Passerelle IP

Pour la `Gateway-IP` dimension, saisissez la valeur suivante :

Valeur	Type	Description
Exemple : `10.xxx.xxx.xx`	Chaîne	Adresse IP de votre Citrix Gateway.

Port de passerelle

Pour la `Gateway-Port` dimension, saisissez la valeur suivante :

Valeur	Type	Description
Exemple : `443`	Chaîne	Numéro de port de votre Citrix Gateway.

Mode de déconnexion

Pour la `Logout-Mode` dimension, saisissez la valeur suivante :

Valeur	Type	Description
`"Internal error"`, `"Inactive time out"`, `"User initiated logout"`, ou `"Administrator killed session"`.	Chaîne	Motif du délai d'expiration ou de la fin de la session VPN.

> **Remarque**
>
> Enclenchez la valeur dans « » si la valeur contient des espaces. **Exemple** : Mode de déconnexion = `"Internal error"`.

NetScaler-IP

Pour la `NetScaler-IP` dimension, saisissez la valeur suivante :

Valeur	Type	Description
Exemple : `10.xxx.xx.xx`	Chaîne	Adresse IP de votre appliance Citrix ADC.

OS

Pour la `OS` dimension, saisissez la valeur suivante :

Valeur	Type	Description
Exemples : `MAC_OS`, `WINDOWS`	Chaîne	Système d'exploitation de la machine utilisateur.

Type d'enregistrement

Pour la `Record Type` dimension, saisissez la valeur suivante :

Valeur	Type	Description
VPN_AI	Chaîne	Indique les événements utilisateur liés à l'authentification.
VPN_IF	Chaîne	Indique les événements utilisateur liés au fichier ICA.
VPN_ST	Chaîne	Indique les événements utilisateur liés à la déconnexion de session.

Méthode d'authentification SSO

Pour la SSO-Authentication-Method dimension, saisissez la valeur suivante :

Valeur	Type	Description
NSAUTH_BEARER, NSAUTH_FORM, NSAUTH_CITRIXAGBASIC NSAUTH_NEGOTIATE, NSAUTH_NTLM, ou NSAUTH_BASIC.	Chaîne	Différentes méthodes d'authentification unique.

IP du serveur

Pour la Server-IP dimension, saisissez la valeur suivante :

Valeur	Type	Description
Exemple : 10.xx.xxx.xx	Chaîne	Adresse IP du serveur principal.

Port serveur

Pour la Server-Port dimension, saisissez la valeur suivante :

Valeur	Type	Description
Exemple : `47054`	Nombre	Numéro de port du serveur principal.

État de la session

Pour la `Session-State` dimension, saisissez la valeur suivante :

Valeur	Type	Description
`"Set Client State"`, `"Authorization State"` `"SSO State"`, et `"Application Bandwidth Update"`	Chaîne	État de la session VPN.

> **Remarque**
>
> Enclenchez la valeur dans « » si la valeur contient des espaces. **Exemple** : Session-State = `"Set Client State"`.

Code d'état

Pour la `Status-Code` dimension, saisissez la valeur suivante :

Valeur	Type	Description
`"Successful login"`, `"Invalid credentials passed"`, `"Post auth failed and connection quarantined"`, `"Login not permitted"`, `"Maximum login failures reached"`	Chaîne	Le code d'état du VPN.

> **Remarque**
>
> Enclenchez la valeur dans « » si la valeur contient des espaces. **Exemple** : Session-Code = `"Successful login"`.

Agent utilisateur

Pour la `User-Agent` dimension, saisissez la valeur suivante :

Valeur	Type	Description
`IPHONEIPAD`, ou `WINPHONE`	Chaîne	L'agent ou l'appareil utilisé pour accéder au VPN.

ID de session VPN

Pour la `VPN-Session-ID` dimension, saisissez la valeur suivante :

Valeur	Type	Description
`c2c290c61dfe4e07247bde1e2142a12`	Chaîne	ID de session attribué par le serveur pour la session VPN d'un utilisateur.

Mode session VPN

Pour la `VPN-Session-Mode` dimension, saisissez la valeur suivante :

Valeur	Type	Description
`"Full Tunnel""ICA Proxy"`, ou `Clientless`	Chaîne	Différents modes de session VPN d'un utilisateur.

> **Remarque**
>
> Enclenchez la valeur dans « » si la valeur contient des espaces. **Exemple** : Session-Code = `"Full Tunnel"`.

Recherche en libre-service pour les stratégies

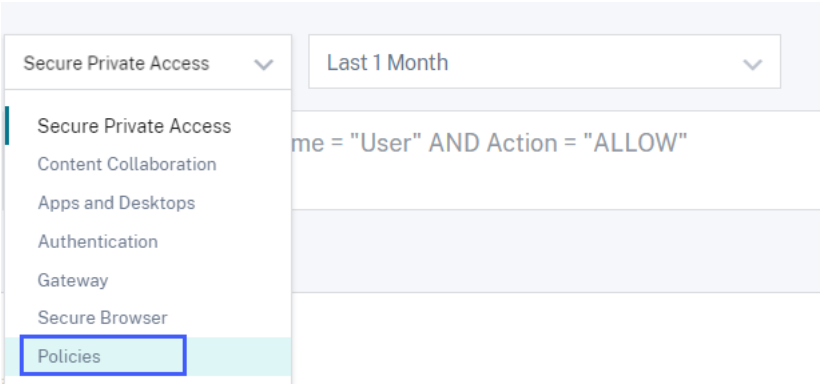
May 6, 2022

Citrix Analytics for Security vous permet de créer des stratégies et d'appliquer des actions en cas d'événements inhabituels ou suspects sur les comptes d'utilisateurs. Lorsque les événements utilisateur respectent vos stratégies définies, les actions sont automatiquement appliquées aux comptes d'utilisateurs pour isoler la menace et empêcher que de futurs événements anormaux ne se produisent. À l'aide de la recherche en libre-service, vous pouvez afficher les événements utilisateur qui ont respecté vos stratégies définies et afficher les actions appliquées à ces événements anormaux.

Pour plus d'informations sur les fonctionnalités de recherche, consultez la rubrique **Recherche en libre-service**.

Sélectionnez le jeu de données Politiques

Pour afficher les événements liés aux stratégies définies, sélectionnez **Stratégies** dans la liste. Par défaut, la page en libre-service affiche les événements du dernier jour. Vous pouvez également sélectionner la période pendant laquelle vous souhaitez afficher les événements.

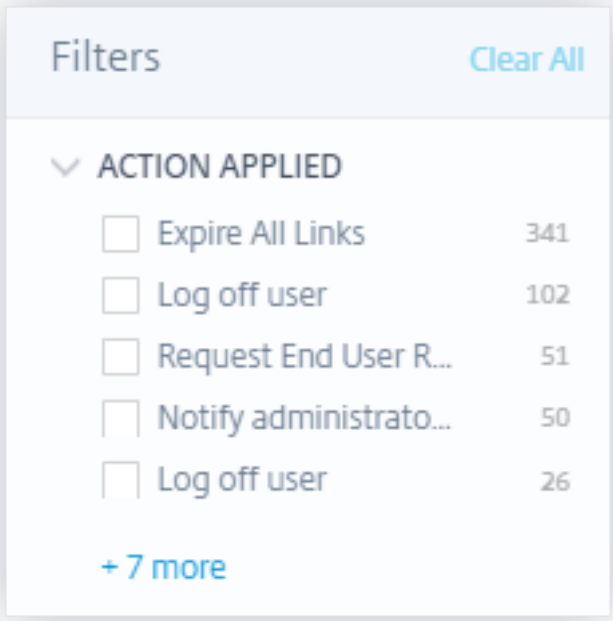


> **Remarque**
>
> Vous pouvez également accéder à la page Recherche en libre-service des stratégies à partir du tableau de bord **Sécurité** > **Utilisateurs** > **Stratégies et actions** . Sélectionnez une stratégie sur le tableau de bord pour afficher les événements utilisateur associés à la stratégie. Pour plus d'informations, consultez le tableau de bord Stratégies et actions .

Sélectionnez les facettes pour filtrer les événements

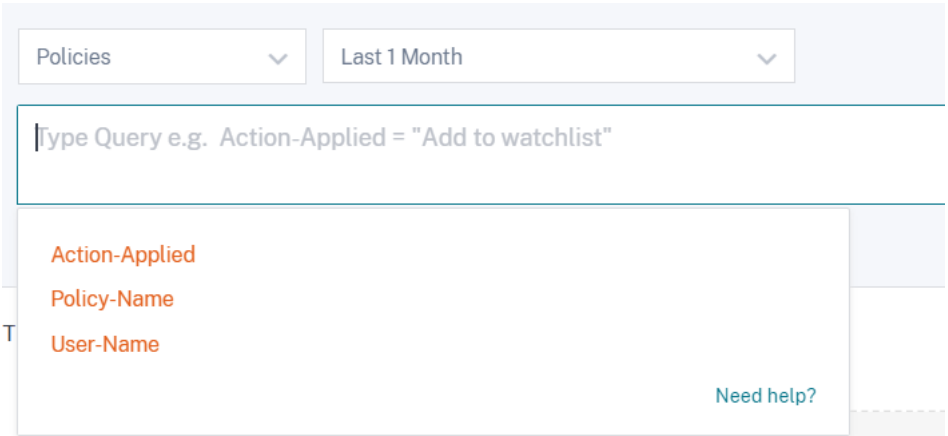
La liste des facettes affiche les actions appliquées aux événements utilisateur. Sélectionnez les actions appliquées dans la liste des facettes et affichez les événements en fonction des actions ap-

pliquées. Pour plus d'informations sur les actions que vous pouvez appliquer lors de la configuration des stratégies, voir Que sont les actions ?



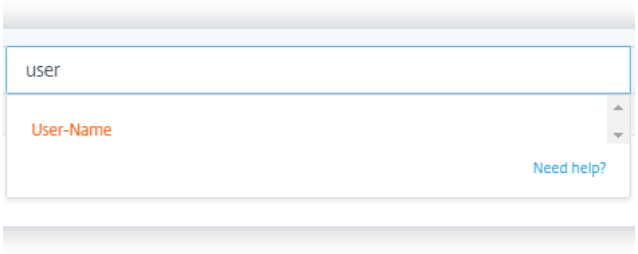
Spécifier la requête de recherche pour filtrer les événements

Placez le curseur dans la zone de recherche pour afficher la liste des dimensions des événements liés aux stratégies. Utilisez les dimensions et les opérateurs pour spécifier votre requête et rechercher les événements requis.

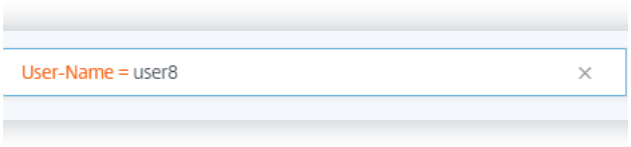


Par exemple, vous souhaitez afficher les événements anormaux d'un utilisateur « utilisateur8 » où l'action appliquée à ces événements est « Désactiver l'utilisateur ». «

1. Entrez « utilisateur » dans la zone de recherche pour obtenir les dimensions associées.

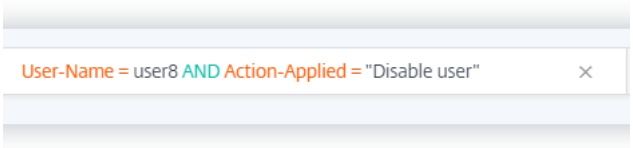


2. Sélectionnez **UserName** et saisissez la valeur « user8"à l'aide de l'opérateur égal.

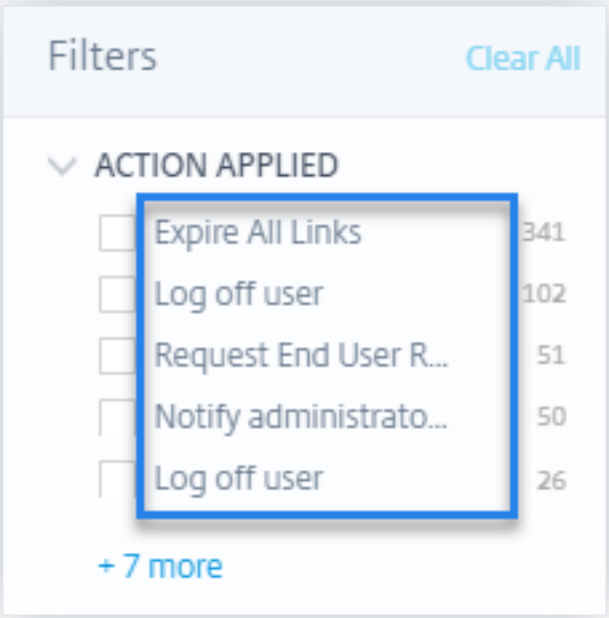


3. Sélectionnez l'opérateur **AND**, puis sélectionnez la dimension **Action-Appliquée** . Entrez la chaîne « Désactiver l'utilisateur » pour **Action-Appliquée à** l'aide de l'opérateur égal.

> **Remarque**
>
> Si la valeur de chaîne contient deux mots ou plus, elle doit être entourée de l'opérateur "" `<!--NeedCopy-->`. Par exemple "`Disable user`"`<!--NeedCopy-->`, « Arrêter l'enregistrement de session ».



Pour identifier les valeurs de chaîne possibles pour **Action-Applied**, développez la liste des facettes et utilisez le nom du filtre comme chaîne dans votre requête de recherche.



4. Sélectionnez la période et cliquez sur **Rechercher** pour afficher les événements dans la table **DATA**.

Recherche en libre-service pour l'isolation à distance du navigateur (Secure Browser)

December 7, 2023

Utilisez la recherche en libre-service pour obtenir des informations sur les sessions de navigation des utilisateurs de Citrix Workspace qui utilisent le Citrix Remote Browser Isolation Service. Citrix Remote Browser Isolation est un service cloud qui fournit une expérience de navigation Internet sécurisée sans compromettre la sécurité du réseau de votre entreprise. Lorsque les utilisateurs accèdent à des applications Web à l'aide de Remote Browser Isolation, des événements tels que la connexion à une session, le lancement de session, les applications publiées et les applications supprimées sont générés pour chaque connexion utilisateur. Citrix Analytics for Security reçoit ces événements et les affiche sur la page en libre-service. Vous pouvez suivre les utilisateurs et leurs sessions de navigation.

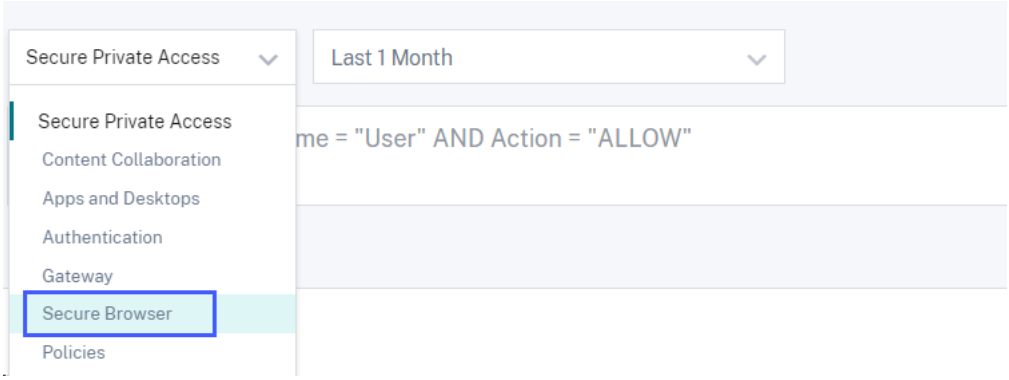
Pour plus d'informations sur les fonctionnalités de recherche, consultez la rubrique **Recherche en libre-service**.

Conditions préalables

Pour recevoir des événements provenant de Remote Browser Isolation, activez le **suivi des noms d'hôtes** dans Remote Browser Isolation afin d'enregistrer les noms d'hôtes des sessions utilisateur. Ces informations sont envoyées à Citrix Analytics pour la sécurité. Pour plus d'informations, voir Gérer les isolations de navigateurs distants publiées.

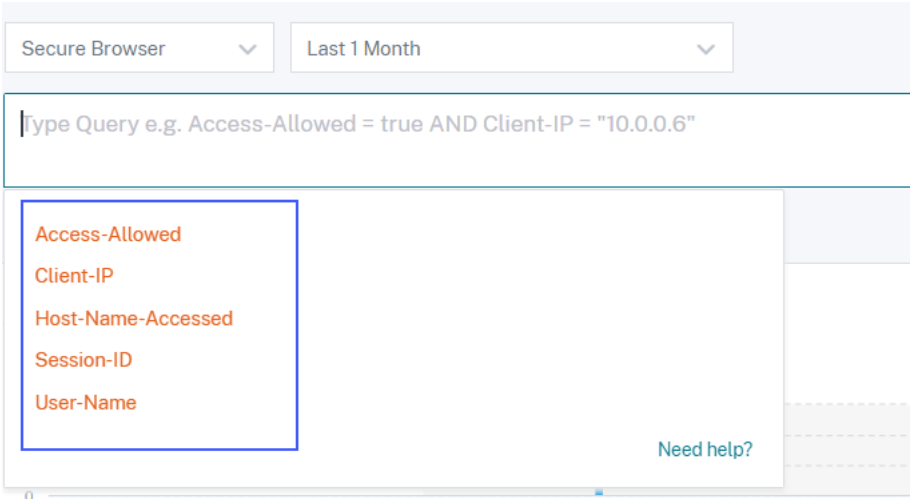
Sélectionner la source de données de Remote Browser Isolation

Pour afficher les événements de Remote Browser Isolation, sélectionnez **Remote Browser Isolation** dans la liste. Par défaut, la page en libre-service affiche les événements du dernier jour. Vous pouvez également sélectionner la période pendant laquelle vous souhaitez afficher les événements.



