Citrix Analytics

Machine translated content

Disclaimer

Die offizielle Version dieses Inhalts ist auf Englisch. Für den einfachen Einstieg wird Teil des Inhalts der Cloud Software Group Dokumentation maschinell übersetzt. Cloud Software Group hat keine Kontrolle über maschinell übersetzte Inhalte, die Fehler, Ungenauigkeiten oder eine ungeeignete Sprache enthalten können. Es wird keine Garantie, weder ausdrücklich noch stillschweigend, für die Genauigkeit, Zuverlässigkeit, Eignung oder Richtigkeit von Übersetzungen aus dem englischen Original in eine andere Sprache oder für die Konformität Ihres Cloud Software Group Produkts oder Ihres Diensts mit maschinell übersetzten Inhalten gegeben, und jegliche Garantie, die im Rahmen der anwendbaren Endbenutzer-Lizenzvereinbarung oder der Vertragsbedingungen oder einer anderen Vereinbarung mit Cloud Software Group gegeben wird, dass das Produkt oder den Dienst mit der Dokumentation übereinstimmt, gilt nicht in dem Umfang, in dem diese Dokumentation maschinell übersetzt wurde. Cloud Software Group kann nicht für Schäden oder Probleme verantwortlich gemacht werden, die durch die Verwendung maschinell übersetzter Inhalte entstehen können.

Contents

Was ist neu

September 22, 2023

Das Ziel von Citrix besteht darin, Citrix Analytics Kunden neue Funktionen und Produktaktualisierungen bereitzustellen, sobald sie verfügbar sind. Neue Releases bieten größeren Wert, daher gibt es keinen Grund, Updates zu verzögern.

Der Prozess ist für die Kunden transparent. Erste Updates werden nur auf interne Sites von Citrix angewendet und erst danach schrittweise auf Kundenumgebungen. Die schrittweise Bereitstellung von Updates in Wellen trägt dazu bei, die Produktqualität zu gewährleisten und die Verfügbarkeit zu maximieren.

Citrix Analytics verfügt über die folgenden Produkte oder Angebote. Weitere Informationen zu den neuen Funktionen und Produktupdates finden Sie unter Was gibt es neue Artikel, die für jedes Angebot spezifisch sind.

- Citrix Analytics für Sicherheit
- Citrix Analytics für Leistung

In diesen Versionshinweisen werden die neuen Funktionen und Produktaktualisierungen speziell für die Citrix Analytics Plattform hervorgehoben.

21. September 2023

Vereinfachen Sie das StoreFront-Onboarding mit PowerShell-Skript

Es wurde ein neues **PowerShell-Skript** eingeführt, das die Überprüfung der Voraussetzungen, die Installation und Konfiguration von StoreFront automatisiert. Der Kunde muss dieses Skript im Administratormodus auf StoreFront ausführen, um das Onboarding und das Deboarding durchzuführen, Selbsttests durchzuführen, Fehler zu beheben und zu überprüfen, ob das Onboarding in die Citrix Analytics Service-GUI erfolgreich ist.

Weitere Informationen finden Sie unter Verbindung zu einer StoreFront-Bereitstellungherstellen.

28. August 2023

Mikroapps-Dienst (Ende des Lebenszyklus)

Der Citrix Mikroapps-Dienst hat das Ende seiner Lebensdauer erreicht und steht Benutzern nicht mehr zur Verfügung.

01. August 2023

Citrix Analytics —Nutzung (Ende des Lebenszyklus)

Citrix Usage Analytics hat das Ende seiner Lebensdauer erreicht und steht Benutzern nicht mehr zur Verfügung.

23. Februar 2023

Behobene Probleme

Vor der Veröffentlichung von Citrix Virtual Apps and Desktops 2112 kann Citrix Analytics die on-premises Sites nicht erkennen, die über Citrix Director verbunden und kürzlich in Citrix Cloud registriert wurden. Sie sehen diese verbundenen Sites also nicht auf Ihrer Site-Karte **zur Überwachung Virtual Apps and Desktops** . Dieses Problem ist jetzt behoben. [CAS-63132]

28. September 2022

Webhooks für Alert-Benachrichtigungen

Sie können Webhooks verwenden, um Citrix Analytics-Warnbenachrichtigungen an alle Anwendungen von Drittanbietern zu senden, für die eingehende Webhook-URLs konfiguriert sind. Webhooks sind HTTP-Callbacks, die Echtzeitnachrichten zwischen den Dienstanbieteranwendungen und Verbraucheranwendungen ermöglichen. Da die Warnmeldungen in Echtzeit gesendet werden, werden Sie benachrichtigt, wenn die Ereignisse eintreten. Weitere Informationen finden Sie unter Webhooks für Alert-Benachrichtigungen.

08. September 2022

Exportlimit beim CSV-Export erhöht

Das Limit für die Anzahl der Zeilen, die Sie mit der Funktion In **CSV-Format exportieren exportieren** können, wurde jetzt von 10.000 Zeilen auf 100.000 Zeilen erhöht. Weitere Informationen finden Sie unter Exportieren der Ereignisse in eine CSV-Datei.

18. August 2022

Problem behoben

- Bei der Self-Service-Suche nach Apps und Desktops wurde der Versionswert der Workspace-App als **NA** (nicht verfügbar) in die heruntergeladene CSV-Datei eingetragen, während er in der Seitenansicht verfügbar war. Dieses Problem ist jetzt behoben. [CAS-70361]

10. August 2022

StoreFront-Onboarding ohne Site-Aggregation

Die Site-Aggregationsabhängigkeit für StoreFront wurde aus der App-Site-Karte **Apps and Desktops —Workspace** entfernt. Sie können die Option **Connect Storefront Deployment** in Ihrer Workspace-Anwendung sehen, auch wenn Sie der Site-Aggregation keine Site hinzugefügt haben. Weitere Informationen finden Sie in der Datenquelle Citrix Virtual Apps and Desktops.

05. April 2022

Secure Workspace Access wurde in Secure Private Access umbenannt

In den Analytics-Dashboards und -Berichten werden alle **Secure Workspace Access-Labels** jetzt als **Secure Private Access** aktualisiert, um sie an den umbenannten Produktnamen anzupassen.

Beispielsweise werden auf der Seite **Datenquellen** und der **Self-Service-Suchseite** die **Secure Workspace Access-Labels** in **Secure Private Access** umbenannt.

21. März 2022

Problem behoben

- Auf der Seite **Suchen** funktionieren automatische Vorschläge für Dimensionen und Operatoren nicht, wenn die vorherige Bedingung Ihrer Suchanfrage einen Dimensionswert enthält, der durch ein Leerzeichen getrennt ist.

  In der folgenden Abfrage funktionieren automatische Vorschläge beispielsweise nicht mehr, nachdem Sie die Stadt als ausgewählt haben `San Jose`. Dieses Problem ist jetzt behoben. [CAS-64126]

10. Februar 2022

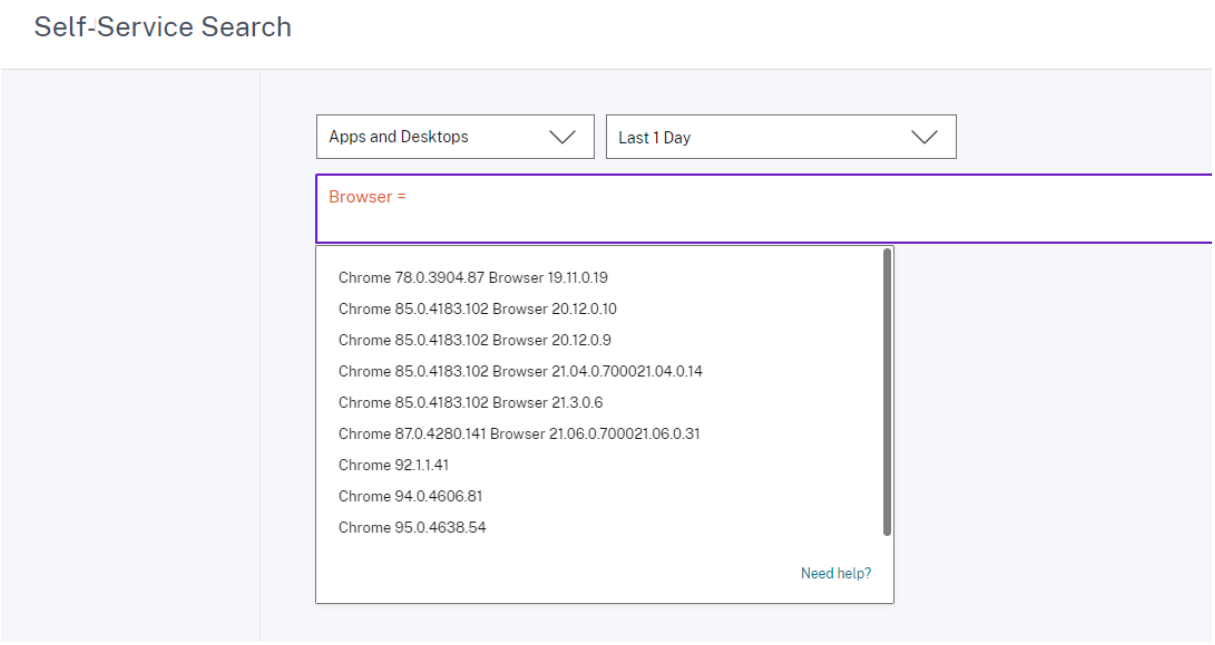
Was ist neu

Automatisch vorgeschlagene Werte für die Dimensionen im Self-Service-Suchfeld Wenn Sie auf der Self-Service-Suchseite eine Dimension und einen gültigen Operator im Suchfeld auswählen, werden die Werte für die Dimension automatisch angezeigt. Wählen Sie einen Wert aus der Liste der automatischen Vorschläge aus oder geben Sie je nach Anwendungsfall manuell einen Wert ein. Wenn Sie einen Wert eingeben, werden die in den Datensätzen verfügbaren übereinstimmenden Werte automatisch vorgeschlagen.

Die für eine Dimension vorgeschlagene Werteliste ist entweder in der Datenbank vordefiniert (bekannte Werte) oder basiert auf historischen Ereignissen.

Wenn Sie beispielsweise die Dimension `Browser` und den Zuweisungsoperator auswählen, werden die bekannten Werte automatisch vorgeschlagen. Sie können je nach Anforderung einen Wert auswählen.

Weitere Informationen finden Sie unter Self-Service-Suche.



20. Dezember 2021

Was ist neu

Access Control wurde in Secure Workspace Access umbenannt In den Analytics-Dashboards und -Berichten werden alle **Zugriffskontroll-Labels** jetzt als **Secure Workspace Access** aktualisiert, um sie an den umbenannten Produktnamen anzupassen.

Beispielsweise werden auf der Seite **Datenquellen** und der **Self-Service-Suchseite** die **Zugriffssteuerungsbezeichnungen** in **Secure Workspace Access**umbenannt.

06. Dezember 2021

Was ist neu

Citrix Analytics wird jetzt in der Region Asien-Pazifik, Süden unterstützt

- Sie können jetzt den asiatisch-pazifischen Süden als Heimatregion auswählen, während Sie Ihr Unternehmen in Citrix Cloud integrieren und den Citrix Analytics Service verwenden. Weitere Informationen finden Sie unter Geografische Überlegungen.
- Citrix Analytics speichert jetzt die Benutzerereignisse und Metadaten Ihrer Organisation in der Region Asien-Pazifik, Süd, wenn Sie sie als Ihre Heimatregion auswählen. Weitere Informationen finden Sie unter Data Governance.
- Informationen zu den Netzwerkanforderungen für die Region Asien-Pazifik Süd finden Sie unter Technische Sicherheit —Überblick.
- Informationen zu unterstützten Datenquellen in der Region Asien-Pazifik, Süden, finden Sie unter Datenquellen.

19. August 2021

Was ist neu

Unterstützung für den Operator IS EMPTY Bei der Self-Service-Suche können Sie jetzt den Operator **IS EMPTY** in Ihrem Zustand verwenden, um nach Null- oder Leerdimension zu suchen.

> **Hinweis**
>
> Der Operator funktioniert nur für stringartige Dimensionen wie App-Name, Browser und Country.

Weitere Informationen finden Sie unter Self-Service-Suche.

14. Juli 2021

Was ist neu

Unterstützung für den Operator IST NICHT LEER Bei der Self-Service-Suche können Sie jetzt den Operator **IST NICHT LEER** in Ihrer Abfrage verwenden, um zu überprüfen, ob die Dimension nicht leer (nicht leer) ist.

> **Hinweis**
>
> Der Operator funktioniert nur für stringartige Dimensionen wie App-Name, Browser und Country.

Weitere Informationen finden Sie unter Self-Service-Suche.

7. Juni 2021

Veraltete Funktion

Citrix Analytics-Demoumgebung wurde entfernt Die **Demo-Links für Security Analytics und Performance Analytics ausprobieren** werden jetzt von der Analytics-Übersichtsseite entfernt. Sie können nicht mehr für jedes Angebot auf die Demo-Umgebung zugreifen. Weitere Informationen zum Zugriff auf Citrix Analytics-Angebote finden Sie unter Erste Schritte.

18. Mai 2021

Was ist neu

Unterstützung für *-Operator mit !=-Operator In Ihrer Suchanfrage können Sie nun den Operator * mit dem Operator ! = verwenden, um die Benutzerereignisse zu finden. Beispiel:

- Um alle Benutzerereignisse zu finden, die nicht mit dem Namen “John”beginnen, verwenden Sie die Abfrage: User-Name != John*
- Um alle Benutzerereignisse zu finden, die nicht mit dem Namen “Smith”enden, verwenden Sie die Abfrage: User-Name != *Smith

> **Hinweis**
>
> Bei den Suchergebnissen wird Groß-/Kleinschreibung beachtet

Weitere Informationen finden Sie unter Self-Service-Suche.

Verbesserte Suchleistenerfahrung auf der Self-Service-Suchseite

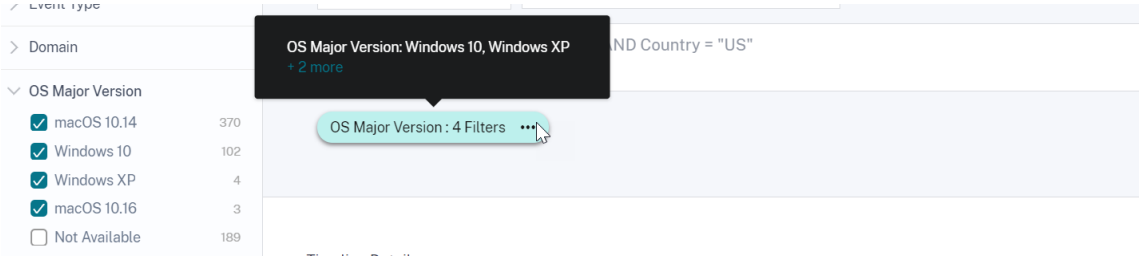
- Die Suchleiste bietet jetzt eine bessere Sicht auf Ihre Abfragen, wenn sie sich auf mehrere Zeilen erstreckt. Verwenden Sie die Bildlaufleiste, um Ihre mehrzeiligen Abfragen zu scrollen. Zuvor war es schwierig, die mehrzeiligen Abfragen einzusehen.

- Das Cursorspring-Problem, das im Safari-Browser beobachtet wurde, ist jetzt behoben.

Weitere Informationen finden Sie unter Self-Service-Suche.

Überarbeitete Chip-Ansicht in der Self-Service-Suche

- Die neu gestalteten Chips bieten Ihnen jetzt einen besseren Überblick über die verschiedenen Facetten, die Sie ausgewählt haben.



- Klicken Sie auf einen Chip, um die Facetten basierend auf Ihren Anforderungen auszuwählen oder aufzuheben.

Problem behoben

- In Citrix Director funktioniert der Link **Gehe zu Analytics** nicht. Dieses Problem wird für einen Benutzer beobachtet, der seine Organisation in der Region der Europäischen Union in Citrix Cloud aufgenommen hat. [CAS-50224]

31. März 2021

Unterstützung der IN- und NOT-IN-Operatoren für die Suchabfrage “Apps und Desktops”

Mit den Apps- und Desktops-Dimensionen `Device ID`, `Domain`, `Event-Type` und `User-Name` können Sie jetzt die folgenden Operatoren verwenden:

- **IN**: Weisen Sie einer Dimension mehrere Werte zu, um die Ereignisse abzurufen, die sich auf einen oder mehrere Werte beziehen.
- **NOT IN**: Weisen Sie einer Dimension mehrere Werte zu und suchen Sie die Ereignisse, die die angegebenen Werte nicht enthalten.

> **Hinweis**
>
> Diese Operatoren gelten nur für die Zeichenfolgenwerte.

Weitere Informationen zu den Betreibern finden Sie unter Self-Service-Suche.

18. März 2021

Was ist neu

Unterstützung für NOT LIKE (!~)-Operator Für die Self-Service-Suchanfrage können Sie jetzt den NOT LIKE (!~)-Operator verwenden. Der Operator sucht nach den Benutzerereignissen nach dem von Ihnen angegebenen übereinstimmenden Muster. Es gibt die Ereignisse zurück, die das angegebene Muster nirgendwo in der Ereigniszeichenfolge enthalten.

Die Abfrage `User-Name !~ "John"` zeigt beispielsweise Ereignisse für Benutzer mit Ausnahme von John, John Smith oder solchen Benutzern an, die den übereinstimmenden Namen "John"enthalten.

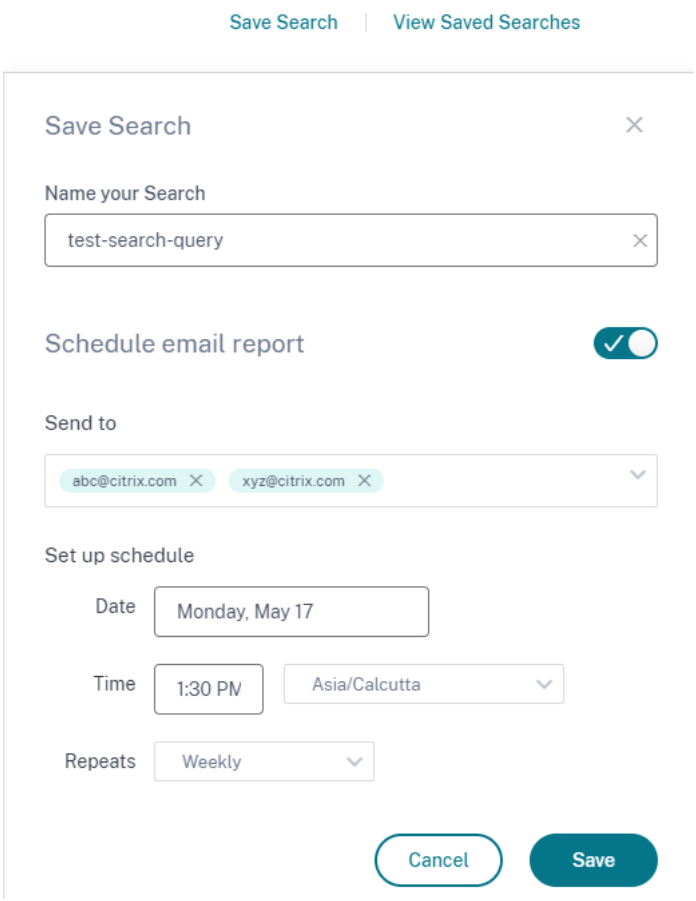
Weitere Informationen finden Sie unter Self-Service-Suche.

23. Februar 2021

Was ist neu

Planen Sie die E-Mail-Zustellung für eine Suchanfrage Auf der Self-Service-Suchseite können Sie beim Speichern einer Suchanfrage auch eine E-Mail-Zustellung planen, um eine Kopie der gespeicherten Suchanfrage und des entsprechenden visuellen Zusammenfassungsberichts an sich und andere Benutzer zu senden. Legen Sie Datum, Uhrzeit und Frequenz fest —täglich, wöchentlich oder monatlich, um mit dem Senden einer E-Mail zu beginnen. Sie können auch die E-Mail-Zustellung der Suchanfragen planen, die Sie zuvor gespeichert haben.

Weitere Informationen finden Sie unter Self-Service-Suche.

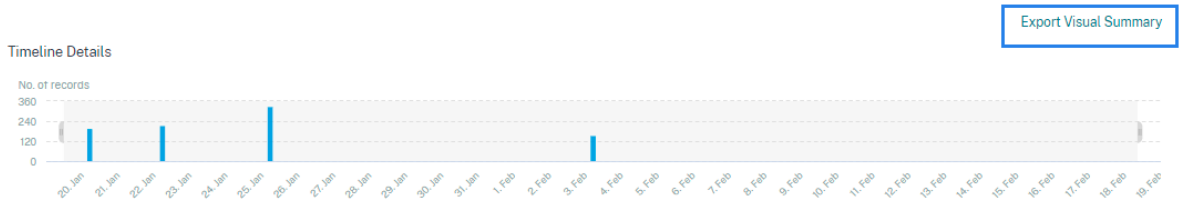


Laden Sie die visuelle Zusammenfassung einer Suchanfrage herunter Auf der Self-Service-Seite können Sie jetzt den visuellen Zusammenfassungsbericht Ihrer Suchanfrage für einen ausgewählten Zeitraum herunterladen und eine Kopie mit anderen Benutzern teilen. Klicken Sie auf **Visual Summary exportieren**, um den visuellen Zusammenfassungsbericht als PDF herunterzuladen.

Der Bericht enthält die folgenden Informationen:

- Die Suchanfrage, die Sie für die Ereignisse angegeben haben.
- Die Facetten (Filter), die Sie auf die Ereignisse angewendet haben.
- Die visuelle Zusammenfassung wie die Zeitleistendiagramme, Balkendiagramme oder Graphen der Suchereignisse.

Weitere Informationen finden Sie unter Self-Service-Suche.

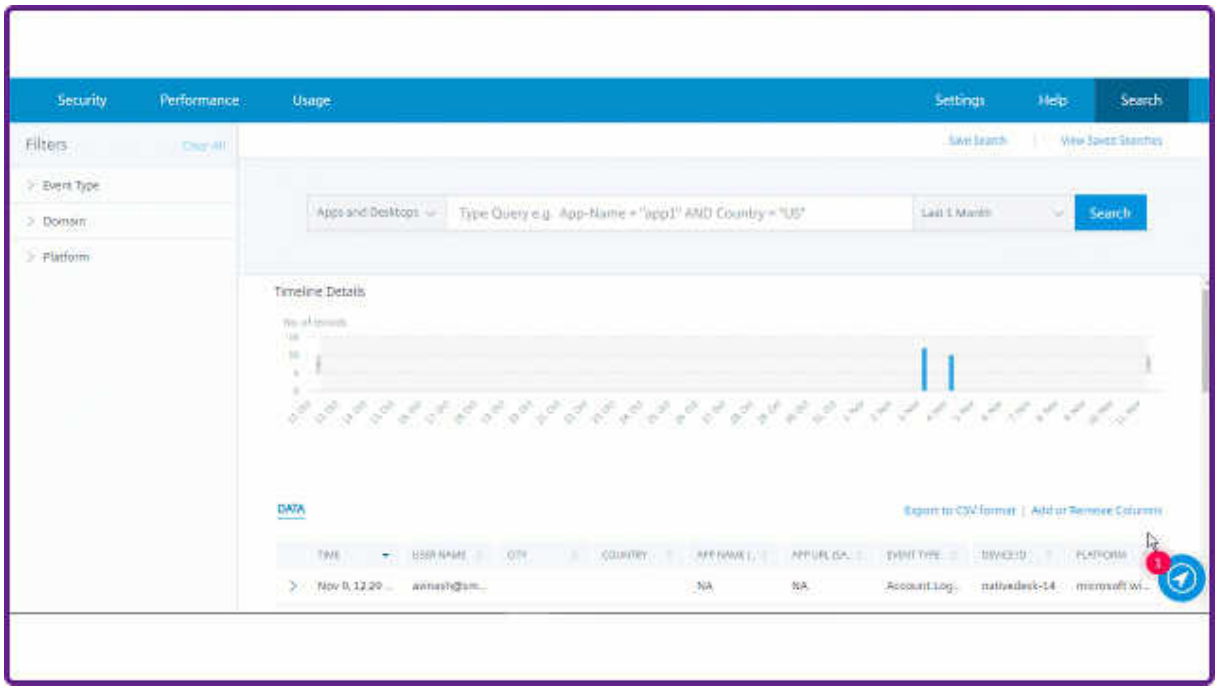


12. November 2020

Neues Feature

Speichern einer Self-Service-Abfrage Nachdem Sie eine Self-Service-Abfrage erstellt haben, können Sie sie für die spätere Verwendung speichern. Die folgenden Optionen werden mit der Abfrage gespeichert:

- Angewandte Suchfilter
- Ausgewählte Datenquelle und Dauer



Weitere Informationen finden Sie unter So speichern Sie die Self-Service-Suche.

20. Oktober 2020

Neue Features

Unterstützung für NetScaler Gateway in der Region der Europäischen Union Citrix Analytics unterstützt jetzt NetScaler Gateway in der EU-Region. Weitere Informationen finden Sie unter NetScaler Gateway-Datenquelle.

09. Juli 2020

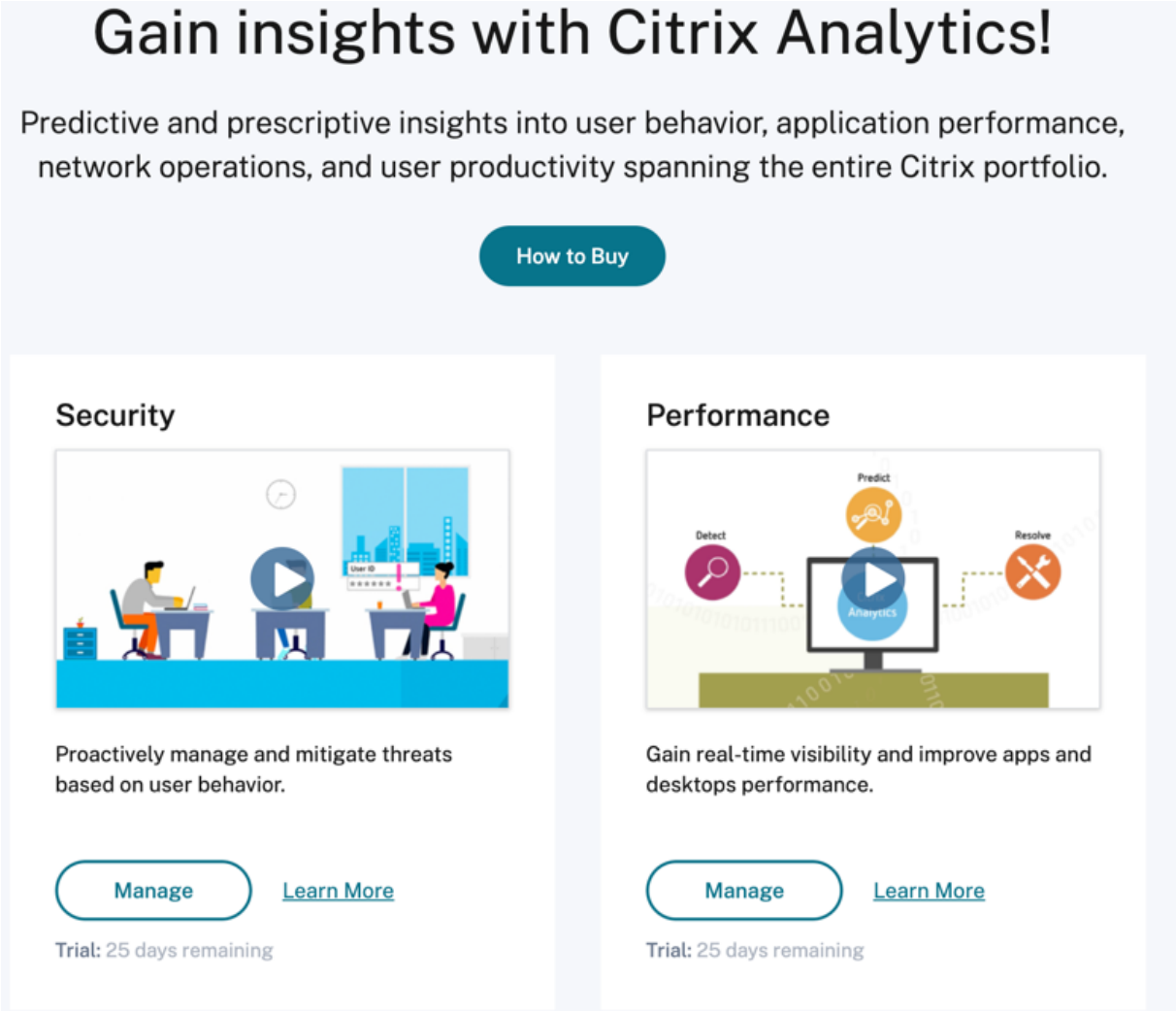
Unterstützung läuft aus

Microsoft Internet Explorer 11 wurde jetzt aus der Liste der unterstützten Browser entfernt. Diese Abwertung ist auf die im Browser beobachtete Sicherheitslücke zurückzuführen. Eine Liste der unterstützten Browser finden Sie unter Systemanforderungen.

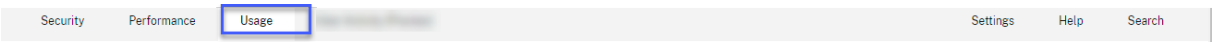
02. Juni 2020

Neue Features

Übersichtsseite und obere Leiste in Analytics neu gestaltet Auf der Analytics-Übersichtsseite wird die Kachel **Verwendung** angezeigt, die die zuvor vorhandene Kachel **Vorgänge** ersetzt. Außerdem wird die **Produktivitätskachel** von dieser Seite entfernt. Um die Übersichtsseite anzuzeigen, wählen Sie **Hilfe** > **Überblick**.



In ähnlicher Weise ersetzt die Registerkarte **Verwendung** in der oberen Leiste die Registerkarte **Operationen** .



20. Februar 2020

Neue Features

Citrix Analytics-Abonnementangebote Citrix bietet Benutzern flexible Kaufoptionen und bietet jetzt drei einzelne abonnementbasierte Citrix Analytics-Produkte an. Citrix Analytics bietet einzigartige Einblicke in Sicherheit oder Leistung (oder beides), basierend auf dem Angebot, das Sie abonnieren.

Sie können die folgenden Citrix Analytics-Abonnementangebote erwerben:

- Citrix Analytics für Sicherheit

- Citrix Analytics für Leistung
- Citrix Analytics für Sicherheit und Leistung (Paket)

Data-Governance protokolliert Neue Protokolle für die folgenden Datenquellen hinzugefügt:

- Citrix Identitätsanbieter
- Citrix Gateway
- Secure Browser
- Microsoft Graph Security
- Microsoft Active Directory

Weitere Informationen finden Sie unter Data Governance.

Behobene Probleme

- Die Self-Service-Suche funktioniert in Internet Explorer 11 nicht richtig. Daher können Sie Ihre Suchanfrage nicht eingeben und einen Suchvorgang ausführen. [CAS-18657]

09. Januar 2020

Behobene Probleme

- Die Walk-Through-Funktion von Citrix Analytics funktioniert für die Benutzer in der Heimatregion der Europäischen Union nicht. [CAS-26297]

18. Dezember 2019

Behobene Probleme

Auf der **Analytics-Kachel** auf der **Citrix Cloud-Seite** wurde die Schaltfläche **Dienst anzeigen** angezeigt. Diese Schaltfläche wurde jetzt in **Verwalten** geändert, um die Benutzererfahrung zu verbessern. [CAS-27922]

12. Dezember 2019

Neue Features

Unterstützung für Microapps Service-Events im asiatisch-pazifischen Süden Die Citrix Analytics-Plattform verarbeitet jetzt Benachrichtigungen vom Microapps-Dienst in der Region Asien-Pazifik Süd. Datensätze, die Leistung,

Stabilität, Nutzung, Sicherheit und Support messen, werden jedoch in den USA aggregiert und gespeichert. Weitere Informationen finden Sie unter Data Governance.

> **Hinweis**
>
> Der Microapps-Dienst wird als Teil von Citrix Workspace angeboten. Weitere Informationen finden Sie in der Microapps-Dokumentation .

04. Dezember 2019

Behobene Probleme

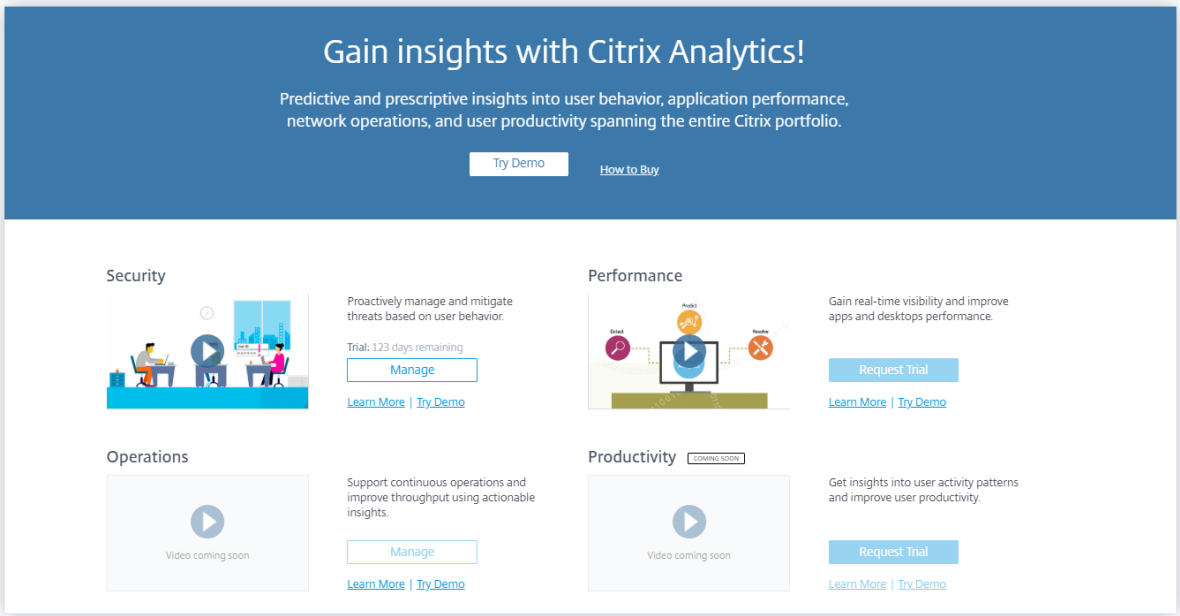
Einige Benutzer in der Region Asien-Pazifik-Süd können sich nicht bei Citrix Analytics anmelden, obwohl sie bei Citrix Cloud eingebunden sind, indem sie **USA** als Heimatregion ausgewählt haben. [CAS-27368]

22. November 2019

Neue Features

Übersichtsseite für Analytics neu gestaltet Die Analytics-Übersichtsseite wurde neu gestaltet, um den Zugriff auf alle Analytics-Angebote von dieser Seite aus zu ermöglichen. Sie können eine Testversion anfordern, die Demo ausprobieren oder Ihr Analytics-Angebot verwalten. Derzeit sind nur Security Analytics und Operations Analytics allgemein verfügbar und daher auf dieser Seite aktiv.

Um die Übersichtsseite anzuzeigen, wählen Sie **Hilfe** > **Überblick**.



21. Oktober 2019

Neue Features

Technische Sicherheit Die technische Sicherheitsübersicht vermittelt Ihnen ein Verständnis der bewährten Sicherheitsmethoden im Zusammenhang mit Citrix Analytics. In diesem Dokument werden der Datenfluss, der Datenschutz, die Netzwerkanforderungen und die Sicherheitsverantwortung beschrieben, die bei der Verwendung von Citrix Analytics berücksichtigt werden müssen.