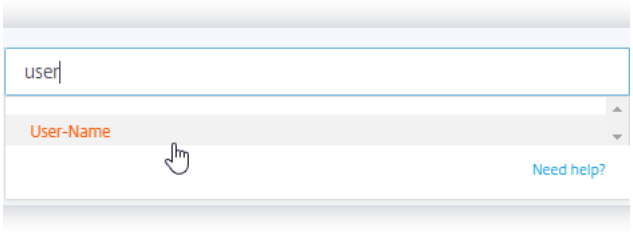
Spécifier la requête de recherche pour filtrer les événements

Placez votre curseur dans la zone de recherche pour afficher la liste des dimensions des événements de Remote Browser Isolation. Utilisez les dimensions et les opérateurs pour spécifier votre requête et rechercher les événements requis.

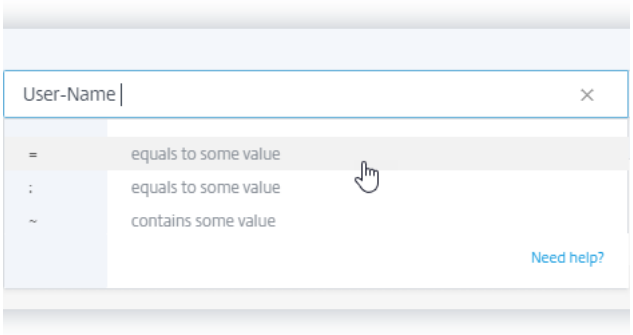


Par exemple, vous souhaitez afficher les détails de l'événement de navigation d'un utilisateur « aa » autorisé à accéder à divers services hôtes tels que google.com, amazon.com.

1. Saisissez « utilisateur » dans la zone de recherche pour afficher les dimensions associées.



2. Cliquez sur **Nom d'utilisateur** et saisissez la valeur « aa » à l'aide de l'opérateur égal.



3. Sélectionnez l'opérateur **AND** et la dimension **Allow-Access** . Attribuez la valeur « true » à **Allow-Access à** l'aide de l'opérateur égal. La valeur « true » indique que l'utilisateur peut accéder aux services hôtes.

4. Sélectionnez la période et cliquez sur **Rechercher** pour afficher les événements dans la table **DATA**.

Afficher les détails de l'événement utilisateur

Vous pouvez consulter les données suivantes reçues de Remote Browser Isolation Service:

- **Heure** : date et heure auxquelles l'événement utilisateur s'est produit.
- **Nom d'utilisateur** : utilisateur qui a initié l'événement.
- **ID de session** : numéro unique attribué à la session utilisateur.
- **IP du client** : adresse IP de la machine utilisateur.

- **Nom d'hôte** : service hôte auquel l'utilisateur accède via le réseau.
- **Autoriser l'accès**- L'utilisateur est autorisé ou refusé l'accès au service hôte.

Recherche en libre-service pour un accès privé sécurisé

April 12, 2024

Utilisez la recherche en libre-service pour obtenir des informations sur les événements d'accès des utilisateurs Citrix Cloud de votre organisation. Les exemples d'événements d'accès sont la catégorie d'URL, la catégorie de contenu, les navigateurs et les appareils. Citrix Analytics for Security reçoit ces événements du service Secure Private Access et les affiche dans la recherche en libre-service. Vous pouvez suivre les utilisateurs et leurs détails d'accès.

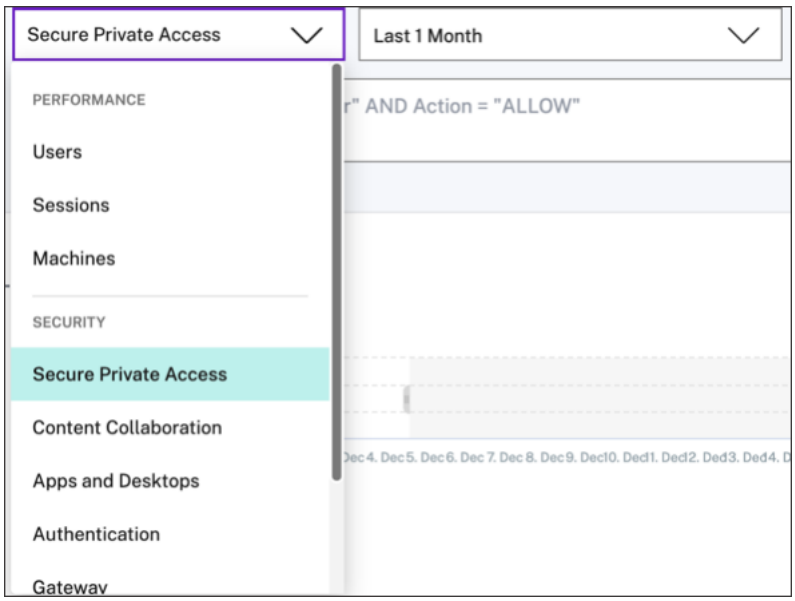
Pour plus d'informations sur les fonctionnalités de recherche, consultez la rubrique **Recherche en libre-service**.

> **Remarque**
>
> Les fonctionnalités suivantes de Citrix Analytics for Security sont affectées par l'abandon du filtrage Web basé sur les catégories par Secure Private Access :
>
> 1. Les champs de données tels que le groupe de catégories, la catégorie et la réputation des URL ne sont plus disponibles sur le tableau de bord Citrix Analytics for Security.
> 2. L'indicateur Risky d'accès au site Web, qui repose sur les mêmes données, est également obsolète et n'est pas déclenché pour les clients.
> 3. Les indicateurs de risque personnalisés existants utilisant les champs de données (catégorie-groupe, catégorie et réputation des URL) et les stratégies associées ne sont plus déclenchés.

Pour plus de détails sur la dépréciation de Secure Private Access, consultez la section Obsolète des fonctionnalités.

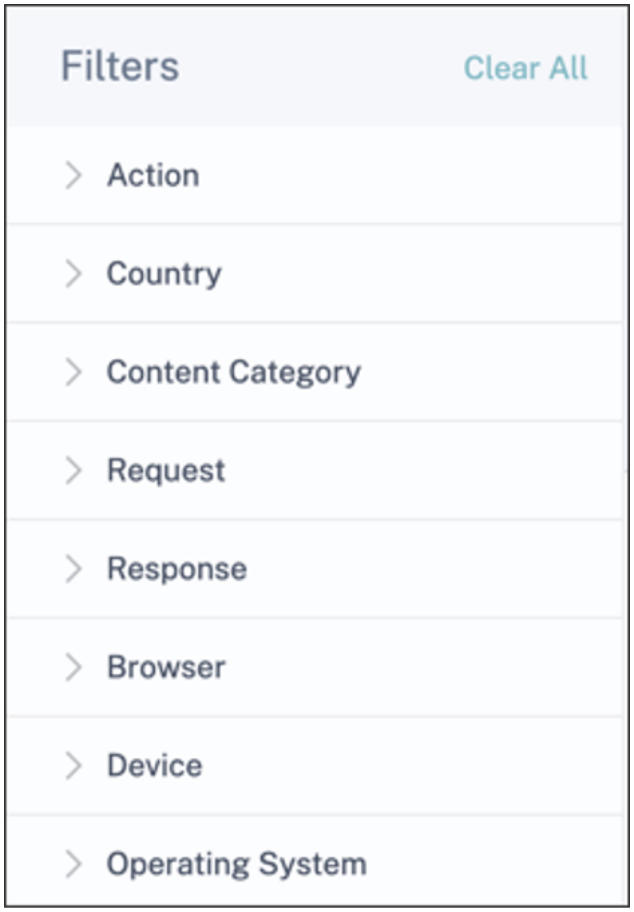
Sélectionnez la source de données Secure Private Access

Pour afficher les événements Secure Private Access, sélectionnez **Secure Private Access** dans la liste. Par défaut, la page en libre-service affiche les événements du dernier jour. Vous pouvez également sélectionner la période pendant laquelle vous souhaitez afficher les événements.



Sélectionnez les facettes pour filtrer les événements

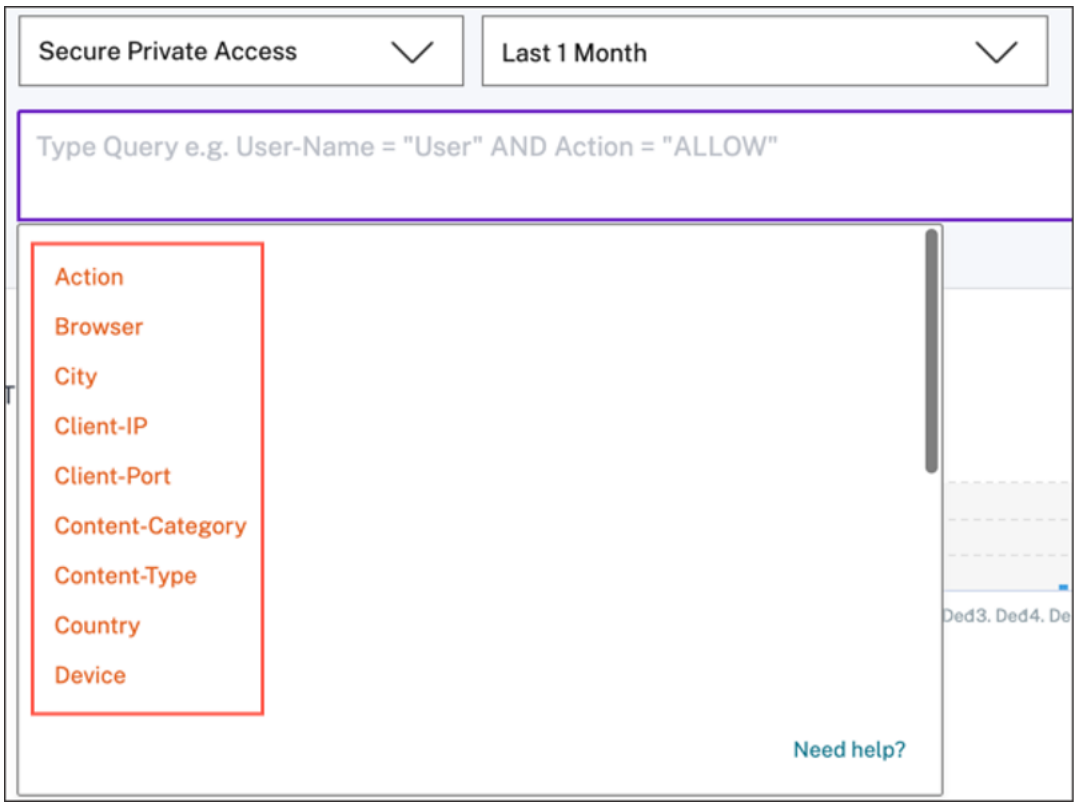
Utilisez les facettes suivantes associées aux événements Secure Private Access.



- **Action**- Recherchez des événements en fonction des actions effectuées sur les applications des utilisateurs, telles que autoriser, bloquer et rediriger.
- **Pays** : recherchez des événements en fonction des emplacements d'accès des utilisateurs.
- **Catégorie de contenu** : recherchez des événements en fonction des catégories de contenus consultés, telles que l'application, l'image et le texte.
- **Request**- Recherchez des événements en fonction des méthodes HTTP telles que GET, POST, PUT, DELETE.
- **Réponse** : recherche des événements en fonction de la réponse HTTP.
- **Navigateur**- Recherchez les événements en fonction des navigateurs utilisés par les utilisateurs.
- **Appareil**- Recherchez des événements en fonction des appareils utilisés tels que les téléphones Android, iPhone, MacBook.
- **Système d'exploitation**- Recherchez les événements en fonction des systèmes d'exploitation installés sur les périphériques.

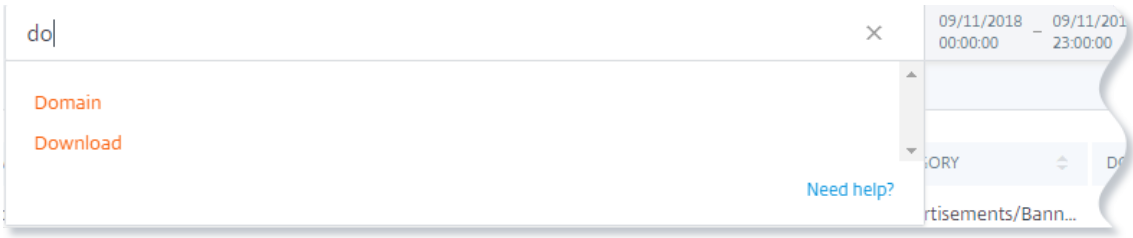
Spécifier la requête de recherche pour filtrer les événements

Placez votre curseur dans la zone de recherche pour afficher la liste des dimensions des événements Secure Private Access. Utilisez les dimensions et les opérateurs pour spécifier votre requête et rechercher les événements requis.

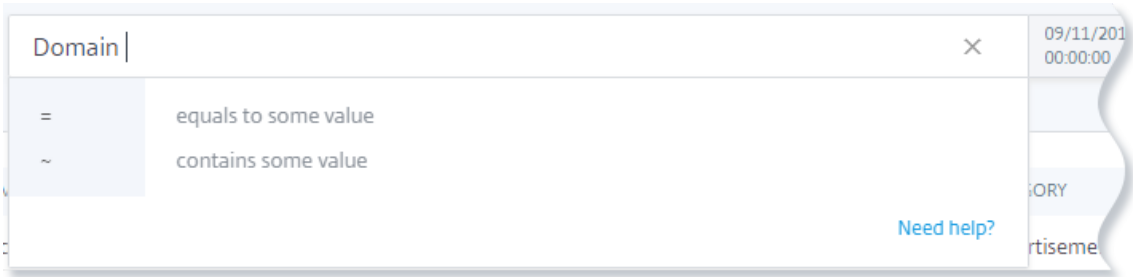


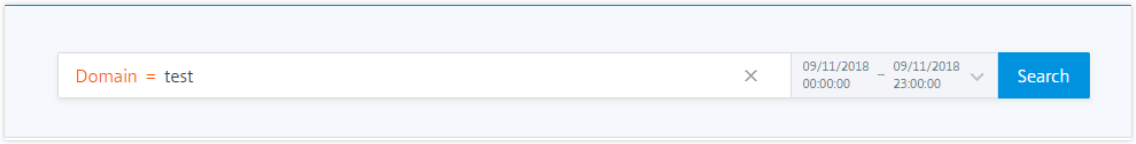
Par exemple, vous souhaitez afficher les domaines de test dans lesquels le volume de téléchargement de données est supérieur à 2 000 octets. Spécifiez votre requête de recherche comme suit :

1. Entrez « faire » dans le champ de recherche pour obtenir les suggestions correspondantes.

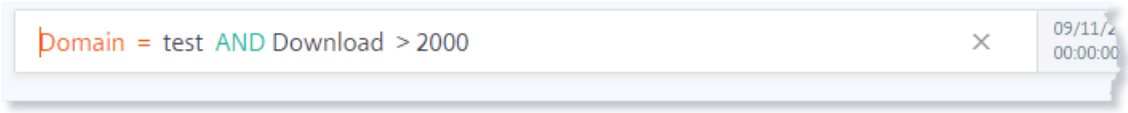


2. Cliquez sur **Domaine**, puis spécifiez la valeur « test » à l'aide de l'opérateur égal.





3. Utilisez l'opérateur **AND**, puis sélectionnez la dimension **Télécharger** . Sélectionnez l'opérateur ** et saisissez le volume de téléchargement en octets.



4. Sélectionnez la période et cliquez sur **Rechercher** pour afficher les événements dans la table **DATA**.

Recherche en libre-service d'applications et de bureaux

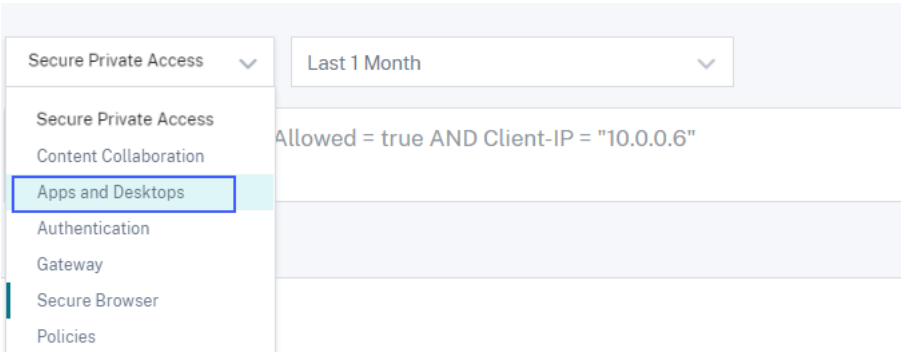
February 9, 2024

Utilisez la recherche en libre-service pour obtenir des informations sur les événements utilisateur reçus à partir de la source de données Citrix Virtual Apps and Desktops et de la source de données Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service). Lorsque les utilisateurs utilisent des applications virtuelles ou des bureaux virtuels, des événements correspondant à leurs activités et à leurs actions sont générés. Le téléchargement de fichiers, la connexion au compte et le démarrage de l'application sont des exemples d'événements utilisateur. Citrix Analytics for Security reçoit ces événements utilisateur et les affiche sur la page en libre-service. Vous pouvez suivre les utilisateurs et leurs activités.