11. September 2019

Behobene Probleme

- Citrix Cloud kann Benutzer nicht auf die regionsspezifische Citrix Analytics-Seite umleiten. [CAS-20559]

20. August 2019

Behobene Probleme

- Die exemplarische Vorgehensweise von Citrix Analytics wird in den Microsoft Edge- und Safari-Browsern nicht korrekt geladen. [CAS-20906]

31. Juli 2019

Neue Features

Unterstützung der Region der Europäischen Union Citrix Analytics unterstützt jetzt die Region der Europäischen Union. Sie können die **Europäische Union** als Heimatregion auswählen, während Sie Ihr Unternehmen in Citrix Cloud integrieren und den Citrix Analytics Service verwenden. Citrix Analytics speichert die Benutzerereignisse und Metadaten für Ihr Unternehmen in der Region Europäische Union. Weitere Informationen zu Citrix Cloud-Regionen finden Sie unter Geografische Überlegungen.

26. Juni 2019

Behobene Probleme

- Citrix Analytics wird in Internet Explorer 11 nicht genau geladen. [CAS-19867]

19. Juni 2019

Behobene Probleme

- Citrix Analytics wird auf Microsoft Edge nicht genau geladen. [CAS-19930]

16. November 2018

Behobene Probleme

- Wenn Sie mit Internet Explorer Version 11.0 auf Citrix Analytics zugreifen, wird die **Citrix Cloud-Navigationsleiste** nicht geladen und Sie können nicht auf das Hamburgermenü zugreifen.

10. Oktober 2018

Architektur- und Plattformverbesserungen

In dieser Version wurden mehrere Architektur- und Plattformverbesserungen vorgenommen, um Leistung, Skalierung, Überwachung, Supportabilität, Sicherheit und Benutzererfahrung zu verbessern.

23. August 2018

Citrix Analytics ist ein Cloud-Dienst, der über Citrix Cloud bereitgestellt wird. Es sammelt Daten über alle Citrix Portfolioprodukte hinweg und bietet umsetzbare Erkenntnisse, die es Administratoren ermöglichen, proaktiv mit Sicherheitsbedrohungen umzugehen, die App-Leistung zu verbessern und den kontinuierlichen Betrieb zu unterstützen. Derzeit bietet Citrix Analytics die folgenden Analyseangebote:

- **Sicherheitsanalysen**: Sortiert und bietet Einblick in das Benutzer- und Entitätsverhalten. Weitere Informationen finden Sie unter Sicherheitsanalysen.
- **Operations Analytics**: Sammelt und präsentiert Informationen über die Aktivitäten von Benutzern, z. B. besuchte Websites und die aufgewendete Bandbreite. Weitere Informationen finden Sie unter Operations Analytics.

Neue Produktnamen

Die von Citrix Analytics unterstützten Citrix Produkte werden jetzt als Teil des einheitlichen Citrix Produktportfolios umbenannt.

Möglicherweise bemerken Sie neue Namen in unseren Produkten und Produktdokumentationen. Dieses Rebranding ist das Ergebnis der Erweiterung des Citrix Portfolios und der Cloud-Strategie. Weitere Informationen zum einheitlichen Portfolio von Citrix finden Sie im Citrix Produkthandbuch.
Die Implementierung dieser Umstellung in unsere Produkte und deren Dokumentation ist ein kontinuierlicher Prozess.

- Inhalte in Produkt und Dokumentation enthalten möglicherweise noch die früheren Namen. Beispielsweise können Sie Instanzen der früheren Namen in Konsolentext, Meldungen, Verzeichnis-/Dateinamen, Screenshots und Diagrammen sehen.
- Es ist möglich, dass einige Elemente (wie Befehle) weiterhin ihre früheren Namen behalten, um zu verhindern, dass bestehende Kundenskripte beschädigt werden.
- Die zugehörige Produktdokumentation und andere Ressourcen (z. B. Videos und Blogposts), zu denen es Links in dieser Produktdokumentation gibt, verwenden möglicherweise weiterhin die früheren Namen.

Bekannte Probleme

September 22, 2023

In diesem Artikel werden die bekannten Probleme beschrieben, die für alle Citrix Analytics-Angebote gelten (Leistung und Sicherheit).

Informationen zu den spezifischen Problemen der einzelnen Angebote finden Sie in den entsprechenden Artikeln zu bekannten Problemen: Sicherheit und Leistung.

- Die **Gateway-Erstzugriffsanzeige von neuer IP** wird für Benutzer ausgelöst, die bei der ersten Anmeldung über das Gateway auf Dienste oder Anwendungen zugreifen. [CAS-57963]

Datenquellen

September 22, 2023

Datenquellen sind die Cloud-Dienste und die on-premises Produkte, die Daten an Citrix Analytics senden.

Citrix Analytics sammelt Daten aus den folgenden Datenquellen:

- **Citrix Datenquellen**. Citrix Cloud-Dienste und on-premises Produkte, die Daten an Citrix Analytics senden. Citrix Analytics erkennt automatisch die Citrix Cloud-Dienste wie Content Collaboration und Endpoint Management, die mit Ihrem Citrix Cloud-Konto verknüpft sind.

  Für on-premises Produkte wie Citrix Gateway und Citrix Virtual Apps and Desktops müssen Sie eine Reihe von Konfigurationen durchführen, um eine Verbindung zu Citrix Analytics herzustellen. Beispielsweise müssen die on-premises Gateway-Instanzen zu Application Delivery Management hinzugefügt werden. Und die on-premises Websites für Virtual Apps and Desktops müssen zu Workspace hinzugefügt werden, oder die StoreFront-Server müssen konfiguriert werden.

- **Externe Datenquellen**. Drittanbieteranwendungen wie Microsoft Graph Security, Microsoft Active Directory, die in Citrix Analytics integriert werden können. Citrix Analytics sammelt nach erfolgreicher Integration Daten aus diesen externen Datenquellen.

Unterstützte Datenquellen

Je nachdem, welches Citrix Analytics-Angebot Sie verwenden, variieren die Datenquellen. In den folgenden Artikeln finden Sie die Datenquellen, die von den einzelnen Angeboten unterstützt werden:

- Von Citrix Analytics for Security unterstützte Datenquellen
- Von Citrix Analytics for Performance unterstützte Datenquellen

Die Datenquellen Citrix Gateway, Citrix DaaS (früher Citrix Virtual Apps and Desktops Service) und Citrix Virtual Apps and Desktops werden von beiden Angeboten unterstützt: Citrix Analytics for Security und Citrix Analytics for Performance. Informationen zu den Onboarding-Schritten, die für beide Angebote gelten, finden Sie in den folgenden Artikeln:

- NetScaler Gateway-Datenquelle
- Citrix Virtual Apps and Desktops-Datenquelle

Citrix Gateway-Datenquelle

April 12, 2024

Die **Gateway-Datenquelle** stellt die on-premises Citrix Gateway-Instanzen in Ihrer Umgebung dar. Citrix Analytics erkennt automatisch die Citrix Application Delivery Management (ADM)-Agent und die Gateway-Instanzen, die dem Citrix ADM Service hinzugefügt wurden.

Wenn Benutzer über Gateway auf Dienste oder Anwendungen zugreifen, empfängt Citrix Analytics die Benutzerzugriffsereignisse in Echtzeit. Die Benutzerereignisse werden verarbeitet, um Sicherheitsbedrohungen zu erkennen.

In diesem Artikel werden die Schritte zum Hinzufügen von Citrix Gateway zu Citrix Analytics beschrieben. Diese Schritte gelten für beide Angebote: Citrix Analytics for Performance und Citrix Analytics for Security.

Voraussetzungen

- Abonnieren Sie Citrix ADM, das in Citrix Cloud angeboten wird. Informationen zu den ersten Schritten mit Citrix ADM finden Sie unter Erste Schritte.
- Verifizierte Citrix ADM-Lizenz. Weitere Informationen zur Citrix ADM-Lizenzierung finden Sie unter Lizenzen.
- Überprüfen Sie die Systemanforderungen und stellen Sie sicher, dass die Anforderungen erfüllt sind.

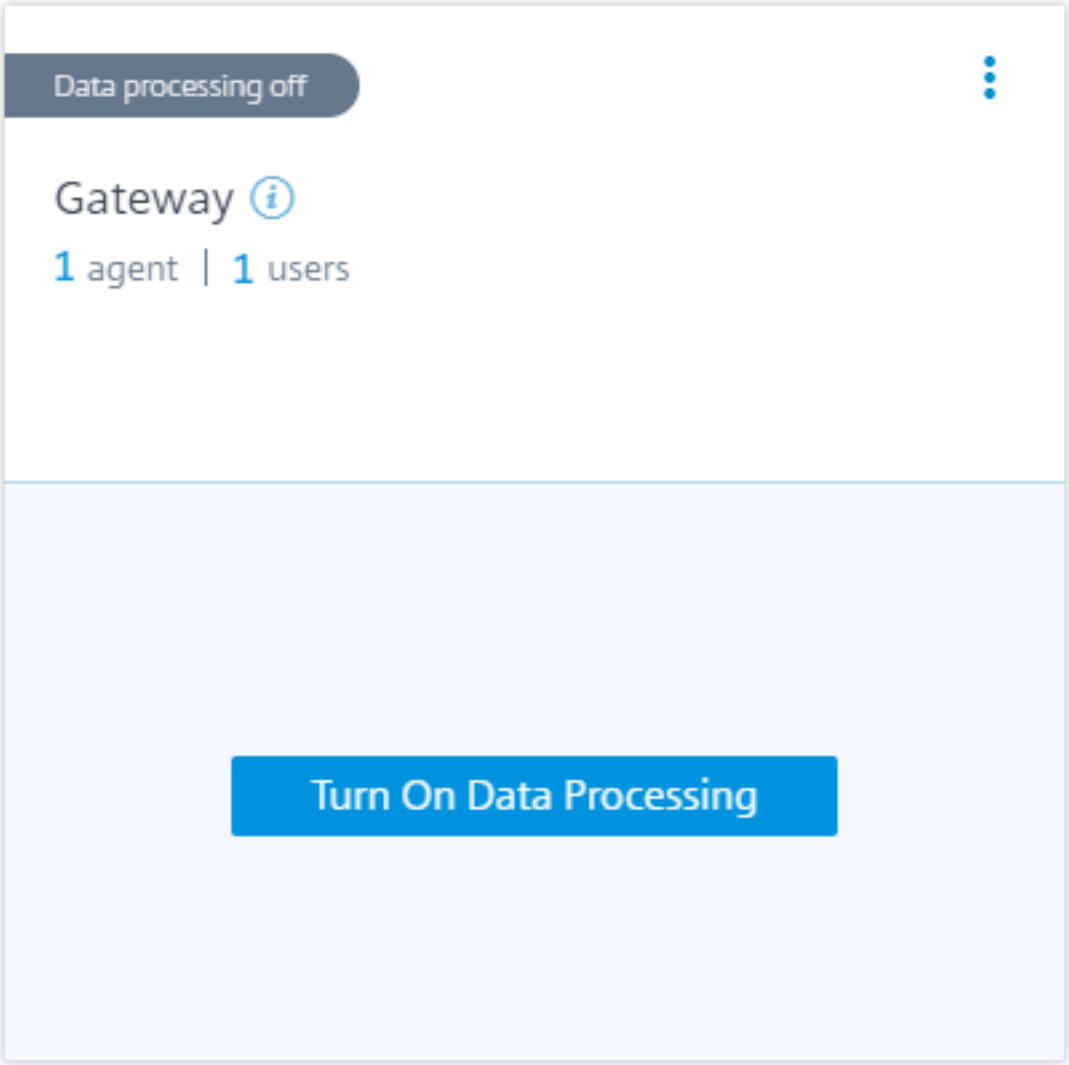
Gateway-Datenquellen zu Citrix ADM hinzugefügt

Citrix Analytics erkennt automatisch die Citrix ADM-Agenten und die Citrix Gateway-Instanzen, die bereits zum Citrix ADM Service hinzugefügt wurden.

So zeigen Sie die Datenquelle an:

Klicken Sie in der oberen Leiste auf **Einstellungen** > **Datenquellen**. Wählen Sie je nach Angebot entweder **Sicherheit** oder **Leistung** aus, um die Gateway-Sitekarte anzuzeigen.

Die erkannten Agenten und die Benutzer werden auf der Gateway-Sitekarte angezeigt. Klicken Sie auf **Datenverarbeitung einschalten**, damit Citrix Analytics mit der Verarbeitung von Daten für diese Datenquelle beginnen kann.

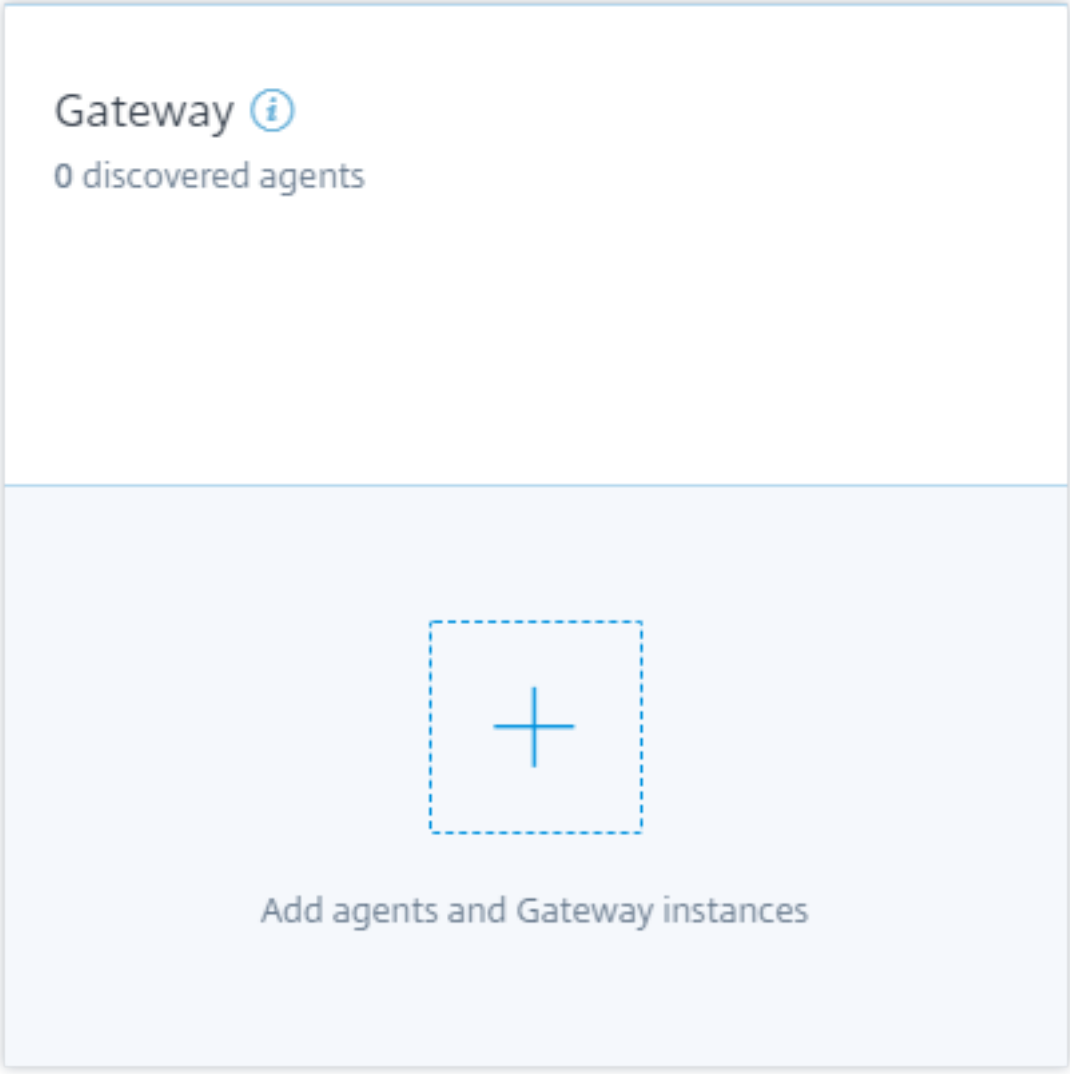


Sie können die empfangenen Ereignisse anzeigen.

Weitere Informationen finden Sie unter Ein einheitlicher Prozess zum Aktivieren von Analysen auf virtuellen Servern, um Citrix Analytics zu aktivieren, falls dies nicht bereits im Citrix ADM Service aktiviert ist.

Gateway-Datenquellen wurden nicht zu Citrix ADM hinzugefügt

Auf der Gateway-Sitekarte werden **0 erkannte Agenten** angezeigt, wenn Citrix ADM-Agents und Citrix Gateway-Instanzen nicht zum Citrix ADM Service hinzugefügt werden.

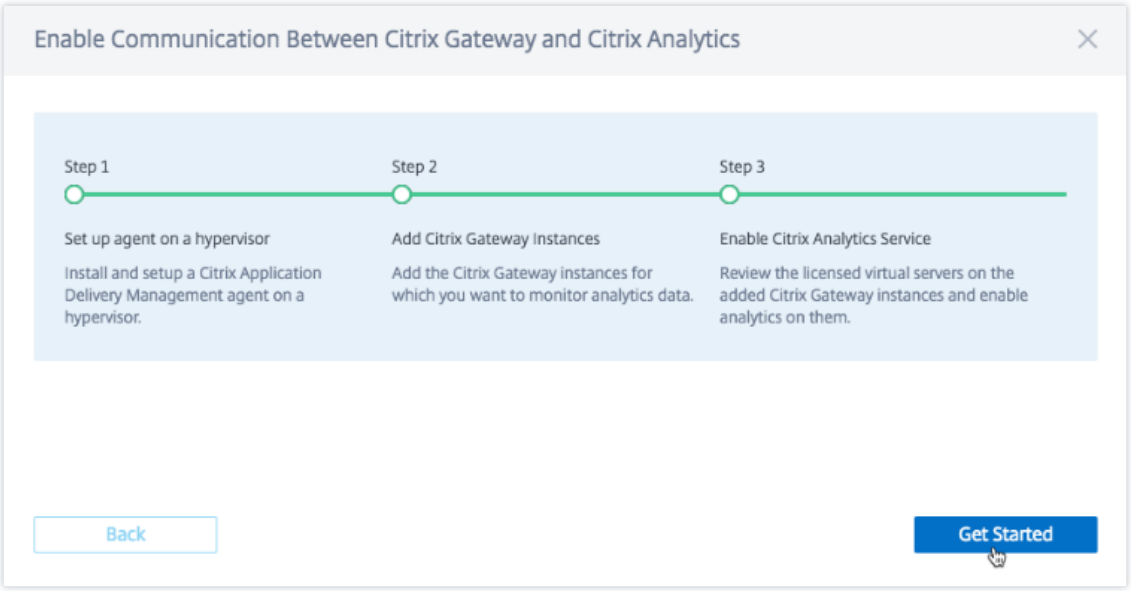


Gehen Sie wie folgt vor, um die Agents und Gateway-Instanzen zu ermitteln:

1. Wenn Sie bereits ein Citrix ADM Serviceabonnement haben, klicken Sie auf der Sitekarte auf **+**, um die Agents und Gateway-Instanzen hinzuzufügen.
2. Wenn Sie kein Abonnement für den Citrix ADM Service haben, müssen Sie ihn abonnieren. Gehen Sie zu Ihrem Citrix Cloud-Konto und gehen Sie wie folgt vor:
    a) Klicken Sie unter **Verfügbare Dienste** auf der Kachel **Application Delivery Management** auf **Verwalten**.
    b) Befolgen Sie die Anweisungen auf dem Bildschirm, um ein Express-Konto für Citrix ADM zu erstellen. Weitere Informationen finden Sie in der Citrix ADM-Dokumentation unter Erste Schritte.
    c) Nachdem Sie das Express-Konto erstellt haben, melden Sie sich wieder bei Analytics an und klicken Sie auf **Einstellungen > Datenquellen > Sicherheit**.

d) Klicken Sie auf der Gateway-Sitekarte auf **+**, um die Agenten und Gateway-Instanzen hinzuzufügen.

3. Klicken Sie auf der folgenden Seite auf **Erste Schritte**.



4. Führen Sie die folgenden Aufgaben aus:

   - Installieren Sie einen Citrix ADM-Agent
   - Fügen Sie Ihre Gateway Instanzen hinzu
   - Analytics auf virtuellen Servern aktivieren

Voraussetzungen

- **Installationsanforderung für Citrix ADM-Agents**: In Ihrem Rechenzentrum können Sie einen Agent auf Citrix Hypervisor, VMware ESXi, Microsoft Hyper-V und Linux KVM Server installieren.

  In der folgenden Tabelle sind die virtuellen Rechenressourcen aufgeführt, die der Hypervisor für den Agent bereitstellen muss.

Komponente	Voraussetzung
RAM	8 GB (32 GB für bessere Leistung empfohlen.)
Virtuelle CPU	4 (8 virtuelle CPUs für bessere Leistung empfohlen)
Speicherplatz	120 GB
Virtuelle Netzwerkschnittstellen	1

Komponente	Voraussetzung
Durchsatz	1 Gbit/s

- **Portanforderungen**: Stellen Sie sicher, dass die folgenden Ports geöffnet sind, damit der Citrix ADM-Agent mit den Citrix Gateway-Instanzen kommunizieren kann.

Typ	Port	Beschreibung
TCP	80/443	Für NITRO-Kommunikation vom Agent zu Citrix Gateway-Instanzen
TCP	22	Für die SSH-Kommunikation vom Agent zur Citrix Gateway-Instanz.
UDP	4739	Für AppFlow-Kommunikation vom Citrix Gateway zum Agent
ICMP	Kein reservierter Port	Erkennen der Netzwerkerreichbarkeit vom Agent zu Citrix Gateway-Instanzen.
SNMP	161, 162	Um SNMP-Ereignisse von der Citrix Gateway-Instanz zum Agent zu empfangen
Syslog	514	Um Syslog-Nachrichten im Agent von der Citrix Gateway-Instanz zu empfangen.
TCP	5557	Für die Protokollstream-Kommunikation von Citrix Gateway-Instanzen zum Agent.

Stellen Sie für die Kommunikation zwischen dem Citrix ADM-Agent und Citrix Analytics sicher, dass der folgende Port geöffnet ist:

Typ	Port	Beschreibung
TCP	443	Für die NITRO-Kommunikation zwischen dem Agent und dem Citrix Application Delivery Management Service.

Stellen Sie für die Kommunikation zwischen dem Citrix ADM-Agent und Citrix Analytics sicher, dass der folgende Endpunkt auf der Positivliste steht:

Endpunkt	US-Region	EU-Region
Ereignis-Hub	`https://cas-eh-ns-alias.servicebus.windows.net/`	`https://cas-eh-ns-eu-alias.servicebus.windows.net/`

Installieren und Einrichten eines Agent

Installieren und konfigurieren Sie den Citrix ADM Service Agent in Ihrer Netzwerkumgebung, um die Kommunikation zwischen Analytics und den Gateway-Instanzen in Ihrem Rechenzentrum zu ermöglichen.

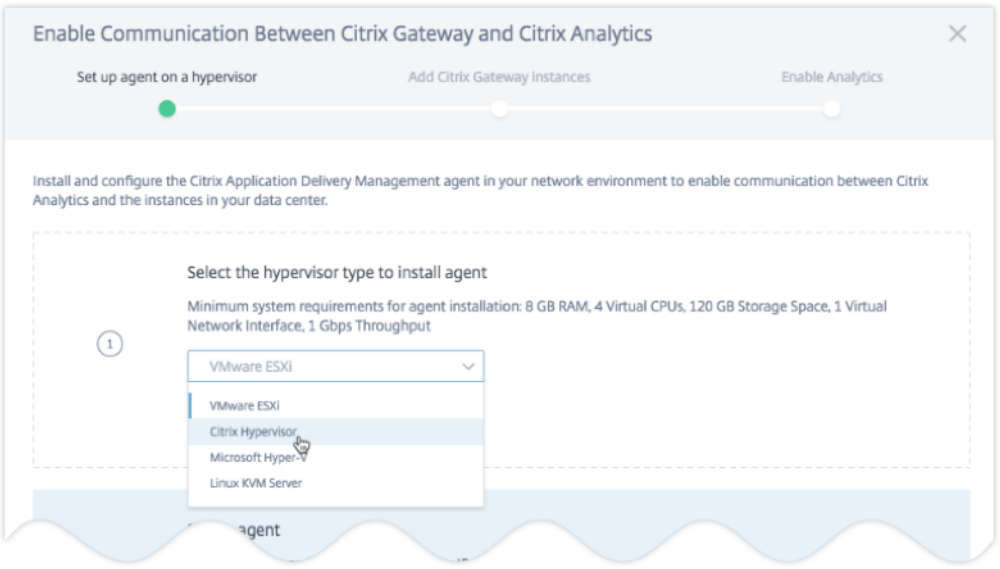
Sie können einen Agent auf den folgenden Hypervisoren in Ihrem Unternehmensrechenzentrum installieren:

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

Gehen Sie wie folgt vor, um einen Agent zu installieren und einzurichten:

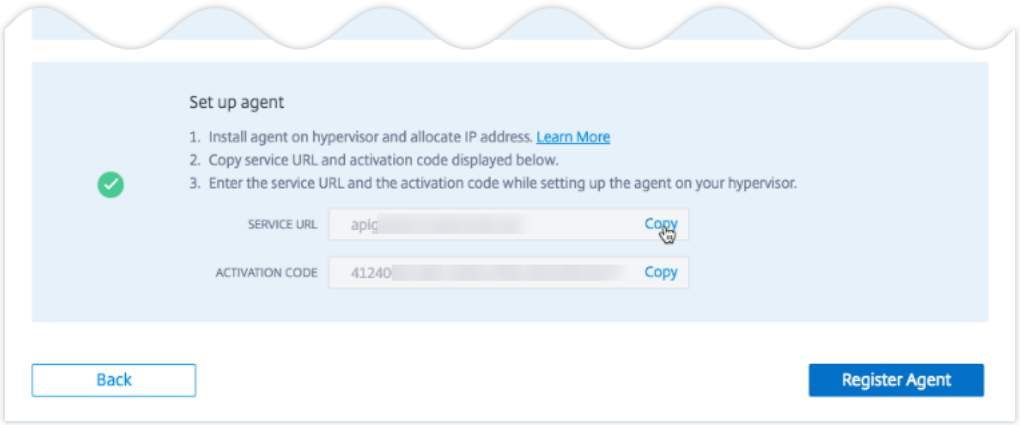
1. Laden Sie das Agent-Image herunter.

   Wählen Sie auf der Seite **Agent auf einem Hypervisor einrichten** den Hypervisor aus und klicken Sie auf **Image herunterladen**, um das Agent-Image auf Ihr lokales System herunterzuladen.



2. Kopieren der Service-URL und des Aktivierungscodes

   Eine Service-URL und ein Aktivierungscode werden generiert und auf der Benutzeroberfläche angezeigt, wie in der folgenden Abbildung dargestellt. (Dieser Vorgang kann einige Sekunden dauern.) Der Agent verwendet die Dienst-URL, um den Dienst zu finden, und den Aktivierungscode, um sich beim Dienst zu registrieren. Geben Sie die Service-URL und den Aktivierungscode ein, während Sie den Agent auf Ihrem Hypervisor installieren.



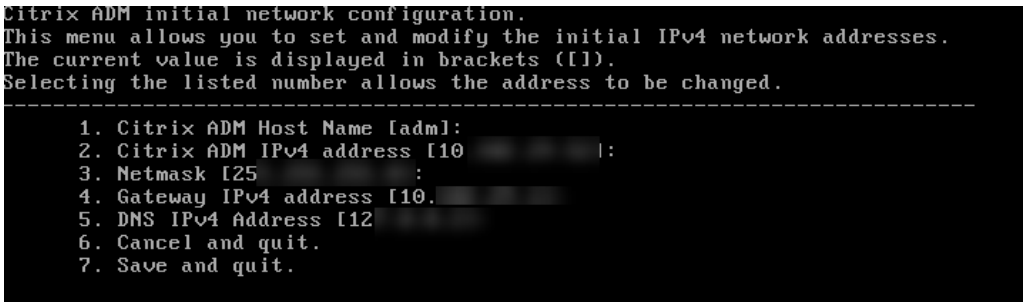
3. Installieren Sie den Agent auf einem Hypervisor.

> **Hinweis**
>
> Bevor Sie mit der Agentinstallation beginnen, müssen Sie Folgendes sicherstellen:
>
> - Sie verfügen über die erforderlichen virtuellen Rechenressourcen, die der Hypervisor für jeden Agent bereitstellen muss: RAM: 8 GB, vCPU: 4, Speicherplatz: 120 GB, virtuelle Netzwerkschnittstelle: 1 und Durchsatz: 1 Gbit/s

- Sie konfigurieren Ihr DNS so, dass es Ihrem Agent den Internetzugang ermöglicht.

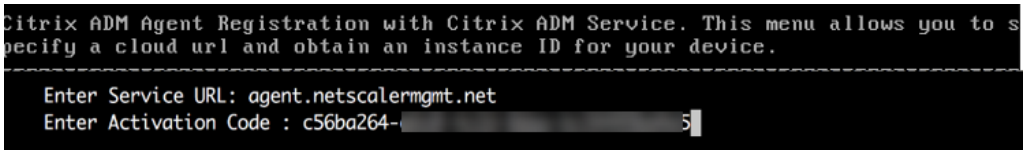
- Führen Sie auf einem Citrix Hypervisor Folgendes aus:

  a) Importieren Sie die Agentimagedatei in Ihren Hypervisor. Konfigurieren Sie auf der Registerkarte **Konsole** die Optionen für die anfängliche Netzwerkkonfiguration, wie im folgenden Beispiel gezeigt.

  Wenn Sie falsche Werte eingegeben haben oder einen Wert ändern möchten, melden Sie sich mit den Standardanmeldeinformationen `nsrecover`/an der Shell-Eingabeaufforderung an`nsroot`. Führen Sie dann den Befehl aus `networkconfig` .

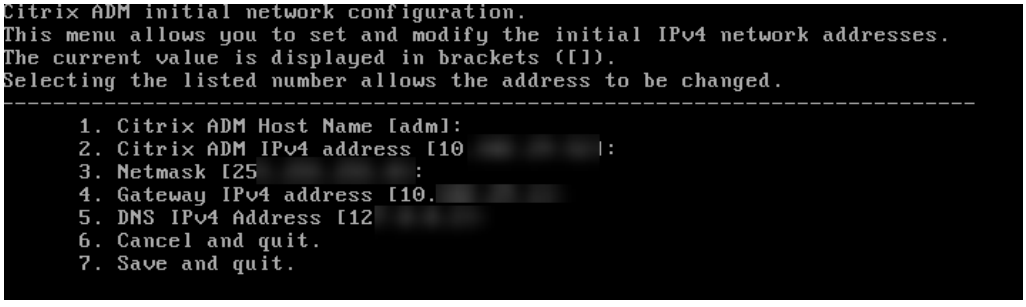
  b) Geben Sie die **Dienst-URL** und den **Aktivierungscode** ein, den Sie beim Herunterladen des Agent-Images gespeichert haben.

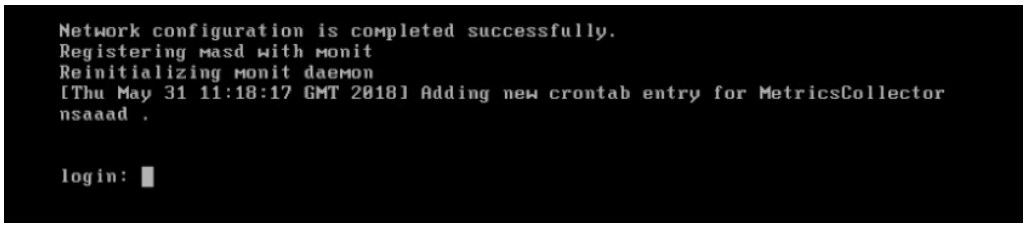
  Wenn Sie die Service-URL oder den Aktivierungscode falsch eingegeben haben, melden Sie sich an der Shell-Eingabeaufforderung des Agent an und führen Sie dann das Skript aus: `deployment_type.py`. Mit diesem Skript können Sie die Service-URL und den Aktivierungscode erneut eingeben.

- Führen Sie auf einem VMware ESXi-Hypervisor Folgendes aus:

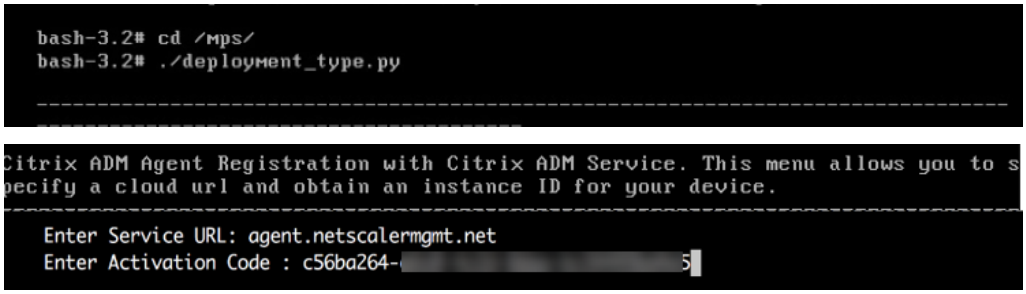
  a) Importieren Sie die Agentimagedatei in Ihren Hypervisor. Konfigurieren Sie auf der Registerkarte **Konsole** die Optionen für die anfängliche Netzwerkkonfiguration, wie im folgenden Beispiel gezeigt.

b) Nachdem Sie das Netzwerk konfiguriert haben, melden Sie sich bei Aufforderung mit den Standardanmeldeinformationen `nsrecover`/`nsroot` an der Shell-Eingabeaufforderung des Agents an.



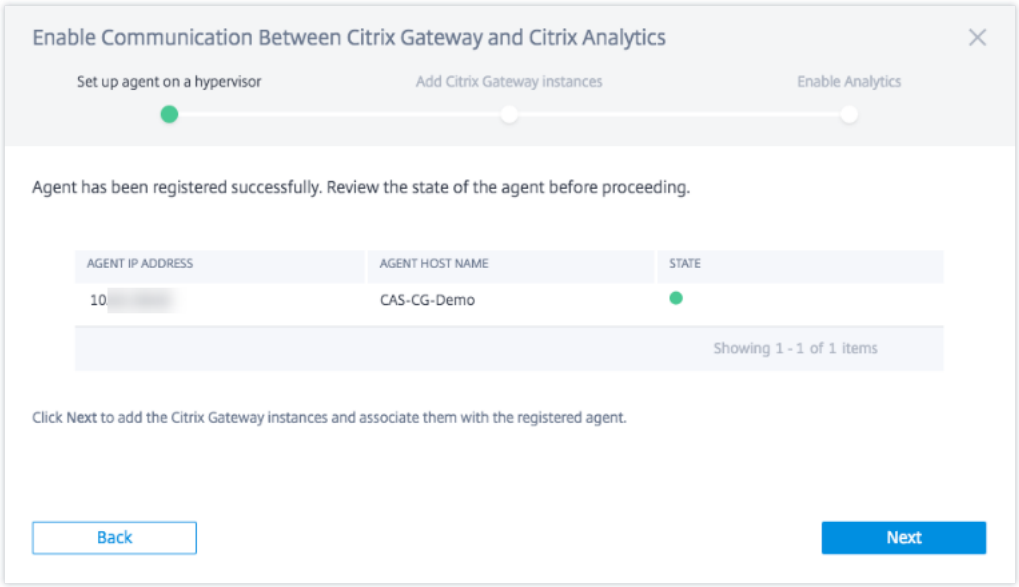
c) Navigieren Sie zum Verzeichnis **/mps**, führen Sie das Skript aus und geben Sie die **Service-URL** und den **Aktivierungscode** ein, den Sie beim Herunterladen des Agent-Images gespeichert haben.