Pour plus d'informations sur les fonctionnalités de recherche, consultez la rubrique **Recherche en libre-service**.

Sélectionnez la source de données Apps and Desktops

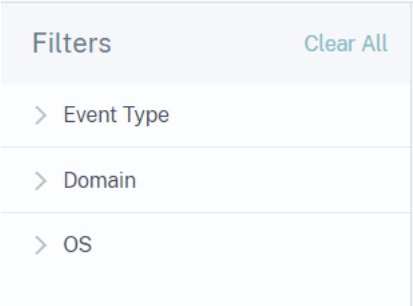
Pour afficher les événements depuis Citrix Virtual Apps and Desktops ou Citrix DaaS, sélectionnez **Apps and Desktops** dans la liste. Par défaut, la page en libre-service affiche les événements du dernier jour. Vous pouvez également sélectionner la période pendant laquelle vous souhaitez afficher les événements.



Par défaut, la page libre-service affiche les événements du dernier mois. La page propose également plusieurs facettes et un champ de recherche pour filtrer et se concentrer sur les événements requis.

Sélectionnez les facettes pour filtrer les événements

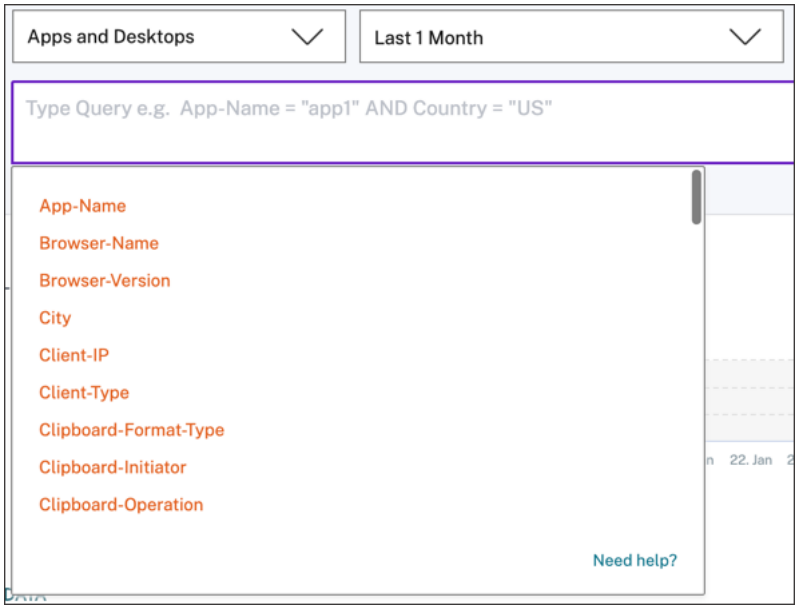
Utilisez les facettes suivantes associées aux événements Apps and Desktops.



- **Type d'événement** : recherchez des événements en fonction du type d'événement, comme la connexion au compte, la fin de l'application et la fin de la session.
- **Domaine**- Rechercher des événements basés sur les domaines tels que citrate.net.
- **OS** : recherchez des événements en fonction des systèmes d'exploitation tels que Chrome, iOS et Windows utilisés sur l'appareil de l'utilisateur. Sélectionnez le nom et les versions du système d'exploitation pour filtrer les événements. Pour plus d'informations sur les versions du système d'exploitation, consultez Valeurs prises en charge pour votre requête de recherche.

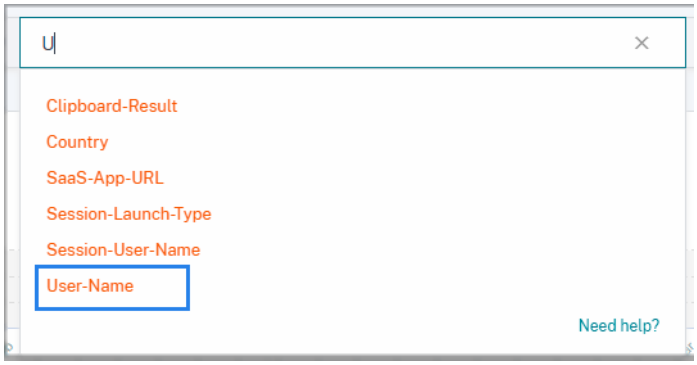
Spécifier la requête de recherche pour filtrer les événements

Placez votre curseur dans la zone de recherche pour afficher la liste des dimensions des événements Apps and Desktops. Utilisez les dimensions et les opérateurs pour spécifier votre requête et rechercher les événements requis.

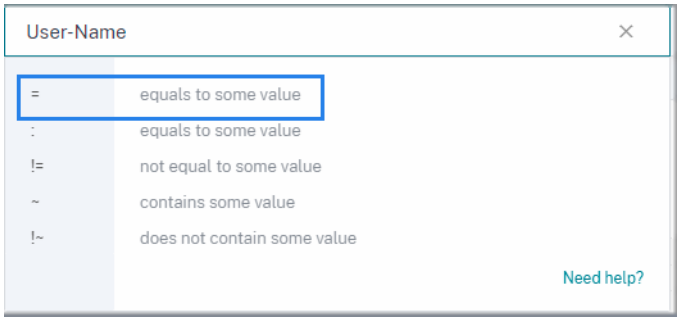


Par exemple, vous souhaitez rechercher des événements pour l'utilisateur « John Doe » qui utilise le système d'exploitation Windows.

1. Entrez « U » dans le champ de recherche pour obtenir les suggestions correspondantes.



2. Cliquez sur **Nom d'utilisateur** et saisissez la valeur « John » à l'aide de l'opérateur égal.



3. Sélectionnez l'opérateur **AND** et la dimension **Nom du système** d'exploitation. Attribuez la valeur « Windows 7 » à l'aide de l'opérateur égal.


```
User-Name = "John" AND OS-Name = "Windows 7"
```

4. Sélectionnez la période et cliquez sur **Rechercher** pour afficher les événements basés sur la table **DATA**.

Types d'événements et champs pris en charge

Les champs suivants sont disponibles pour tous les types d'événements à l'exception de VDA.Print :

- City
- IP du client
- Pays
- ID de l'appareil
- Nom de l'OS
- Version d'OS
- Informations supplémentaires du système d'exploitation
- Heure
- Nom d'utilisateur
- Version de l'application Workspace
- État de l'application Workspace

Le tableau suivant décrit les types d'événements disponibles pour la source de données Apps and Desktops et les champs spécifiques à chaque type d'événement.

Valeur	Description	Champs
`Account.Logon`	Se déclenche lorsque vous vous connectez au Store via l'application Citrix Workspace. **Remarque** : Account.Logon n'est pas disponible pour le client HTML5.	Vérifiez les champs communs comme décrit ci-dessus.

Valeur	Description	Champs
`Session.Logon`	Se déclenche lorsque vous vous connectez à votre session virtuelle.	Politiques de protection des applications, domaine, type de lancement de session, nom du serveur de session, nom d'utilisateur de session
`Session.End`	Se déclenche lorsque vous mettez fin à votre session virtuelle.	Domaine, type de lancement de session, nom du serveur de session, nom d'utilisateur de session
`App.Start`	Se déclenche lorsque vous démarrez une session d'application virtuelle. **Remarque** : Ce type d'événement ne s'applique pas lorsque l'application est lancée au cours de la session de bureau.	Nom de l'application, domaine, type de lancement de session, nom du serveur de session, nom d'utilisateur de session
`App.End`	Se déclenche lorsque vous mettez fin à une session d'application virtuelle. **Remarque** : Ce type d'événement ne s'applique pas lorsque l'application est lancée au cours de la session de bureau.	Nom de l'application, domaine, type de lancement de session, nom du serveur de session, nom d'utilisateur de session

Valeur	Description	Champs
`File.Download`	Se déclenche lorsqu'un utilisateur copie un fichier depuis une session virtuelle distante vers l'appareil client. Il n'est pas déclenché pour les transferts de fichiers qui se produisent au cours des sessions virtuelles. **Remarque** : Ce type d'événement est envoyé uniquement lorsque le serveur autorise la redirection de fichiers (consultez les paramètres de redirection de fichiers pour plus de détails) et que la préférence d'**accès aux fichiers** de l'espace de travail client est définie sur **Lecture et écriture**.	Domaine, type de périphérique de téléchargement, nom du fichier de téléchargement, chemin du fichier de téléchargement, taille du fichier de téléchargement, nom du serveur de session, nom d'utilisateur de session

Valeur	Description	Champs
`Printing`	Se déclenche lorsque vous imprimez un fichier alors que l'application Citrix Workspace lance une session via une imprimante cliente. **Remarque** : L'application Citrix Workspace présente deux limitations techniques qui affectent les événements d'impression. Tout d'abord, la télémétrie du nom du document imprimé n'est pas incluse dans l'événement d'impression en raison d'un problème connu sur toutes les variantes de plate-forme. Deuxièmement, la télémétrie relative à la taille du fichier imprimé n'est pas incluse dans l'événement d'impression pour Windows en raison d'une autre limitation technique connue. Pour collecter ces ensembles de données (nom du fichier/taille du fichier), utilisez l'événement VDA.print. Pour plus d'informations, voir Activation de la télémétrie d'impression pour Citrix DaaS.	Nom du navigateur, version du navigateur, domaine, nom de l'imprimante, format du fichier d'impression, taille du fichier d'impression, nom du serveur de session, nom d'utilisateur de session
`AppProtection.ScreenCapture`	Se déclenche lorsqu'un utilisateur essaie de capturer une capture d'écran pendant une session protégée. **Remarque** : Pour plus d'informations, consultez la section Protection des applications.	Titres des applications protégées, nom de l'outil de capture d'écran, chemin de l'outil de capture d'écran

Valeur	Description	Champs
App.SaaS.Launch	Se déclenche lorsque l'application Citrix Workspace lance une application SaaS dans Citrix Enterprise Browser.	Nom du navigateur, version du navigateur, nom de l'application SaaS, URL de l'application SaaS
App.SaaS.End	Se déclenche lorsque l'application Citrix Workspace ferme une application SaaS dans Citrix Enterprise Browser.	Nom du navigateur, version du navigateur, URL de l'application SaaS
App.SaaS.Clipboard	Déclenche lorsqu'une opération de presse-papiers est effectuée dans Citrix Enterprise Browser.	Nom du navigateur, version du navigateur, taille du format des détails du presse-papiers, type de format des détails du presse-papiers, initiateur des détails du presse-papiers, résultat des détails du presse-papiers, fonctionnement du presse-papiers, URL de l'application SaaS
App.SaaS.File.Download	Déclenche lorsqu'un fichier est téléchargé dans Citrix Enterprise Browser.	Nom du navigateur, version du navigateur, type de périphérique de téléchargement, chemin du fichier de téléchargement, taille du fichier de téléchargement
App.SaaS.File.Print	Se déclenche lorsque l'impression est lancée dans Citrix Enterprise Browser.	Nom du navigateur, version du navigateur, nom du fichier d'impression, nom de l'application SaaS, URL de l'application SaaS
App.SaaS.Url.Navigate	Se déclenche lorsque Citrix Enterprise Browser parcourt une URL.	Nom du navigateur, version du navigateur, nom de l'application SaaS, URL de l'application SaaS

Valeur	Description	Champs
Citrix.EventMonitor.AppStart	Se déclenche lorsqu'une application ajoutée à la liste de surveillance des applications du serveur d'enregistrement de session est démarrée au cours d'une session de bureau virtuel.	Nom de l'application
Citrix.EventMonitor.AppEnd	Se déclenche lorsqu'une application ajoutée à la liste de surveillance des applicationsdu serveur d'enregistrement de session est arrêtée au cours d'une session de bureau virtuel.	Nom de l'application
Citrix.EventMonitor.Clipboard	Se déclenche lorsqu'une action du presse-papiers a été exécutée au cours d'un enregistrement de session.	Type de format de données du presse-papiers, nom du processus, titre de la fenêtre
Citrix.EventMonitor.FileTransfer	Se déclenche lorsqu'un utilisateur transfère un fichier entre une session de bureau virtuel et la machine de l'utilisateur.	Taille du fichier, sens de fonctionnement (hôte vers client, client vers hôte), chemin source, chemin de destination
Citrix.EventMonitor.RegistryChange	Déclenche lorsqu'une opération de registre est effectuée. Les opérations de registre possibles sont les suivantes : créer, supprimer, renommer, définir une valeur et supprimer une valeur.	Fonctionnement du registre, nom du registre, chemin du registre, ID du processus, chemin du fichier de processus
Citrix.EventMonitor.SessionEnd	Se déclenche à la fin de l'enregistrement d'une session.	Description
Citrix.EventMonitor.SessionLaunch	Se déclenche lorsqu'un enregistrement de session a commencé.	Type d'enregistrement de session
Citrix.EventMonitor.TopMost	Déclenche lorsque la fenêtre située en haut de l'écran change.	Nom de l'application

Valeur	Description	Champs
Citrix.EventMonitor.IdleStart	Déclenche lorsque la session devient inactive.	Vérifiez les champs communs comme décrit ci-dessus.
Citrix.EventMonitor.IdleEnd	Déclenche à la fin d'une session inactive.	Vérifiez les champs communs comme décrit ci-dessus.
Citrix.EventMonitor.WebBrowsing	Se déclenche lorsque l'utilisateur interagit avec des pages Web sur des navigateurs au cours d'une session de bureau virtuel.	Nom de l'application, URL
Citrix.EventMonitor.FileCreate	Déclenche lorsqu'un fichier ou un dossier est créé dans une session de bureau virtuel dans le chemin du système de fichiers surveillé.	Nom du fichier, chemin du fichier, taille du fichier
Citrix.EventMonitor.FileRename	Déclenche lorsqu'un fichier ou un dossier est renommé dans une session de bureau virtuel à l'intérieur du chemin du système de fichiers surveillé.	Vérifiez les champs communs comme décrit ci-dessus.
Citrix.EventMonitor.FileMove	Se déclenche lorsqu'un fichier ou un dossier du chemin du système de fichiers surveillé est déplacé dans une session de bureau virtuel ou entre des hôtes de session (VDA) et des appareils clients.	Vérifiez les champs communs comme décrit ci-dessus.
Citrix.EventMonitor.FileDelete	Déclenche lorsqu'un fichier ou un dossier situé dans le chemin du système de fichiers surveillé est supprimé lors d'une session de bureau virtuel.	Nom du fichier, chemin du fichier, taille du fichier

Valeur	Description	Champs
`Citrix.EventMonitor.CDMUSBDriveAttach`	Se déclenche lorsqu'un périphérique de stockage de masse USB mappé CDM (Client Drive Mapping) est inséré dans un client à partir duquel la session virtuelle Apps and Desktop est connectée.	Vérifiez les champs communs comme décrit ci-dessus.
`Citrix.EventMonitor.GenericUSBDriveAttach`	Se déclenche lorsqu'un périphérique de stockage de masse USB redirigé générique est inséré dans un client à partir duquel la session virtuelle d'applications et de bureau est connectée.	Vérifiez les champs communs comme décrit ci-dessus.
`Citrix.EventMonitor.RDPConnection`	Se déclenche lorsqu'un utilisateur crée une connexion de bureau à distance au sein d'une machine VDA.	IP de destination, ID de processus
`Citrix.EventMonitor.UserAccountModification`	Déclencheurs pour tous les types d'opérations de compte utilisateur, à savoir la création, l'activation, la désactivation, la suppression, les changements de nom et la modification du mot de passe.	Description, nom d'utilisateur cible
`VDA.Print`	Se déclenche lorsqu'un travail d'impression est lancé dans Apps and Desktops. **Remarque** : Cet événement s'applique uniquement à la source de données Citrix DaaS. Pour plus d'informations, voir Activation de la télémétrie d'impression pour Citrix DaaS.	Nom d'utilisateur du document, nom de la machine, nom du fichier d'impression, taille du fichier d'impression, nom de l'imprimante, heure, nombre total de copies imprimées, total de pages imprimées

Valeur	Description	Champs
`VDA.Clipboard`	Se déclenche lorsqu'une opération de presse-papiers est effectuée dans Apps and Desktops. **Remarque** : Cet événement s'applique uniquement à la source de données Citrix DaaS. Pour plus d'informations, consultez la section Activation de la télémétrie du presse-papiers pour Citrix DaaS.	Type de format du bloc-notes, fonctionnement du bloc-notes, sens de fonctionnement du bloc-notes, Fonctionnement autorisé du bloc-notes, taille du bloc-notes, nom de la machine

> **Remarque**
>
> Tous les événements d'enregistrement de session nécessitent que la stratégie de journalisation de leurs événements soit activée sur le serveur d'enregistrement de session. Pour plus d'informations, consultez la section Créer une stratégie de détection d'événements personnalisée.