> **Hinweis**
>
> Sie können dieselbe Image-Datei verwenden, um mehrere Agent zu installieren. Sie können jedoch nicht denselben Aktivierungscode für mehr als einen Agent verwenden. Um einen neuen Aktivierungscode zu generieren, greifen Sie auf Citrix Analytics zu, und klicken Sie im Setup-Agent in einem Hypervisor-Schritt erneut auf **Image herunterladen**. Ein neuer Aktivierungscode wird generiert.

4. Registrieren Sie den Agent.

   Nach erfolgreicher Agentregistrierung wird der Agent neu gestartet, um den Installationsvorgang abzuschließen. Nachdem der Agent neu gestartet wurde, greifen Sie auf Citrix Analytics zu, klicken Sie auf **Agent registrieren**, und überprüfen Sie dann den Status des Agent.

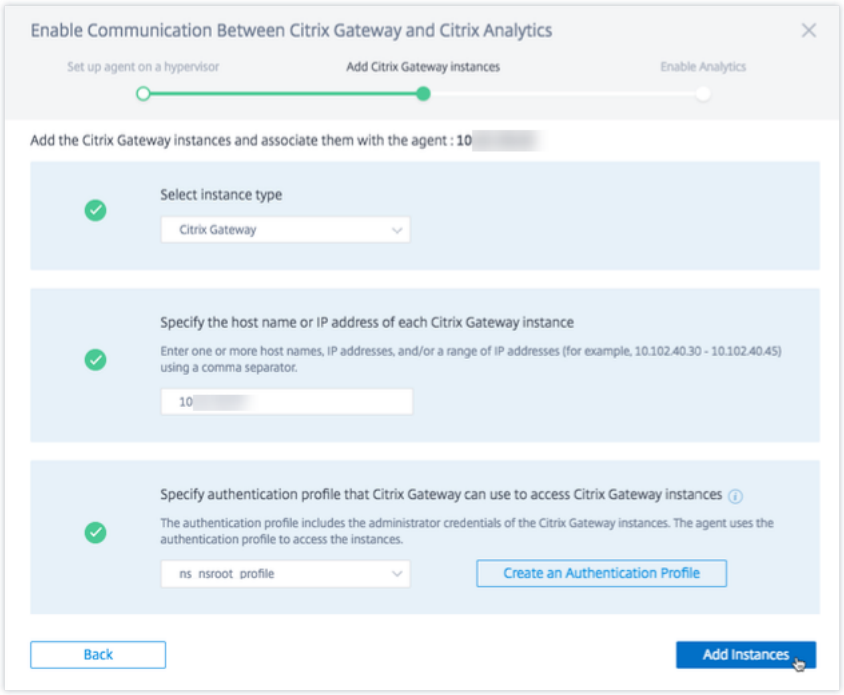


Wenn sich der Agent-Status im Status UP befindet, der mit einem grünen Punkt daneben gekennzeichnet ist, klicken Sie auf **Weiter**, um Instanzen zum Dienst hinzuzufügen.

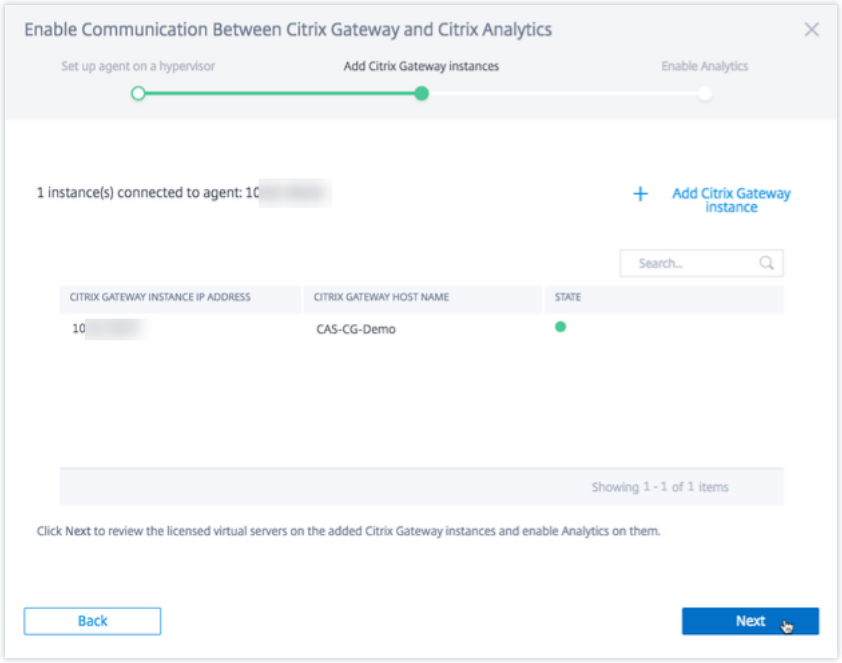
Citrix Gateway-Instanzen hinzufügen

Instanzen sind Citrix Gateway-Appliances oder virtuelle Appliances, die Datenquellen für Citrix Analytics darstellen.

1. Wählen Sie auf der Seite **Citrix Gateway Instanzen hinzufügen** den Instance-Typ aus und geben Sie Hostnamen oder IP-Adressen oder den IP-Adressbereich der zu erkennenden Gateway-Instanzen an.
2. Erstellen Sie ein Authentifizierungsprofil, mit dem der Agent auf die Gateway-Instanzen zugreifen kann Dieses Profil ist die Administratoranmeldeinformationen einer Gateway-Instanz. Klicken Sie dann auf **Instanzen hinzufügen**.



Nachdem die Instanzen hinzugefügt wurden, können Sie die Anzahl der Instanzen anzeigen, die erfolgreich erkannt wurden. Um weitere Instanzen hinzuzufügen, klicken Sie auf **Citrix Gateway-Instanz hinzufügen**.



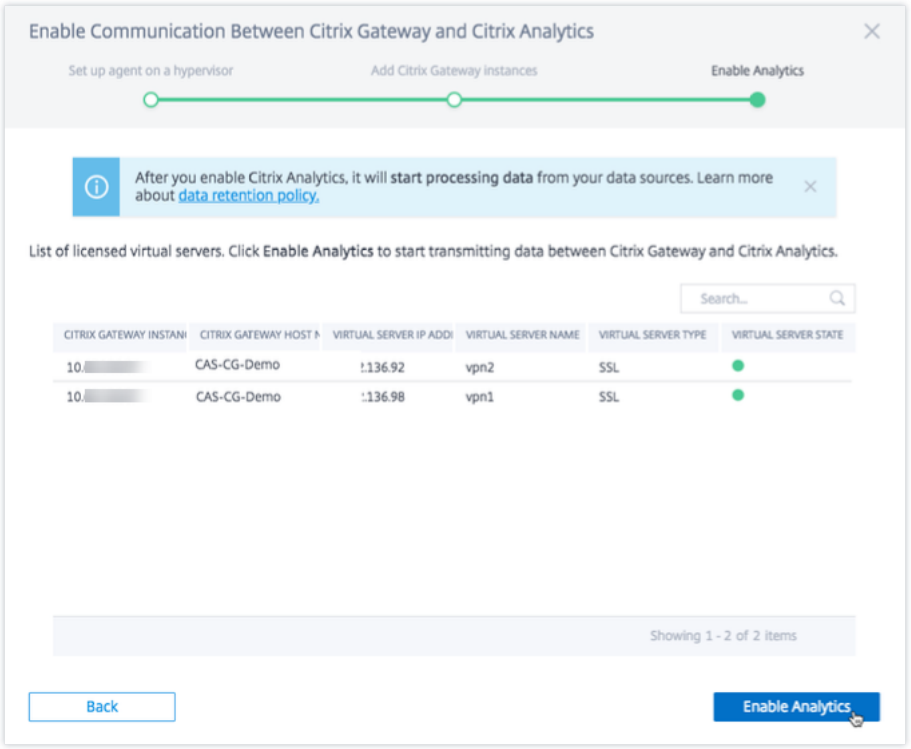
Klicken Sie auf **Weiter**, um Analysen zu aktivieren.

Analytik aktivieren

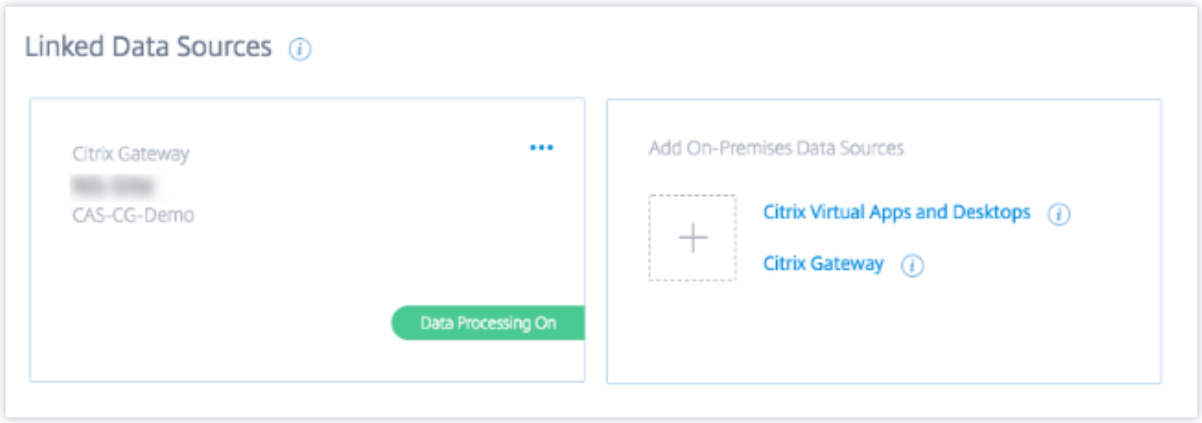
Citrix Analytics erkennt automatisch die lizenzierten virtuellen Server auf den hinzugefügten Citrix Gateway Instanzen. Aktivieren Sie Analysen auf allen erkannten virtuellen Servern.

Auf der Seite **Analytics aktivieren** werden standardmäßig alle lizenzierten virtuellen Server aus den Gateway-Instanzen angezeigt. Überprüfen Sie die Liste der lizenzierten virtuellen Server und klicken Sie auf **Analytics aktivieren**, um Analysen auf den virtuellen Servern zu ermöglichen.

> **Hinweis**
>
> Es kann einige Zeit dauern, bis die virtuellen Server, etwa 10 Minuten, auf der Seite angezeigt werden.



Der Status der Site-Karte ändert sich in **Datenverarbeitung am**. Sie können die empfangenen Ereignisse anzeigen.



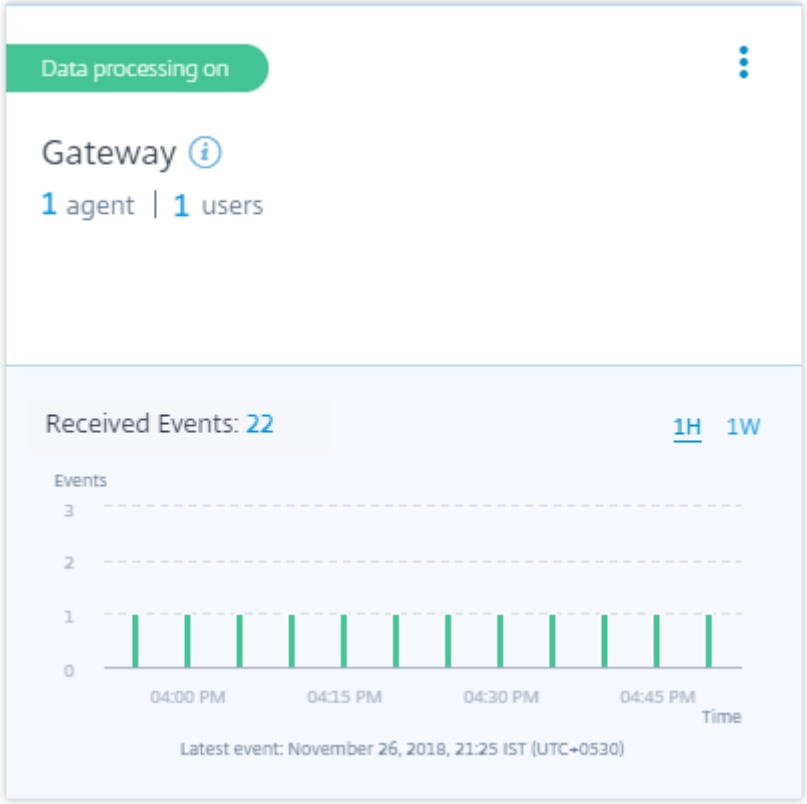
Das Onboarding-Video ansehen

Das folgende Video zeigt die Schritte zum Onboarding einer Gateway-Instanz:

Dies ist ein eingebettetes Video. Klicken Sie auf den Link, um das Video anzusehen

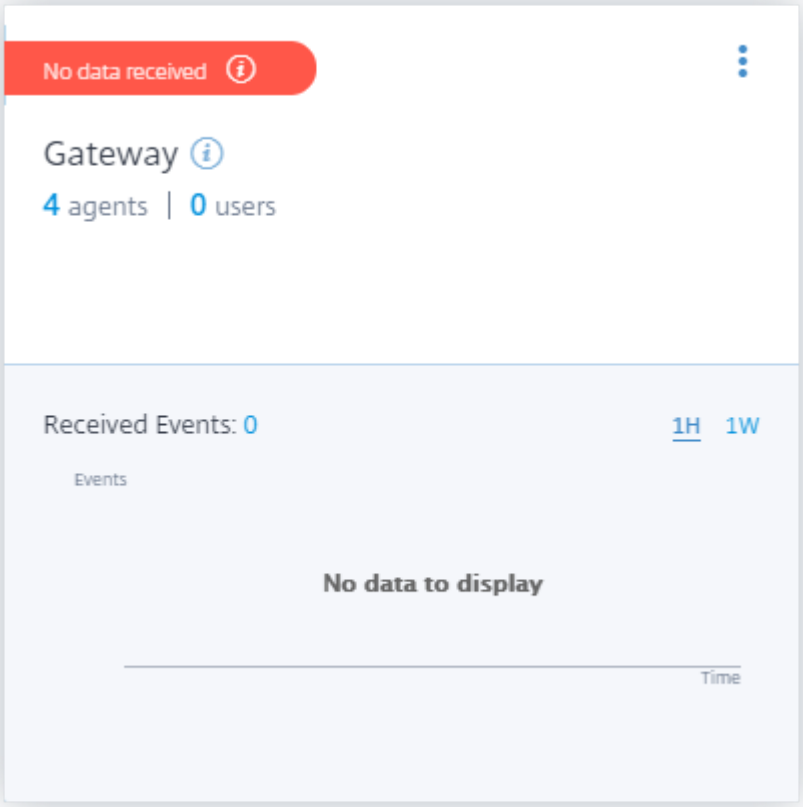
Empfangene Ereignisse, Benutzer und Agents anzeigen

Die Sitekarte zeigt die Anzahl der Gateway-Benutzer, NetScaler ADM-Agents und die Ereignisse an, die in der letzten Stunde von der Datenquelle empfangen wurden. Dies ist die Standardzeitauswahl. Sie können auch 1 Woche (**1 W**) auswählen und die Daten anzeigen. Klicken Sie auf der Seite Benutzer auf die Anzahl der **Benutzer**, die angezeigt werden sollen. Klicken Sie auf die Anzahl der Agents, um die Citrix Gateway-Instanzen und die Agents anzuzeigen.



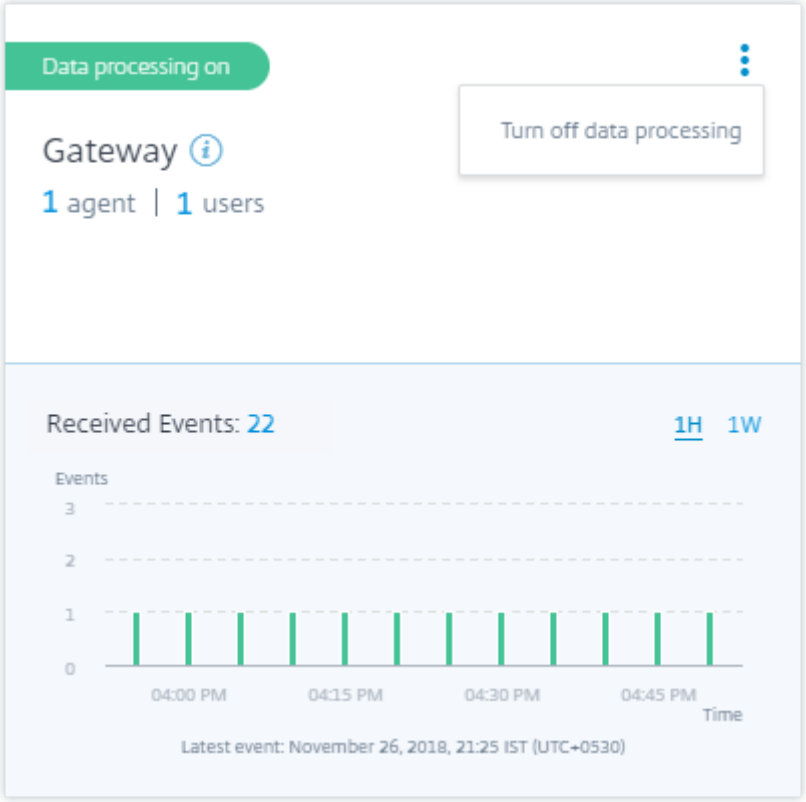
Nachdem Sie die Datenverarbeitung aktiviert haben, wird auf der Sitekarte möglicherweise der Status **No data received** angezeigt. Dieser Status wird aus zwei Gründen angezeigt:

1. Wenn Sie die Datenverarbeitung zum ersten Mal aktiviert haben, dauert es eine gewisse Zeit, bis die Ereignisse den Ereignis-Hub in Citrix Analytics erreichen. Wenn Citrix Analytics die Ereignisse empfängt, ändert sich der Status in **Data processing on**. Wenn sich der Status nach einiger Zeit nicht ändert, aktualisieren Sie die Seite **Datenquellen**.
2. Analytics hat in der letzten Stunde keine Ereignisse von der Datenquelle erhalten.

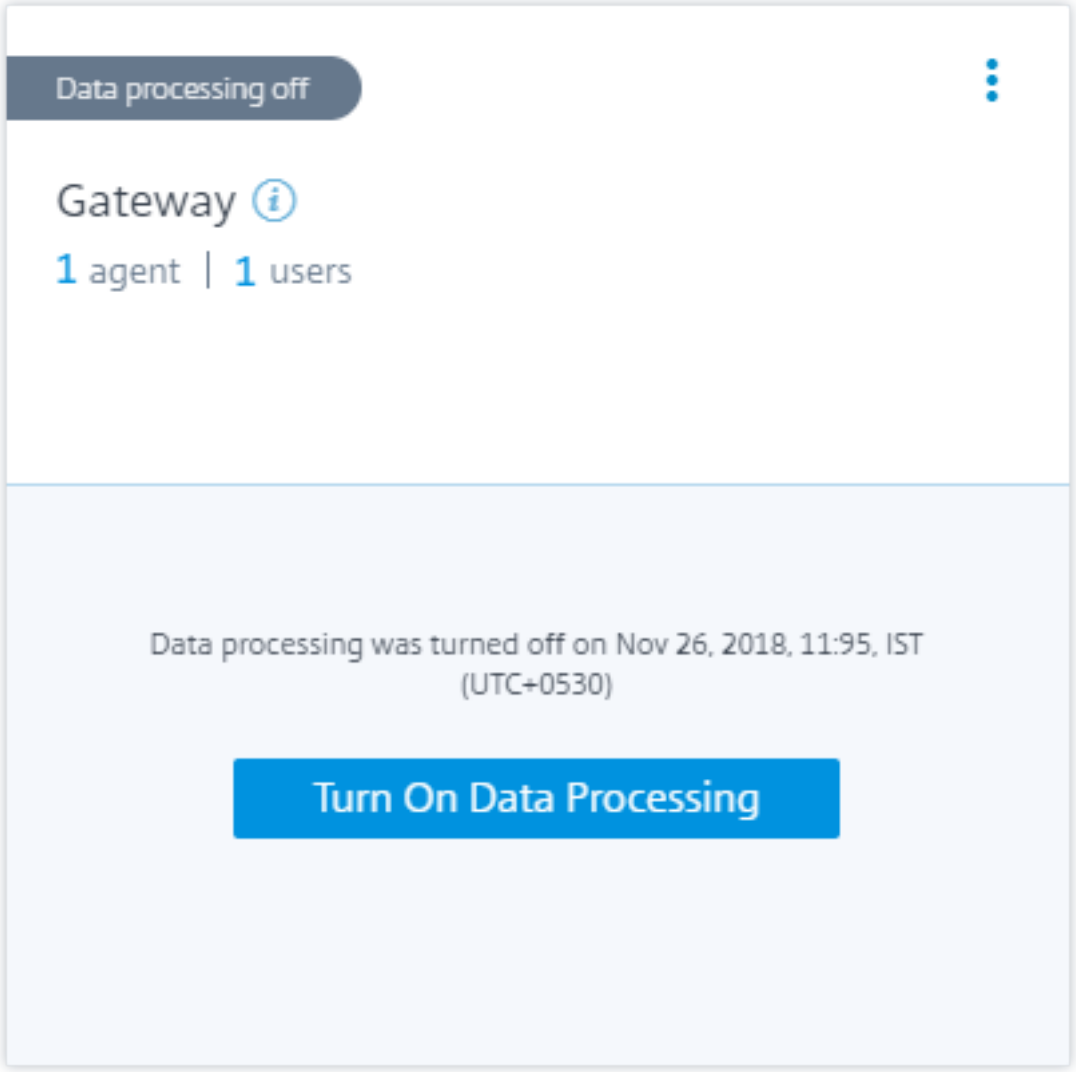


Aktivieren oder Deaktivieren der Datenverarbeitung

Um die Datenverarbeitung zu beenden, klicken Sie auf die vertikale Ellipse (⋮) auf der Sitekarte, und klicken Sie dann auf **Datenverarbeitung ausschalten**. Citrix Analytics beendet die Verarbeitung von Daten für diese Datenquelle.

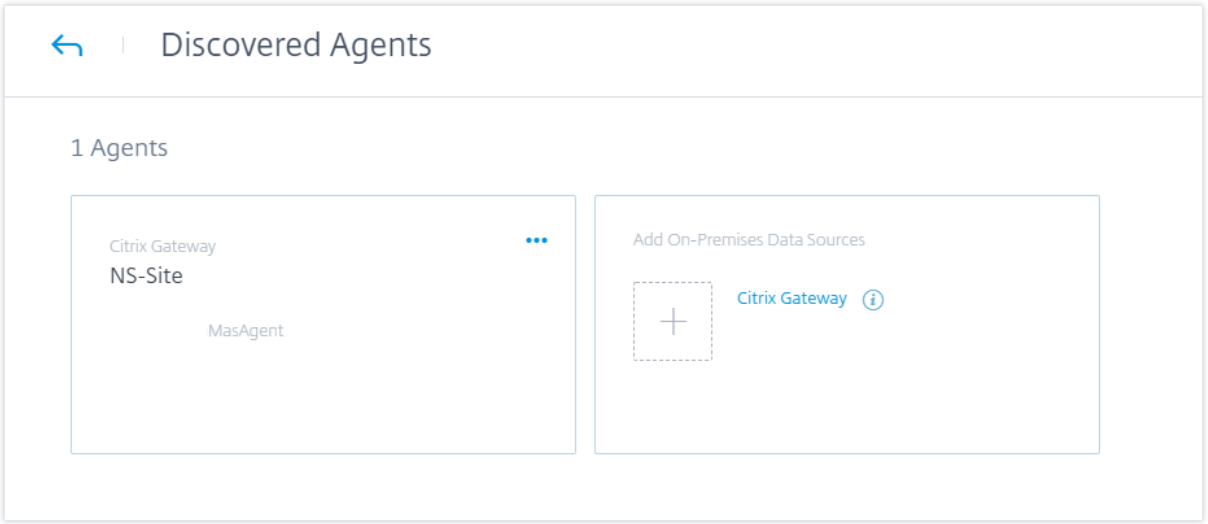


Um die Datenverarbeitung wieder zu aktivieren, klicken Sie auf **Datenverarbeitung einschalten**.



Weitere Gateway-Instanzen hinzufügen

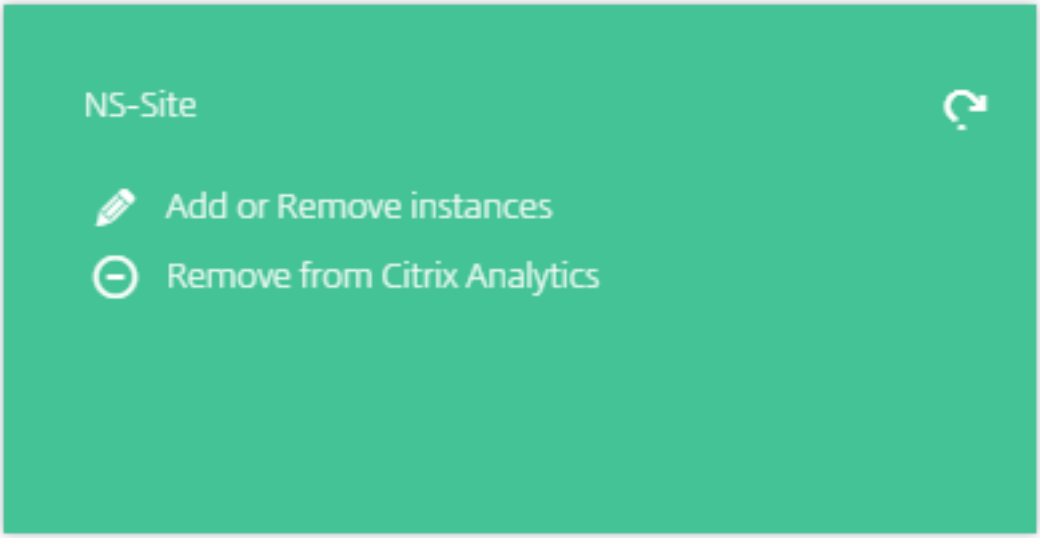
Wenn Sie weitere Gateway-Instanzen hinzufügen möchten, klicken Sie auf die Anzahl der Agent auf der Gateway-Sitekarte, um die Seite **Discovered Agents** anzuzeigen. Klicken Sie in der Kachel **Lokale Datenquellen hinzufügen** auf **Citrix Gateway**.



Datenquelle verwalten

Sie können auch weitere Instanzen zu einem Agent hinzufügen oder Instanzen entfernen, die einem Agent zugeordnet sind. Sie können den Agent und die zugehörigen Instanzen auch aus Citrix Analytics entfernen.

Drehen Sie eine Agent-Site-Karte um und führen Sie einen der folgenden Schritte aus



- **Instanzen hinzufügen oder entfernen**. Sie können einem Agent weitere Gateway-Instanzen hinzufügen und Analytics auf den auf diesen Instanzen konfigurierten virtuellen Servern aktivieren. Sie können auch Instanzen entfernen, die einem Agent hinzugefügt wurden. Wenn Sie eine Instanz von einem Agent trennen, kann Citrix Analytics nicht mit dieser Instanz kommunizieren.

- **Aus Citrix Analytics entfernen**. Nachdem Sie eine Agent-Site entfernt haben, hört Citrix Analytics auf, Daten von den mit diesem Agent verknüpften Instanzen zu sammeln. Alle zuvor verarbeiteten Daten sind jedoch während der Aufbewahrungsfrist verfügbar.

Datenquelle für Citrix Virtual Apps and Desktops

April 12, 2024

In diesem Artikel werden die Schritte zum Verbinden Ihrer on-premises Citrix Virtual Apps and Desktops-Sites mit Citrix Analytics über StoreFront beschrieben. Die in diesem Artikel genannten Onboarding-Schritte gelten für beide Angebote: Citrix Analytics for Performance (Performance Analytics) und Citrix Analytics for Security (Security Analytics).

Die für jedes Angebot spezifischen Onboarding-Schritte finden Sie in den folgenden Artikeln:

- On-Premises Citrix Virtual Apps and Desktops-Sites mit Citrix Analytics for Performance konfigurieren
- Konfigurieren von Citrix Virtual Apps and Desktops und Citrix DaaS-Datenquelle für Citrix Analytics for Security

Integrieren von Citrix Virtual Apps and Desktops on-premises Sites mit StoreFront

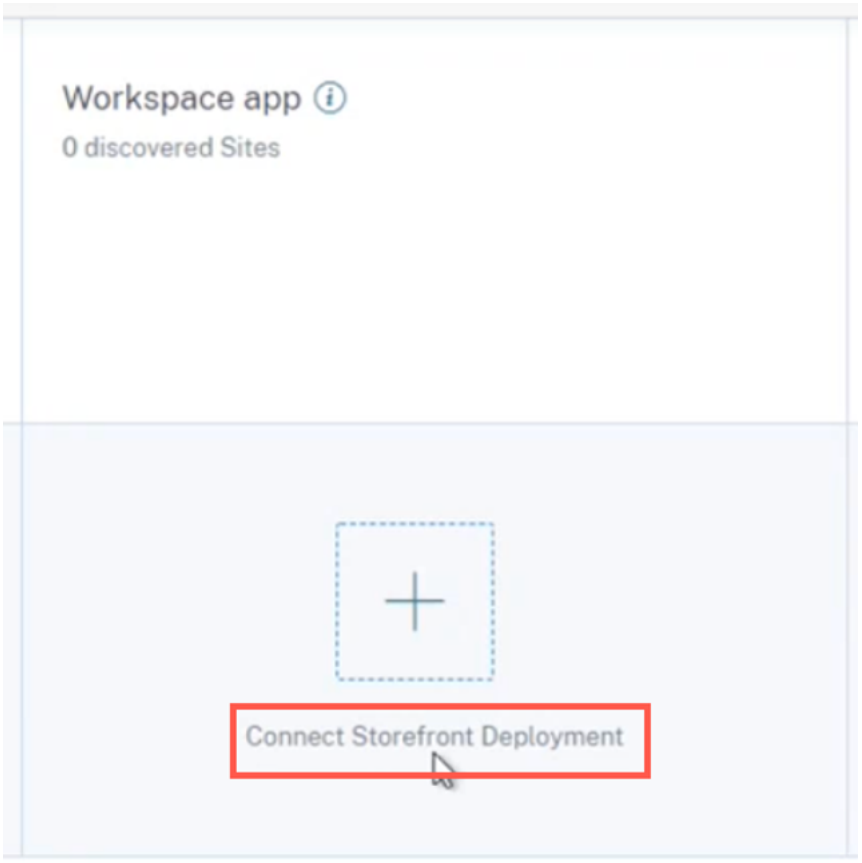
Wenn Ihre Organisation eine on-premises StoreFront-Bereitstellung verwendet, müssen Sie Ihre StoreFront-Server so konfigurieren, dass die Citrix Workspace-App Ereignisse an Citrix Analytics senden kann. Citrix Analytics verarbeitet Ereignisse, um umsetzbare Einblicke in die Leistung Ihrer Citrix IT-Infrastruktur und das Benutzerverhalten zu erhalten.

Weitere Informationen zum Konfigurieren einer StoreFront-Bereitstellung für Citrix Analytics finden Sie im Citrix Analytics Service Analytics-Dienstartikel in der StoreFront-Dokumentation.

Zuvor mussten Kunden, die die on-premises Sites von Citrix Apps and Desktops nutzten, die Site-Aggregation verwenden, um die on-premises Sites für Citrix Analytics for Security and Performance zu integrieren.

Sie können jetzt lokale Sites von Citrix Apps and Desktops integrieren, ohne von der Site-Aggregation abhängig zu sein.

Sie können die Option **Connect Storefront Deployment** in Ihrer Workspace-Anwendung sehen, auch wenn Sie der Site-Aggregation keine Site hinzugefügt haben.



Voraussetzungen

Bevor Sie beginnen, stellen Sie Folgendes sicher:

- Ihre StoreFront-Version muss 1906 oder höher sein.
- Die StoreFront-Bereitstellung muss eine Verbindung zu den folgenden Adressen herstellen können:
  - https://*.cloud.com
  - https://api.analytics.cloud.com
- In der StoreFront-Bereitstellung muss Port 443 für ausgehende Internetverbindungen geöffnet sein. Alle Proxyserver im Netzwerk müssen diese Kommunikation mit Citrix Analytics zulassen.
- Wenn die StoreFront-Bereitstellung auf einem Webserver gehostet wird, der einen Webproxy für die Verbindung mit dem Internet verwendet, muss der Proxy für jeden Store manuell konfiguriert werden, um ausgehenden Datenverkehr zuzulassen. StoreFront verwendet nicht automatisch die Proxy-Einstellung des Host-Webservers. Weitere Informationen finden Sie unter Konfigurieren einer StoreFront-Bereitstellung, die auf einem Webserver gehostet wird, der HTTP-Proxy verwendet.

- Auf die StoreFront-Bereitstellung muss mit einem der folgenden Clients zugegriffen werden:
  - Citrix Receiver für Websites in HTML5-kompatiblen Browsern.

    > **Hinweis**
    >
    > Wenn Sie ein HTML5-Benutzer sind, können Citrix Virtual Apps and Desktops Ereignisse starten, wenn bestimmte Konfigurationen in StoreFront aktiviert sind. Informationen zu den Konfigurationsschritten finden Sie im Artikel Installieren in der Citrix Workspace-App für HTML5-Dokumentation. Für druckbezogene Ereignisse müssen zusätzliche Richtlinien in StoreFront konfiguriert werden. Weitere Informationen finden Sie im Artikel PDF-Druck in der Citrix Workspace-App für HTML5-Dokumentation.

  - Citrix Workspace App 1907 für Windows oder höher.
  - Citrix Workspace App 2006 für Linux oder höher.
  - Citrix Workspace App 2006 für Mac oder höher
- Wenn Sie Citrix Virtual Apps and Desktops 7 1912 LTSR verwenden, ist die unterstützte StoreFront-Version 1912.

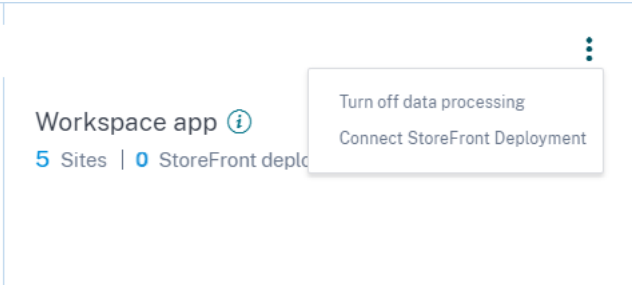
Verbinden mit einer StoreFront-Bereitstellung

Sie können auf folgende Weise eine Verbindung zu einer StoreFront-Bereitstellung herstellen:

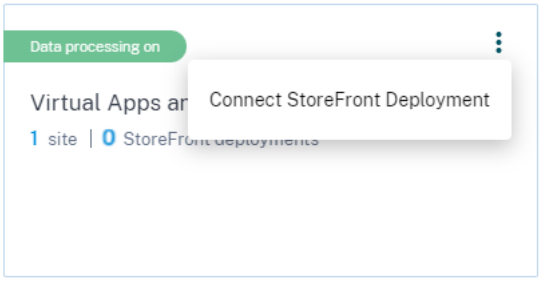
- Mit den Site-Karten **Apps und Desktops - Workspace-App** und **Apps und Desktops - Überwachen**
- Im Bereich **Empfehlungen**

Verbindung mit den Site Karten “Apps und Desktops - Workspace-App”und “Apps und Desktops - Überwachen”herstellen

1. Navigieren Sie zu **Einstellungen > Datenquellen > Sicherheit**. Klicken Sie auf der App-Site-Karte **Apps und Desktops** —**Workspace** auf die vertikalen Ellipsen (⋮), und wählen Sie dann **StoreFront-Bereitstellung verbinden** aus.