Valeurs prises en charge pour votre requête de recherche

Entrez les valeurs suivantes pour les dimensions afin de définir votre requête de recherche.

Dimension	Valeur	Type	Description
`App-Name`	Sessions d'application ou de bureau. Exemples de sessions d'application : Une session sans nom de batterie : `#Cloud - Excel 2016` Et une session avec le nom de batterie : `XA65PROD#Concur`	Chaîne	Nom d'une application ou d'un bureau lancé.

Dimension	Valeur	Type	Description
	Exemples de sessions de bureau : Une session sans nom de batterie : #SINXIAP0616 $S1-1et une session avec le nom de batterie de serveurs : XA65PROD# SINXIAP0616 $S1 -1		
App-Protection-Policies	Exemple : AntiScreenCaptureEnabled	Chaîne	Politiques de protection des applications actives pour la session.
Browser-Name	Exemple : Google Chrome, navigateur Citrix Enterprise, Microsoft Edge, FIREFOX, SAFARI	Chaîne	Nom du navigateur
Browser-Version	Exemple : 80.0.3987.122, 101.0.9999.0	Chaîne	Version du navigateur
City	Exemples : Santa Clara, Houston, Chicago	Chaîne	Le nom de la ville d'un utilisateur.
Client-IP	Une adresse IP. Exemple : 10.10.10.10	Chaîne	Adresse IP du point de terminaison utilisateur.
Client-Type	Android, Windows, Macintosh, Chrome, HTML5, Unix/Linux, iOS, enregistrement de session, moniteur	Chaîne	Indique différents types d'applications Citrix Workspace en fonction des systèmes d'exploitation ou de la source de données d'origine.

Dimension	Valeur	Type	Description
Clipboard-Format-Type	Exemples : text, html, CF_UNICODETEXT	Chaîne	Format de données copié dans le presse-papiers.
Clipboard-Initiator	Exemples : Clavier, menu contextuel, javascript	Chaîne	Indique comment l'opération du presse-papiers a été lancée. **Remarque** : Supporté uniquement par les applications SaaS.
Clipboard-Operation	Copier, couper, coller ou placer	Chaîne	Indique quelle opération du presse-papiers est effectuée. **Remarque** : L'opération de **placement** indique que les données sont placées dans le presse-papiers. Cela ne garantit pas si les données du presse-papiers ont été collées ou utilisées par le client. Cette opération n'est prise en charge que pour VDA.Clipboard Event.
Clipboard-Operation-Direction	Du client à l'hôte, de l'hôte au client	Chaîne	Indique le sens de fonctionnement du presse-papiers. **Remarque** : Pris en charge uniquement par Apps and Desktop (Citrix DaaS) Presse-papiers Operation.

Dimension	Valeur	Type	Description
Clipboard-Operation-Permitted	Autorisé ou refusé	Chaîne	Indique si l'utilisation du presse-papiers est autorisée dans les applications et la session de bureau. **Remarque** : Pris en charge uniquement par Apps and Desktop (Citrix DaaS) Presse-papiers Operation.
Clipboard-Result	Succès ou blocage	Chaîne	Indique le résultat de l'opération du presse-papiers. **Remarque** : Supporté uniquement par les applications SaaS.
Clipboard-Size	Exemples : 10, 20	Nombre	Taille des données (en octets) actuellement stockées dans le presse-papiers.
Country	Exemples : États-Unis, Inde	Chaîne	Le nom du pays d'un utilisateur.
Description	**Pour les** `Citrix.EventMonitor.UserAccountModification` **événements** : un compte utilisateur a été créé, un compte utilisateur a été activé, une tentative a été faite pour réinitialiser le mot de passe d'un compte.	Chaîne	Décrit l'état de modification du compte utilisateur, par exemple si le compte a été créé, supprimé, renommé ou si une tentative a été faite pour réinitialiser le mot de passe.

Dimension	Valeur	Type	Description
	Pour les `Citrix.EventMonitor.SessionEnd` **événements**suivants : Inconnu, Déconnexion, Annulation, Déconnexion, Déclencheur et Incomplet		Décrit la raison de la fin de l'enregistrement de session.
`Destination-IP`	Exemple : 10.60.110.xxx	Chaîne	Adresse IP du poste de travail distant.
`Destination-Path`	Exemple : \H$\Desktop\Folder\example.txt	Chaîne	Le chemin final du fichier une fois le transfert terminé.
`Device-ID`	Exemple : cb781185-18ad-4f45-b75f	Chaîne	ID de périphérique utilisé pour les licences, le nom du client ou l'ID matériel du système d'exploitation.
`Domain`	Exemple : exemple.com	Structure	Le nom de domaine d'un serveur qui a envoyé une demande.
`Download-Device-Type`	Exemples : USB, disque dur, RemoteDrive, CD-ROM ou téléchargements par navigateur.	Chaîne	Type d'appareil sur lequel le fichier est téléchargé ou transféré.
`Download-File-Format`	Exemple : txt, PDF, xlsx, docx	Chaîne	Le format du fichier téléchargé.
`Download-File-Name`	Exemple : example-file.txt	Chaîne	Nom du fichier téléchargé.
`Download-File-Path`	Exemple : C:\Users\admin\Desktop	Chaîne	Chemin d'accès du fichier téléchargé.

Dimension	Valeur	Type	Description
Download-File-Size	Exemple : 8.05	Nombre	Taille du fichier téléchargé en kilo-octets.

Dimension	Valeur	Type	Description
Event-Type	Account.Logon, Session.Logon, Session.End, App.Start, App.End, File.Download, Printing, AppProtection.ScreenCapture, App.SaaS.Launch, App.SaaS.End, App.SaaS.Clipboard, App.SaaS.File.Download, App.SaaS.File.Print, App.SaaS.Url.Navigate, Citrix.EventMonitor.AppStart, Citrix.EventMonitor.AppEnd, Citrix.EventMonitor.TopMost, Citrix.EventMonitor.WebBrowsing, Citrix.EventMonitor.FileCreate, Citrix.EventMonitor.FileRename, Citrix.EventMonitor.FileMove, Citrix.EventMonitor.FileDelete, Citrix.EventMonitor.CDMUSBDriveAttach, Citrix.EventMonitor.GenericUSBDriveAttach, Citrix.EventMonitor.RDPConnection, Citrix.EventMonitor.UserAccountModification, VDA.Print, VDA.Clipboard, Citrix.EventMonitor.RegistryChange, Citrix.EventMonitor.SessionLaunch, Citrix.EventMonitor.SessionEnd,	Chaîne	Pour plus de détails, consultez la section [Types d'événements et champs pris en charge.] (#event-types-and-supported-fields)

Dimension	Valeur	Type	Description
Jail-Broken	Oui ou Non	Chaîne	Indique si l'appareil est enraciné ou non. **Remarque** : Si cette dimension est absente, l'appareil n'est pas rooté. Cette clé s'applique à l'application Citrix Workspace pour appareils iOS et Android.
Operation-Direction	Hôte vers client/Client vers hôte	Chaîne	Indique la direction du transfert de fichiers.
OS-Extra-Info	Exemple : 20G80, Service Pack 1, 19043	Chaîne	Indique les informations supplémentaires relatives au système d'exploitation, telles que les numéros de version, les service packs et les correctifs.
OS-Name	Exemple : macOS 11, Windows 7, Android 8.1, Windows 10 Enterprise	Chaîne	Indique le nom du système d'exploitation.
OS-Version	Exemple : 11.5.1, 14.7.1, 2009	Chaîne	Indique la version du système d'exploitation
Print-File-Format	Exemples : PDF, PS, DOCX	Chaîne	Format du fichier imprimé.
Print-File-Name	Exemple : example-file.pdf	Chaîne	Nom du fichier imprimé.
Print-File-Size	Exemples : 10, 20	Chaîne	Taille du fichier imprimé en octets.
Printer-Name	Exemple : testprinter-1	Chaîne	Nom de l'imprimante utilisée.

Dimension	Valeur	Type	Description
Process-ID	Exemple : 11248	Chaîne	Fait référence à l'ID de processus utilisé pour identifier le processus spécifique qui exécute deux actions : **créer un nouveau processus** et **établir une connexion de bureau à distance**. L'ID de processus est actuellement associé uniquement à l'événement Citrix.EventMonitor.RDPConnection.
Protected-App-Titles	Exemple : Admin Desktop - Citrix Workspace	Chaîne	Nom de l'application exécutée dans la session protégée.
Registry-Name	Nom du registre modifié	Chaîne	Le nom du registre qui a été modifié.
Registry-Operation	Rename, Create, Delete, SetValue, DeleteValue	Chaîne	Indique quelle opération de registre a été effectuée.
Registry-Path	Chemin du registre modifié	Chaîne	Le chemin du registre qui a été modifié.
SaaS-App-Name	Exemple : Workday	Chaîne	Nom de l'application SaaS.
SaaS-App-URL	Exemple : https://xyz.com|String	Chaîne	URL de l'application SaaS ou URL de la passerelle/du proxy. **Remarque** : L'URL de la passerelle/du proxy apparaît dans l'événement App.Saas.Launch lorsque l'application SaaS est lancée initialement.

Dimension	Valeur	Type	Description
Screen-Capture-Tool-Name	Exemple : ScreenShotTool.exe	Chaîne	Nom de l'outil de capture d'écran.
Screen-Capture-Tool-Path	Exemple : c:\Program files (x86)\ScreenContent Client	Chaîne	Chemin de l'outil de capture d'écran.
Session-Launch-Type	Application ou ordinateur de bureau	Chaîne	Indique si la session lancée est de type application ou bureau.
Session-Recording-Type	Enregistrement classique/Enregistrement d'événements uniquement	Chaîne	Indique le type d'enregistrement de session lancé.
Session-Server-Name	Exemples : bureau hébergé, Cloud-VDA-1	Chaîne	Nom de l'application ou du bureau auquel vous êtes connecté tel qu'il a été reçu d'un serveur.
Session-User-Name	Exemples : utilisateur de démonstration, utilisateur de test	Chaîne	Nom d'utilisateur reçu du serveur.
Source-Path	Exemple : C:\Users\admin\Desktop\example.txt	Chaîne	Le chemin initial du fichier avant son transfert.
Target-User-Name	Exemples : user01	Chaîne	Actuellement, le nom d'utilisateur cible est uniquement utilisé pour l'événement Citrix.EventMonitor.UserAccountModif dans lequel c'est le compte utilisateur qui a été modifié.
Total-Copies-Printed	Exemples : 1, 2	Nombre	Nombre total de copies imprimées par l'utilisateur.

Dimension	Valeur	Type	Description
Total-Pages-Printed	Exemples : 1,2	Nombre	Nombre total de pages du document imprimées par l'utilisateur.
User-Name	nom d'utilisateur ou Domaine \ nom d'utilisateur	Chaîne	Le nom d'utilisateur ou le domaine \ nom d'utilisateur. Utilisé pour la connexion StoreFront. Si l'ouverture de session StoreFront ne se fait pas via l'application Citrix Workspace pour HTML5 ou Chrome, cette valeur est identique à celle reçue du serveur.
VDA-Name	Exemple : TSVDA-19-01.xd.Local	Chaîne	Indique le nom de la machine VDA.
Window-Title	Exemple : Administrateur - 01 Command Prompt	Chaîne	Indique le titre de la fenêtre dans laquelle l'opération de presse-papiers a été effectuée.
Workspace-App-Version	Exemple : 20.8.0.3 (2008)	Chaîne	Version de l'application Citrix Workspace ou de Citrix Receiver installée sur l'appareil de l'utilisateur et utilisée pour lancer des applications virtuelles et des sessions de bureau à distance.

Dimension	Valeur	Type	Description
Workspace-App-Status	Pris en charge ou non	Chaîne	Indique si la version installée de l'application Citrix Workspace ou de Citrix Receiver sur l'appareil de l'utilisateur est prise en charge ou non par Citrix Analytics for Security. Passez la souris sur **Non pris en charge** lorsque l'application Workspace n'est pas prise en charge. Une fenêtre contextuelle contenant un lien permettant d'afficher la liste des versions prises en charge s'affiche. Lorsqu'une version de l'application Workspace est sur le point de devenir non prise en charge, une bannière s'affiche sur la page de recherche en libre-service, répertoriant les versions prises en charge disponibles vers lesquelles vous pouvez lancer une mise à niveau.

Format de dénomination du système d'exploitation

Citrix Analytics reçoit les détails du système d'exploitation (SE) d'une machine utilisateur et les traduit en nom du système d'exploitation, version du système d'exploitation et informations supplémentaires sur le système d'exploitation.

- Le**nom du système d'exploitation** indique le nom du système d'exploitation.
- La**version du système d'exploitation** indique l'ID de version ou la version de lancement du système d'exploitation.
- Les**informations supplémentaires du système d'exploitation** indiquent les informations supplémentaires du système d'exploitation, telles que les numéros de version, les Service Packs et les correctifs.

Le tableau suivant fournit quelques exemples du format de numérotation des versions des systèmes d'exploitation.

Nom de l'OS	Version d'OS	Informations supplémentaires du système d'exploitation
macOS 11	11.5.1	20G80
iOS 14	14.7.1	Non disponible
Windows 10 Entreprise	2009	19043
Windows 7	6.1	Service Pack 1
Android 8.1	8.1.0	Non disponible

> **Remarques**
>
> - Pour obtenir les détails du système d'exploitation pour Mac version 11.x ou ultérieure, la version client recommandée est l'application Citrix Workspace pour Mac 2108 ou version ultérieure.
> - Les détails du système d'exploitation pour Windows 10 ne sont actuellement pas disponibles.

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.

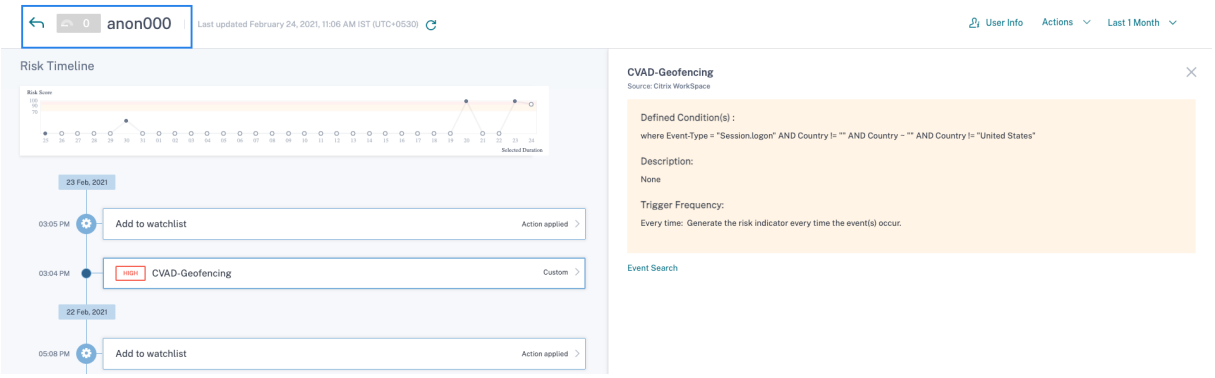
- Vérifiez que les utilisateurs anonymes sont des utilisateurs légitimes.
- Résoudre les problèmes de transmission d'événements à partir d'une source de données.
- Déclenchez des événements Virtual Apps and Desktops, des événements SaaS et vérifiez la transmission des événements à Citrix Analytics for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

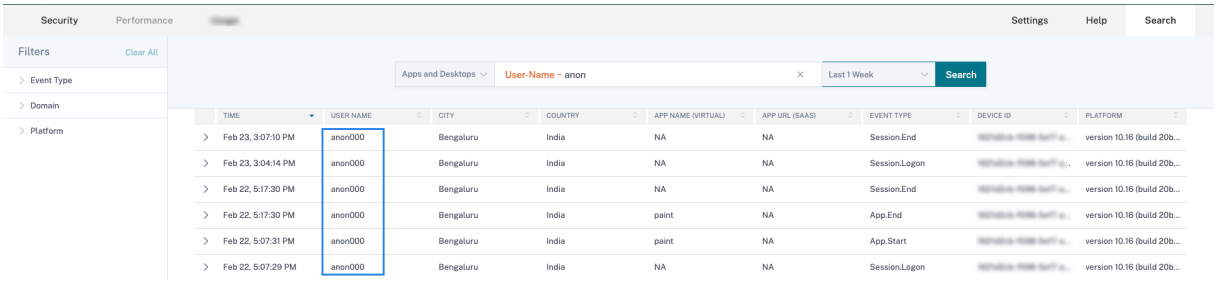
Vérifiez que les utilisateurs anonymes sont des utilisateurs légitimes

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

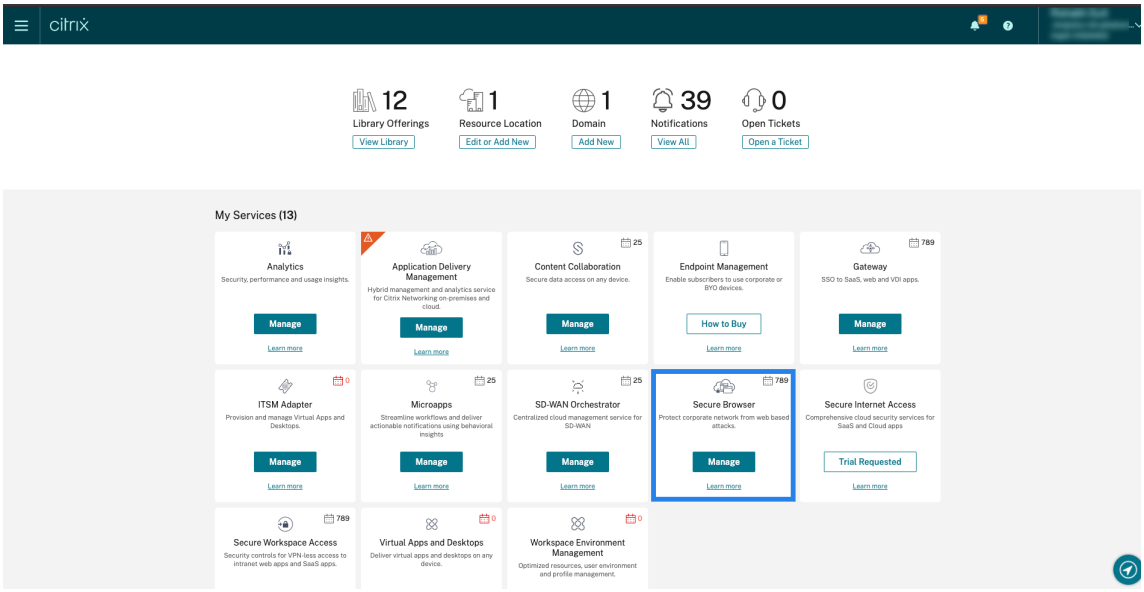
Utilisateur utilisant des applications de navigateur sécurisées publiées

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.