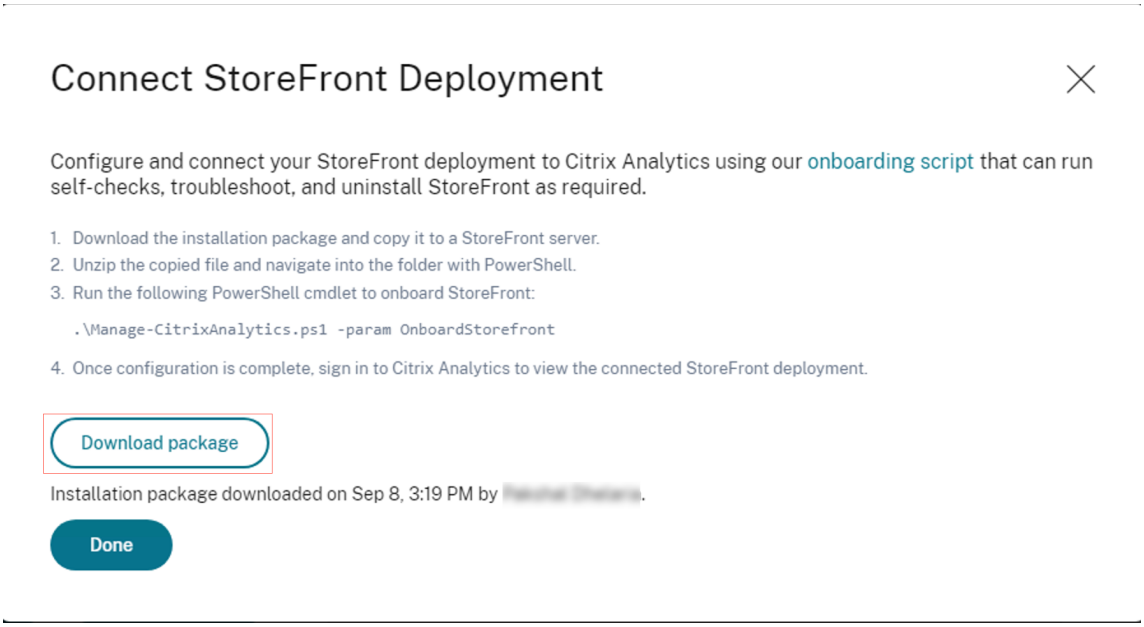


2. Navigieren Sie zu **Einstellungen > Datenquellen > Leistung**. Klicken Sie auf der Sitekarte **Apps and Desktops** —**Monitoring** auf die vertikalen Ellipsen (), und wählen Sie dann **StoreFront-Bereitstellung verbinden** aus.



Der StoreFront-Onboarding-Assistent oder das Popup **Connect StoreFront Deployment** wird angezeigt.

3. Klicken Sie auf **Paket herunterladen**.



> **Hinweis**
>
> Die Datei enthält sensible Informationen. Bewahren Sie die Datei an einem sicheren Speicherort auf.

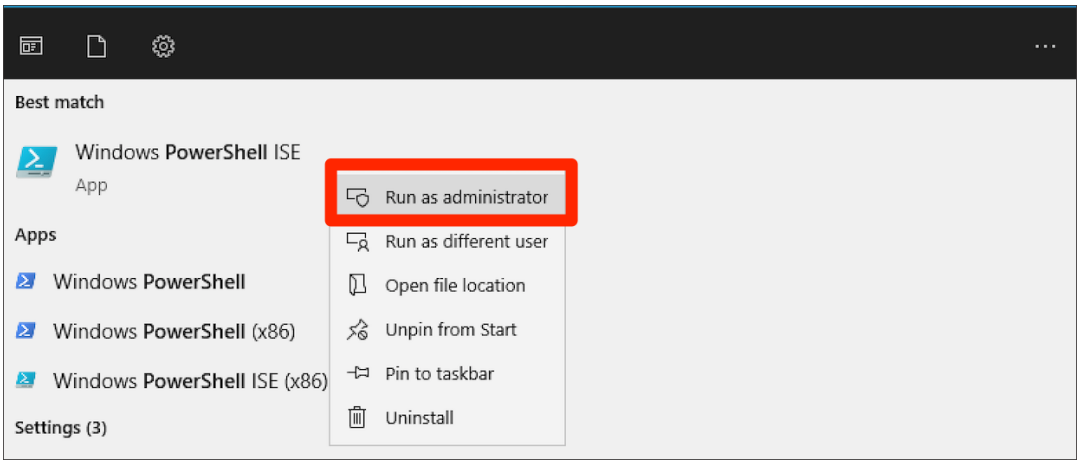
4. Konfigurieren der StoreFront-Bereitstellung:

   a) Kopieren Sie das Installationspaket auf den StoreFront-Server.

   b) Entpacken Sie die kopierte Datei und navigieren Sie in den Ordner in PowerShell.

   c) Sie müssen den folgenden Befehl als Administrator ausführen, um StoreFront zu integrieren:

.\Manage-CitrixAnalytics.ps1 –param OnboardStorefront



Weitere Optionen oder Parameter finden Sie im Abschnitt PowerShell-Skript.

d) Öffnen Sie den StoreFront-Server und führen Sie das PowerShell-Skript aus.

e) Wenn die StoreFront-Site auch nach der Ausführung von OnboardStorefront nicht in der Benutzeroberfläche von Citrix Analytics Service angezeigt wird, führen Sie den Befehl iisreset aus.

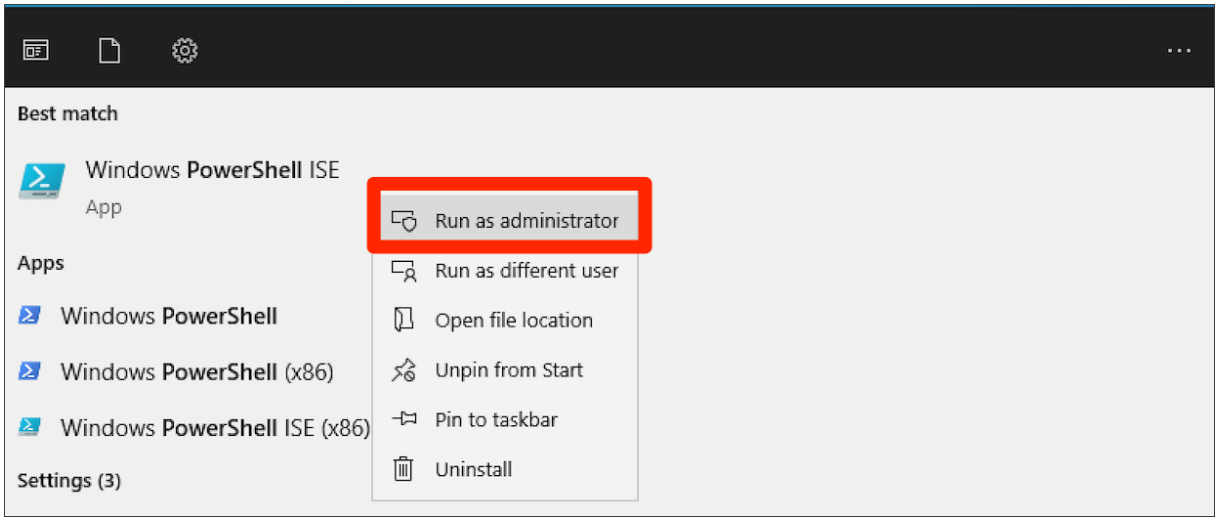
f) Melden Sie sich bei der Citrix Analytics Service GUI an und überprüfen Sie, ob die Cluster-ID mit der vom Skript in der Konsole angemeldeten übereinstimmt.

g) Sobald die Konfiguration abgeschlossen ist, melden Sie sich bei Citrix Analytics an, um die verbundene StoreFront-Bereitstellung anzuzeigen.

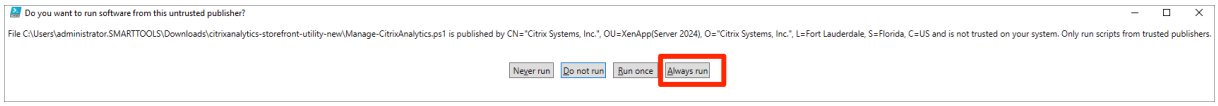
5. Nachdem die Konfiguration erfolgreich war, klicken Sie auf **Fertig**.
6. Klicken Sie auf **Datenverarbeitung einschalten**, damit Citrix Analytics die Daten verarbeiten kann.

PowerShell-Skript

Ein neues PowerShell-Skript wurde eingeführt, um den StoreFront-Onboarding-Prozess für Citrix Analytics Service zu vereinfachen. Dieses PowerShell-Skript automatisiert die Prüfung der Voraussetzungen, die Installation und Konfiguration von StoreFront. Das PowerShell-Skript muss im Administratormodus ausgeführt werden.



Kunden können dieses PowerShell-Skript auf StoreFront ausführen, um das Onboarding und Deboarding durchzuführen, Selbstprüfungen durchzuführen, Fehler zu beheben und zu überprüfen, ob das Onboarding in die Citrix Analytics Service-GUI erfolgreich ist. Wenn ein Kunde das Skript zum ersten Mal ausführt, erscheint eine Sicherheitswarnung zur Bestätigung für den Herausgeber. Wählen Sie die Option Immer ausführen, wenn der Herausgeber vertrauenswürdig ist.



Das PowerShell-Skript ist auf der **Connect StoreFront-Bereitstellungsseite** in einer ZIP-Datei zusammen mit der Datei StoreFrontConfiguration.json, einigen CCAuth- und DLL-Dateien verfügbar. Die PowerShell-Skriptprotokolle werden in der Datei cas-logs im Ordner **Downloads** gespeichert.

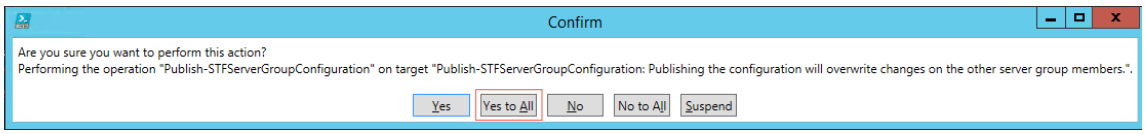
Das PowerShell-Skript unterstützt die folgenden Parameter:

- **SelfCheck**: Der Parameter **SelfCheck** wird verwendet, um zu überprüfen, ob die Voraussetzungen für das StoreFront-Onboarding erfüllt sind. Er überprüft die StoreFront-Installation, die erforderliche Version, die ausgehende Verbindung, die Netzwerkkonnektivität des cURL Analytics-Servers, die Internetverbindung, die Servergruppenkonfiguration und alle vorhandenen Citrix Analytics Service-Konfigurationen. Verwenden Sie den folgenden Befehl, um den **Selfcheck** auszuführen:

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

- **OnboardStorefront**: Der Parameter **OnboardStorefront** führt schnell eine Selbstprüfung durch, um zu überprüfen, ob das Setup für die Citrix Analytics Service-Konfiguration bereit ist. Wenn das Setup fertig ist, importiert es die Citrix Analytics Service-Konfiguration und veröffentlicht die Änderungen auf anderen Servern in der Servergruppe. Für eine Servergruppe wird der Befehl PublishConfiguration automatisch vom Skript aus ausgeführt, um die StoreFront-Konfiguration auf allen Servern innerhalb dieser StoreFront zu veröffentlichen. Sie

können ein Pop-up sehen, um die Aktion `PublishConfiguration` zu bestätigen. Wählen Sie die Schaltfläche **Ja für alle**.



Sobald die Konfigurationsveröffentlichung erfolgreich abgeschlossen wurde, ruft das Skript die Citrix Analytics Service API auf, um zu überprüfen, ob StoreFront in die Citrix Analytics Service-GUI integriert ist. Um diese API aufzurufen, ist ein privater Schlüssel für die Authentifizierung erforderlich. Um diesen privaten Schlüssel zu generieren, benötigen Sie die CCAuth- und DLL-Dateien sowie die Anmeldeinformationen, die in Ihrer heruntergeladenen JSON-Datei verfügbar sind.

> **Hinweis:**
>
> Sobald der StoreFront-Onboarding-Prozess abgeschlossen ist, kann es zwei bis fünf Minuten dauern, bis StoreFront in der Citrix Analytics Service-GUI angezeigt wird. Wenn die StoreFront-Site nicht in der Benutzeroberfläche von Citrix Analytics Service angezeigt wird, müssen Sie einen IISRESET ausführen, um die Internetinformationsdienste zurückzusetzen.

Verwenden Sie den folgenden Befehl, um **OnboardStoreFront** auszuführen:

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

- **IsOnboarded**: Der Parameter **IsOnboarded** wird verwendet, um zu überprüfen, ob StoreFront in die Citrix Analytics Service-GUI integriert ist. Das Skript wartet eine Minute, bevor es beendet wird. Es kann jedoch bis zu fünf Minuten dauern, bis StoreFront nach erfolgreichem Onboarding in der GUI angezeigt wird. Sie müssen diesen Befehl ausführen, um ihn zu überprüfen. Dieser Befehl hat auch die Abhängigkeit von CCAuth und DLL-Dateien. Verwenden Sie den folgenden Befehl, um **IsOnboarded** auszuführen:

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

- **Troubleshoot**: Wenn die StoreFront-Site nach einer Wartezeit von fünf Minuten nicht in der Benutzeroberfläche von Citrix Analytics Service angezeigt wird, müssen Sie einen IISRESET ausführen, um die Internetinformationsdienste zurückzusetzen. Wenn die StoreFront-Site immer noch nicht in der GUI angezeigt wird, verwenden Sie den Parameter **Troubleshoot**. Es hilft Ihnen bei der Behebung von Verbindungsproblemen und beim Sammeln von Protokollen. Verwenden Sie den folgenden Befehl, um **Troubleshoot** auszuführen:

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

  Der Parameter zur Fehlerbehebung ist für die folgenden zwei Anwendungsfälle nützlich:

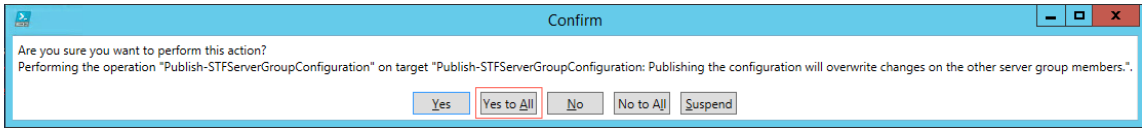
- **Anwendungsfall 1**: Im Rahmen der Selbstprüfung wird eine Firewallregel erstellt, wenn curlAnalytics fehlgeschlagen ist. Diese Firewallregel öffnet einen 443-Port und überprüft dessen Konnektivität mit Analytics. Wenn nicht, bedeutet das, dass der Analytics-Server nicht erreichbar ist und das Skript von hier aus beendet wird. Führen Sie das Skript erneut aus, sobald die Konnektivität zum Citrix Analytics Service wiederhergestellt ist.
- **Anwendungsfall 2**: Wenn die cURL einwandfrei funktioniert hat und die StoreFront-Site dennoch nicht in der GUI wiedergegeben wird, muss der Administrator die ZIP-Datei des DebugView-Tools von Download DebugView herunterladen, entpacken und im Ordner **Downloads** ablegen. Das PowerShell-Skript deinstalliert zuerst den Citrix Analytics Service, wenn er bereits konfiguriert ist. Es ermöglicht die ausführliche Protokollierung. Anschließend wird das DebugView-Tool gestartet und der Citrix Analytics Service neu installiert. Schließlich stoppt es DebugView und deaktiviert die ausführliche Protokollierung.

Die Debugansichtsprotokolle können erfasst und mit dem Citrix Support geteilt werden. Der Citrix Administrator debuggt weiter und versucht, das Problem herauszufinden und zu beheben. Die Protokolle werden generiert und als Protokolldatei im DebugView-Ordner gespeichert.

Sie müssen die folgenden drei Protokolldateien für den Citrix Administrator freigeben:

- Die DebugView-Protokolldatei (Downloads\ DebugView\ log)
- Die StoreFront-Protokolldatei (C:\Program Files\ Citrix\ Receiver StoreFront\ Admin\ trace)
- Die CAS-Protokolldatei. Diese Protokolle werden als Teil der Ausführung des Skripts generiert und im Ordner **Downloads > cas-logs** gespeichert.

Für eine Servergruppe wird der Befehl `PublishConfiguration` automatisch ausgeführt, wenn das Skript versucht, das Onboarding von StoreFront auszuführen oder aufzuheben. Der Befehl PublishConfiguration hilft dabei, die StoreFront-Konfiguration auf allen Servern in diesem StoreFront zu veröffentlichen. Sie können ein Pop-up sehen, um diese Aktion zu bestätigen. Wählen Sie die Schaltfläche **Ja für alle**.



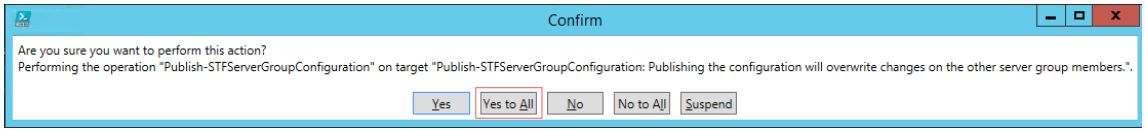
- **DeboardStoreFront**: Der Parameter DeboardStoreFront wird für das Deboarding des StoreFront-Servers vom Citrix Analytics Service verwendet. Verwenden Sie den folgenden Befehl, um DeboardStoreFront auszuführen:

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

  Das PowerShell-Skript entfernt zunächst alle Citrix Analytics Service-Konfigurationen aus StoreFront und stellt sicher, dass das Entfernen erfolgreich ist. Anschließend wird geprüft, ob die ServerGroup vorhanden ist, und veröffentlicht dann die Konfiguration, sodass die

entfernten Konfigurationen in allen StoreFront veröffentlicht werden. Schließlich ruft es DeleteSiteOnboarded auf. Wenn die Site nicht aus der Citrix Analytics Service-GUI gelöscht wird, müssen Sie die StoreFront-Site mit StoreFront Deployment und von der Workspace Application-Sitekarte unter der StoreFront-Bereitstellung manuell löschen.

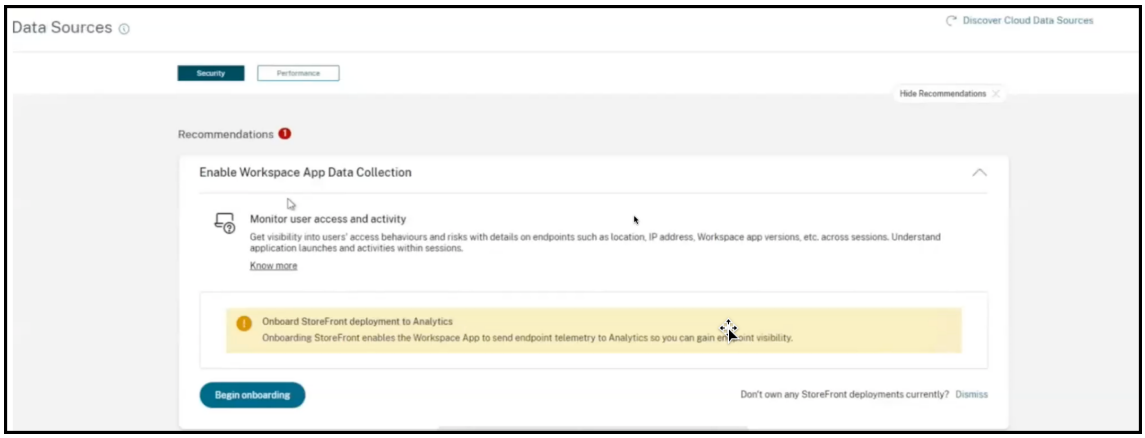
Für eine Servergruppe wird der Befehl PublishConfiguration automatisch vom Skript aus ausgeführt, um die StoreFront-Konfiguration auf allen Servern innerhalb dieser StoreFront zu veröffentlichen. Sie können ein Pop-up sehen, um diese Aktion zu bestätigen. Wählen Sie die Schaltfläche **Ja für alle**.



Verbindung im Bereich “Empfehlungen”herstellen

Im Bereich **Empfehlungen** auf der Seite **Datenquellen wird** der Benutzer darüber informiert, wie wichtig das Onboarding von Datenquellen ist. Es hilft dem Benutzer, die Datenquellen einfach zu integrieren, und bietet dem Benutzer auch die Möglichkeit, alle verfügbaren Datenquellen zu überprüfen und sicherzustellen, dass alle verfügbaren Datenquellen integriert wurden.

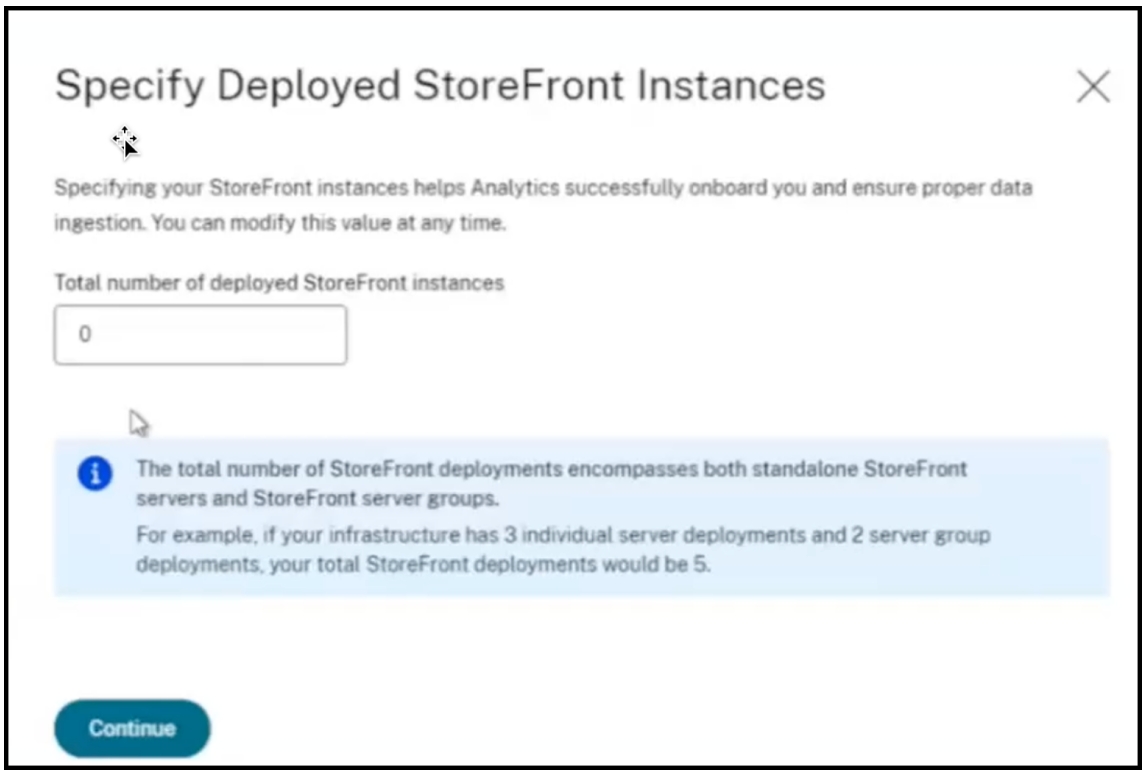
1. Wenn Sie das Security Analytics-Angebot verwenden, wählen Sie **Einstellungen > Datenquellen > Sicherheit**aus.
2. Wenn Sie das Performance Analytics-Angebot verwenden, navigieren Sie zu **Einstellungen > Datenquellen > Leistung**.
3. Lesen Sie auf der Seite **Datenquellen** die Informationen und Empfehlungen im Bereich **Empfehlungen**, um die Onboard-StoreFront-Bereitstellung zu integrieren.



> **Hinweis**
>
> Durch das Onboarding einer StoreFront-Datenquelle kann die Workspace-App Teleme-

> triedaten zur Sichtbarkeit von Endpunkten an Analytics senden.

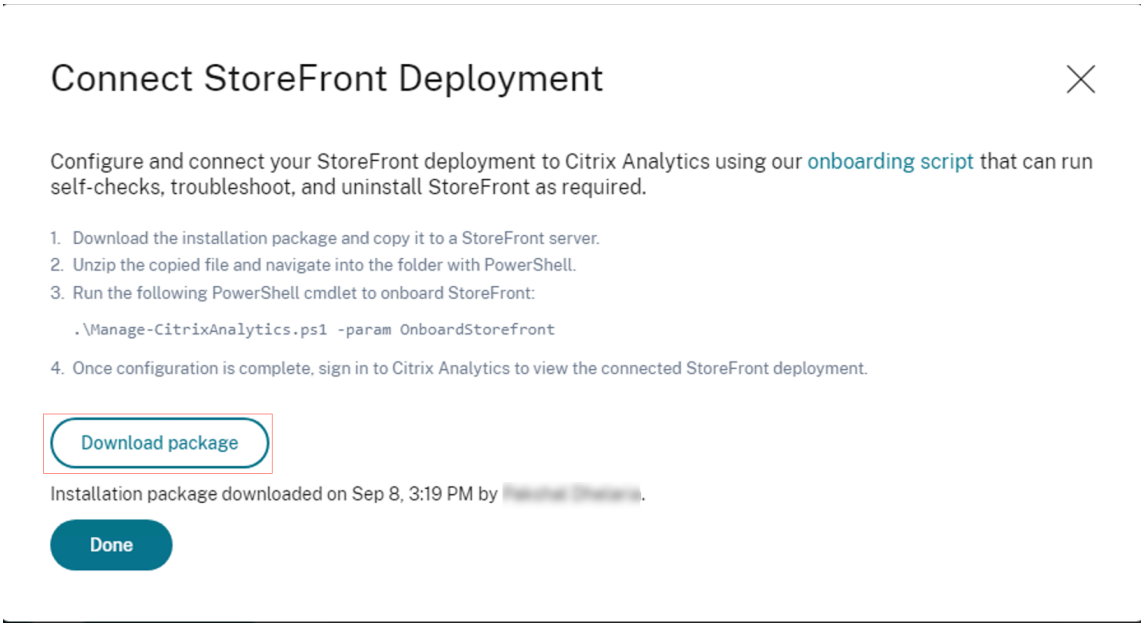
4. Klicken Sie auf **Begin onboarding**. Die Seite **Bereitgestellte StoreFront-Instanzen angeben** wird angezeigt.



5. Um sicherzustellen, dass Analytics die Datenquelle erfolgreich integriert, geben Sie die **Gesamtzahl der bereitgestellten StoreFront-Instanzen** an.

> **Hinweis:**
>
> Die **Gesamtzahl der bereitgestellten StoreFront-Instanzen** ist die Gesamtzahl der StoreFront-Gruppen und nicht die Anzahl der einzelnen StoreFront-Server.

6. Klicken Sie auf **Weiter**. Der StoreFront-Onboarding-Assistent oder das Popup **Connect StoreFront Deployment** wird angezeigt.
7. Klicken Sie auf der **Connect StoreFront-Bereitstellungsseite** auf Paket herunterladen, um das Installationspaket herunterzuladen.



> **Hinweise**
>
> Die Datei enthält sensible Informationen. Bewahren Sie die Datei an einem sicheren Speicherort auf.
>
> Sie können ein Paket herunterladen und es nur für das Onboarding einer StoreFront-Gruppe verwenden. Wenn Sie mehrere StoreFront-Gruppen haben, müssen Sie das Paket für jede StoreFront-Gruppe separat herunterladen. Nachdem das Onboarding einer StoreFront-Gruppe mit einem Paket abgeschlossen ist, laden Sie das Paket erneut herunter und setzen Sie das Onboarding für die nächste StoreFront-Gruppe fort.
>
> Wenn das StoreFront-Onboarding aufgrund eines Problems innerhalb von zwei Tagen mit einem Paket nicht korrekt abgeschlossen wird, müssen Sie nach zwei Tagen ein neues Paket herunterladen. Die ist nötig, weil der Schlüssel im Paket abläuft, wenn das Onboarding nicht innerhalb von zwei Tagen erfolgreich abgeschlossen wird.

8. Konfigurieren der StoreFront-Bereitstellung:

   a) Kopieren Sie das Installationspaket auf den StoreFront-Server.

   b) Entpacken Sie die kopierte Datei und navigieren Sie in den Ordner in PowerShell.

   c) Führen Sie den folgenden Befehl aus, um StoreFront zu integrieren:

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

   d) Öffnen Sie den StoreFront-Server und führen Sie das PowerShell-Skript aus.

   e) Wenn die StoreFront-Site nicht in der Benutzeroberfläche von Citrix Analytics Service angezeigt wird, führen Sie den folgenden Befehl aus:


```
Execute iisreset
```

f) Protokollieren und überprüfen Sie die Cluster-ID, die im PowerShell-Skript verfügbar ist.

g) Sobald die Konfiguration abgeschlossen ist, melden Sie sich bei Citrix Analytics an, um die verbundene StoreFront-Bereitstellung anzuzeigen.

9. Nachdem die Konfiguration erfolgreich war, klicken Sie auf **Fertig**.

Wenn Sie das Onboarding über den Bereich "**Empfehlungen**"**durchführen**, ruft das System die Anzahl der StoreFront-Bereitstellungen ab, die Sie in den Citrix Analytics Service integriert haben. Der Bereich **Empfehlungen** wird angezeigt, und Sie können die integrierten StoreFront-Bereitstellungen überprüfen. Sie können die Nachricht im Bereich **Empfehlungen** überprüfen und auf **Als abgeschlossen markieren**klicken.

> **Hinweis**
>
> Der Bereich **Empfehlungen** und die Meldungen werden erst ausgeblendet, wenn alle deklarierten StoreFront-Bereitstellungen integriert sind.

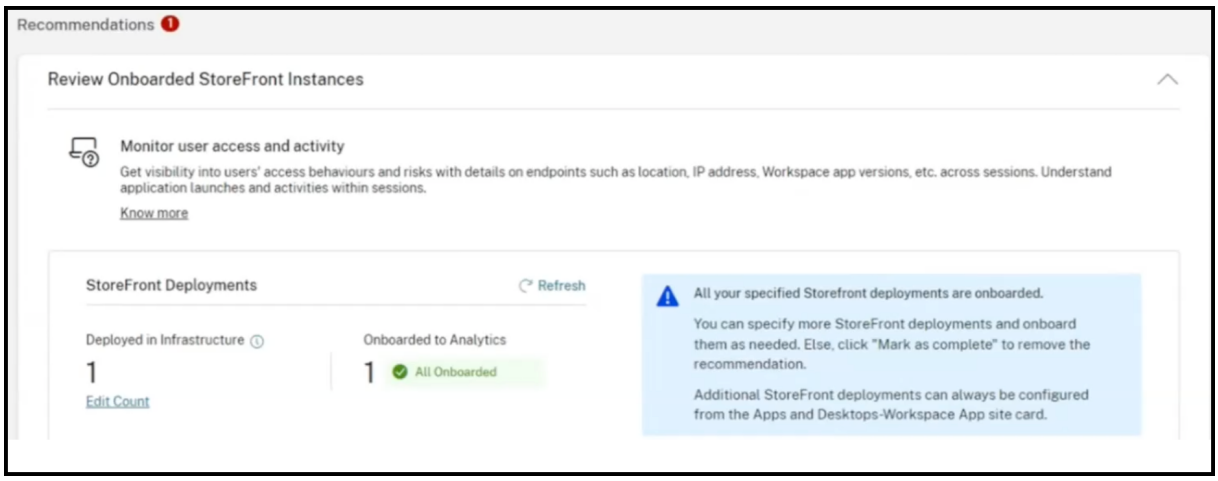
1. Klicken Sie auf **Datenverarbeitung einschalten**, damit Citrix Analytics die Daten verarbeiten kann.

Bereich "Empfehlungen"überprüfen

Im Bereich **Empfehlungen** können Sie die Anzahl der deklarierten StoreFront-Bereitstellungen mit der Anzahl der integrierten StoreFront-Bereitstellungen vergleichen.

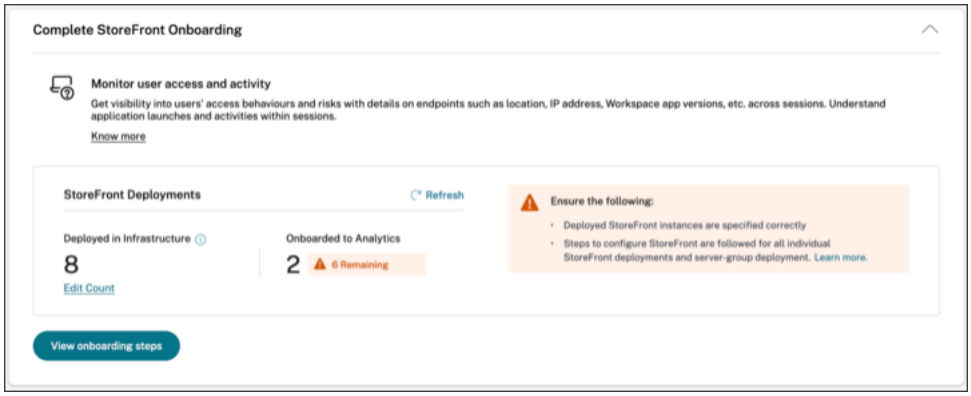
Wenn die Anzahl der deklarierten StoreFront-Bereitstellungen der Anzahl der integrierten StoreFront-Bereitstellungen entspricht, wird die Meldung All Onboarded angezeigt, die darauf hinweist, dass **alle** StoreFront-Bereitstellungen integriert sind. Sie können die Nachricht im Bereich **Empfehlungen** überprüfen und auf **Als abgeschlossen markieren**klicken.

> **Hinweis**
>
> Wenn Sie weitere StoreFront-Bereitstellungen integrieren möchten, klicken Sie auf **Onboarding-Schritte anzeigen**. Daraufhin wird erneut der StoreFront-Onboarding-Assistent oder das Popup **Connect StoreFront-Deployment** angezeigt.



Wenn die Anzahl der deklarierten StoreFront-Bereitstellungen geringer ist als die Anzahl der integrierten StoreFront-Bereitstellungen, klicken Sie auf **Anzahl bearbeiten**. Daraufhin wird die Seite **Bereitgestellte Storefront-Instanzen angeben** angezeigt. Sie können dann die **Gesamtzahl der bereitgestellten StoreFront-Instanzen** eingeben und auf **Weiter** klicken. Der StoreFront-Onboarding-Assistent oder das Popup **StoreFront-Bereitstellung verbinden** werden erneut angezeigt. Folgen Sie den Schritten, um weitere StoreFront-Bereitstellungen zu integrieren.

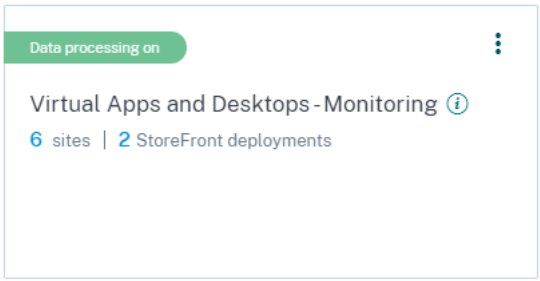
> **Hinweis:**
>
> Die **Gesamtzahl der bereitgestellten StoreFront-Instanzen** ist die Gesamtzahl der StoreFront-Gruppen und nicht die Anzahl der einzelnen StoreFront-Server.



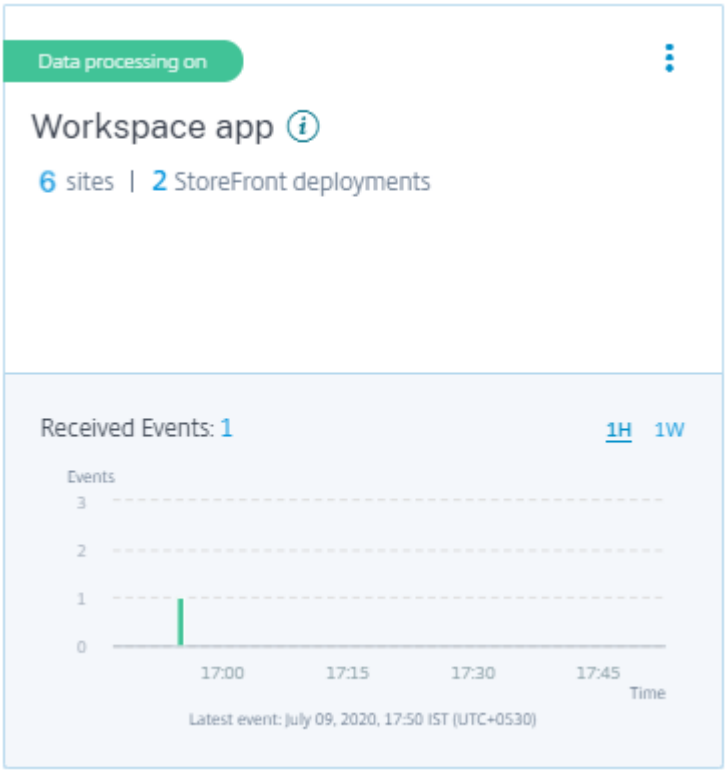
Anzeigen verbundener StoreFront-Bereitstellungen

Die StoreFront-Bereitstellungen werden nur dann auf der Sitekarte angezeigt, wenn die Konfiguration erfolgreich war. Die Sitekarte zeigt an, wie viele StoreFront-Bereitstellungen Verbindungen mit Citrix Analytics hergestellt haben.

- Wenn Sie das Performance Analytics-Angebot verwenden, werden auf der Sitekarte **Apps and Desktops** —**Monitoring** folgende Informationen angezeigt:

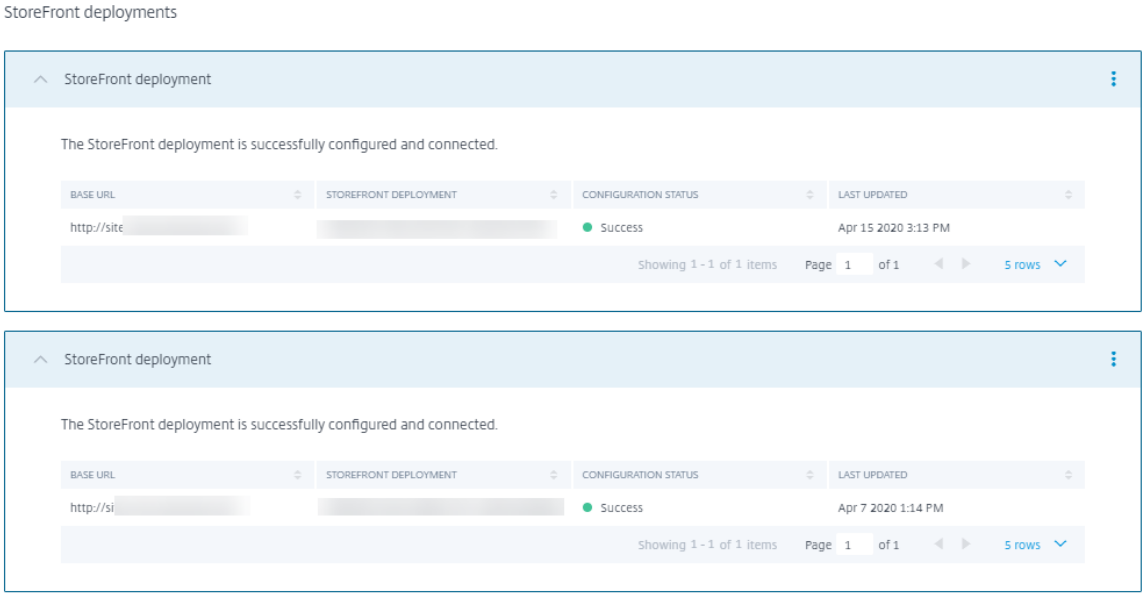


- Wenn Sie das Security Analytics-Angebot verwenden, werden auf der Sitekarte der **Workspace-App** die folgenden Informationen angezeigt:



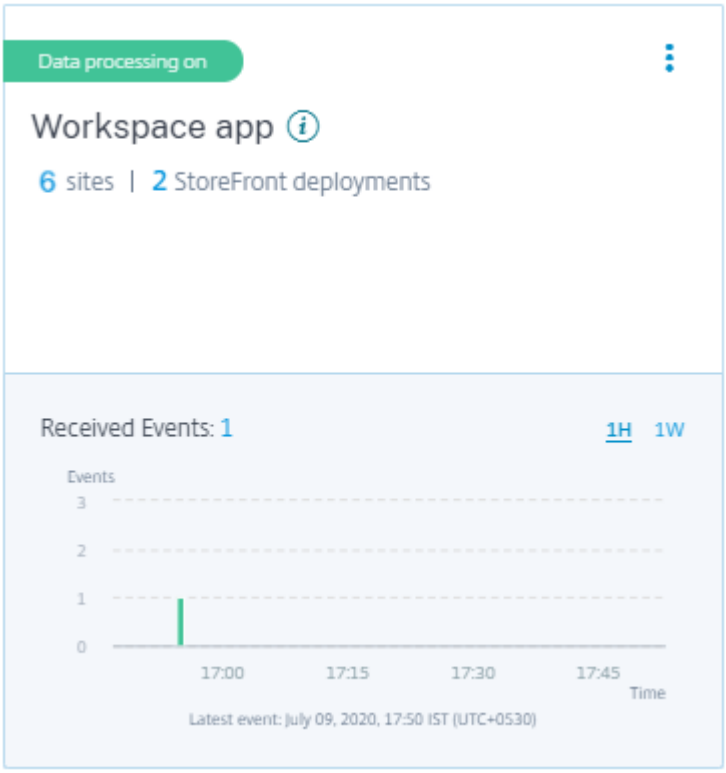
Klicken Sie auf die Anzahl der StoreFront-Bereitstellungen auf der Sitekarte, um die Servergruppen anzuzeigen.

Jede StoreFront-Bereitstellung wird durch eine Basis-URL und eine ServerGroupID dargestellt.



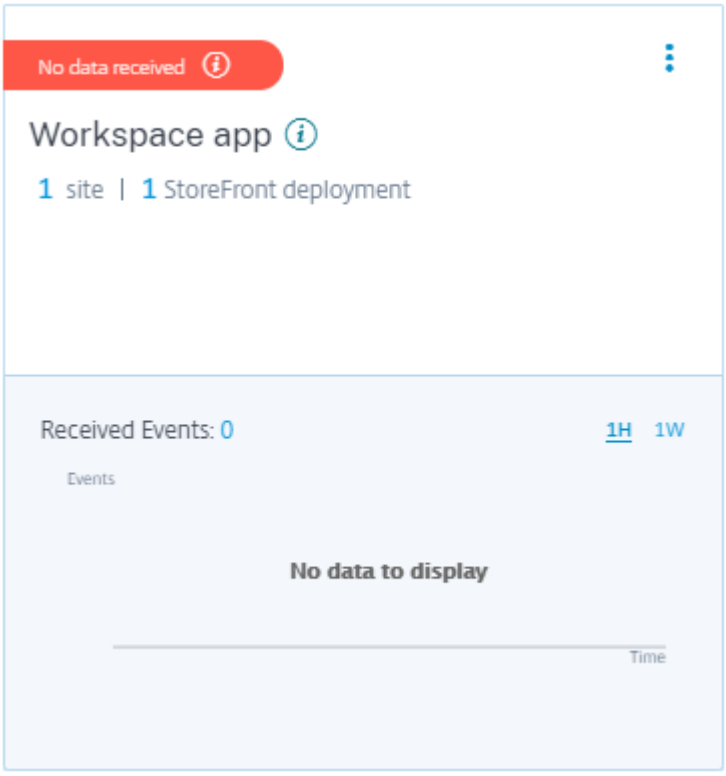
Wenn Sie das Security Analytics-Angebot verwenden, zeigt die Site-Karte auch die folgenden Informationen zu den empfangenen Ereignissen an:

- Die Ereignisse, die in der letzten Stunde von den StoreFront-Bereitstellungen empfangen wurden. Dies ist die Standardzeitauswahl. Sie können auch 1 Woche (1 W) auswählen und die Daten anzeigen. Klicken Sie auf die Anzahl der eingegangenen Ereignisse, um die Ereignisse auf der Self-Service-Suchseite anzuzeigen.



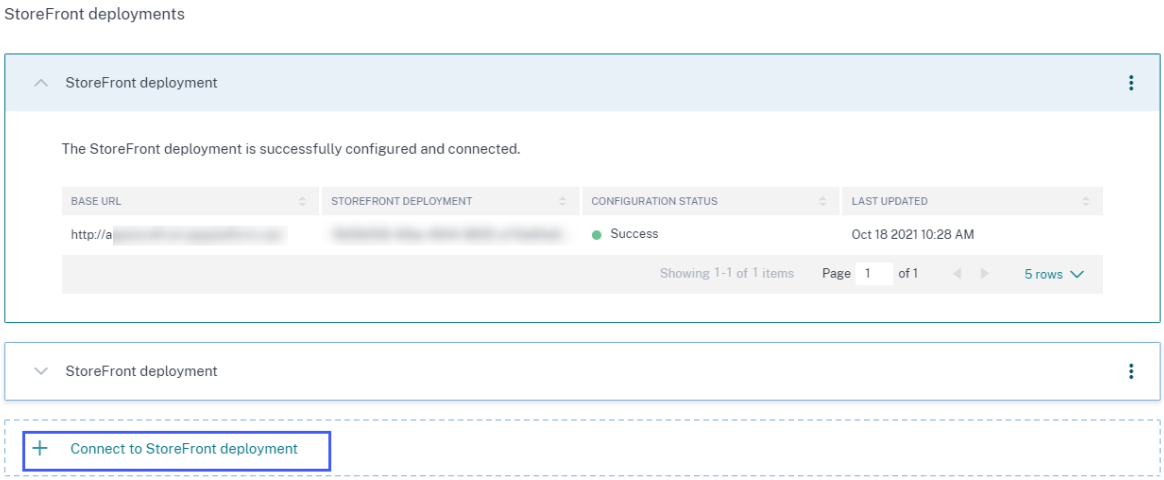
- Nachdem Sie die Datenverarbeitung aktiviert haben, wird auf der Sitekarte möglicherweise der Status **No data received** angezeigt. Dieser Status wird aus zwei Gründen angezeigt:

  1. Wenn Sie die Datenverarbeitung zum ersten Mal aktiviert haben, dauert es eine gewisse Zeit, bis die Ereignisse den Ereignis-Hub in Citrix Analytics erreichen. Wenn Citrix Analytics die Ereignisse empfängt, ändert sich der Status in **Data processing on**. Wenn sich der Status nach einiger Zeit nicht ändert, aktualisieren Sie die Seite **Datenquellen**.
  2. Citrix Analytics hat in der letzten Stunde keine Ereignisse von der Datenquelle empfangen.



StoreFront-Bereitstellungen hinzufügen oder entfernen

Um eine StoreFront-Bereitstellung hinzuzufügen, klicken Sie im Abschnitt **StoreFront-Bereitstellungen auf Mit**StoreFront-Bereitstellungen**verbinden** . Laden Sie die Konfigurationsdatei herunter und folgen Sie den Schritten zum Konfigurieren einer StoreFront-Bereitstellung.



So stoppen Sie die Ereignisübertragung von einer konfigurierten StoreFront-Bereitstellung und entfernen sie aus Citrix Analytics:

1. Wechseln Sie zur StoreFront-Bereitstellung, die Sie aus Citrix Analytics entfernen möchten. Führen Sie den folgenden Befehl aus, um die Konfigurationseinstellungen von Ihrem StoreFront-Server zu entfernen:

```
Remove-STFCasConfiguration
```

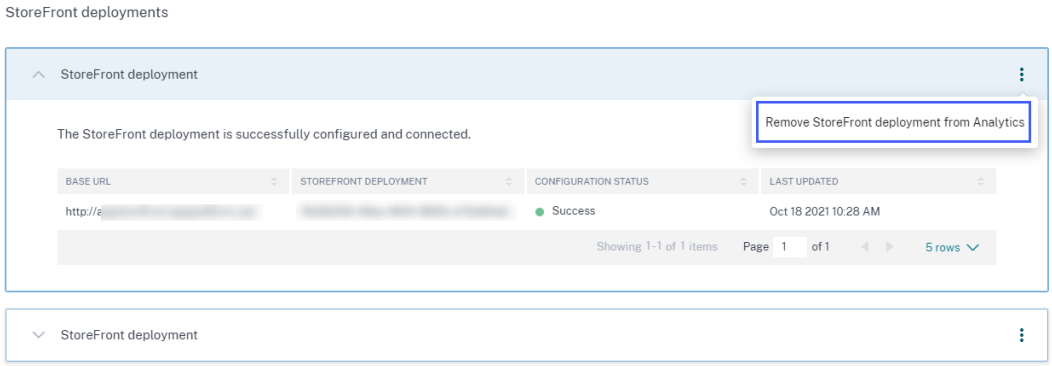
2. Wenn Sie eine Multiserverbereitstellung verwenden, führen Sie den folgenden Befehl aus, um die Änderungen zu übertragen und die Konfigurationseinstellungen von allen Servern in der StoreFront-Servergruppe zu entfernen:

```
Publish-STFServerGroupConfiguration
```

3. Führen Sie den folgenden Befehl aus, um zu überprüfen, ob die Konfigurationseinstellungen erfolgreich entfernt wurden. Der Befehl gibt nichts zurück, wenn die Einstellungen erfolgreich entfernt wurden.

```
Get-STFCasConfiguration
```

4. Melden Sie sich wieder bei Citrix Analytics an und wählen Sie im Abschnitt **StoreFront-Bereitstellungen die StoreFront-Bereitstellung** aus. Klicken Sie auf die vertikale Ellipse () und wählen Sie **StoreFront-Bereitstellungen aus Analytics entfernen**aus.



> **Hinweis**
>
> Führen Sie die angegebenen Befehle in der StoreFront-Bereitstellung aus, bevor Sie sie aus Citrix Analytics entfernen. Wenn Sie die Befehle nicht ausführen, erhält Citrix Analytics die Ereignisse weiterhin und die StoreFront-Bereitstellung wird beim nächsten Ereignispooling-Zyklus erneut hinzugefügt.

Konfigurieren einer StoreFront-Bereitstellung auf einem Webserver, der HTTP-Proxy verwendet

Wenn ein StoreFront auf einem Webserver gehostet wird, der einen Webproxy verwendet, um eine Verbindung zum Internet herzustellen, muss der Store manuell für die Registrierung bei Citrix Analyt-

ics konfiguriert werden. Für diese Konfiguration müssen Sie der Datei web.config des Stores einen Abschnitt <system.net> hinzufügen. Sie müssen jeden Store in der StoreFront-Bereitstellung konfigurieren, der Ereignisse an Citrix Analytics sendet.

Es gibt zwei Methoden, mit denen Sie den Abschnitt <system.net> zur Datei web.config des Stores hinzufügen können:

- Stellen Sie die Store-Proxy-Konfiguration über PowerShell für einen oder mehrere Stores ein (empfohlene Methode).
- Fügen Sie manuell einen Abschnitt <system.net> zur Datei web.config des Stores hinzu.

Weitere Informationen zu diesen Methoden finden Sie im Artikel Konfigurieren von StoreFront für die Verwendung eines Webproxys zur Kontaktaufnahme mit Citrix Cloud und zur Registrierung bei Citrix Analytics in der StoreFront-Dokumentation.

Data Governance

December 12, 2023

Dieser Abschnitt enthält Informationen zur Erfassung, Speicherung und Aufbewahrung von Protokollen durch den Citrix Analytics Service. Alle großgeschriebenen Begriffe, die nicht im Abschnitt Definitionen definiert sind, haben die in der Citrix Endbenutzer-Dienstleistungsvereinbarungangegebene Bedeutung.

Citrix Analytics wurde entwickelt, um Kunden Einblick in Aktivitäten in ihrer Citrix Computerumgebung zu bieten. Citrix Analytics ermöglicht es Sicherheitsadministratoren, die Protokolle auszuwählen, die sie überwachen möchten, und basierend auf der protokollierten Aktivität gezielte Maßnahmen zu ergreifen. Diese Erkenntnisse helfen Sicherheitsadministratoren, den Zugriff auf ihre Computerumgebungen zu verwalten und Kundeninhalte in der Computerumgebung des Kunden zu schützen.

Datenresidenz

Citrix Analytics-Protokolle werden getrennt von den Datenquellen verwaltet und in mehreren Microsoft Azure Cloud-Umgebungen zusammengefasst, die sich in den USA, der Europäischen Union und dem asiatisch-pazifischen Süden befinden. Die Speicherung der Protokolle hängt von der Heimatregion ab, die von den Citrix Cloud-Administratoren beim Onboarding ihrer Organisationen in Citrix Cloud ausgewählt wurde. Wenn Sie beispielsweise beim Onboarding Ihres Unternehmens in Citrix Cloud die **europäische Region** auswählen, werden Citrix Analytics-Protokolle in Microsoft Azure-Umgebungen in der Europäischen Union gespeichert.

Weitere Informationen finden Sie unter Citrix Cloud Services Kundeninhalte und Protokollierung sowiegeografische Überlegungen.

Datensammlung

Citrix Cloud-Dienste sind dazu dienen, Protokolle an Citrix Analytics zu übertragen. Protokolle werden aus den folgenden Datenquellen gesammelt:

- Citrix ADC (on-premises) zusammen mit einem Abonnement für Citrix Application Delivery Management
- Citrix Endpoint Management
- NetScaler Gateway (on-premises)
- Citrix Identitätsanbieter
- Citrix Secure Browser
- Citrix Secure Private Access
- Citrix Virtual Apps and Desktops
- Citrix DaaS (früher Citrix Virtual Apps and Desktops Service)
- Microsoft Active Directory
- Microsoft Graph Security

Datenübertragung

Citrix Cloud-Protokolle werden sicher an Citrix Analytics übertragen. Wenn der Administrator der Kundenumgebung Citrix Analytics explizit aktiviert, werden diese Protokolle analysiert und in einer Kundendatenbank gespeichert. Dasselbe gilt für Citrix Virtual Apps and Desktops
Datenquellen mit konfiguriertem Citrix Workspace.

Für Citrix ADC-Datenquellen wird die Protokollübertragung nur initiiert, wenn der Administrator Citrix Analytics explizit für die bestimmte Datenquelle aktiviert.

Steuerung von Daten

An Citrix Analytics gesendete Protokolle können vom Administrator jederzeit ein- oder ausgeschaltet werden.

Wenn diese Option für on-premises Citrix ADC-Datenquellen deaktiviert ist, wird die Kommunikation zwischen der jeweiligen ADC-Datenquelle und Citrix Analytics gestoppt.

Wenn alle für andere Datenquellen deaktiviert sind, werden die Protokolle für die jeweilige Datenquelle nicht mehr analysiert und in Citrix Analytics gespeichert.

Datenaufbewahrung

Citrix Analytics-Protokolle werden in identifizierbarer Form für maximal 13 Monate oder 396 Tage aufbewahrt. Alle Protokolle und zugehörige Analysedaten wie Benutzerrisikoprofile, Details zur Bewertung des Nutzerrisikos, Details zu Benutzerrisikoereignissen, Benutzerbeobachtungsliste, Benutzeraktionen und Benutzerprofil werden für diesen Zeitraum aufbewahrt.

Wenn Sie beispielsweise Analytics für eine Datenquelle am 1. Januar 2021 aktiviert haben, werden die am 1. Januar 2021 gesammelten Daten standardmäßig bis zum 31. Januar 2022 in Citrix Analytics aufbewahrt. In ähnlicher Weise werden die am 15. Januar 2021 gesammelten Daten bis zum 15. Februar 2022 usw. aufbewahrt.

Diese Daten werden für den Standarddatenaufbewahrungszeitraum gespeichert, auch wenn Sie die Datenverarbeitung für die Datenquelle deaktiviert oder die Datenquelle aus Citrix Analytics entfernt haben.

Citrix Analytics löscht alle Kundeninhalte 90 Tage nach Ablauf des Abonnements oder des Testzeitraums.

Datenexport

In diesem Abschnitt werden die aus Citrix Analytics for Security und Citrix Analytics for Performance exportierten Daten erläutert.

Citrix Analytics for Performance sammelt und analysiert Leistungsmetriken aus den Datenquellen.

Sie können die Daten von der Self-Service-Suchseite als CSV-Datei herunterladen.

Citrix Analytics for Security sammelt Benutzerereignisse aus verschiedenen Produkten (Datenquellen). Diese Ereignisse werden verarbeitet, um Einblick in das riskante und ungewöhnliche Verhalten der Benutzer zu erhalten. Sie können diese verarbeiteten Daten in Bezug auf Risikoeinblicke der Benutzer und Benutzerereignisse in Ihren Service System Information and Event Management (SIEM) exportieren.

Derzeit können die Daten auf zwei Arten aus Citrix Analytics for Security exportiert werden:

- Integrieren von Citrix Analytics for Security in Ihren SIEM-Dienst
- Herunterladen der Daten von der Self-Service-Suchseite als CSV-Datei.

Wenn Sie Citrix Analytics for Security in Ihren SIEM-Dienst integrieren, werden die Daten entweder mithilfe des nach Norden gebundenen Kafka-Themas oder eines LogStash-basierten Datenconnectors an Ihren SIEM-Dienst gesendet.

Derzeit können Sie in die folgenden SIEM-Dienste integrieren:

- Splunk (durch Herstellen einer Verbindung über das Citrix Analytics-Add-on)
- Jeder SIEM-Dienst, der Kafka-Thema oder LogStash-basierte Datenconnectors wie Elasticsearch und Microsoft Azure Sentinel unterstützt

Sie können die Daten auch mithilfe einer CSV-Datei in Ihren SIEM-Dienst exportieren. Auf der Self-Service-Suchseite können Sie die Daten (Benutzerereignisse) für eine Datenquelle anzeigen und diese Daten als CSV-Datei herunterladen. Weitere Informationen zur CSV-Datei finden Sie unter Self-Service-Suche.

> **Wichtig**
>
> Nachdem die Daten in Ihren SIEM-Dienst exportiert wurden, ist Citrix nicht für die Sicherheit, Speicherung, Verwaltung und Verwendung der exportierten Daten in Ihrer SIEM-Umgebung verantwortlich.

Sie können die Datenübertragung von Citrix Analytics for Security zu Ihrem SIEM-Dienst ein- oder ausschalten.

Informationen zu den verarbeiteten Daten und der SIEM-Integration finden Sie unter Integration von Sicherheitsinformationen und Ereignismanagement (SIEM) und Citrix Analytics-Datenformat für SIEM.

Anlage zur Sicherheit von Citrix Diensten

Detaillierte Informationen zu den auf Citrix Analytics angewendeten Sicherheitskontrollen, einschließlich Zugriff und Authentifizierung, Sicherheitsprogramm-Management, Business Continuity und Incident-Management, sind in der Citrix Services Security Exhibit enthalten.

Definitionen

Kundeninhalte sind alle Daten, die zur Speicherung in ein Kundenkonto hochgeladen werden, oder Daten in einer Kundenumgebung, auf die Citrix Zugriff zur Erbringung von Diensten erhält.

Protokoll bezeichnet eine Aufzeichnung von Ereignissen mit Bezug zu den Services, darunter Messdaten zu Leistung, Stabilität, Nutzung, Sicherheit und Unterstützung.

Dienste bezeichnet die oben beschriebenen Citrix Cloud Services für die Zwecke von Citrix Analytics.

Datenerfassungsvertrag

Durch das Hochladen Ihrer Daten in Citrix Analytics und die Nutzung der Funktionen von Citrix Analytics erklären Sie sich damit einverstanden, dass Citrix technische, Benutzer- oder verwandte Informationen über Ihre Citrix Produkte und Dienstleistungen sammelt, speichert, überträgt, pflegt, verarbeitet und verwendet.

Citrix behandelt die empfangenen Informationen immer gemäß der Citrix Datenschutzrichtlinie.

Anhang: gesammelte Protokolle

- Citrix Analytics für Sicherheitsprotokolle
- Citrix Analytics for Performance Leistungsprotokolle

Citrix Analytics für Sicherheitsprotokolle

Allgemeine Protokolle

Im Allgemeinen enthalten Citrix Analytics-Protokolle die folgenden Header-Identifikationsdatenpunkte:

- Header-Schlüssel
- Geräte-Identifikation
- Identifizierung
- IP-Adresse
- Organisation
- Produkt
- Produktversion
- System-Zeit
- Mandanten-ID
- Typ
- Benutzer: E-Mail, ID, SAM-Kontoname, Domäne, UPN
- Version

Citrix Endpoint Management-Dienstprotokolle

Die Citrix Endpoint Management-Dienstprotokolle enthalten die folgenden Datenpunkte:

- Konformität
- Unternehmen im Besitz
- Geräte-ID
- Geräte-Modell
- Gerätetyp
- Geo Breitengrad
- Geo Längengrad
- Hostname
- IMEI
- IP-Adresse
- Jail Broken
- Letzte Aktivität
- Verwaltungsmodus
- Betriebssystem
- Betriebssystemversion
- Informationen zur Plattform
- Grund
- Seriennummer
- Betreut

Citrix Secure Private Access-Protokolle

- AAA-Benutzername
- Name der Auth Policy-Aktion
- Authentifizierungssitzung ID
- URL anfragen
- Richtlinienname der URL Kategorie
- VPN Sitzungskennung

- VServer-IP
- AAA-Benutzer-E-Mail-ID
- Aktueller Vorlagencode
- App FQDN
- App-Name
- App Name Vserver LS
- Anwendungsflags
- Authentifizierungstyp
- Phase der Authentifizierung
- Authentifizierungsstatuscode
- Backend-Server-DST-IPv4-Adresse
- IPv4-Adresse des Backend-Servers
- IPv6-Adresse des Backend-Servers
- Kategorie Domainname
- Kategorie Domainquelle
- Client-IP
- 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
- Anwendungs-ID des NetScaler Gateway Service
- Name der NetScaler Gateway Service-App
- App-Typ des NetScaler Gateway Service
- NetScaler-Partitions-ID
- Observation Domain ID
- Observation Point ID
- Origin Res Status
- Origin Rsp Len
- Protocol Identifier
- Rate Limit Identifier Name
- Datensatztyp
- Aktionstyp des Responders
- Response-Medientyp
- Srv Flow Flags Rx
- Srv Flow Flags Tx
- Srvr Fast Retx Count
- Server TCP-Jitter
- Srvr TCP Packets Retransmitted
- Srvr TCP Rto Count
- Srvr TCP Null-Fensteranzahl
- 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
- Abonnenten-Kennung
- 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 End 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 Cnt
- Trans Clt Tot Tx Oct Cnt
- 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 Cnt
- Trans Svr Tot Tx Oct Cnt
- Transaktion-ID
- URL-Kategorie
- URL Category Group

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

Citrix Virtual Apps and Desktops und Citrix DaaS-Protokolle

Die Citrix Virtual Apps and Desktops und Citrix DaaS-Protokolle enthalten die folgenden Datenpunkte:

- App-Name
- Browser
- Kunden-ID
- Details: Formatgröße, Formattyp, Initiator, Ergebnis
- Geräte-ID
- Gerätetyp
- Feedback
- Feedback-ID
- Dateiname
- Datei-Pfad
- Größe der Datei
- Ist wie
- Jail Broken
- Job-Details: Dateiname, Format, Größe
- Ort: Geschätzt, Breitengrad, Längengrad

  > **Hinweis**
  >
  > Die Standortinformationen werden auf Stadt- und Landesebene bereitgestellt und stellen keine genaue Geolocation dar.

- Lange CMD-Leitung

- Modul-Dateipfad
- Vorgang
- Betriebssystem
- Zusätzliche Informationen zur Plattform
- Name des Druckers
- Frage
- Fragen-ID
- SaaS-App-Name
- Sitzungsdomäne
- Name des Sitzungsservers
- Benutzername der Sitzung
- Sitzungs-GUID
- Zeitstempel
- Time Zone: Bias, DST, Name
- Total Copies Printed
- Total Pages Printed
- Typ
- URL
- Benutzeragent

Citrix ADC-Protokolle

Die Citrix ADC-Protokolle enthalten die folgenden Datenpunkte:

- Container
- Dateien
- Format
- Typ

Citrix DaaS Standard für Azure-Protokolle

Die Citrix DaaS Standard for Azure-Protokolle enthalten die folgenden Datenpunkte:

- App-Name
- Browser
- Details: Formatgröße, Formattyp, Initiator, Ergebnis
- Geräte-ID
- Gerätetyp
- Dateiname
- Datei-Pfad
- Größe der Datei
- Jail Broken
- Job-Details: Dateiname, Format, Größe
- Ort: Geschätzt, Breitengrad, Längengrad

  > **Hinweis**
  >
  > Die Standortinformationen werden auf Stadt- und Landesebene bereitgestellt und stellen keine genaue Geolocation dar.

- Lange CMD-Leitung
- Modul-Dateipfad
- Vorgang
- Betriebssystem
- Zusätzliche Informationen zur Plattform
- Name des Druckers
- SaaS-App-Name
- Sitzungsdomäne
- Name des Sitzungsservers
- Benutzername der Sitzung
- Sitzungs-GUID
- Zeitstempel
- Time Zone: Bias, DST, Name

- Typ
- URL
- Benutzeragent

Citrix Identity Provider-Protokolle

- Benutzer-Login:
  - Authentication Domains: Name, Product, IdP Type, IdP Display Name
    - IdP Properties: App, Auth Type, Customer Id, Client Id, Directory, Issuer, Logo, Resources, TID
    - Verlängerungen:
      - 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

NetScaler Gateway Protokolle

- Transaktions-Ereignisse:

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

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

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

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

- Metrikereignisse:
  - 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

Secure Browser-Protokolle

- Anwendung veröffentlichen:
  - 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

  - Logs after the published application: Authentication, Browser, Change Id, Created, Customer Name, Destination, 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 URL, Whitelist Internal URL, Whitelist Redirect URL

- Anwendung löschen:
  - 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
  - Logs after the published application: Authentication, Browser, Change Id, Created, Customer Name, Destination, 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 URL, Whitelist Internal URL, Whitelist Redirect URL
- Anwendungs-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
  - Logs after the published application: Authentication, Browser, Change Id, Created, Customer Name, Destination, 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 URL, Whitelist Internal URL, Whitelist Redirect URL
- Anspruch erstellen:
  - 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
- Anspruchsupdate:

  - 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
- Sitzung verbinden:
  - 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
- Start der Sitzung:
  - 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

Microsoft Graph-Sicherheitsprotokoll

- Mandanten-Id
- Benutzer-ID
- Indikator-ID
- Indikator UUID
- Uhrzeit des Ereignisses
- Zeit erstellen
- Kategorie der Warnung

- Ort der Anmeldung
- Anmelde-IP
- Anmelde-Typ
- Typ des Benutzerkontos
- Informationen des Anbieters
- Anbieter-Anbieterinformationen
- Sicherheitsrisikostatus
- Sicherheitsrisikoschweregrad

Microsoft Active Directory Protokolle

- Mandanten-Id
- Zeit sammeln
- Typ
- Directory-Kontext
- Gruppen
- Identität
- Benutzertyp
- Kontoname
- Anzahl schlechter Kennwörter
- Ort
- Allgemeiner Name
- Firma
- Land
- Tage bis zum Ablauf des Kennworts
- Abteilung
- Beschreibung
- Anzeigename
- Ausgezeichneter Name
- E-Mail

- Fax-Nummer
- Vorname
- Gruppenkategorie
- Umfang der Gruppe
- Telefon zu Hause
- Initialen
- IP-Telefon
- Ist das Konto aktiviert
- Ist das Konto gesperrt
- Ist Sicherheitsgruppe
- Nachname
- Managerin
- Mitglied von
- Handy
- Pager
- Kennwort läuft nie ab
- Name des physischen Zustellbüros
- Postfach
- PLZ
- Primäre Gruppen-ID
- Status
- Adresse
- Titel
- Benutzerkontensteuerung
- Liste der Benutzergruppen
- Benutzerprinzipalname
- Telefon für die Arbeit

Citrix Analytics for Performance Leistungsprotokolle

- 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
- Host
- 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

Technische Sicherheit

April 12, 2024

Der in Citrix Cloud gehostete Analytics-Dienst sammelt Daten über Citrix Portfolioprodukte und Produkte von Drittanbietern. Diese Produkte werden als Datenquellen bezeichnet. Citrix Analytics unterstützt sowohl Cloud- als auch on-premises Datenquellen. Die Informationen in diesem Dokument gelten für Citrix Analytics und seine Datenquellen.

Datenfluss

Citrix Analytics erkennt automatisch die Citrix Cloud-Datenquellen, die für die Kunden abonniert sind. Die on-premises Datenquellen erfordern jedoch eine zusätzliche Konfiguration für die Integration in Citrix Analytics. Sie müssen beispielsweise Ihre Citrix Virtual Apps and Desktops-Sites zu Citrix Workspace hinzufügen, bevor Citrix Analytics die Sites erkennen kann. In ähnlicher Weise müssen Sie bei on-premises Citrix Gateway einen Citrix ADM Agent konfigurieren. Weitere Informationen zum Aktivieren von Citrix Analytics für die Datenquellen finden Sie unter Aktivieren von Analytics auf Citrix Datenquellen.

Sie können einige Produkte von Drittanbietern wie Microsoft Graph Security und Microsoft Active Directory in Citrix Analytics integrieren. Weitere Informationen finden Sie in den folgenden Artikeln:

- Analytics auf Microsoft Graph-Sicherheit aktivieren
- Integrieren von Analytics mit Microsoft Active Directory

Citrix Analytics kann auch Risikoinformationen an eine kundeneigene Splunk-Umgebung senden. Diese Integration erfordert die Bereitstellung und Konfiguration des **Citrix Analytics Add-ons für Spunk** in der Splunk-Umgebung. Weitere Informationen finden Sie unter Splunk-Integration.

Ohne Zustimmung des Kunden verarbeitet Citrix Analytics keine Ereignisse, die von den Datenquellen empfangen wurden. Um die Ereignisse aus den Datenquellen zu verarbeiten, muss der Analytics-Administrator die Datenverarbeitung aktivieren. Weitere Informationen zur Datenerfassung, -speicherung und -aufbewahrung durch Analytics finden Sie unter Daten-Governance.

Netzwerkanforderungen

- **Anforderungen für Citrix Cloud-Dienste**: Um die Citrix Cloud-Dienste verwenden zu können, müssen Sie in der Lage sein, über den HTTPS-Port 443 eine Verbindung zu den erforderlichen Citrix Adressen herzustellen. Weitere Informationen finden Sie unter Anforderungen an die Internetkonnektivität.
- **Citrix Analytics-Anforderungen**: Überprüfen Sie die Systemanforderungen, bevor Sie Citrix Analytics verwenden. Zusätzlich zu den Citrix Cloud-Anforderungen müssen die folgenden Endpunktadressen über den HTTPS-Port 443 zugänglich sein, um den Citrix Analytics Service verwenden zu können.