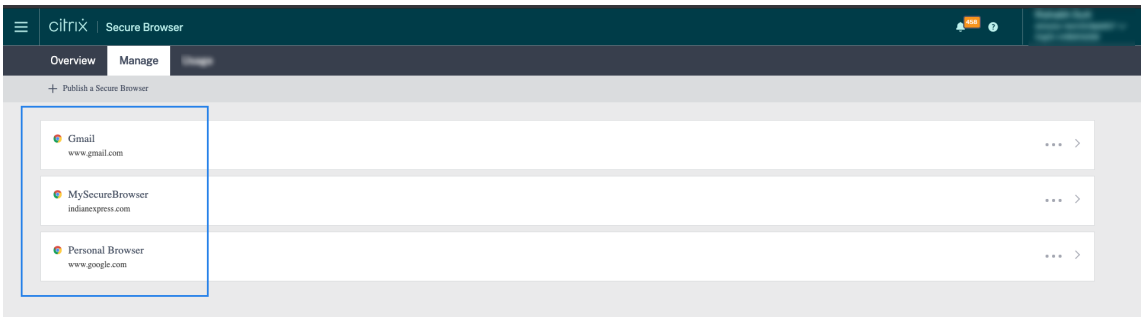
Les applications de navigateur sécurisées utilisent la fonctionnalité de session anonyme de Citrix DaaS.

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.

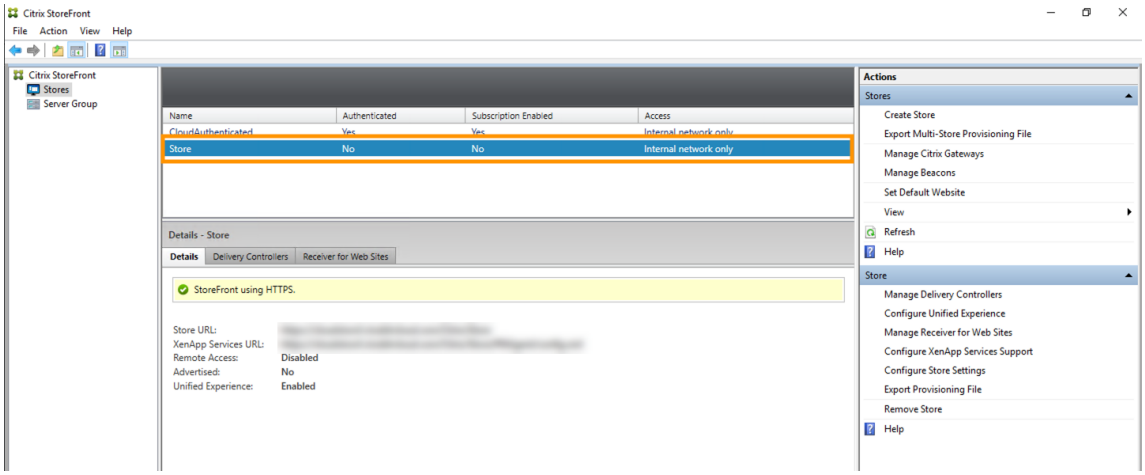
Vous pouvez donc considérer l'utilisateur comme un utilisateur légitime de votre organisation. Vous n'avez pas besoin d'appliquer d'action si aucun comportement à risque n'est associé à l'utilisateur.

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 ?

Séquence	Chèques
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 ?

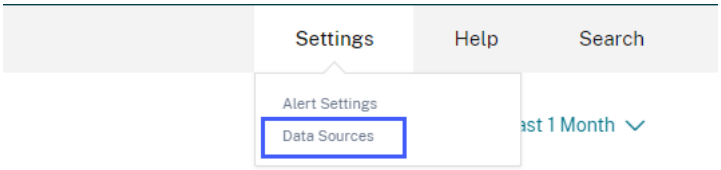
Assurez-vous que toutes vos sources de données sont découvertes et que vous avez activé le traitement des données pour elles. Si vous n'activez pas le traitement des données pour une source de données, les utilisateurs utilisant la source de données ne sont pas découverts. Cette situation peut créer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

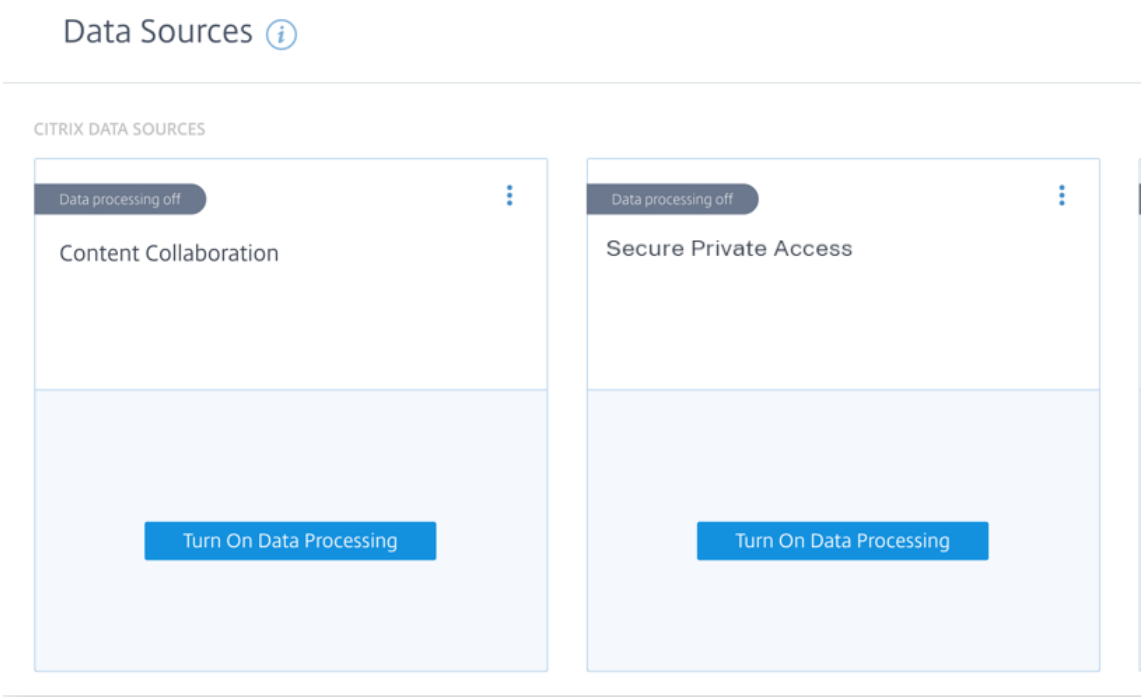
Pour découvrir vos sources de données et activer les analyses, procédez comme suit :

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.

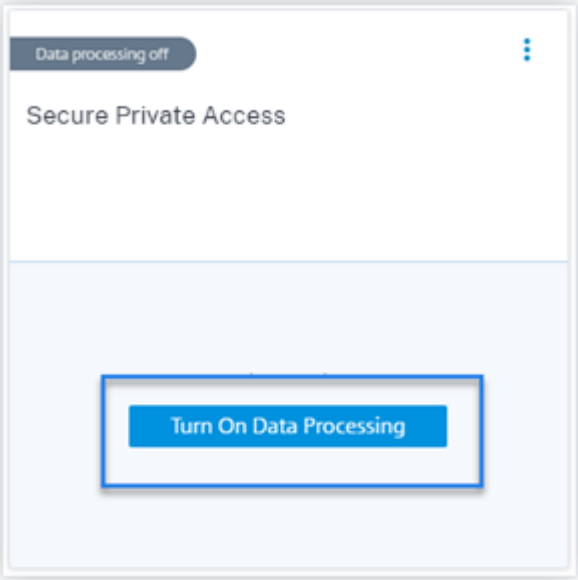


2. Sur la page **Sources de données**, les sources de données découvertes apparaissent sous forme de fiches de site. Par défaut, le traitement des données est désactivé.

> **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 ?

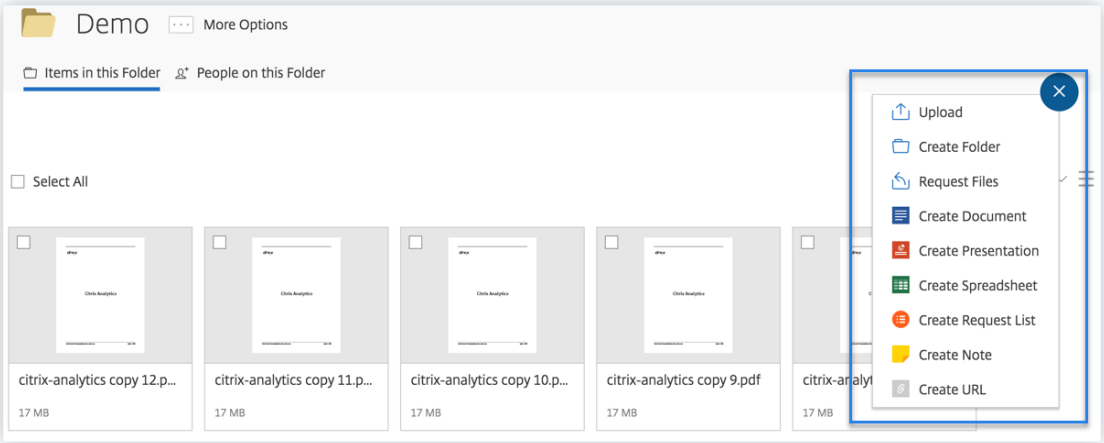
Citrix Analytics reçoit des événements utilisateur provenant des sources de données lorsque les utilisateurs utilisent activement les sources de données. Les utilisateurs doivent effectuer certaines activités sur la source de données pour générer des événements. Par exemple, pour recevoir des événements 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.

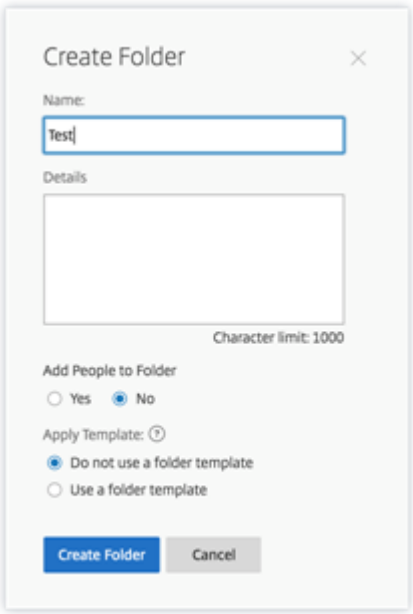
Si vous ne voyez aucun événement utilisateur dans Citrix Analytics pour votre source de données, il est fort probable que les utilisateurs ne soient pas actifs à ce moment-là.

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.

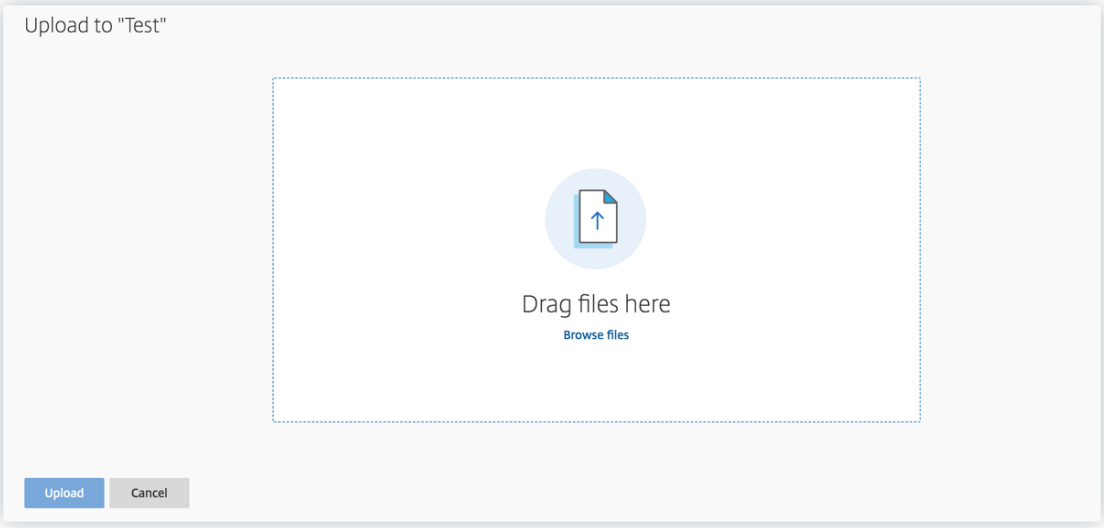
1. Ouvrez une session sur le service Citrix Apps and Desktops.
2. Effectuez certaines activités habituelles de l'utilisateur, telles que créer un dossier, télécharger des fichiers, télécharger des fichiers ou supprimer des fichiers.



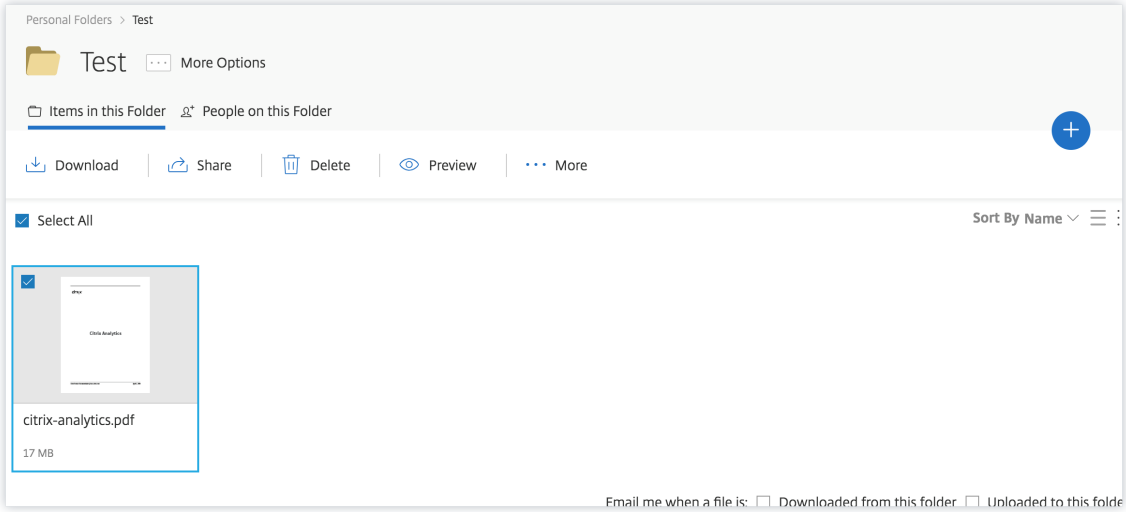
3. Par exemple, créez un dossier Test.



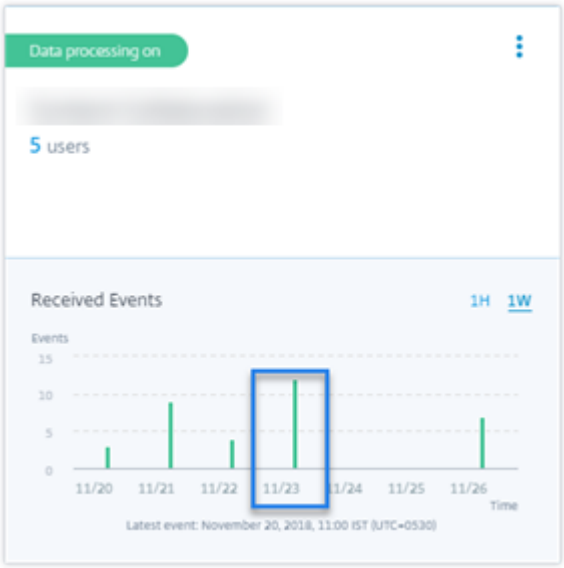
4. Téléchargez des fichiers locaux.