Endpunkt	Region der Vereinigten Staaten	Region der Europäischen Union	Asien-Pazifik Süd
Admin-Benutzeroberfläche	https://analytics.cloud.com/	https://analytics-eu.cloud.com/	https://analytics-aps.cloud.com/
Admin-Benutzeroberfläche (CDN)	https://cas-api-cdn-ep.azureedge.net/	https://cas-api-cdn-ep-eu.azureedge.net/	https://cas-api-cdn-ep-aps.azureedge.net/
API-Dienste	https://api.analytics.cloud.com/	https://api.analytics-eu.cloud.com/	https://api.analytics-aps.cloud.com/
API-Dienste (Leistungsanalyse)	https://api-a.was.cloud.com/	https://api-eu-a.was.cloud.com/	https://api-aps-a.was.cloud.com/

Endpunkt	Region der Vereinigten Staaten	Region der Europäischen Union	Asien-Pazifik Süd
	https://api-b.was.cloud.com/	https://api-eu-b.was.cloud.com/	https://api-ap-s-b.was.cloud.com/
Öffentliche IP abrufen	https://locus.analytics.cloud.com/	https://locus.analytics.cloud.com/	https://locus.analytics.cloud.com/
Event Hub (Gilt nicht für Citrix ADM-Agent)	https://citrixanalyticseh-alias.servicebus.windows.net/ https://citrixanalyticseh2-alias.servicebus.windows.net/	https://citrixanalyticsehe-alias.servicebus.windows.net/	https://citrixanalyticsehaps-alias.servicebus.windows.net/
Ereignis-Hub (für Citrix ADM-Agent)	https://cas-eh-ns-alias.servicebus.windows.net/ undhttps://cas-eh-ns2-alias.servicebus.windows.net/	https://cas-eh-ns-eu-alias.servicebus.windows.net/	https://cas-eh-ns-aps-alias.servicebus.windows.net/
Bulk-Upload	https://casstoragebulk.blob.core.windows.net/	https://casstorebulkeu.blob.core.windows.net/	https://casstorebulkaps.blob.core.windows.net/

> **Hinweis**
>
> Citrix Analytics hat die Unterstützung für TLS 1.0 und TLS 1.1 für die meisten der vorhergehenden Endpunkte eingestellt.

- **Installation von Citrix Cloud Connector**: Bei einigen Datenquellen wie Citrix Endpoint Management, Citrix Virtual Apps and Desktops und Microsoft Active Directory müssen Sie einen Cit-

rix Cloud Connector an Ihrem Ressourcenstandort installieren. Der Citrix Cloud Connector ist ein Kommunikationskanal zwischen Citrix Cloud und Ihren Ressourcenstandorten. Nach der Installation des Citrix Cloud Connector müssen Sie die Webproxy-Einstellungen konfigurieren. Weitere Informationen finden Sie unter Konfiguration von Cloud Connector-Proxy und Firewall.

- **Citrix Analytics-Endpoints für die SIEM-Integration**: Um Citrix Analytics in Ihre Sicherheitsinformationen und Ereignisverwaltung (SIEM)zu integrieren, stellen Sie sicher, dass die folgenden Endpunkte in der Zulassungsliste in Ihrem Netzwerk enthalten sind:

Endpunkt	Region der Vereinigten Staaten	Region der Europäischen Union	Asien-Pazifik Süd

Kafka Broker	`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`

Identitäts- und Zugriffsverwaltung

- Um auf Citrix Analytics zuzugreifen, müssen Sie Ihr Citrix Cloud-Konto verwenden. Standardmäßig verwendet Citrix Cloud den Citrix Identitätsanbieter zur Verwaltung der Identitätsinformationen für alle Benutzer in einem Citrix Cloud-Konto. Sie können auch andere Identitätsanbieter verwenden, wie in Identitäts- und Zugriffsmanagement beschrieben.
- Citrix Analytics unterstützt delegierte Administratorberechtigungen. Sie können einem Benutzer eine schreibgeschützte Administratorberechtigung zuweisen, um Analytics in Ihrem Unternehmen zu verwalten. Weitere Informationen finden Sie unter Verwalten von Administratorrollen.

Datenresidenz

Citrix Cloud verwaltet die Steuerungsebene für Citrix Analytics. Von den Datenquellen empfangene Daten werden in mehreren Microsoft Azure-Umgebungen gespeichert. Diese Umgebungen befinden sich in den Vereinigten Staaten, der Europäischen Union und dem asiatisch-pazifischen Süden. Der

Speicherort hängt von der Heimatregion ab, die von den Citrix Cloud-Administratoren beim Onboarding ihrer Organisationen in Citrix Cloud ausgewählt wurde. Weitere Informationen finden Sie in den folgenden Artikeln:

- Geografische Überlegungen
- Data Governance

Datenschutz

Citrix Analytics empfängt Daten aus den abonnierten Citrix Cloud-Datenquellen, on-premises Datenquellen und den Produkten von Drittanbietern. Die empfangenen Daten werden nur verarbeitet, wenn der Kunde über eine Citrix Cloud-Berechtigung verfügt und der Analytics-Administrator die Datenverarbeitung für jede der abonnierten Datenquellen explizit aktiviert hat.

Citrix Analytics schützt die Daten der Kunden mithilfe der folgenden Sicherheitsmaßnahmen:

- Citrix Cloud-Authentifizierung für Analytics-Benutzer. Weitere Informationen finden Sie unter Identitäts- und Zugriffsmanagement.
- Mandantenbasierte Datenzugriffskontrollen, die vom Datendienst und der Datenzugriffsebene durchgesetzt werden.
- Starke Datenisolierung pro Kunde oder Mandant in allen Datenspeichern im Data Lake und Data Warehouse.
- TLS-verschlüsselte Datenübertragung zwischen den verschiedenen Mikrodiensten und Datenspeichern, anwendbar für die öffentlichen Endpunkte (APTS/Ein-/Ausgänge) der Plattform und innerhalb der Plattform.
- Hohe Standards bei TLS-Endpunkten. TLS 1.0 und TLS 1.1 sind deaktiviert.
- Verschlüsselter Datenspeicher mit Verschlüsselungsschlüsseln und Geheimnissen, die in entsprechenden Schlüsseltresoren gespeichert werden.
- Starke Zugriffssteuerung für Benutzerverwaltung für Servicebetrieb und Support bei gleichzeitigem Schutz der Kundenprotokolle.
- Schwachstellensuche, Angriffserkennung, Anti-Malware, Rootkit-Scans werden zusammen mit Azure Security Center verwendet.

Wie bei allen Citrix Cloud-Diensten unterliegt die Datenerfassung ausschließlich dem End User Service Agreement (EUSA). Weitere Informationen finden Sie in den folgenden Vereinbarungen:

- Nutzer-Vereinbarungen
- Datenschutzrichtlinien von Citrix

- Citrix Datenverarbeitungsvertrag
- Anlage zur Sicherheit von Citrix Diensten
- Citrix Cloud Services: Kundeninhalte und Protokollhandhabung
- Citrix Datenschutz- und Compliance-Informationen

Verantwortung für die Sicherheit

Verantwortungsbereich von Citrix

Citrix ist für die Sicherung der gesamten Infrastruktur und Daten verantwortlich, die sich in den von Citrix verwalteten Cloud-Umgebungen befinden, die Citrix Analytics hosten. Citrix ist dafür verantwortlich, regelmäßige Softwareupdates und Patches in der Cloud-Umgebung anzuwenden, um Sicherheitslücken zu beheben.

Verantwortung des Kunden

Citrix Kunden sind für die Sicherung ihrer Datenquellen, Richtliniendurchsetzungspunkte und Sicherheitsinformationen- und Ereignisverwaltungssysteme (SIEM) verantwortlich, die in Citrix Analytics integriert sind. Dazu gehören:

- Lokale Datenquellen, die Kunden gehören und von ihnen verwaltet werden:
  - **Lokale Datenquellen**: Citrix Gateway, Citrix Virtual Apps and Desktops, Microsoft Active Directory
  - **SIEM**: Splunk und alle anderen Produkte von Drittanbietern, die die Kafka-Broker zum Lesen von Ereignissen aus Citrix Analytics verwenden.
- Vom Kunden bereitgestellte Administratoranmeldeinformationen für die Verwaltung von Citrix Cloud-Diensten, einschließlich Citrix Analytics.
- Kundeneigene Administratorkonten, die E-Mails oder Benachrichtigungen von Citrix Cloud-Diensten erhalten.
- Vom Kunden bereitgestellte Administratoranmeldeinformationen für die Bereitstellung und Integration der Agents wie Citrix ADM Agents. Der Zugriff auf diese Agenten muss eingeschränkt werden, da sie die Schlüssel lokal speichern, um mit Citrix Analytics zu kommunizieren.
- Von Citrix Analytics generierte Anmeldeinformationen zum Konfigurieren des **Citrix Analytics Add-ons für Splunk**.

- Endbenutzergeräte, die unter Windows, Mac, Android und iOS ausgeführt werden, um eine Verbindung zu Citrix Cloud oder Citrix Workspace herzustellen und in Datenquellen integriert zu werden.

Weitere Informationen zu Sicherheitsbestimmungen finden Sie in den folgenden Dokumenten:

- Leitfaden zur sicheren Bereitstellung für die Citrix Cloud-Plattform
- Dokumentation zu Citrix Workspace
- Technische Sicherheitsübersicht für Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service)
- Sicherheitsüberlegungen für Citrix Virtual Apps and Desktops
- Sichern der StoreFront-Bereitstellung - Dokumentation
- Technische Sicherheit —Überblick für Citrix Endpoint Management
- Citrix Secure Private Access Service-Dokumentation
- Sicherer Bereitstellungshandbuch für Citrix ADC
- Citrix ADM -Systemanforderungen

Systemanforderungen

September 22, 2023

Bevor Sie Citrix Analytics verwenden, müssen Sie die Lizenzinformationen, Softwareanforderungen und Browseranforderungen überprüfen.

Citrix Analytics-Abonnements

Sie benötigen gültige Abonnements, um die folgenden Analytics-Produkte verwenden zu können:

- Citrix Analytics für Sicherheit
- Citrix Analytics für Leistung

Weitere Informationen finden Sie unter Citrix Cloud-Dienste.

Anforderungen an Datenquellen

Die Datenquellen sind die Produkte, die Ereignisse an Citrix Analytics senden. Je nach den Citrix Analytics-Angeboten, die Sie verwenden, variieren die Datenquellen. In den folgenden Artikeln finden Sie die Datenquellen, die von den einzelnen Angeboten unterstützt werden:

- Von Citrix Analytics for Security unterstützte Datenquellen
- Von Citrix Analytics for Performance unterstützte Datenquellen

Unterstützte Browser

Um auf Citrix Analytics zuzugreifen, muss Ihre Arbeitsstation über den folgenden unterstützten Webbrowser verfügen:

- Aktuelle Version von Google Chrome
- Aktuelle Version von Mozilla Firefox
- Aktuelle Version von Microsoft Edge
- Aktuelle Version von Apple Safari

Administratorrollen für Citrix Analytics verwalten

May 5, 2023

Standardmäßig hat ein Citrix Cloud-Administrator volle Zugriffsberechtigungen auf alle abonnierten Dienste in seinem Citrix Cloud-Konto. Mit den vollen Zugriffsberechtigungen kann der Administrator alle Funktionen und Funktionen eines abonnierten Dienstes nutzen.

Als Citrix Cloud-Administrator mit vollem Zugriff können Sie andere Administratoren in Ihr Citrix Cloud-Konto einladen, um die abonnierten Dienste Ihrer Organisation zu verwalten. Sie können dann ihre Zugriffsberechtigungen definieren und ihnen erlauben, bestimmte Funktionen in den abonnierten Diensten zu verwalten.

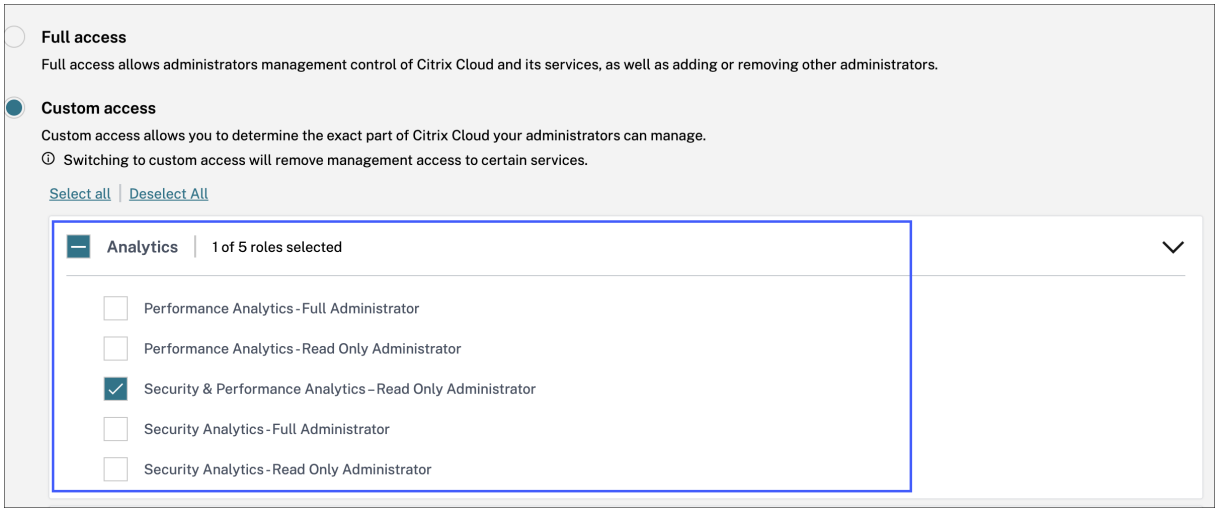
Neue Administratoren können auf zwei Arten hinzugefügt werden:

1. Individuell als Benutzer von Citrix Identity und Azure AD/Active Directory. Weitere Informationen finden Sie unter Verwalten von Citrix Cloud-Administratoren.
2. Verwenden von Gruppen in Azure Active Directory. Weitere Informationen finden Sie unter Administratorgruppen verwalten.

Administratoren können sich mit ihren Citrix Cloud-, Active Directory- oder Azure Active Directory-Konten bei Citrix Cloud anmelden und je nach Rolle auf bestimmte Funktionen zugreifen und Aufgaben ausführen.

Für Citrix Analytics können Sie Ihren Administratoren die folgenden benutzerdefinierten Rollen zuweisen:

Rolle	Berechtigung
Leistungsanalyse —Volladministrator	Weist den Citrix Cloud-Administratoren von Performance Analytics volle Zugriffsberechtigung zu.
Performance Analytics —Administrator mit Schreibschutz	Weist den Citrix Cloud-Administratoren von Performance Analytics schreibgeschützte Zugriffsberechtigungen zu.
Sicherheits- und Leistungsanalysen — Administrator mit Schreibschutz	Weist den Citrix Cloud-Administratoren von Security Analytics und Performance Analytics schreibgeschützte Zugriffsberechtigungen zu.
Sicherheitsanalysen —Volladministrator	Weist den Citrix Cloud-Administratoren von Security Analytics volle Zugriffsberechtigung zu.
Sicherheitsanalysen —Nur-Lese-Administrator	Weist den Citrix Cloud-Administratoren von Security Analytics schreibgeschützte Zugriffsberechtigungen zu.



Hinweise

- Wenn Sie mehrere Rollen für einen Administrator auswählen, wird die Rolle mit höherem Zugriff wirksam.

> - Wenn einem Benutzer direkt als Benutzer und über eine Azure Active Directory-Gruppe Zugriff gewährt wird, wird der dem Benutzer individuell gewährte Zugriff wirksam.
> - Azure Active Directory-Gruppen können nur als benutzerdefinierte Administratoren hinzugefügt werden. Die Administratorrolle mit vollem Zugriff ist für Gruppen nicht verfügbar.
> - Die Administratoren mit der Rolle "**Nur-Lese-Administrator**", die zuvor verfügbar waren, wurden in "**Sicherheit und Leistung —Nur-Lese-Administrator**"umbenannt.
> - Die Administratoren mit der Rolle "**Sicherheit und Performance Analytics —Nur-Lese-Administrator** "und "**Performance Analytics —Schreibgeschützter Administrator** "erhalten keine E-Mail-Benachrichtigungen von Citrix Analytics.

Weitere Informationen zu den angebotsspezifischen Rollen finden Sie in den folgenden Artikeln:

- Verwalten von Administratorrollen für Performance Analytics
- Administratorrollen für Security Analytics verwalten

Erste Schritte

April 12, 2024

In diesem Dokument wird beschrieben, wie Sie zum ersten Mal mit Citrix Analytics beginnen.

Schritt 1: Anmelden bei Citrix Cloud

Um Citrix Analytics verwenden zu können, benötigen Sie ein Citrix Cloud-Konto. Gehen Sie zu https://citrix.cloud.com und melden Sie sich mit Ihrem vorhandenen Citrix Cloud-Konto an.

Wenn Sie kein Citrix Cloud-Konto haben, müssen Sie zuerst ein Citrix Cloud-Konto erstellen oder einem vorhandenen Konto beitreten, das von einer anderen Person in Ihrer Organisation erstellt wurde. Ausführliche Prozesse und Anweisungen zur weiteren Vorgehensweise finden Sie unter Anmelden für Citrix Cloud.

Schritt 2: Zugriff auf Analytics

Sie können auf eine der folgenden Arten auf Analytics zugreifen:

- **Fordern Sie eine Testversion des Citrix Analytics-Angebots an**. Nachdem Sie sich bei Citrix Cloud angemeldet haben, klicken Sie im Abschnitt **Verfügbare Dienste** auf der **Analytics-Kachel** auf **Verwalten**, um die Analytics-Übersichtsseite anzuzeigen.

  Auf der Übersichtsseite werden die Analytics-Angebote —**Sicherheit** und **Leistung**—angezeigt.

  - Klicken Sie für Security Analytics und Performance Analytics auf **Testversion anfordern**, um die Testversion des Angebots zu verwenden. Sie erhalten eine E-Mail, wenn Ihre Anfrage genehmigt wurde und die Testversion verfügbar ist. Sie können die Testversion für einen Zeitraum von maximal 60 Tagen nutzen. Weitere Informationen zu Testversionen von Diensten finden Sie unter Citrix Cloud Service Trials.

  Auf der Citrix Cloud-Seite wechselt die **Analytics-Kachel** zum Abschnitt **Meine Dienste** .

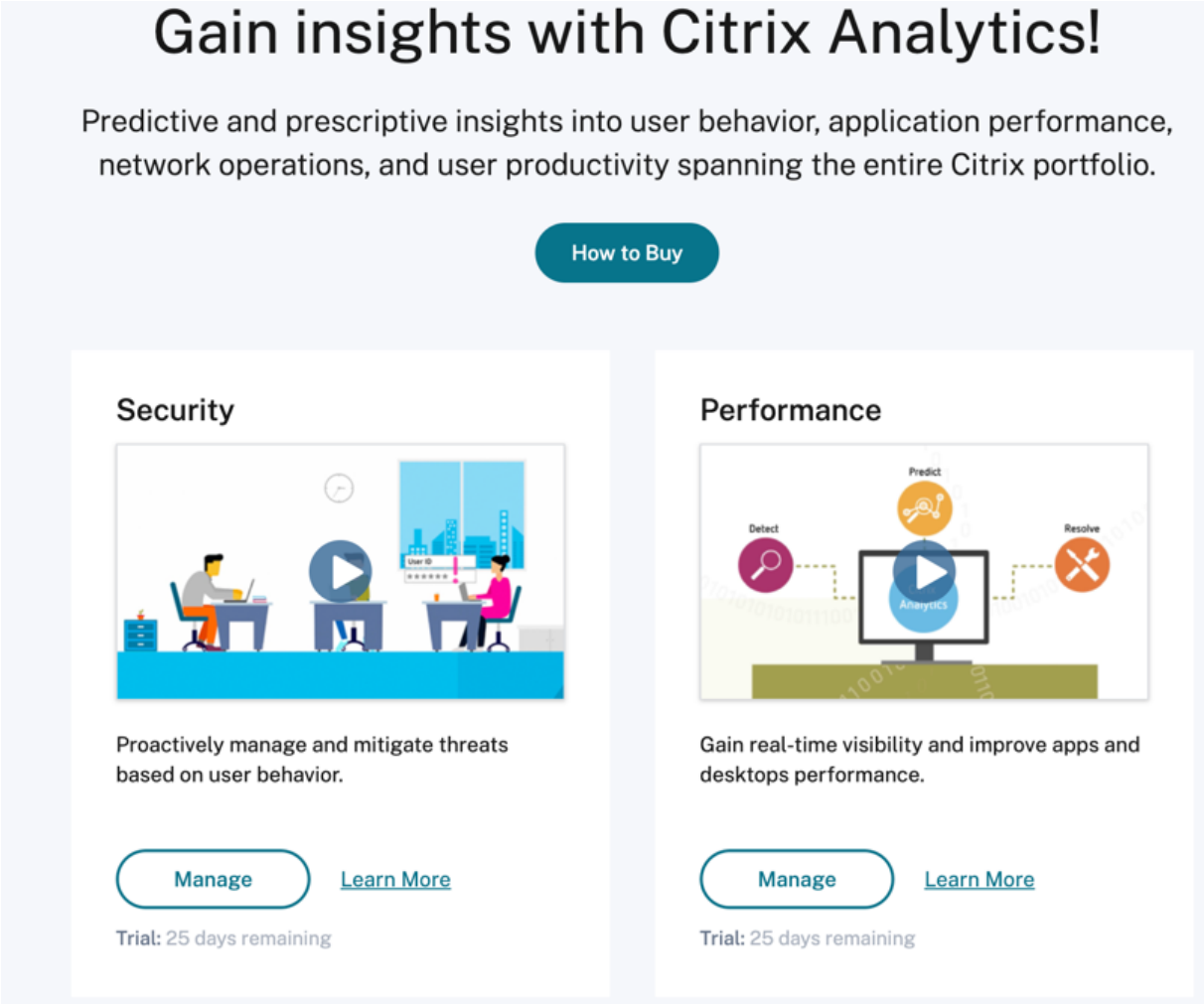
- **Abonnieren Sie Citrix Analytics**. Sie können die folgenden Citrix Analytics-Abonnements erwerben:

  - Citrix Analytics für Sicherheit
  - Citrix Analytics für Leistung
  - Citrix Analytics für Sicherheit und Leistung

  Citrix Analytics for Security und Citrix Analytics for Performance werden als Zusatzdienst mit den Citrix Workspace-Paketen Workspace Standard, Workspace Premium und Workspace Premium Plus angeboten. Weitere Informationen finden Sie unter Citrix Cloud-Dienste.

Schritt 3: Analytics verwalten

Wenn Sie für Security Analytics und Performance Analytics über die erforderlichen Abonnements verfügen oder für den Zugriff auf die Testversion autorisiert sind, ändert sich auf der Analytics-Übersichtsseite die Schaltfläche **Testversion anfordern** für das Angebot in **Verwalten**. Klicken Sie auf **Verwalten**, um das Benutzer-Dashboard für jedes Angebot anzuzeigen.



Analytics erkennt automatisch die Citrix Cloud-Dienste (Datenquellen), die Ihrem Citrix Cloud-Konto zugeordnet sind. Um Ihre erkannten Datenquellen anzuzeigen, klicken Sie auf **Einstellungen > Datenquellen** und dann auf die gewünschte Registerkarte —**Sicherheit** oder **Leistung**.

Weitere Informationen zu den einzelnen Analytics-Angeboten finden Sie unter

- Citrix Analytics für Sicherheit
- Citrix Analytics für Leistung

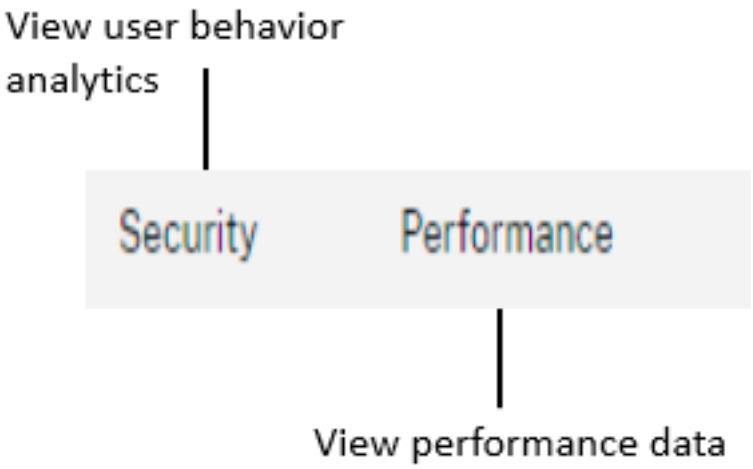
Überblick

May 4, 2022

Machen Sie sich mit den wichtigsten Steuerelementen auf der Analytics-Benutzeroberfläche vertraut.

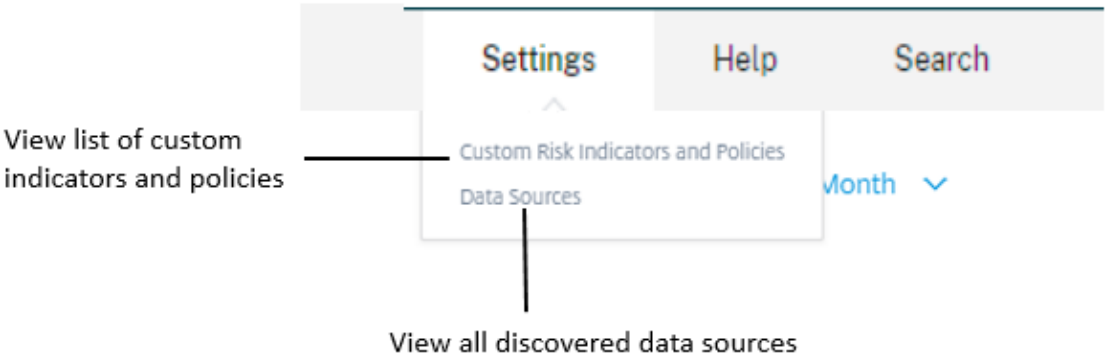
Oberste Leiste

Navigieren Sie in der oberen Leiste zu den verschiedenen Analytics-Angeboten.

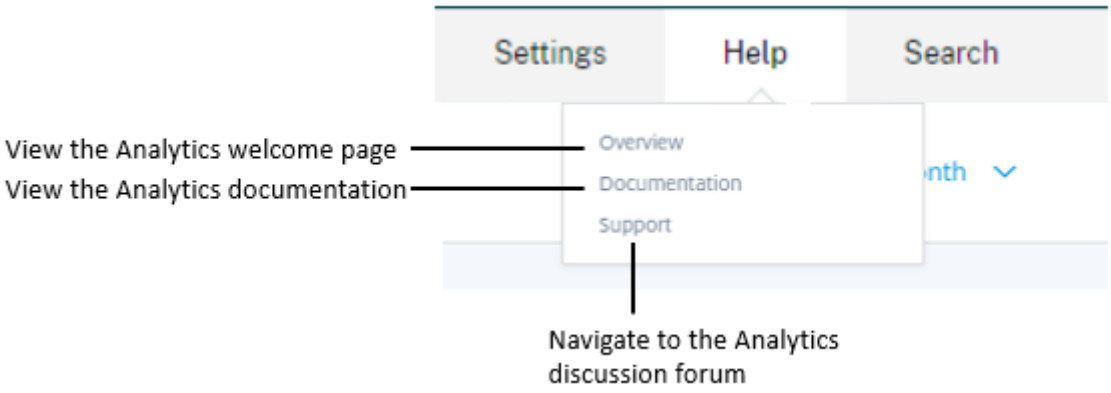


Menü “Einstellungen”

Navigieren Sie im Menü **Einstellungen** zur Seite Indikatoren und Richtlinien oder zur Seite Datenquellen .

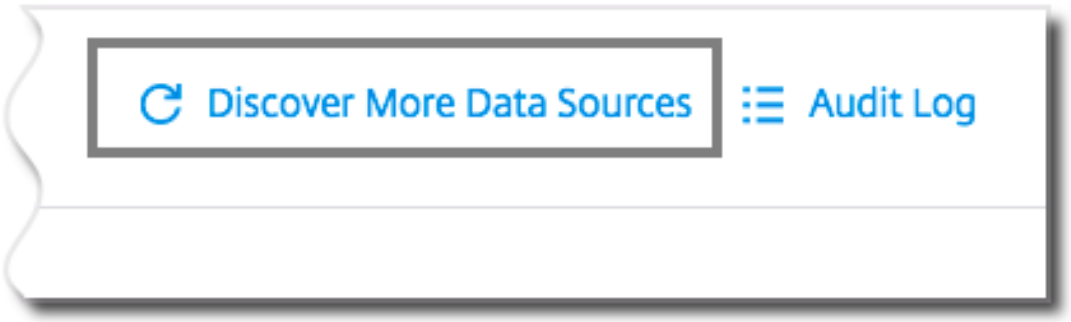


Menü “Hilfe”



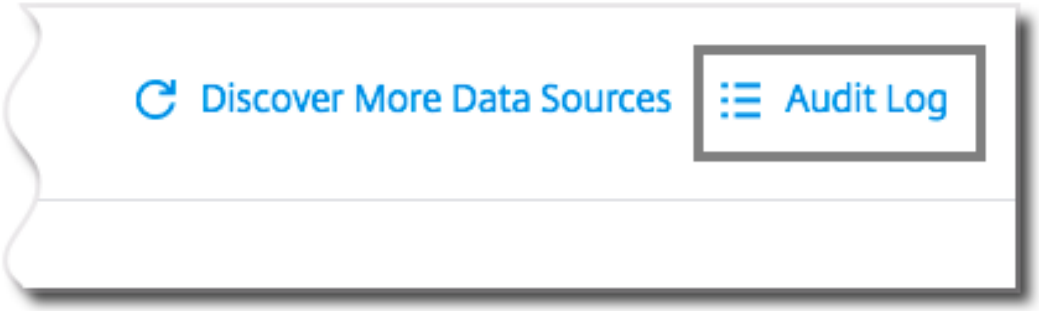
Entdecken Sie weitere Datenquellen

Entdecken Sie neu hinzugefügte Datenquellen oder zuvor gelöschte Datenquellen.



Protokoll der Prüfung

Navigieren Sie zur Seite Überwachungsprotokoll, auf der alle in Analytics generierten Ereignisse aufgeführt sind.



Self-Service-Suche

December 12, 2023

Was ist Self-Service-Suche?

Mit der Self-Service-Suchfunktion können Sie Benutzerereignisse suchen und filtern, die von Ihren Datenquellen empfangen wurden. Sie können die zugrunde liegenden Benutzerereignisse und ihre Attribute untersuchen. Diese Ereignisse helfen Ihnen, Datenprobleme zu identifizieren und zu beheben. Auf der Suchseite werden verschiedene Facetten (Dimensionen) und Metriken für eine Datenquelle angezeigt. Sie können Ihre Suchanfrage definieren und Filter anwenden, um die Ereignisse anzuzeigen, die Ihren definierten Kriterien entsprechen. Standardmäßig zeigt die Self-Service-Suchseite Benutzerereignisse für den letzten Tag an.

Derzeit ist die Self-Service-Suchfunktion für die folgenden Datenquellen verfügbar:

- Authentication
- Gateway
- Secure Browser
- Secure Private Access
- Apps und Desktops
- Leistungsfähige Benutzer, Maschinen und Sitzungen

Sie können auch eine Self-Service-Suche nach Ereignissen durchführen, die Ihren definierten Richtlinien entsprechen. Weitere Informationen finden Sie unter Self-Service-Suche nach Richtlinien.

So greifen Sie auf die Selbstbedienungssuche zu

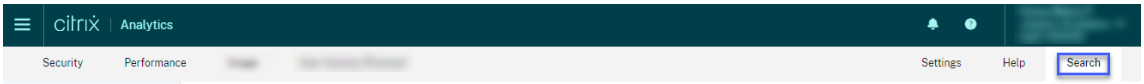
Mit den folgenden Optionen können Sie auf die Self-Service-Suche zugreifen:

- **Obere Leiste**: Klicken Sie in der oberen Leiste auf **Suchen**, um alle Benutzerereignisse für die ausgewählte Datenquelle anzuzeigen.
- **Risikozeitleiste auf einer Benutzerprofilseite**: Klicken Sie auf **Ereignissuche**, um die Ereignisse für den jeweiligen Benutzer anzuzeigen.

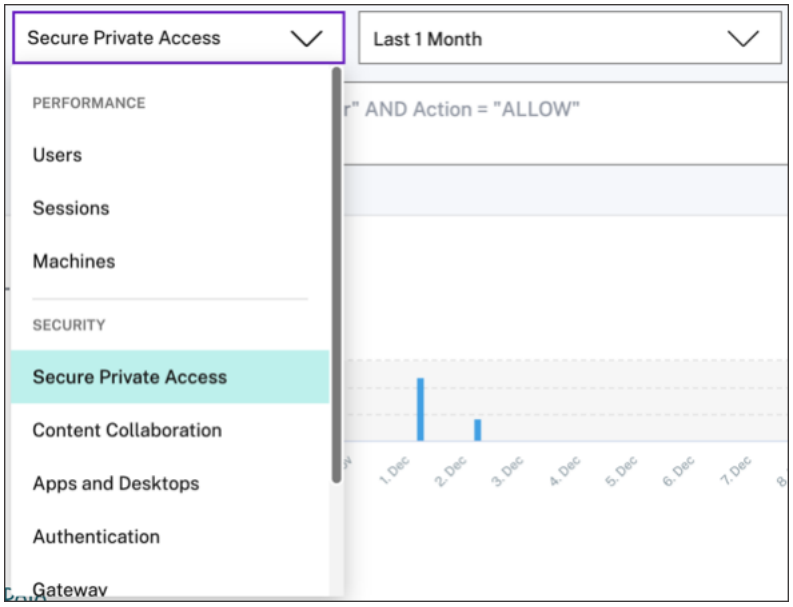
Self-Service-Suche aus der oberen Leiste

Verwenden Sie diese Option, um von einer beliebigen Stelle in der Benutzeroberfläche aus zur Self-Service-Suchseite zu gelangen.

1. Klicken Sie auf **Suchen**, um die Self-Service-Seite anzuzeigen.



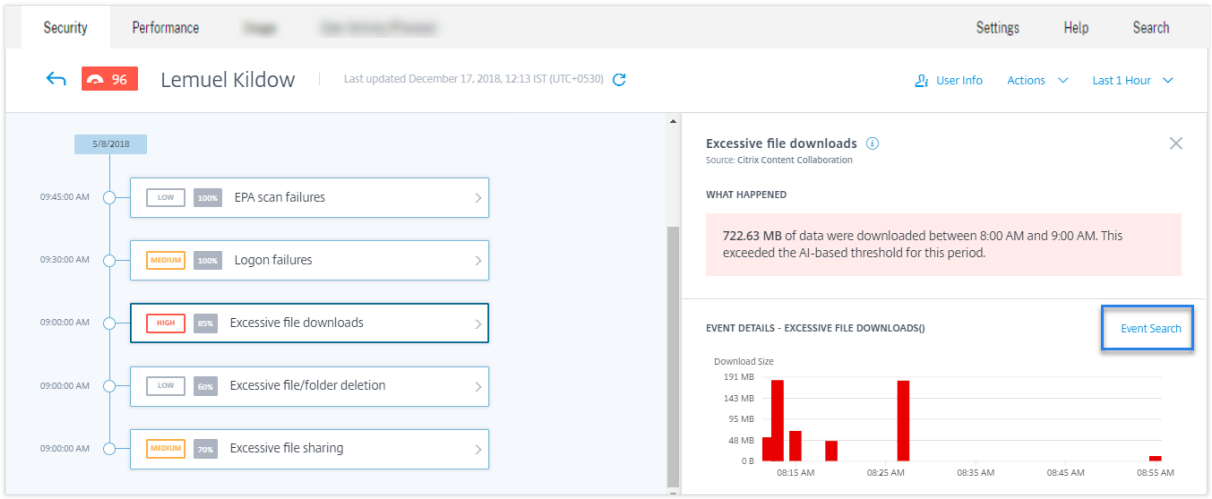
2. Wählen Sie die Datenquelle und den Zeitraum aus, um die entsprechenden Ereignisse anzuzeigen.



Self-Service-Suche aus der Risikozeitleiste des Benutzers

Verwenden Sie diese Option, wenn Sie die Benutzerereignisse anzeigen möchten, die mit einem Risikoindikator verknüpft sind.

Wenn Sie einen Risikoindikator aus der Zeitleiste eines Benutzers auswählen, wird im rechten Bereich der Risikoindikatorinformationen angezeigt. Klicken Sie auf **Ereignissuche**, um die Ereignisse zu untersuchen, die dem Benutzer und der Datenquelle zugeordnet sind (für die der Risikoindikator ausgelöst wird) auf der Self-Service-Suchseite.



Weitere Informationen zum Zeitplan für das Benutzerrisiko finden Sie unter Risikozeitleiste.