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 :

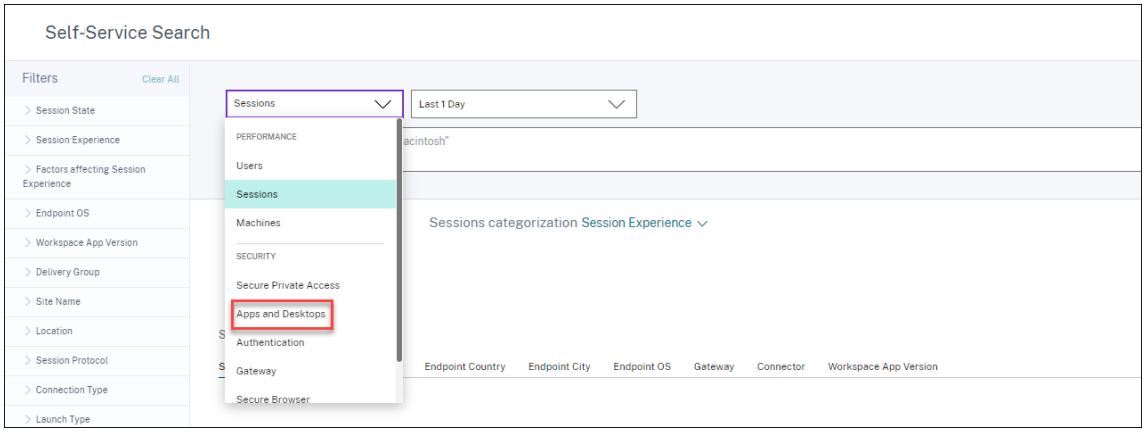
- **Utilisateur Windows** : connectez-vous à votre Citrix Virtual Apps and Desktops et Citrix DaaS application Citrix Workspace pour Windows 1907 ou version ultérieure.
- **Utilisateur Mac** : connectez-vous à Citrix Virtual Apps and Desktops et Citrix DaaS l'aide de l' application Citrix Workspace pour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

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

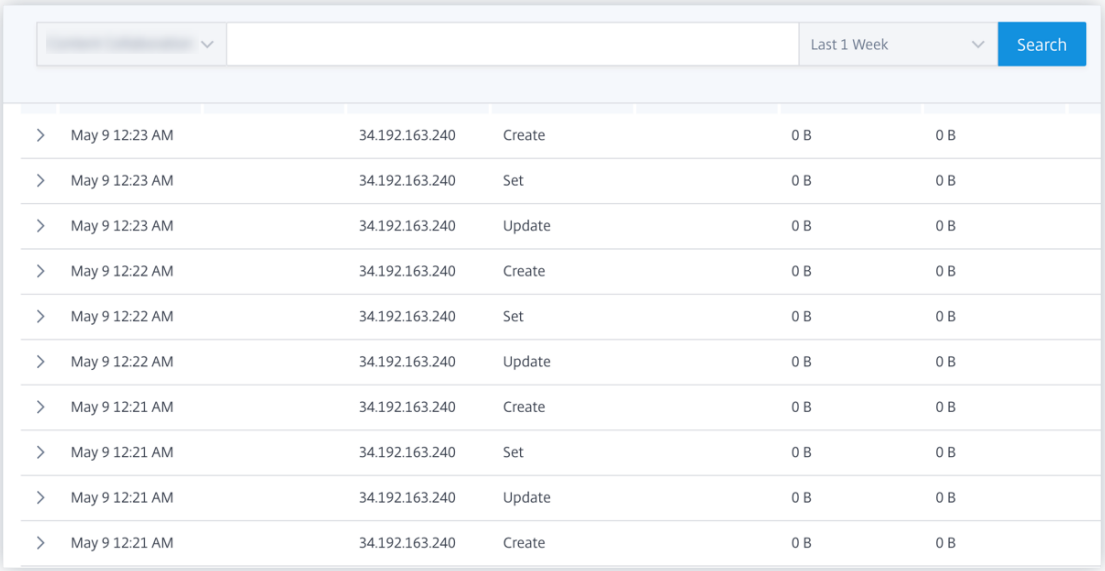
Effectuez cette dernière vérification pour vous assurer que les événements sont transmis avec précision à Citrix Analytics.

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.

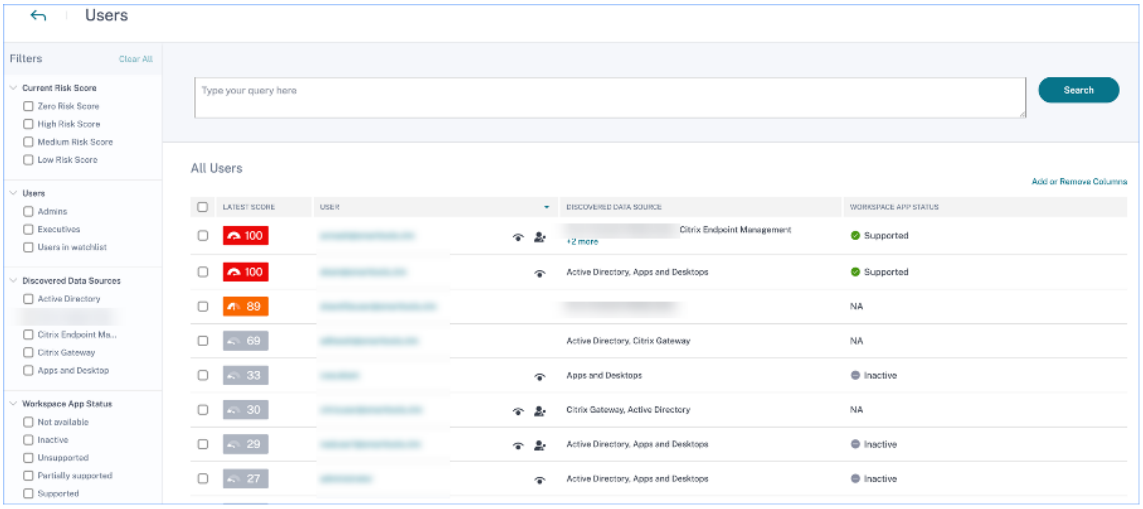
Contrôle 8 : les utilisateurs sont-ils découverts par Analytics ?

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

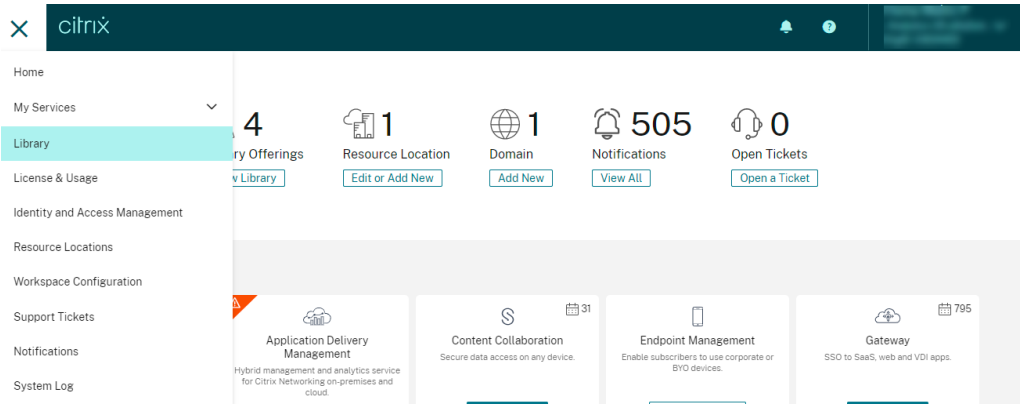
Cette section décrit les procédures permettant de déclencher des événements Apps and Desktops, des événements SaaS et de vérifier que Citrix Analytics for Security reçoit activement ces événements utilisateur.

Conditions préalables

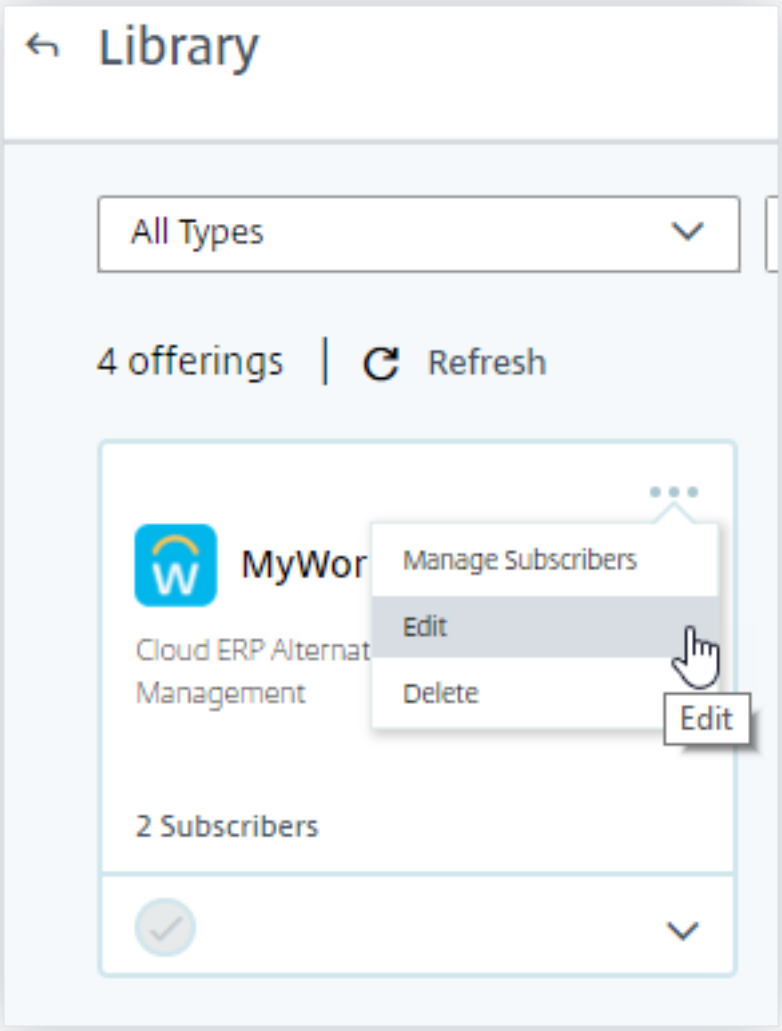
- Si vous utilisez des sites locaux de Citrix Virtual Apps and Desktops, intégrez vos sites locaux à Citrix Analytics et activez le traitement des données à partir de la fiche de site. Si vous utilisez Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service), activez le traitement des données 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.

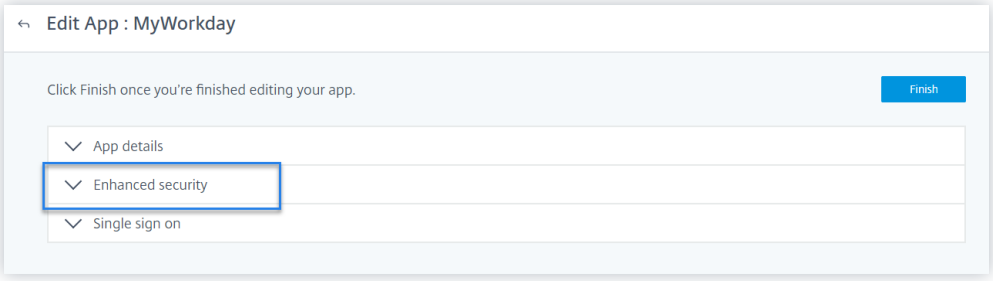
- Pour déclencher les événements SaaS tels que le lancement d'applications SaaS, la navigation par URL d'application SaaS, le téléchargement de fichiers d'applications SaaS, vous devez utiliser une application SaaS configurée à partir de Workspace. Les applications SaaS les plus utilisées sont Salesforce, 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**.



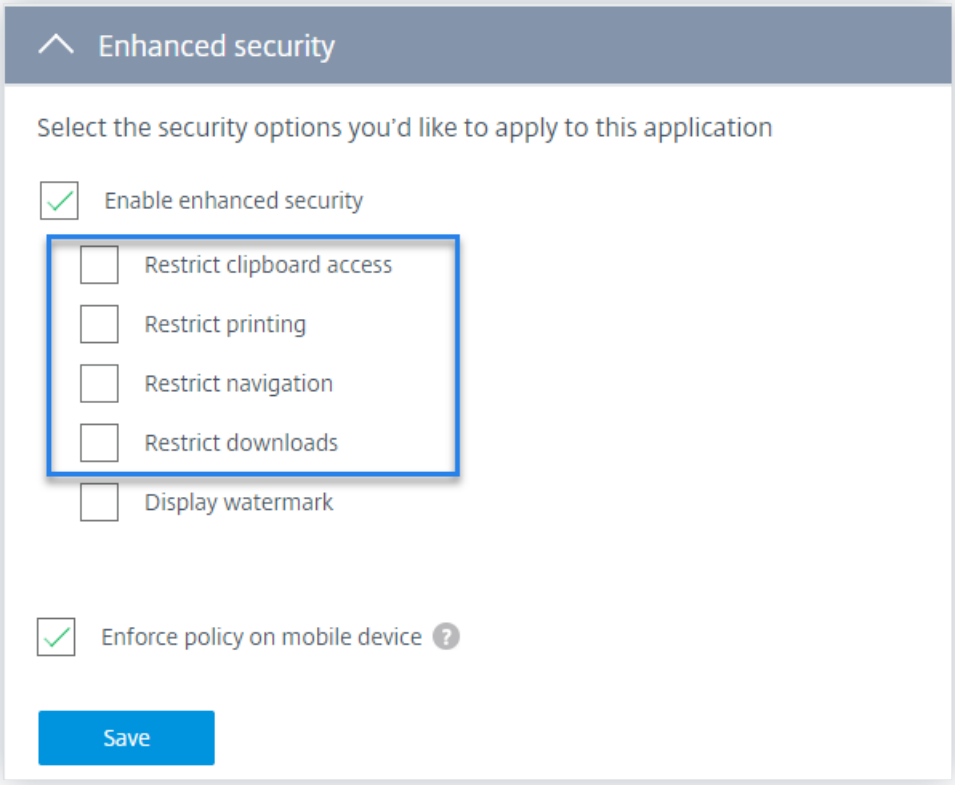
    2. Sur la page **Bibliothèque**, identifiez l'application SaaS que vous souhaitez utiliser pour vérifier les événements. Par exemple, Workday.
    3. Cliquez sur les points de suspension, puis sélectionnez **Modifier**.



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

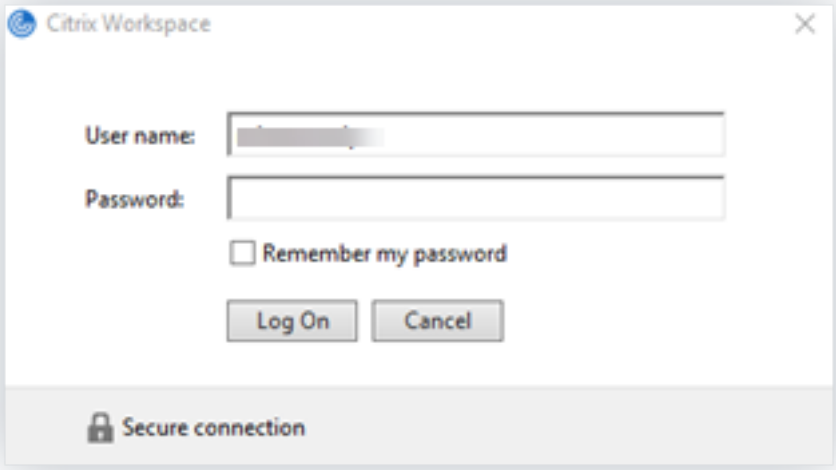
Effectuez les étapes suivantes dans l'ordre pour déclencher les événements dans votre environnement Apps and Desktops et vérifier que Citrix Analytics for Security reçoit activement ces événements.

> **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

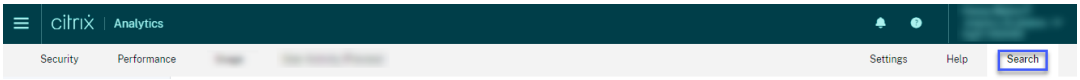
> d'exemple. Vous pouvez utiliser toutes les applications SaaS configurées depuis votre espace de travail pour déclencher les événements SaaS.