So verwenden Sie die Self-Service-Suche

Verwenden Sie die folgenden Funktionen auf der Self-Service-Suchseite:

- Facetten zum Filtern Ihrer Events.
- Suchfeld, um Ihre Abfrage einzugeben und Ereignisse zu filtern.
- Zeitauswahl zur Auswahl des Zeitraums.
- Timeline-Details zum Anzeigen der Ereignisdiagramme.
- Ereignisdaten zum Anzeigen der Ereignisse.
- Exportieren Sie ins CSV-Format, um Ihre Suchereignisse als CSV-Datei herunterzuladen.
- Exportieren Sie eine visuelle Zusammenfassung, um den visuellen Zusammenfassungsbericht Ihrer Suchanfrage herunterzuladen.
- Mehrspaltige Sortierung, um die Ereignisse nach mehreren Spalten zu sortieren.

Verwenden von Facetten zum Filtern von Ereignissen

Facetten sind die Zusammenfassung von Datenpunkten, die ein Ereignis darstellen. Facetten variieren je nach Datenquelle. Die Facetten für die Secure Private Access-Datenquelle sind beispielsweise

Reputation, Aktionen, Standort und Kategoriegruppe. Während die Facetten für Apps und Desktops Ereignistyp, Domäne und Plattform sind.

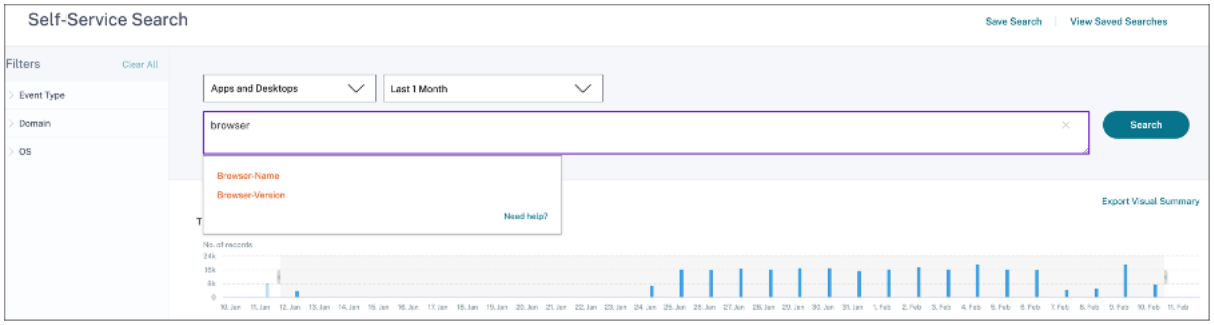
Wählen Sie die Facetten aus, um Ihre Suchergebnisse zu filtern. Die ausgewählten Facetten werden als Chips angezeigt.

Weitere Informationen zu den Facetten, die jeder Datenquelle entsprechen, finden Sie im Self-Service-Suchartikel für die Datenquelle, die weiter oben in diesem Artikel erwähnt wird.

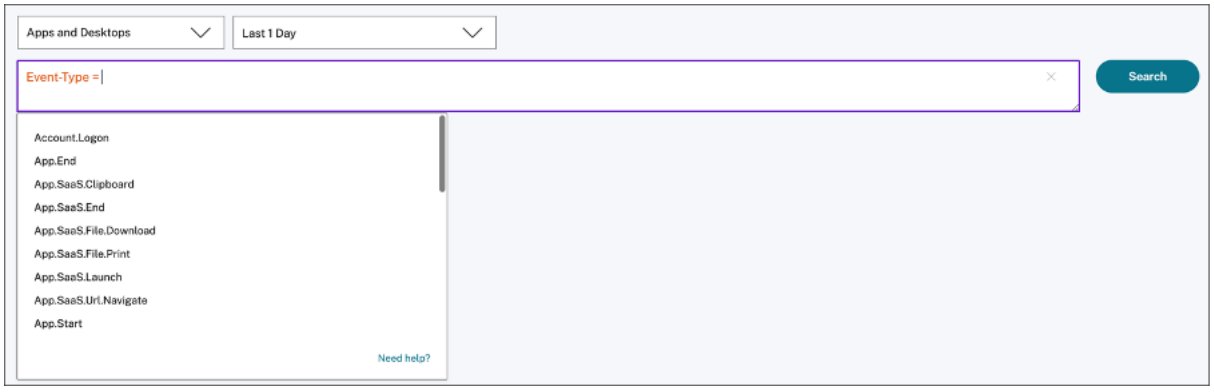
Verwenden Sie die Suchabfrage im Suchfeld, um Ereignisse zu filtern

Wenn Sie den Cursor in das Suchfeld setzen, zeigt das Suchfeld eine Liste von Dimensionen an, die auf den Benutzerereignissen basieren. Diese Dimensionen variieren je nach Datenquelle. Verwenden Sie die Dimensionen und die gültigen Operatoren, um Ihre Suchkriterien zu definieren und nach den erforderlichen Ereignissen zu suchen.

Bei der Self-Service-Suche nach Apps und Desktops erhalten Sie beispielsweise die folgenden Werte für die Dimension `Browser`. Verwenden Sie die Dimension, um Ihre Abfrage einzugeben, wählen Sie den Zeitraum aus, und klicken Sie dann auf **Suchen**.



Wenn Sie bestimmte Dimensionen wie `Event-Type` und `Clipboard-Operation` zusammen mit einem gültigen Operator auswählen, werden die Werte der Dimension automatisch angezeigt. Sie können einen Wert aus den vorgeschlagenen Optionen auswählen oder je nach Ihren Anforderungen einen neuen Wert eingeben.



Unterstützte Operatoren bei Suchanfragen Verwenden Sie die folgenden Operatoren in Ihren Suchanfragen, um Ihre Suchergebnisse zu verfeinern.

Betreiber	Beschreibung	Beispiel	Ausgabe
	Weisen Sie einer Suchdimension einen Wert zu.	Benutzername: John	Zeigt Ereignisse für den Benutzer John an.
=	Weisen Sie einer Suchdimension einen Wert zu.	Benutzername = John	Zeigt Ereignisse für den Benutzer John an.
~	Suchen Sie Ereignisse mit ähnlichen Werten.	Benutzername ~ test	Zeigt Ereignisse mit ähnlichen Benutzernamen an.
" "	Schließen Sie Werte getrennt durch Leerzeichen ein.	Benutzername = "John Smith"	Zeigt Ereignisse für den Benutzer John Smith an.
< >	Suchen Sie nach einem relationalen Wert.	Datenvolumen > 100	Zeigt Ereignisse an, bei denen das Datenvolumen größer als 100 GB ist.
AND	Suchereignisse, bei denen die angegebenen Bedingungen zutreffen.	Benutzername: John AND Datenvolumen > 100	Zeigt Ereignisse von Benutzer John an, bei denen das Datenvolumen größer als 100 GB ist.
! ~	Überprüft Ereignisse auf das von Ihnen angegebene übereinstimmende Muster. Dieser NOT LIKE Operator gibt die Ereignisse zurück, die das übereinstimmende Muster nirgendwo in der Ereigniszeichenfolge enthalten.	Benutzername! ~ John	Zeigt Ereignisse für die Benutzer an, außer John, John Smith oder solche Benutzer, die den übereinstimmenden Namen "John" enthalten.

Betreiber	Beschreibung	Beispiel	Ausgabe
! =	Prüft Ereignisse auf die genaue Zeichenfolge, die Sie angeben. Dieser NOT EQUAL-Operator gibt die Ereignisse zurück, die die genaue Zeichenfolge nicht irgendwo in der Ereigniszeichenfolge enthalten.	Country != USA	Zeigt Ereignisse für Länder mit Ausnahme der USA an.
*	Suchen Sie Ereignisse, die den angegebenen Strings entsprechen. Derzeit wird der Operator * nur mit den folgenden Operatoren :, = und != unterstützt. Bei den Suchergebnissen wird Groß-/Kleinschreibung beachtet	Benutzername = John*	Zeigt Ereignisse für alle Benutzernamen an, die mit John beginnen.
		Benutzername = *John*	Zeigt Ereignisse für alle Benutzernamen an, die John enthalten.
		Benutzername = *Smith	Zeigt Ereignisse für alle Benutzernamen an, die mit Smith enden.
		Benutzername: John*	Zeigt Ereignisse für alle Benutzernamen an, die mit John beginnen.
		Benutzername: *John*	Zeigt Ereignisse für alle Benutzernamen an, die John enthalten.
		Benutzername: *Smith	Zeigt Ereignisse für alle Benutzernamen an, die mit Smith enden.

Betreiber	Beschreibung	Beispiel	Ausgabe
		Benutzername! = John*	Zeigt Ereignisse für alle Benutzernamen an, die nicht mit John beginnen.
		Benutzername! = *Schmied	Zeigt Ereignisse für alle Benutzernamen an, die nicht mit Smith enden.
`IN`	Weisen Sie einer Suchdimension mehrere Werte zu, um die Ereignisse abzurufen, die sich auf einen oder mehrere Werte beziehen. **Hinweis**: Derzeit können Sie diesen Operator mit den folgenden Dimensionen von Apps und Desktops- `Device ID`, `Domain` `Event-Type`, und verwenden `User-Name`. Dieser Operator ist nur für die String-Werte anwendbar.	Benutzername IN (John, Kevin)	Finden aller Ereignisse im Zusammenhang mit John oder Kevin.

Betreiber	Beschreibung	Beispiel	Ausgabe
`NOT IN`	Weisen Sie einer Suchdimension mehrere Werte zu und suchen Sie die Ereignisse, die die angegebenen Werte nicht enthalten. **Hinweis**: Derzeit können Sie diesen Operator mit den folgenden Dimensionen von Apps und Desktops- `Device ID`, `Domain` `Event-Type`, und verwenden `User-Name`. Dieser Operator ist nur für die String-Werte anwendbar.	Benutzername NICHT IN (John, Kevin)	Finde die Events für alle Benutzer außer John und Kevin.
`IS EMPTY`	Sucht nach Nullwert oder leerem Wert für eine Dimension. Dieser Operator funktioniert nur für Dimensionen vom Typ Zeichenfolge wie `App-NameBrowser`, und `Country`. Es funktioniert nicht für Dimensionen vom Typ Nicht-Zeichenfolge (Zahl) wie `Upload-File-` `SizeDownload-` `File-Size`, und `Client-IP`.	Land IST LEER	Finden Sie Ereignisse, bei denen der Ländername nicht verfügbar oder leer ist (nicht angegeben).

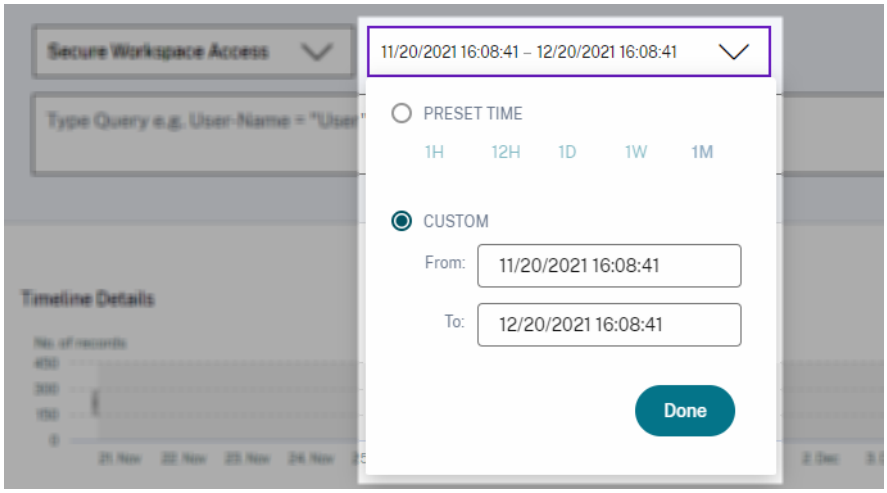
Betreiber	Beschreibung	Beispiel	Ausgabe
`IS NOT EMPTY`	Überprüft, ob kein Nullwert oder ein bestimmter Wert für eine Dimension vorhanden ist. Dieser Operator funktioniert nur für Dimensionen vom Typ Zeichenfolge wie `App-NameBrowser`, und `Country`. Es funktioniert nicht für Dimensionen vom Typ Nicht-Zeichenfolge (Zahl) wie `Upload-File-SizeDownload-File-Size`, und `Client-IP`.	Land IST NICHT LEER	Finden von Ereignissen, bei denen der Ländername verfügbar oder angegeben ist.
`OR`	Sucht nach Werten, bei denen eine oder beide Bedingungen zutreffen.	(User-Name = `John*` OR User-Name = `*Smith`) AND Event-Type = “Session.Logon”	Zeigt `Session.Logon`-Ereignisse für alle Benutzernamen an, die mit John beginnen oder mit Smith enden.

> **Hinweis**
>
> Verwenden Sie für den Operator NOT **EQUAL** beim Eingeben der Werte für die Dimensionen in Ihrer Abfrage die genauen Werte, die auf der Self-Service-Suchseite für eine Datenquelle verfügbar sind. Bei den Dimensionswerten wird die Groß-/Kleinschreibung

Weitere Informationen zum Angeben Ihrer Suchanfrage für die Datenquelle finden Sie im Self-Service-Suchartikel für die oben in diesem Artikel erwähnte Datenquelle.

Wählen Sie die Zeit, um das Ereignis anzuzeigen

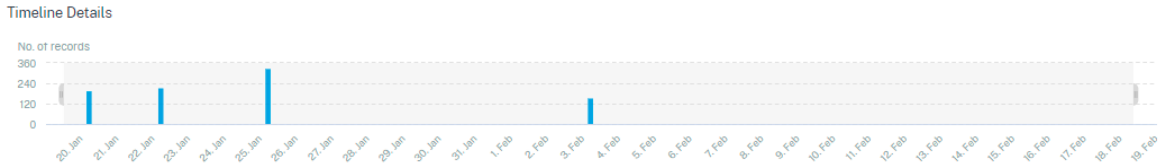
Wählen Sie eine voreingestellte Zeit aus oder geben Sie einen benutzerdefinierten Zeitraum ein und klicken Sie auf **Suchen**, um die Ereignisse anzuzeigen.



Zeigen Sie die Details der Zeitleiste an

Die Zeitleiste bietet eine grafische Darstellung von Benutzerereignissen für den ausgewählten Zeitraum. Bewegen Sie die Auswahlbalken, um den Zeitraum auszuwählen und die Ereignisse anzuzeigen, die dem ausgewählten Zeitraum entsprechen.

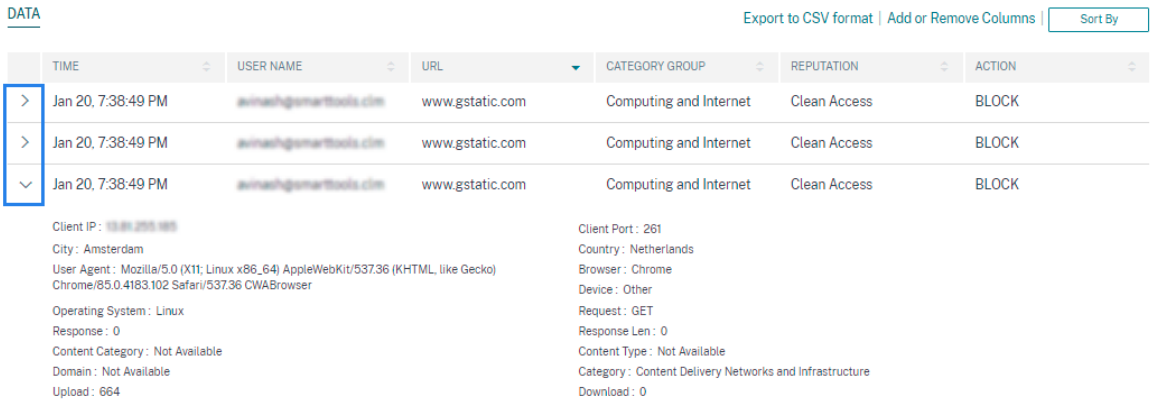
Die Abbildung zeigt Timeline-Details für Zugriffsdaten.



Ereignisse anzeigen

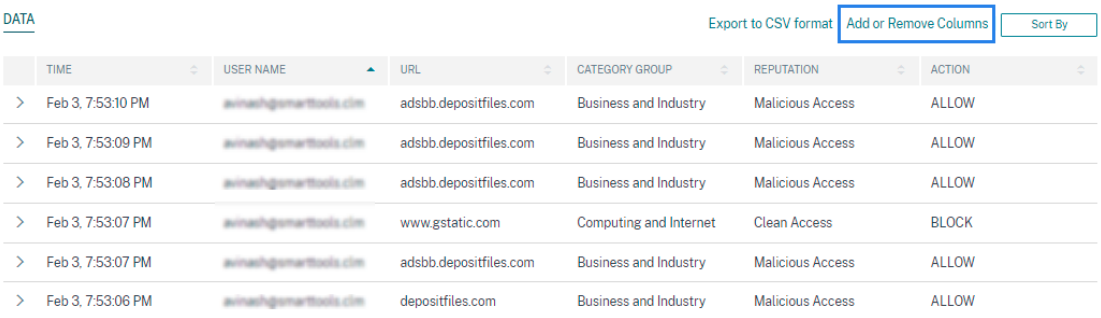
Sie können die detaillierten Informationen zum Benutzerereignis anzeigen. Klicken Sie in der Tabelle **DATEN** auf den Pfeil für jede Spalte, um die Details des Benutzerereignisses anzuzeigen.

Die Abbildung zeigt die Details zu den Zugriffsdaten des Benutzers.

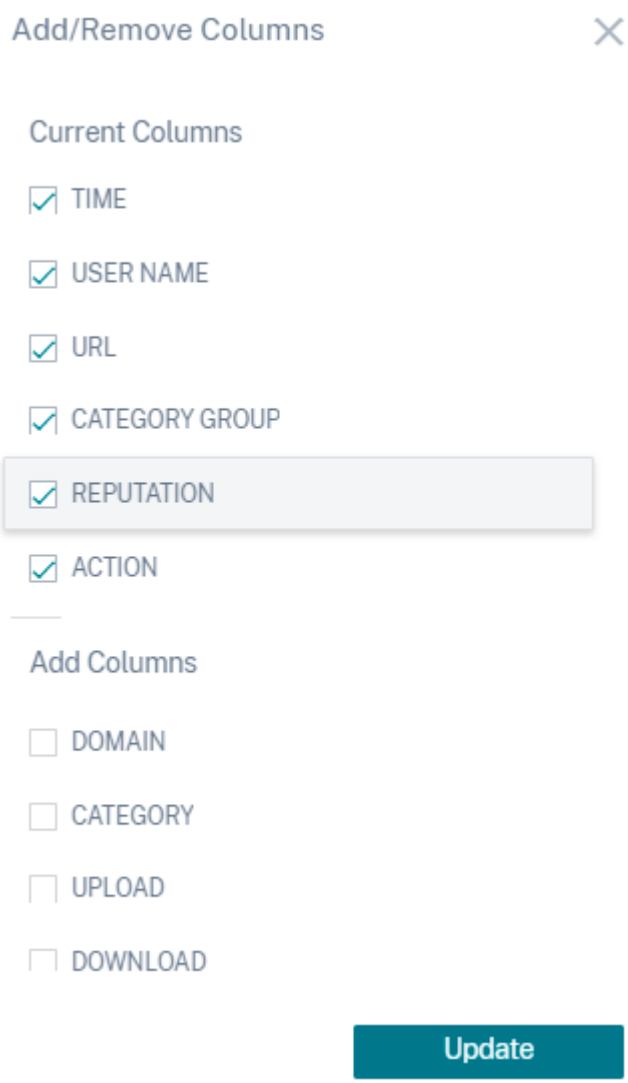


Spalten hinzufügen oder entfernen Sie können der Ereignistabelle entweder Spalten hinzufügen oder daraus entfernen, um die entsprechenden Datenpunkte anzuzeigen oder auszublenden. Führen Sie folgende Schritte aus:

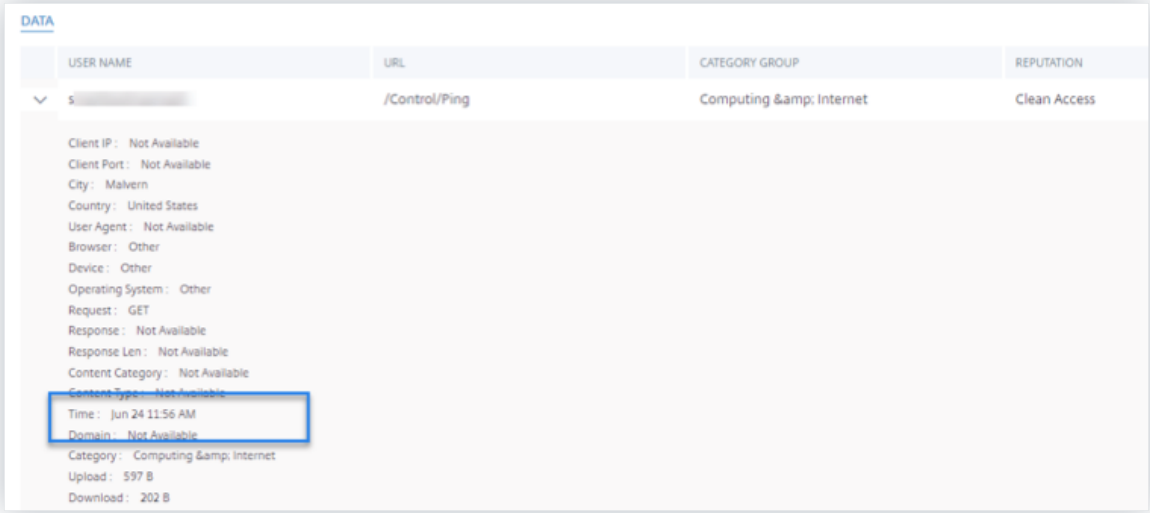
1. Klicken Sie auf **Spalten hinzufügen oder entfernen**.



2. Markieren oder heben Sie die Auswahl der Datenelemente in der Liste auf und klicken Sie dann auf **Aktualisieren**.

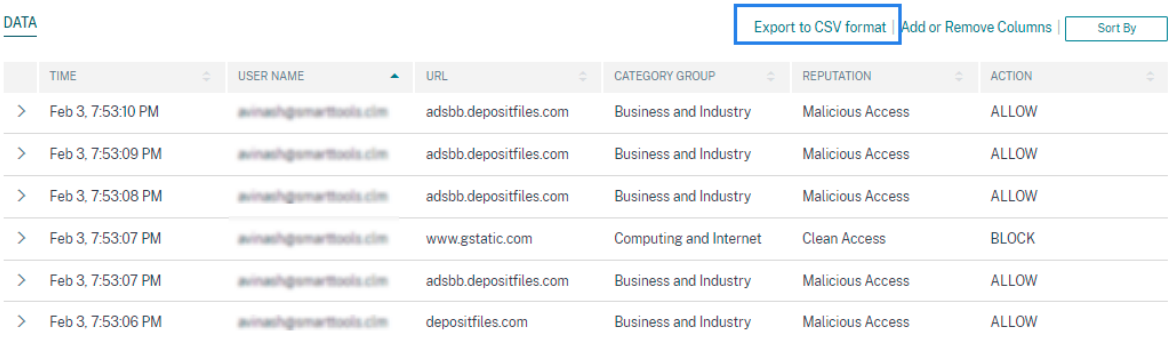


Wenn Sie einen Datenpunkt aus der Liste abwählen, wird die entsprechende Spalte aus der Ereignistabelle entfernt. Sie können diesen Datenpunkt jedoch anzeigen, indem Sie die Ereigniszeile für einen Benutzer erweitern. Wenn Sie beispielsweise den **TIME-Datenpunkt** aus der Liste abwählen, wird die Spalte **TIME** aus der Ereignistabelle entfernt. Um den Zeitdatensatz anzuzeigen, erweitern Sie die Ereigniszeile für einen Benutzer.



Exportieren Sie die Ereignisse in eine CSV-Datei

Exportieren Sie die Suchergebnisse in eine CSV-Datei und speichern Sie sie als Referenz. Klicken Sie auf In **CSV-Format** exportieren, um die Ereignisse zu exportieren und die generierte CSV-Datei herunterzuladen. Mit der Funktion In **CSV-Format exportieren** können Sie 100.000 Zeilen exportieren.



Visuelle Zusammenfassung exportieren

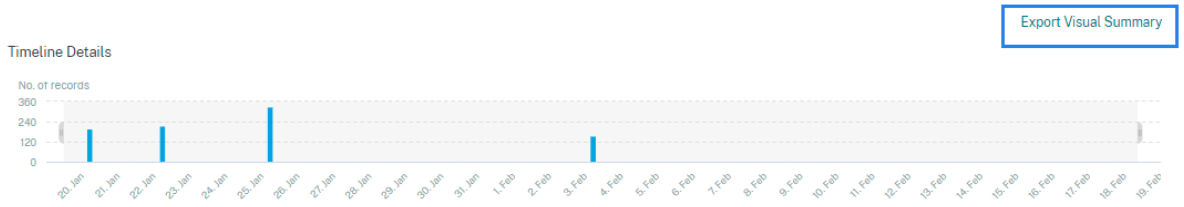
Sie können den visuellen Zusammenfassungsbericht Ihrer Suchanfrage herunterladen und eine Kopie mit anderen Benutzern, Administratoren oder Ihrem Führungsteam teilen.

Klicken Sie auf **Visual Summary exportieren**, um den visuellen Zusammenfassungsbericht als PDF herunterzuladen. Der Bericht enthält die folgenden Informationen:

- Die Suchanfrage, die Sie für die Ereignisse für den ausgewählten Zeitraum angegeben haben.
- Die Facetten (Filter), die Sie für den ausgewählten Zeitraum auf die Ereignisse angewendet haben.

- Die visuelle Zusammenfassung wie die Zeitleistendiagramme, Balkendiagramme oder Diagramme der Suchereignisse für den ausgewählten Zeitraum.

Für eine Datenquelle können Sie den visuellen Zusammenfassungsbericht nur herunterladen, wenn die Daten in visuellen Formaten wie Balkendiagrammen und Zeitleistendetails angezeigt werden. Andernfalls ist diese Option nicht verfügbar. Sie können beispielsweise den visuellen zusammenfassenden Bericht der Datenquellen wie Apps und Desktops, Sessions herunterladen, in dem Sie Daten als Zeitachsendetails und Balkendiagramme sehen. Für Datenquellen wie Benutzer und Maschinen sehen Sie Daten nur im Tabellenformat. Daher können Sie keinen visuellen Zusammenfassungsbericht herunterladen.

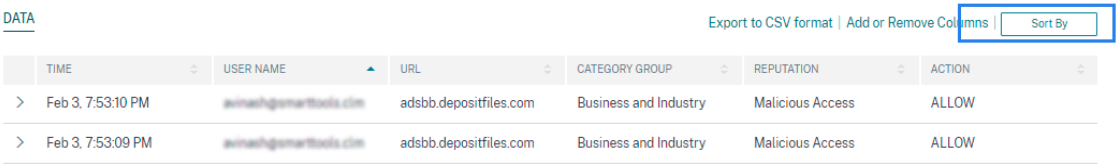


Mehrspaltige Sortierung

Die Sortierung hilft bei der Organisation Ihrer Daten und bietet eine bessere Sichtbarkeit. Auf der Self-Service-Suchseite können Sie die Benutzerereignisse nach einer oder mehreren Spalten sortieren. Die Spalten repräsentieren die Werte verschiedener Datenelemente wie Benutzername, Datum und Uhrzeit und URL. Diese Datenelemente variieren basierend auf den ausgewählten Datenquellen.

Gehen Sie wie folgt vor, um eine mehrspaltige Sortierung durchzuführen:

1. Klicken Sie auf **Sortieren nach**.

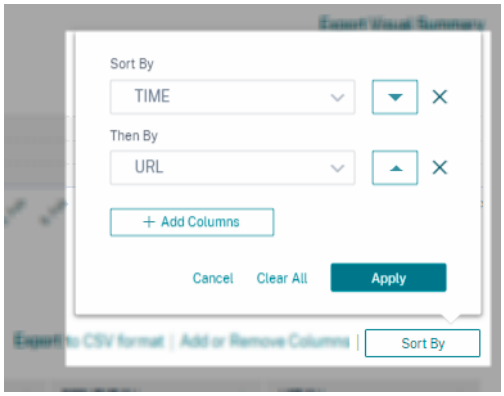


2. Wählen Sie eine Spalte aus der Liste **Sortieren nach** aus.
3. Wählen Sie die Sortierreihenfolge - aufsteigend (Pfeil nach oben) oder absteigend (Pfeil nach unten), um die Ereignisse in der Spalte zu sortieren.
4. Klicken Sie auf **+ Spalten hinzufügen**.
5. Wählen Sie eine weitere Spalte aus der Liste **Dann vorbei** aus.
6. Wählen Sie die Sortierreihenfolge aus - aufsteigend (Pfeil nach oben) oder absteigend (Abwärtsfehler), um die Ereignisse in der Spalte zu sortieren.

> **Hinweis**
>
> Sie können bis zu sechs Spalten hinzufügen, um die Sortierung durchzuführen.

7. Klicken Sie auf **Anwenden**.
8. Wenn Sie die vorherigen Einstellungen nicht anwenden möchten, klicken Sie auf **Abbrechen**. Um die Werte der ausgewählten Spalten zu entfernen, klicken Sie auf **Alle löschen**.

Das folgende Beispiel zeigt eine mehrspaltige Sortierung der Secure Private Access-Ereignisse. Die Ereignisse werden nach Zeit (in der neuesten bis ältesten Reihenfolge) und dann nach URL (in alphabetischer Reihenfolge) sortiert.



Alternativ können Sie mit der **Umschalttaste** eine mehrspaltige Sortierung durchführen. Drücken Sie die **Umschalttaste** und klicken Sie auf die Spaltenüberschriften, um die Benutzerereignisse zu sortieren.

So speichern Sie die Self-Service-Suche

Als Administrator können Sie eine Self-Service-Abfrage speichern. Diese Funktion spart Zeit und Mühe beim Umschreiben der Abfrage, die Sie häufig für die Analyse oder Fehlerbehebung verwenden. Die folgenden Optionen werden mit der Abfrage gespeichert:

- Angewandte Suchfilter
- Ausgewählte Datenquelle und Dauer

Gehen Sie wie folgt vor, um eine Selbstbedienungsabfrage zu speichern:

1. Wählen Sie die erforderliche Datenquelle und Dauer aus.
2. Geben Sie eine Abfrage in die Suchleiste ein.
3. Wenden Sie die erforderlichen Filter an.
4. Klicken Sie auf **Suche speichern**.
5. Geben Sie den Namen an, um die benutzerdefinierte Abfrage zu speichern.

> **Hinweis Stellen Sie**
>
> sicher, dass der Abfragename eindeutig ist. Andernfalls wird die Abfrage nicht gespeichert.

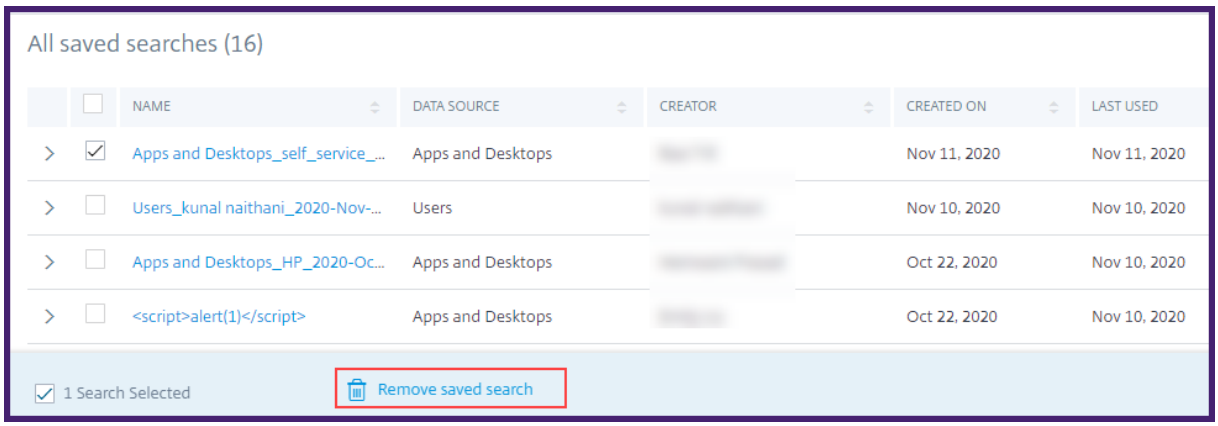
6. Aktivieren Sie die Schaltfläche **E-Mail-Bericht planen**, wenn Sie regelmäßig eine Kopie des Suchanfrageberichts an sich und andere Benutzer senden möchten. Weitere Informationen finden Sie unter Planen einer E-Mail für eine Suchanfrage.
7. Klicken Sie auf **Speichern**.

So zeigen Sie die gespeicherten Suchanfragenan:

1. **Klicken Sie auf Gespeicherte Suchen**
2. Klicken Sie auf den Namen der Suchanfrage.

So entfernen Sie eine gespeicherte Suche:

1. **Klicken Sie auf Gespeicherte Suchen**
2. Wählen Sie die Suchabfrage aus, die Sie gespeichert haben.
3. Klicke auf **Gespeicherte Suche entfernen**.



So ändern Sie eine gespeicherte Suche:

1. **Klicken Sie auf Gespeicherte Suchen**
2. Klicken Sie auf den Namen der Suchabfrage, die Sie gespeichert haben.
3. Ändern Sie die Suchanfrage oder die Facettenauswahl basierend auf Ihren Anforderungen.
4. Klicken Sie auf **Suche aktualisieren > Speichern**, um zu aktualisieren, und speichern Sie die geänderte Suche unter demselben Suchanfragenamen.
5. Wenn Sie die geänderte Suche unter einem neuen Namen speichern möchten, klicken Sie auf den Abwärtspfeil und dann auf **Als neue Suche speichern > Speichern unter**.

Wenn Sie die Suche durch einen neuen Namen ersetzen, wird die Suche als neuer Eintrag gespeichert. Wenn Sie den vorhandenen Suchnamen beim Ersetzen beibehalten, setzen die geänderten Suchdaten die vorhandenen Suchdaten außer Kraft.

> **Hinweis**
>
> - Nur ein Abfrage-Besitzer kann seine gespeicherten Suchanfragen ändern oder entfernen.
> - Sie können die gespeicherte Adresse des Suchlinks kopieren, um sie mit einem anderen Benutzer zu teilen.

Planen Sie eine E-Mail für eine Suchanfrage

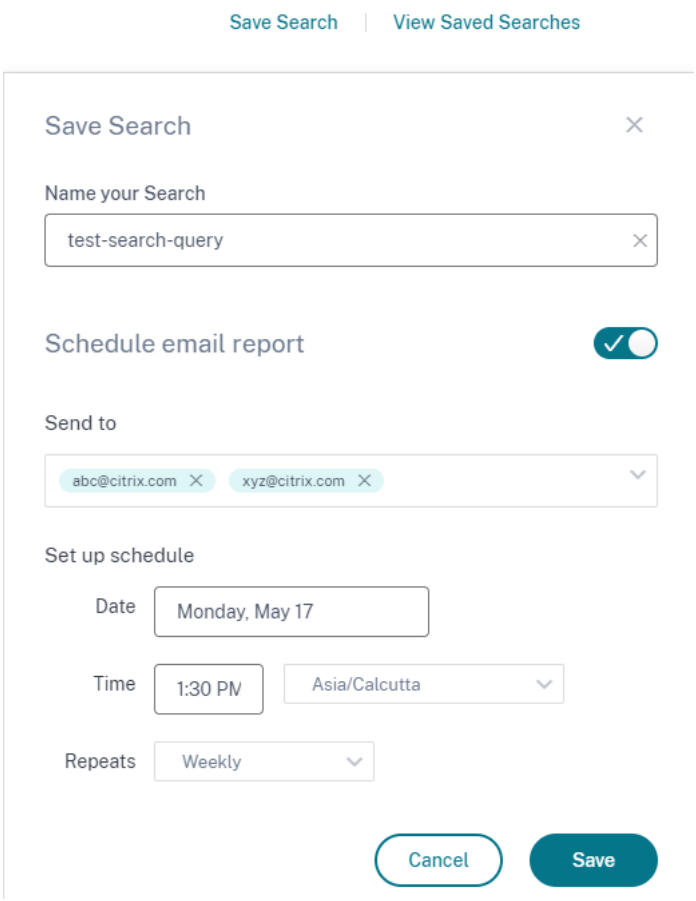
Sie können in regelmäßigen Abständen eine Kopie des Suchanfrageberichts an sich und andere Benutzer senden, indem Sie einen Zeitplan für die E-Mail-Zustellung einrichten.