- **Ouverture de session de compte**

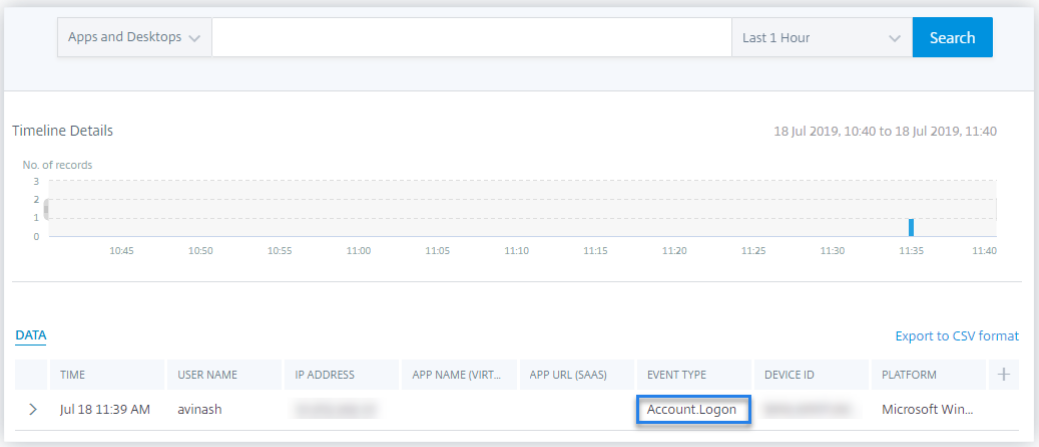
  1. Lancez l'application Citrix Workspace ou Citrix Receiver pour accéder à votre Workspace ou StoreFront.
  2. Entrez vos informations d'identification pour vous connecter à l'application Citrix Workspace ou à Citrix Receiver.



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

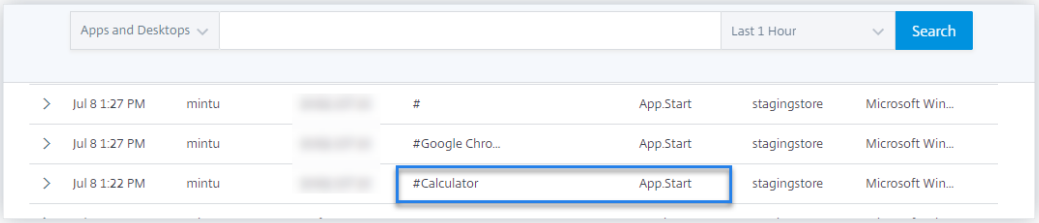


  5. Dans la page de recherche, affichez les données de l'événement **Account.Logon** . Développez la ligne pour afficher les détails de l'événement.



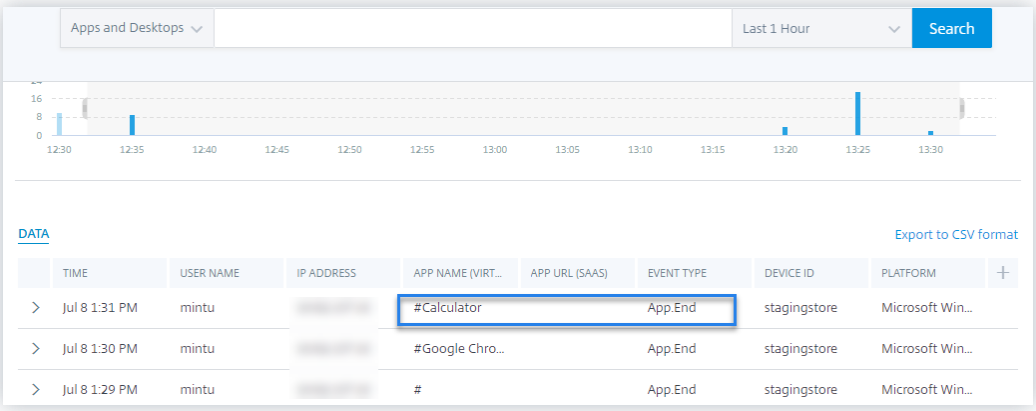
- **Démarrage de l'application**

  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.



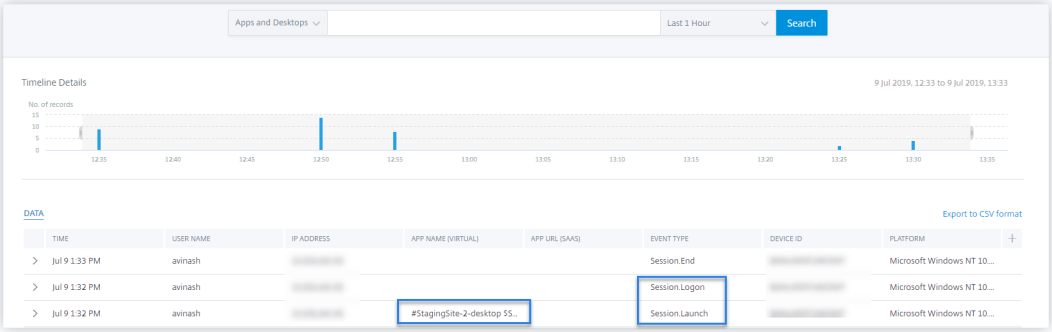
- **Fin de l'application**

  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**

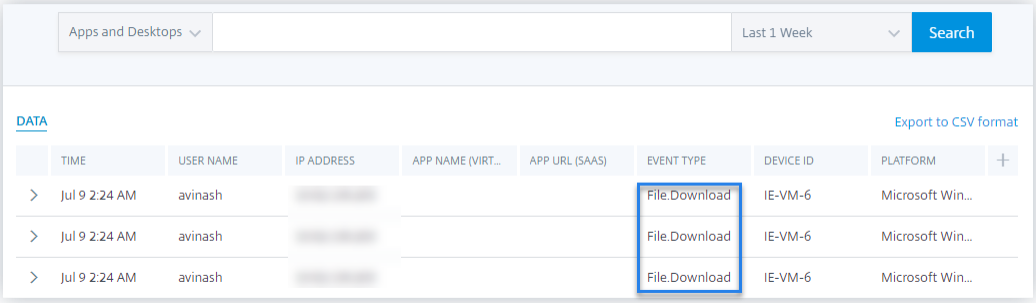
  1. Lancez l'application Citrix Workspace ou Citrix Receiver pour accéder à votre Workspace ou StoreFront.
  2. Lancez votre bureau virtuel.
  3. Accédez à Citrix Analytics.
  4. Cliquez sur **Rechercher** et sélectionnez **Applications et postes de travail**.
  5. Dans la page de recherche, affichez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



- **Téléchargement de fichier**

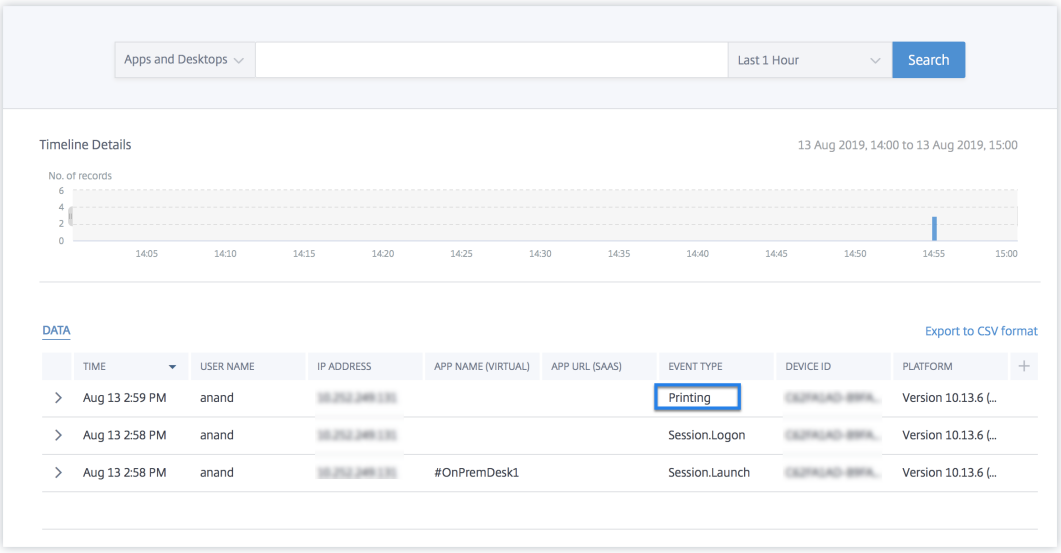
  1. Lancez l'application Citrix Workspace ou Citrix Receiver pour accéder à votre Workspace ou StoreFront.
  2. Lancez votre bureau virtuel.
  3. Copiez un fichier depuis votre bureau virtuel vers votre ordinateur local.
  4. Accédez à Citrix Analytics.
  5. Cliquez sur **Rechercher** et sélectionnez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



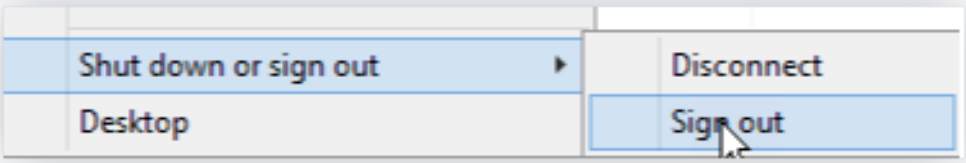
- **Impression**

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.

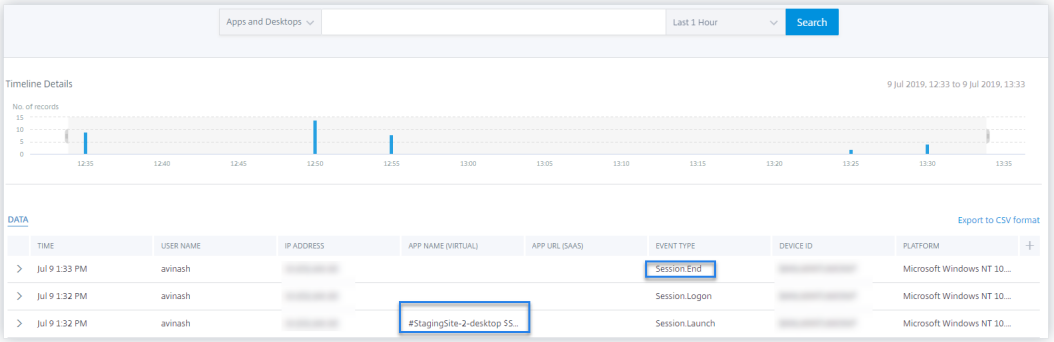


- **Fin de session**

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.

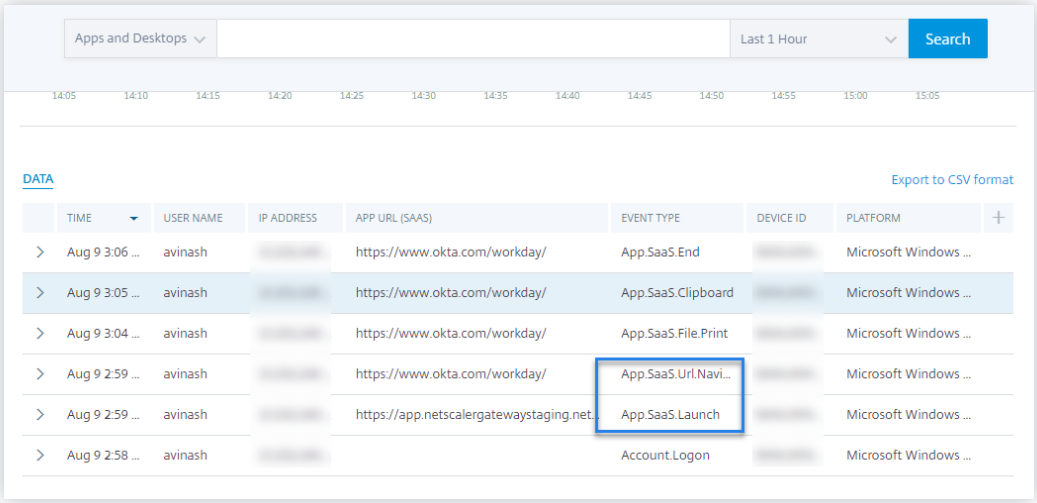


- **Lancement d'applications SaaS et navigation dans les URL des applications SaaS**

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.

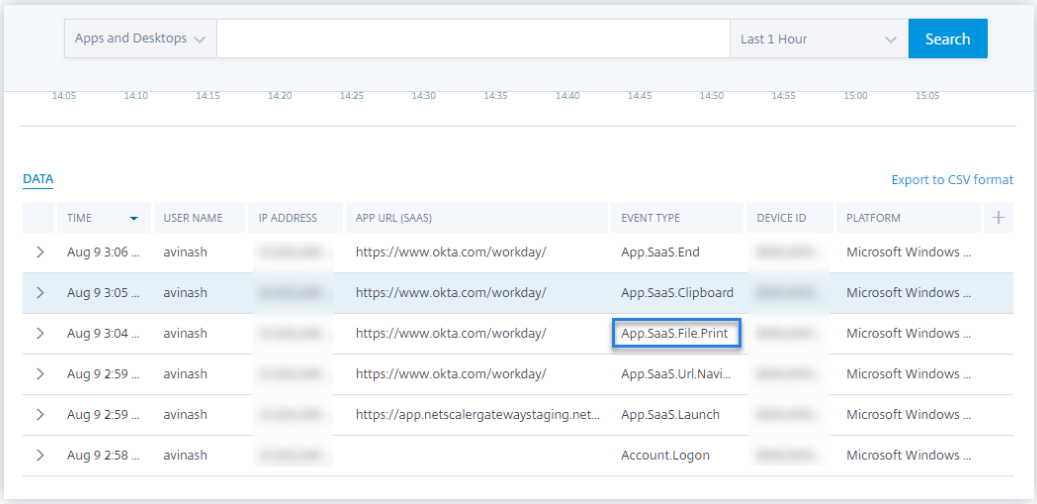


- **Impression de fichiers d'applications SaaS**

  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.

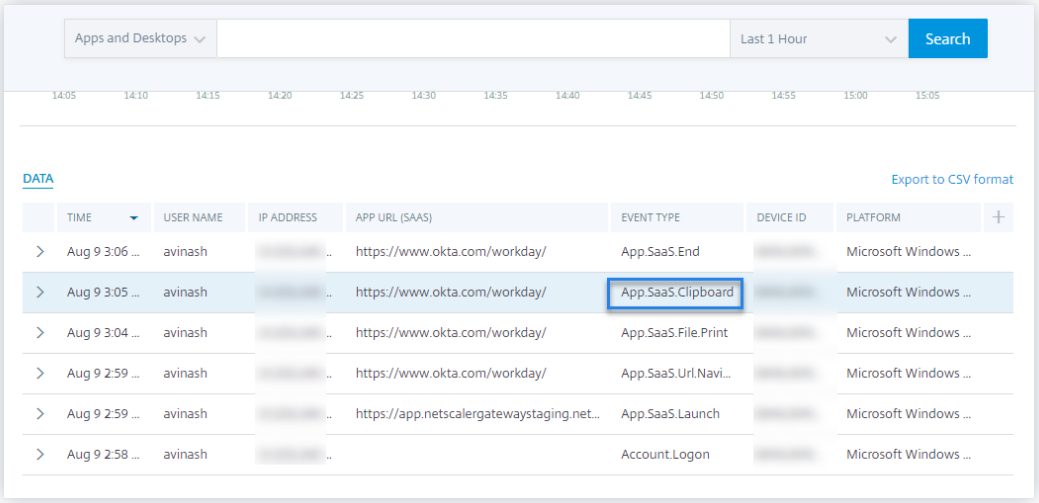


- **Accès au presse-papiers des applications SaaS**

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.

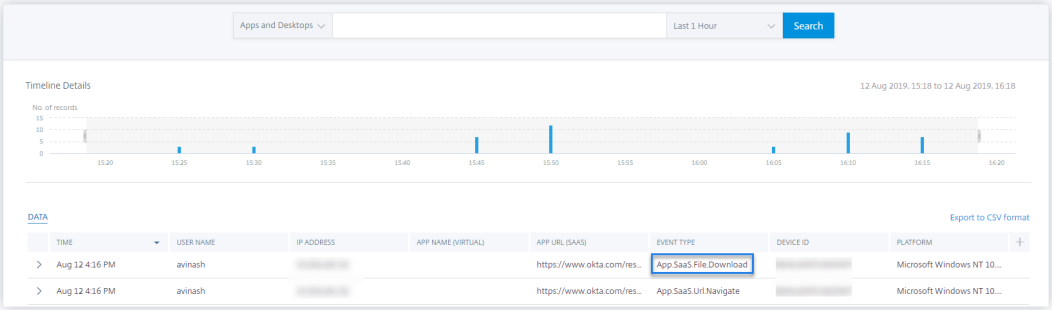


- **Téléchargement de fichiers SaaS App**

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

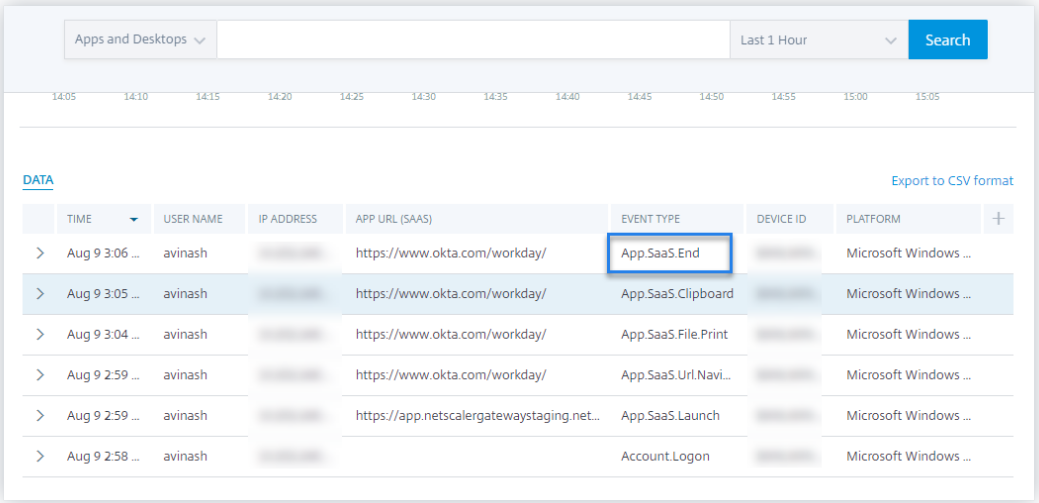
   > **Remarque**
   >
   > Assurez-vous que l'option **Restreindre les téléchargements** est désactivée dans la section Sécurité renforcée. Pour plus d'informations, consultez les **conditions préalables**.

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.

Aucun événement utilisateur reçu de la version de l'application Citrix Workspace prise en charge

July 14, 2022

Si vous ne voyez aucun événement provenant d'un utilisateur qui utilise une version de l'application Citrix Workspace prise en charge par Citrix Analytics, le problème peut être lié à l'un des éléments suivants :

- Configuration du StoreFront
- Exigence de lancement Web

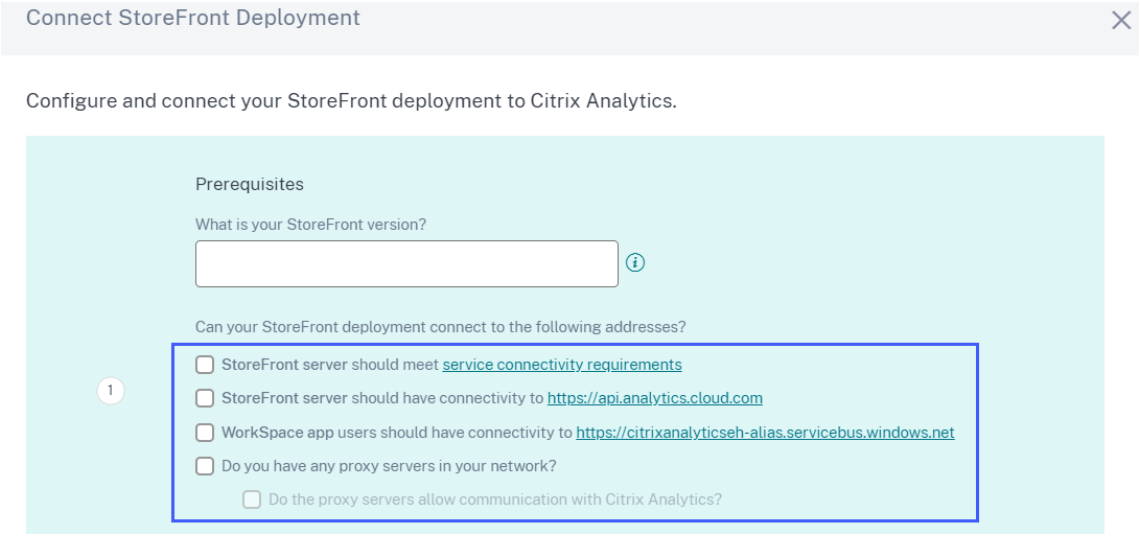
Configuration du StoreFront

Si un déploiement StoreFront est connecté à Citrix Analytics, vérifiez l'**horodatage de la dernière mise à jour**. L'heure doit être mise à jour au moins une fois par semaine si les utilisateurs accèdent activement à StoreFront. Les mises à jour fréquentes indiquent une connexion saine entre le déploiement StoreFront et Citrix Analytics. Sinon, il y a des problèmes de connectivité.

Vérifiez les exigences de connectivité suivantes :

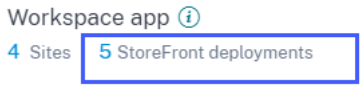
- Le serveur StoreFront doit répondre aux exigences du système et de la connectivité.
- Le serveur StoreFront doit pouvoir se connecter à `https://api.analytics.cloud.com`
- Les utilisateurs de l'application Workspace doivent pouvoir se connecter à `https://citrixanalyticseh-alias.servicebus.windows.net`

- Votre serveur proxy doit autoriser la connexion à Citrix Analytics Event Hub :
  - **Région des États-Unis** : `https://citrixanalyticseh-alias.servicebus.windows.net/`
  - **Région de l'Union européenne** : `https://citrixanalyticseheu-alias.servicebus.windows.net/`
  - **Région sud de l'Asie-Pacifique** : `https://citrixanalyticsehaps-alias.servicebus.windows.net/`

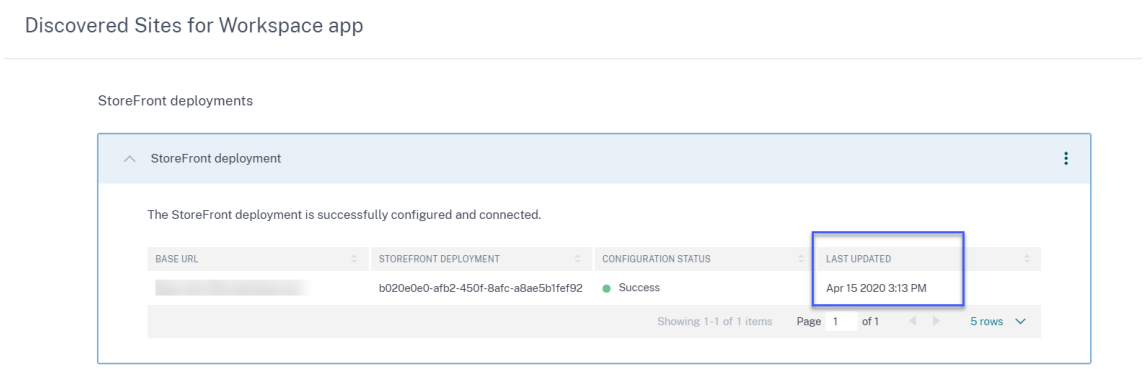


Pour vérifier l'heure de la dernière mise à jour :

1. Cliquez sur **Paramètres > Sources de données**.
2. Sur la fiche de site de l'application Workspace, cliquez sur le nombre de serveurs StoreFront connectés.



3. Sur le déploiement StoreFront, vérifiez l'heure de la dernière mise à jour.



Si le dernier horodatage mis à jour n'est pas mis à jour fréquemment, même après avoir satisfait aux exigences de connectivité, reconfigurez votre StoreFront. Pour plus d'informations, consultez la section Onboard Virtual Apps and Desktops Sites using StoreFront.

Exigence de lancement Web

Un utilisateur peut lancer des applications et bureaux virtuels de l'une des manières suivantes :

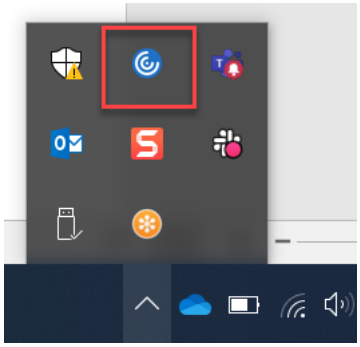
- Accédez au Citrix Store ou à Citrix Workspace via l'application Citrix Workspace. Cette approche s'appelle le lancement natif.
- Ouvrez l'URL du magasin Citrix ou l'URL Citrix Workspace dans un navigateur Web. Cliquez sur une application ou un bureau virtuel pour télécharger le fichier ICA correspondant. Ouvrez ensuite le fichier ICA à l'aide d'un navigateur Web pour lancer l'application ou le bureau virtuel. Cette approche s'appelle le lancement Web.

Pour le lancement Web, assurez-vous que la machine utilisateur doit disposer de l'un des clients suivants en fonction du système d'exploitation de l'appareil.

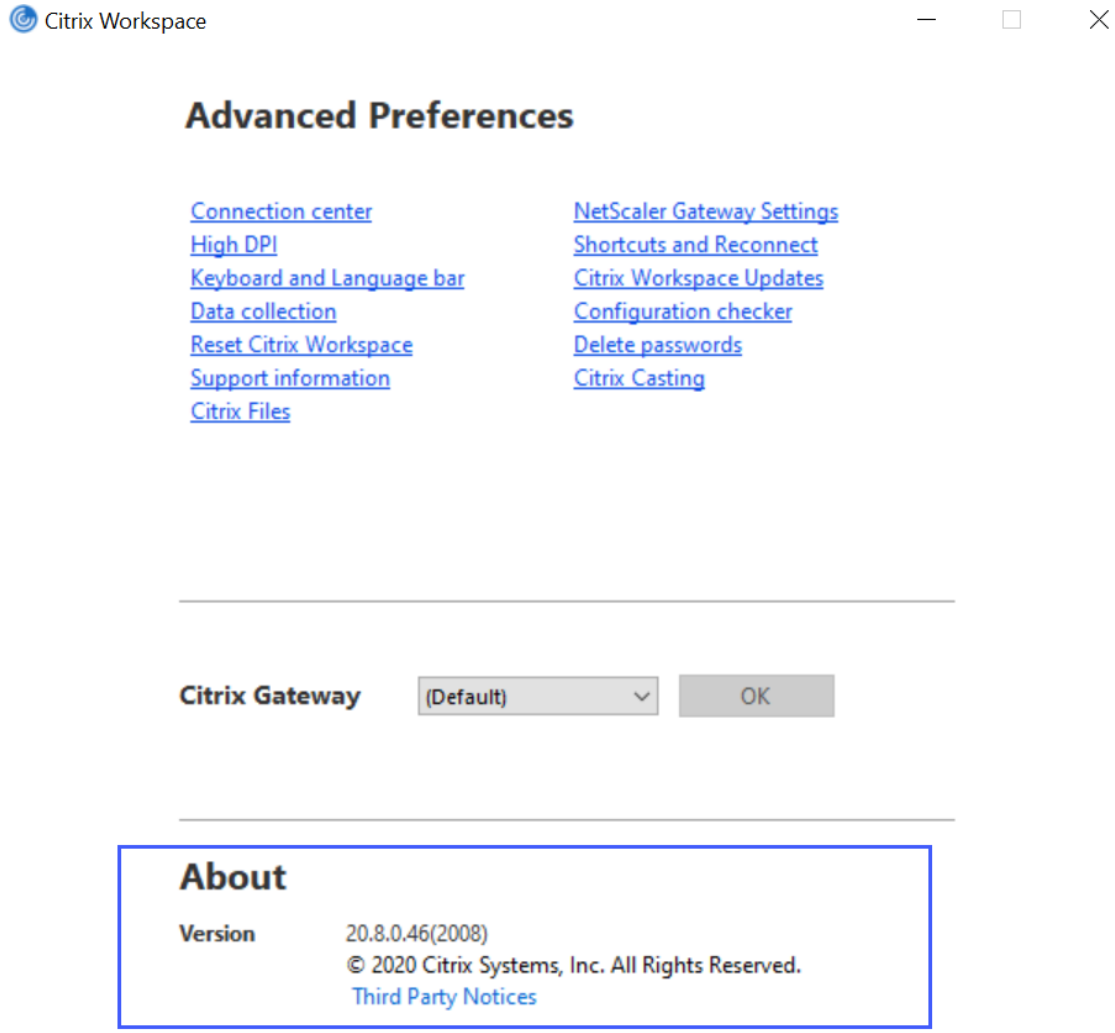
Client	Version	Créer
Application Citrix Workspace pour Windows	2006.1 ou version ultérieure	20.6.0.38 ou version ultérieure
Application Citrix Workspace pour Mac	2006 ou version ultérieure	20.06.0.7 ou version ultérieure

Pour vérifier la version de l'application Citrix Workspace, procédez comme suit :

1. Sur la machine locale de l'utilisateur, cliquez avec le bouton droit de la souris sur l'icône de l'application Citrix Workspace.



2. Cliquez sur **Préférences avancées** et consultez la section **À propos** pour afficher la version.



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.
EnableCASUseAuditorUniqueID	Computer/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

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 :

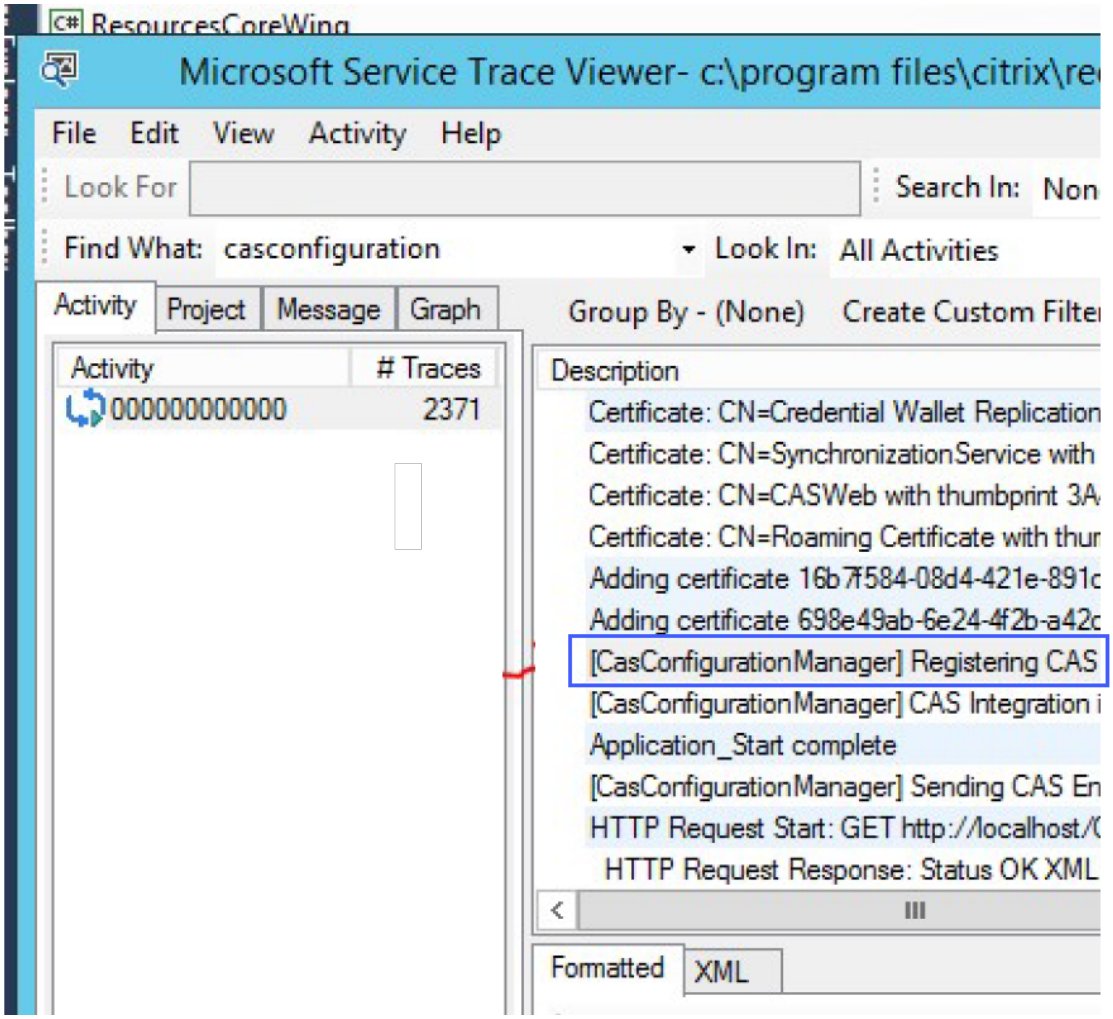
   ```
   Get-STFCasConfiguration
   ```

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 :

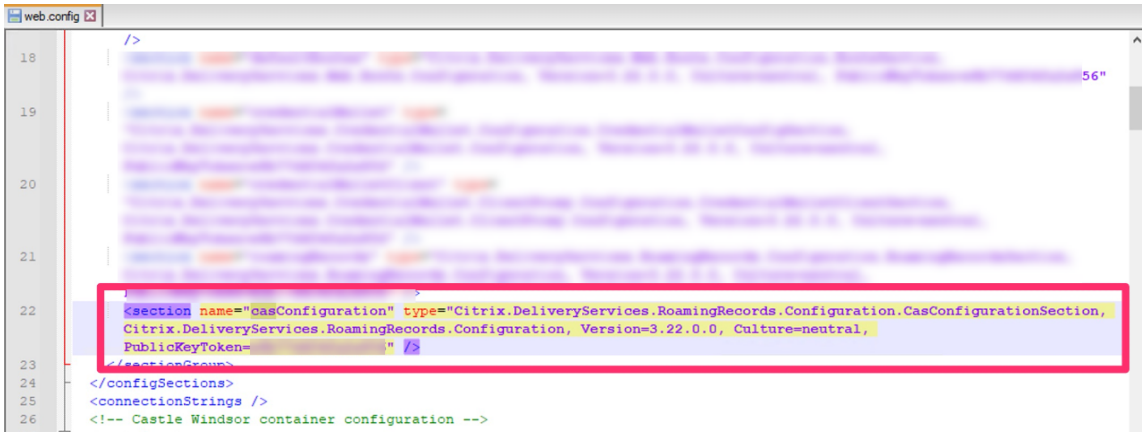

```
C:\Program Files\Citrix\Receiver StoreFront\Admin\trace
```

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.