Diese Option ist nur verfügbar, wenn Ihr Suchanfragebericht Daten in visuellen Formaten wie Balkendiagrammen und Zeitachsendetails enthält. Andernfalls können Sie keine E-Mail-Zustellung planen. Sie können beispielsweise eine E-Mail für Datenquellen wie Apps und Desktops, Sessions planen, in der Sie Daten als Zeitachsendetails und Balkendiagramme sehen. Für Datenquellen wie Benutzer und Maschinen sehen Sie Daten nur im Tabellenformat. Daher können Sie keine E-Mail planen.

Planen Sie eine E-Mail beim Speichern einer Suchanfrage

Richten Sie beim Speichern einer Suchanfrage einen Zeitplan für die E-Mail-Zustellung wie folgt ein:

1. Aktivieren Sie im Dialogfeld **Suche speichern** die Schaltfläche **E-Mail-Bericht planen** .



2. Geben Sie die E-Mail-Adressen der Empfänger ein oder fügen Sie sie ein.

   > **Hinweis**
   >
   > E-Mail-Gruppen werden nicht unterstützt.

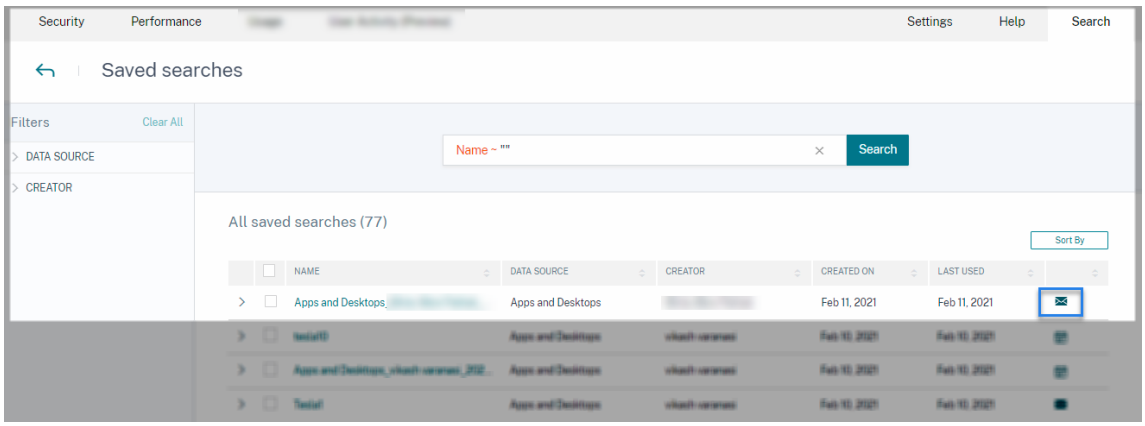
3. Legen Sie Datum und Uhrzeit für die E-Mail-Zustellung fest.
4. Wählen Sie die Lieferfrequenz aus - täglich, wöchentlich oder monatlich.
5. Klicken Sie auf **Speichern**.

Planen Sie eine E-Mail für eine bereits gespeicherte Suchanfrage

Wenn Sie einen E-Mail-Lieferplan für eine Suchanfrage einrichten möchten, die Sie zuvor gespeichert haben, gehen Sie wie folgt vor:

1. **Klicken Sie auf Gespeicherte Suchen**
2. Gehen Sie zu der Suchanfrage, die Sie erstellt haben. Klicken Sie auf das Symbol **Diese Abfrage per E-Mail senden** .

> **Hinweis**
>
> Nur ein Abfragebesitzer kann die E-Mail-Zustellung seiner gespeicherten Suchanfrage planen.



3. Aktivieren Sie die Schaltfläche **E-Mail-Bericht planen** .
4. Geben Sie die E-Mail-Adressen der Empfänger ein oder fügen Sie sie ein.

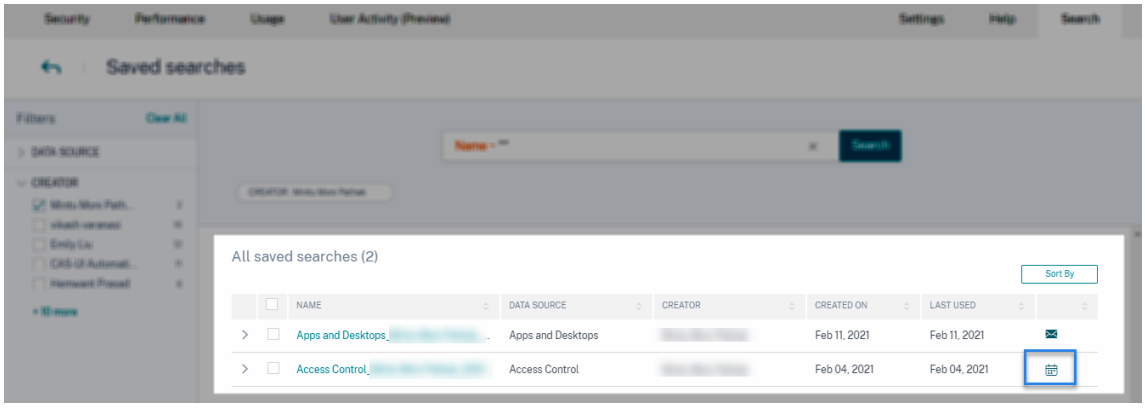
> **Hinweis**
>
> E-Mail-Gruppen werden nicht unterstützt.

5. Legen Sie Datum und Uhrzeit für die E-Mail-Zustellung fest.
6. Wählen Sie die Lieferfrequenz aus - täglich, wöchentlich oder monatlich.
7. Klicken Sie auf **Speichern**.

Stoppen Sie einen E-Mail-Lieferplan für eine Suchanfrage

1. **Klicken Sie auf Gespeicherte Suchen**
2. Gehen Sie zu der Suchanfrage, die Sie erstellt haben. Klicken Sie auf das Symbol **E-Mail-Lieferplan anzeigen** .

> **Hinweis**
>
> Nur ein Abfragebesitzer kann den E-Mail-Zeitplan seiner gespeicherten Suchanfrage stoppen.



3. Deaktivieren Sie die Schaltfläche **E-Mail-Bericht planen** .
4. Klicken Sie auf **Speichern**.

Inhalt per E-Mail

Die Empfänger erhalten von "Citrix Cloud - Benachrichtigungen donotreplynotifications@citrix.com" eine E-Mail über den Suchanfragebericht. Der Bericht ist als PDF-Dokument beigefügt. Die E-Mail wird in einem regelmäßigen Intervall gesendet, das von Ihnen in den Einstellungen für **E-Mail-Bericht planen** definiert wurde.

Der Suchanfragebericht enthält die folgenden Informationen:

- Die Suchanfrage, die Sie für die Ereignisse für den ausgewählten Zeitraum angegeben haben.
- Die Facetten (Filter), die Sie auf die Ereignisse angewendet haben.
- Die visuelle Zusammenfassung wie die Zeitleistendiagramme, Balkendiagramme oder Graphen der Suchereignisse.

Berechtigungen für Administratoren mit Vollzugriff und Nur-Lese-Zugriff

- Wenn Sie ein Citrix Cloud-Administrator mit vollem Zugriff sind, können Sie alle auf der **Suchseite** verfügbaren Funktionen nutzen.
- Wenn Sie ein Citrix Cloud-Administrator mit schreibgeschütztem Zugriff sind, können Sie nur die folgenden Aktivitäten auf der **Suchseite** ausführen:
  - Zeigen Sie die Suchergebnisse an, indem Sie eine Datenquelle und den Zeitraum auswählen.
  - Geben Sie eine Suchabfrage ein und sehen Sie sich die Suchergebnisse an.
  - Zeigen Sie die gespeicherten Suchergebnisse anderer Administratoren an.

- Exportieren Sie die visuelle Zusammenfassung und laden Sie die Suchergebnisse als CSV-Datei herunter.

Informationen zu den Administratorrollen finden Sie unter Verwalten von Administratorrollen für Citrix Analytics.

Einstellungen für Warnungen

December 12, 2023

Citrix Analytics generiert Warnungen auf der Grundlage der Warnrichtlinienkriterien. Sie können so konfigurieren, dass Warnmeldungen von Citrix Analytics for Security and Performance per E-Mail und Webhook empfangen werden.

- E-Mail-Verteilerliste
- Webhook für Alert-Benachrichtigungen

Sie können die E-Mail-Benachrichtigung für Benachrichtigungen von Citrix Analytics for Security formatieren.

- E-Mail-Einstellungen für Endbenutzer

E-Mail-Verteilerlisten

December 12, 2023

Wenn Sie die Aktion **Administrator (e) benachrichtigen** entweder manuell oder durch Erstellen einer Richtlinie anwenden, wird eine Benachrichtigung an die ausgewählten Administratoren über den Risikoindikator gesendet.

> **WICHTIG**
>
> Sie können Administratoren aus den Citrix Cloud-Domänen und anderen Nicht-Citrix Cloud-Domänen in Ihrer Organisation auswählen.

Um Benachrichtigungen an die entsprechenden Gruppen von Administratoren zu senden, erstellen Sie eine Verteilerliste mit ihren E-Mail-Adressen.

Mit der E-Mail-Verteilerliste können Sie Folgendes tun:

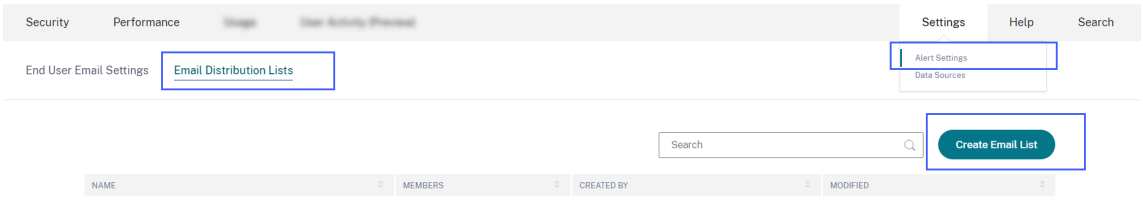
- Erstellen Sie eine gemeinsame E-Mail-Verteilerliste mit Mitgliedern aus verschiedenen Domänen in Ihrer Organisation.

- Benachrichtigen Sie alle Mitglieder auf einmal.
- Sparen Sie Zeit und Mühe bei der Auswahl der Administratoren aus verschiedenen Domänen.
- Verwalten und pflegen Sie die E-Mail-Verteilerlisten basierend auf Ihren Anforderungen, z. B. das Hinzufügen neuer Mitglieder oder das Entfernen vorhandener Mitglieder.

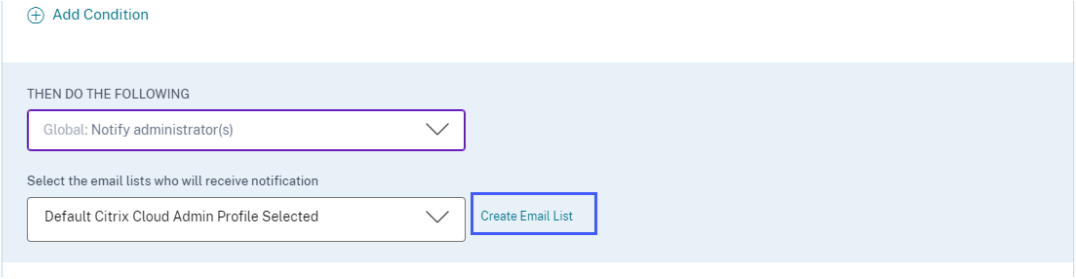
E-Mail-Verteilerliste erstellen

So erstellen Sie eine E-Mail-Verteilerliste:

1. Klicken Sie auf **Einstellungen > Warnungseinstellungen > E-Mail-Verteilerlisten > E-Mail-Liste erstellen**.



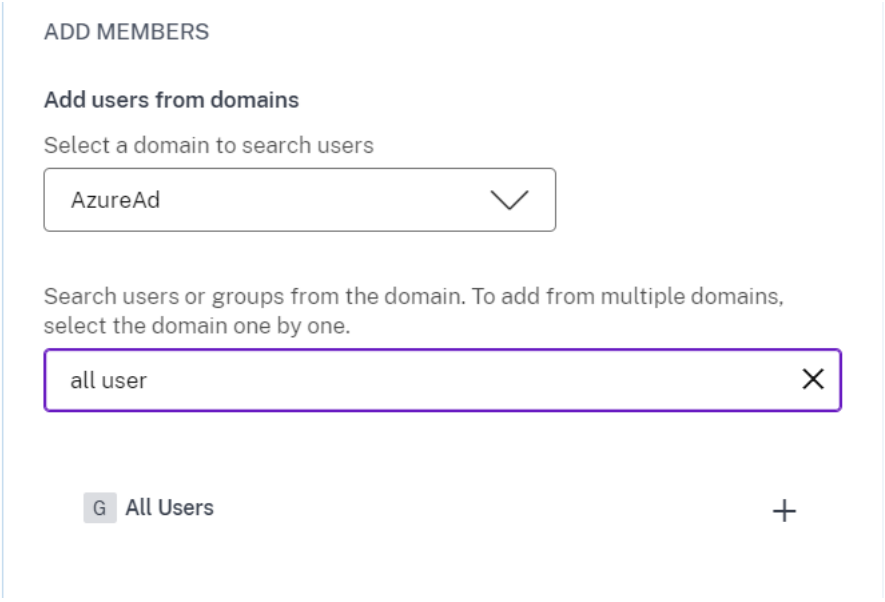
   Alternativ können Sie auch eine E-Mail-Verteilerliste aus einer Richtlinie erstellen. Ändern Sie eine vorhandene Richtlinie oder erstellen Sie eine Richtlinie und wählen Sie die Aktion **Administrator (e) benachrichtigen** aus. Klicken Sie auf den Link **E-Mail-Liste erstellen** .



2. Geben Sie einen Namen und eine Beschreibung der E-Mail-Verteilerliste ein, um deren Zweck zu ermitteln.
3. Verwenden Sie die folgenden Optionen, um Mitglieder zur E-Mail-Verteilerliste hinzuzufügen:
   - **Benutzer aus Domains hinzufügen**. Für diese Option müssen Ihre Domänen mit Citrix Cloud verbunden sind.
   - **Benutzer per E-Mail-Adressen hinzufügen**. Verwenden Sie diese Option, wenn Sie Benutzer hinzufügen möchten, die sich außerhalb Ihrer ausgewählten Domänen befinden.
4. Um Benutzer aus Domänen hinzuzufügen, wählen Sie eine Domäne aus und suchen Sie nach den Benutzern oder Benutzergruppen.

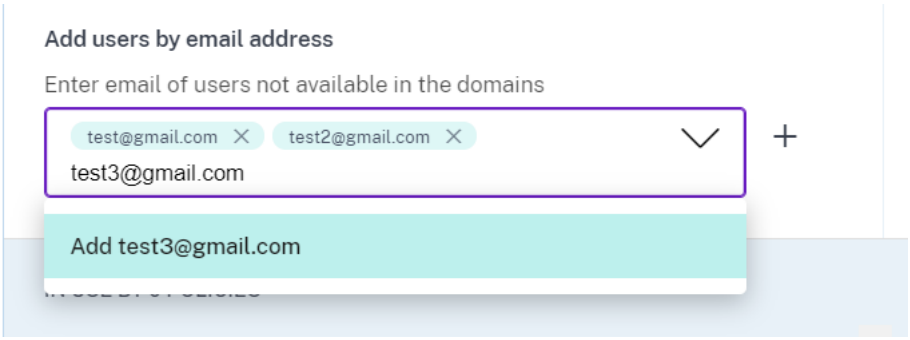
> **Hinweis**
>
> Sie können auch Benutzer und Benutzergruppen aus mehreren Domänen hinzufügen, indem Sie die Domänen nacheinander auswählen. Suchen und fügen Sie für jede Domäne die Benutzer oder die Benutzergruppe hinzu.

5. Klicken Sie neben dem Benutzer oder der Benutzergruppe auf das Symbol **Hinzufügen** .



6. Um Benutzer hinzuzufügen, die in der von Ihnen ausgewählten Domain nicht verfügbar sind, geben Sie entweder die E-Mail-Adressen der Benutzer oder die E-Mail-Verteilerlisten ein.

> **Hinweis**
>
> Stellen Sie vor der Eingabe einer E-Mail-Verteilerliste sicher, dass Sie von außerhalb des Netzwerks Ihrer Organisation auf die E-Mail-Verteilerliste zugreifen können. Wenn Sie eine organisationsinterne E-Mail-Verteilerliste hinzufügen, können die Mitglieder der Liste keine Benachrichtigungen von Citrix Analytics erhalten.



7. Klicken Sie auf **E-Mail-Liste erstellen**.

E-Mail-Verteilerliste anzeigen

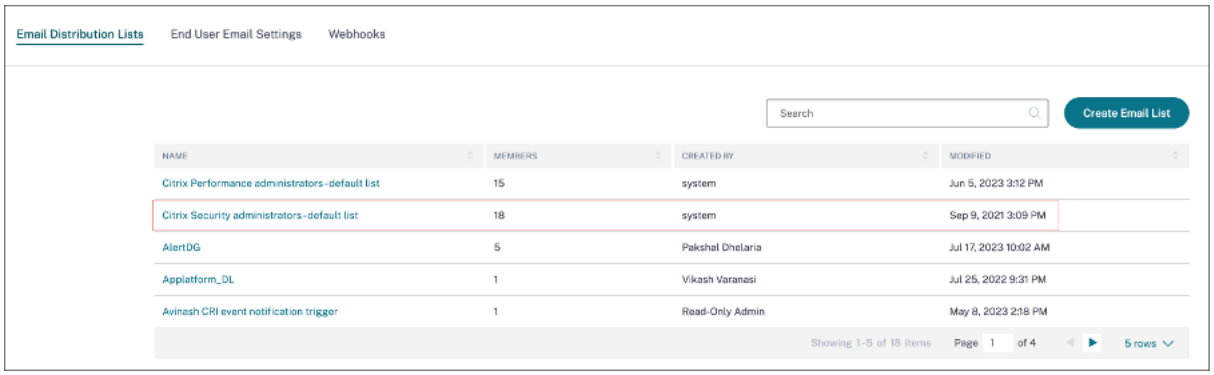
Um Ihre E-Mail-Verteilerlisten anzuzeigen, klicken Sie auf **Einstellungen > Warnungseinstellungen > E-Mail-Verteilerlisten**.

Auf der Seite werden alle E-Mail-Verteilerlisten angezeigt, die in Ihrem Konto erstellt wurden. Wählen Sie eine E-Mail-Verteilerliste aus, um die Mitglieder anzuzeigen oder die Liste zu ändern.

Sie sehen eine standardmäßig erstellte E-Mail-Verteilerliste in Ihrem Konto. Es enthält die Citrix Cloud-Administratoren, deren Option **E-Mail-Benachrichtigungen** in ihren Citrix Cloud-Konten aktiviert ist. Sie können die Standardliste nicht löschen oder ändern.

> **Hinweis**
>
> Für die Standard-E-Mail-Verteilerliste speichert Citrix Analytics die Informationen über die Administratoren, deren E-Mail-Benachrichtigungen aktiviert sind. Der Cache wird alle 24 Stunden einmal aktualisiert. Wenn also ein Administrator die Einstellungen für E-Mail-Benachrichtigungen ändert, wird diese Änderung nach 24 Stunden in Citrix Analytics aktualisiert.
>
> Wenn beispielsweise ein Citrix Cloud-Administrator seine E-Mail-Benachrichtigungen aktiviert, erhält er nach 24 Stunden Benachrichtigungen, nicht sofort. Wenn ein Citrix Cloud-Administrator seine E-Mail-Benachrichtigungen deaktiviert, erhält er ebenfalls nach 24 Stunden keine Benachrichtigungen mehr.

Die Standardverteilerliste für Sicherheitsadministratoren umfasst jetzt sowohl vollständige als auch benutzerdefinierte Administratoren, für die die Option **E-Mail-Benachrichtigungen** in ihren Citrix Cloud-Konten aktiviert ist.



Ändern einer E-Mail-Verteilerliste

So ändern Sie eine E-Mail-Verteilerliste:

1. Klicken Sie auf **Einstellungen > Warnungseinstellungen > E-Mail-Verteilerlisten**.

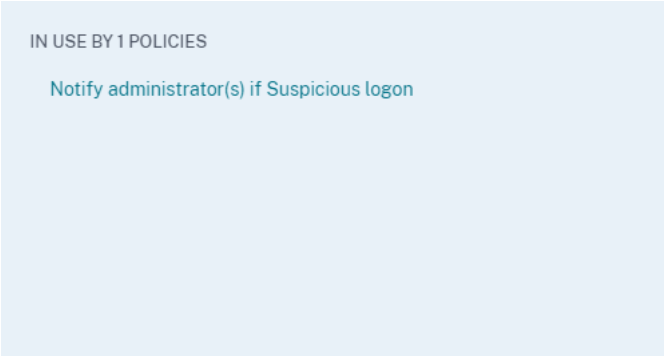
2. Klicken Sie auf die E-Mail-Verteilerliste, die Sie ändern möchten.
3. Aktualisieren Sie in der E-Mail-Verteilerliste die erforderlichen Details wie Name, Beschreibung und fügen Sie Mitglieder hinzu oder entfernen Sie sie.
4. Klicken Sie auf **Änderungen speichern**.

Löschen einer E-Mail-Verteilerliste

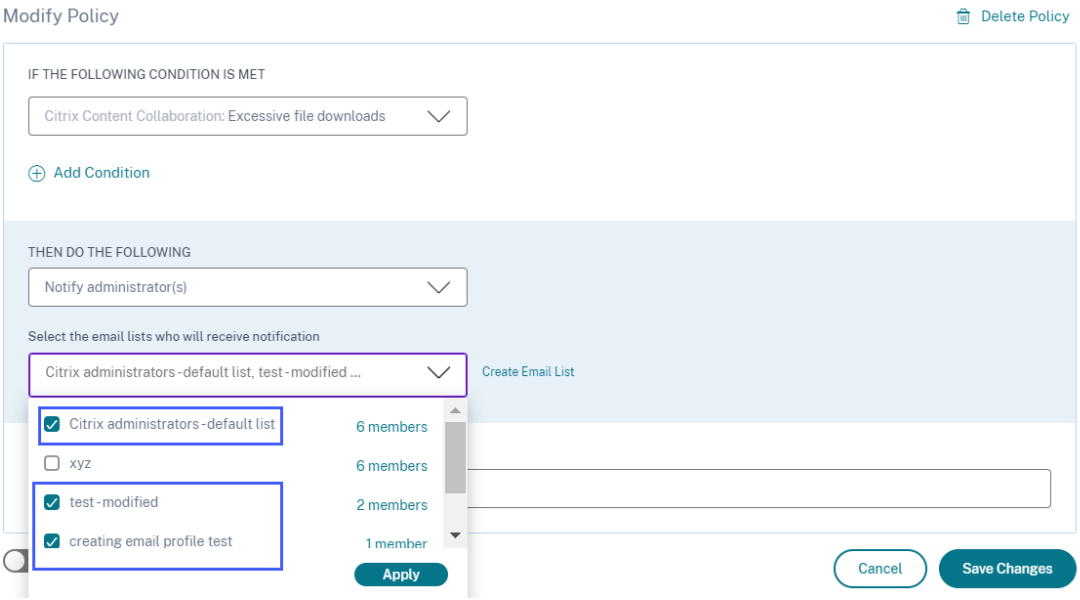
Sie können eine E-Mail-Verteilerliste nur löschen, wenn sie nicht mit Richtlinien verknüpft ist. Wenn es mit einigen Richtlinien verknüpft ist, müssen Sie zuerst die E-Mail-Verteilerliste aus den zugehörigen Richtlinien entfernen.

So löschen Sie eine E-Mail-Verteilerliste:

1. Klicken Sie auf **Einstellungen > Warnungseinstellungen > E-Mail-Verteilerlisten**.
2. Klicken Sie auf die E-Mail-Verteilerliste, die Sie löschen möchten.
3. Zeigen Sie in der E-Mail-Verteilerliste die zugehörigen Richtlinien an.



4. Klicken Sie auf die Richtlinie, um sie zu öffnen und die E-Mail-Verteilerlisten zu entfernen. Sie können die Richtlinie auch löschen, wenn Sie möchten.



5. Klicken Sie auf **Änderungen speichern** und kehren Sie zur E-Mail-Verteilerliste zurück.
6. Öffnen Sie die E-Mail-Verteilerliste und klicken Sie auf das Symbol **Löschen** .

Webhook für Alert-Benachrichtigungen

June 19, 2023

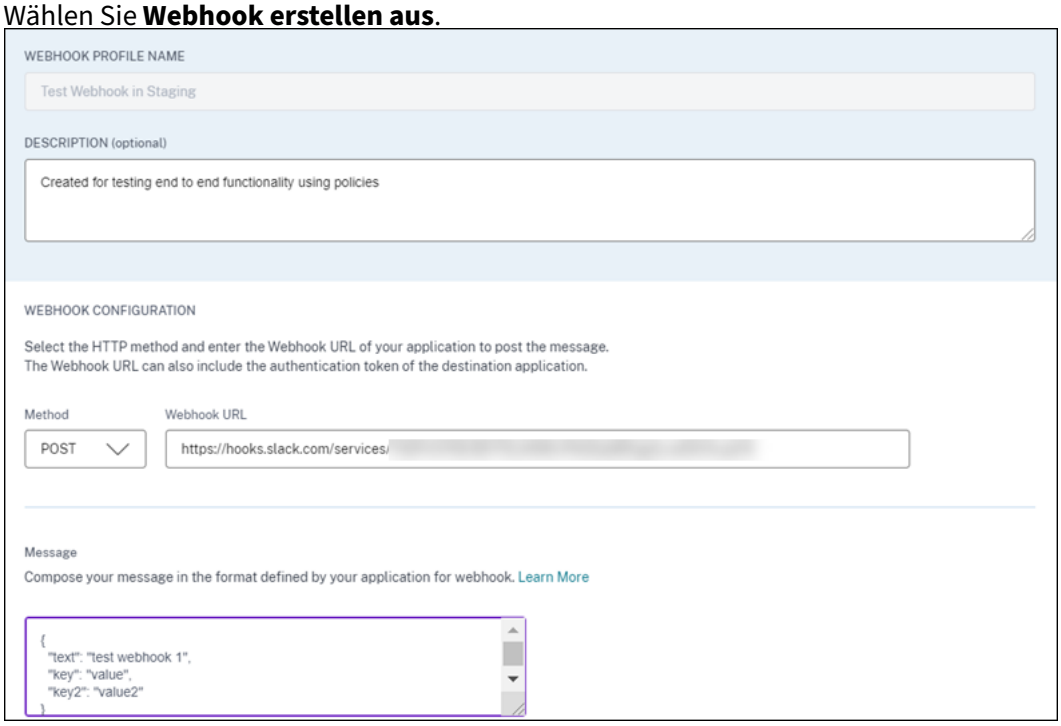
Sie können Webhooks verwenden, um Citrix Analytics-Warnbenachrichtigungen an alle Anwendungen von Drittanbietern zu senden, für die eingehende Webhook-URLs konfiguriert sind. Webhooks sind HTTP-Callbacks, die Echtzeitnachrichten zwischen den Dienstanbieteranwendungen und Verbraucheranwendungen ermöglichen. Da die Warnmeldungen in Echtzeit gesendet werden, werden Sie benachrichtigt, wenn die Ereignisse eintreten.

Wenn Citrix Analytics eine Warnung auslöst, sendet der zugehörige Webhook die Warnmeldung an die URL der Zielanwendung. Die Warnung wird in Form einer JSON-Nutzlast über die HTTP POST- oder PUT-Anforderung gesendet. Wenn ein Benutzer beispielsweise einen Risikoindikator auslöst oder die Leistung einer VDI-Maschine sinkt, können Sie einen Webhook einrichten, um die Warnbenachrichtigungen an Ihren Slack-Kanal zu senden.
Durch das Einrichten von Webhooks für das Alert-Management können Sie Benachrichtigungen in Echtzeit in Ihren Anwendungen erhalten. Sie können rechtzeitig Maßnahmen ergreifen, um das Sicherheitsrisiko zu verringern oder die Leistung Ihrer Citrix Virtual Apps and Desktops-Bereitstellung zu verbessern.

Webhook-Profil erstellen

So erstellen Sie die Webhook-Profile in Citrix Analytics:

1. Melden Sie sich bei Citrix Analytics an.
2. Klicken Sie je nach abonniertem Angebot auf **Verwalten**, um auf Security Analytics oder Performance Analytics zuzugreifen.
3. Klicken Sie in der oberen Leiste auf **Einstellungen > Warnungseinstellungen > Webhook**.
4. Wählen Sie **Webhook erstellen aus**.



5. Geben Sie einen Profilnamen und eine Beschreibung des Webhooks ein, um seinen Zweck zu identifizieren.
6. Wählen Sie die HTTP-Methode und die Webhook-URL Ihrer Anwendung aus, um die Warnmeldung zu senden.

> **Hinweis:**
> Normalerweise werden die ausgehenden Webhooks über die HTTP POST-Anforderung gesendet. Sie können auch ein Authentifizierungstoken in die Webhook-URL Ihrer Anwendung aufnehmen.

7. Geben Sie die Nachricht über die Warnung ein, die Sie an die Webhook-URL senden möchten. Die Nachricht muss in den von der Zielanwendung definierten Formaten wie JSON oder XML strukturiert sein. Weitere Informationen finden Sie in den Webhook-Beispielen.

8. (Optional) Geben Sie die Header-Schlüssel und -Werte für die Nachricht ein. Der Header kann Authentifizierungstoken oder andere benutzerdefinierte Schlüssel-Wert-Paare enthalten, um die Nutzlast sicher an Ihre Anwendung zu senden.
9. Um die Webhook-Konfiguration zu überprüfen, klicken Sie auf **Test**.
   Der Test validiert die ausgehende Webhook-URL, die Payload-Struktur und die Header-Schlüssel. Wenn in Ihrer Konfiguration keine Probleme gefunden werden, erhalten Sie die Meldung "Test erfolgreich".

Beispiele für Webhook-Konfigurationen

Der Abschnitt enthält Beispiele für die Konfiguration von Webhooks, um Warnungen an Anwendungen von Drittanbietern wie Slack und Microsoft Teams zu senden.

> **Hinweis:**
> Informationen zum Abrufen der Webhook-URL und der erforderlichen Konfigurationen für den Webhook finden Sie in der Produktdokumentation der Drittanbieteranwendungen.

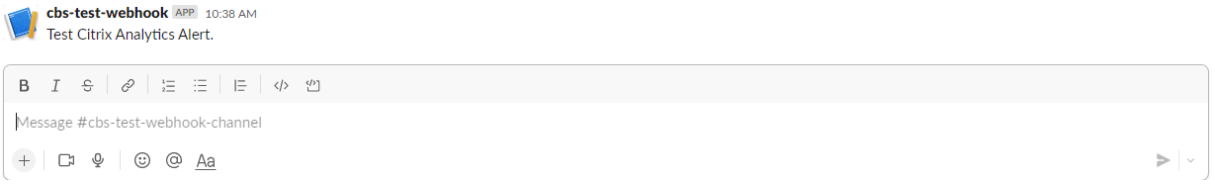
Warnmeldung an Slack senden

Stelle sicher, dass du in Slack die folgenden Aufgaben erledigt hast, bevor du eine Benachrichtigung sendest:

1. Erstellen Sie eine Slack-App für Citrix Analytics, falls Sie noch keine haben.
2. Aktivieren Sie für die App die Funktion Eingehender Webhook und erstellen Sie einen eingehenden Webhook.
3. Wählen Sie einen Kanal aus, in dem die App die Nachricht veröffentlicht.
4. Wenn Sie die App autorisieren, erhalten Sie die Webhook-URL zum Senden der Nachricht.
   Weitere Informationen finden Sie unter Erste Schritte mit eingehenden Webhooks.

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

Ausgabe



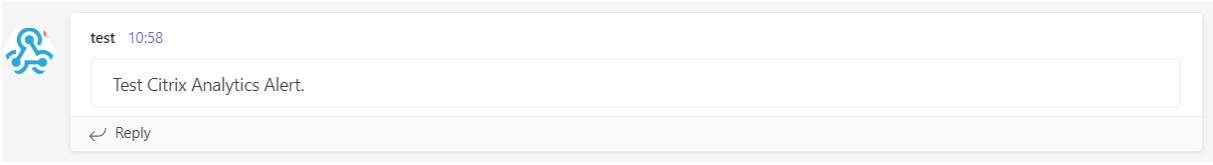
Warnmeldung an Microsoft Teams senden

Stellen Sie in Microsoft Teams sicher, dass Sie die folgenden Aufgaben ausgeführt haben, bevor Sie eine Warnung senden:

1. Erstellen Sie eine Teams-Gruppe innerhalb von Teams, falls Sie noch keine haben.
2. Erstellen Sie einen Webhook-Connector. Weitere Informationen finden Sie in den Schritten, die im Artikel Erstellen und Senden von Nachrichten beschrieben werden.
3. Holen Sie sich die URL für den Webhook.

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

Ausgabe



Citrix Analytics für Sicherheit (Sicherheitsanalysen)

February 9, 2024

Mit dem Vorteil, von überall, zu jeder Zeit und auf jedem Gerät in jedem Netzwerk aus zu arbeiten, werden sensible Unternehmensdaten stärker offengelegt als wenn Benutzer nur von einer isolierten Unternehmenszentrale aus arbeiten. Böswillige Benutzer haben eine große Angriffsfläche zum Ziel. IT-Teams sind beauftragt, eine hervorragende Benutzererfahrung zu bieten, ohne die Sicherheit zu beeinträchtigen. Citrix Analytics for Security kann helfen, diese Lücke zu schließen, wobei der Schwerpunkt auf Benutzersicherheit liegt.

Was ist Sicherheitsanalysen?

Citrix Analytics for Security bewertet kontinuierlich das Verhalten von Benutzern von Citrix Virtual Apps and Desktops, Benutzern von Citrix DaaS (früher Citrix Virtual Apps and Desktops Service) und Citrix Workspace-Benutzern. Es wendet Maßnahmen zum Schutz sensibler Unternehmensinformationen an. Die Aggregation und Korrelation von Daten über Netzwerke, virtualisierte Anwendungen

und Desktop-Tools hinweg ermöglicht die Generierung wertvoller Erkenntnisse und gezielterer Maßnahmen zur Bekämpfung von Sicherheitsbedrohungen für Benutzer. Machine Learning unterstützt außerdem hochgradig prädiktive Ansätze zur Identifizierung böswilliger Benutzerverhalten.

Features

- Optimierte Erkenntnisse aus allen Citrix Produkten und Partnerintegrationen. Weitere Informationen finden Sie unter Self-Service-Suche.
- Einfach zu verwendende Dashboards bieten einen vollständigen Überblick über das Benutzerverhalten. Weitere Informationen finden Sie unter Benutzer-Dashboard.
- Erkennen und mindern Sie bösartiges Benutzerverhalten mithilfe von maschinellem Lernen und angepassten Richtlinien mit automatisierten Aktionen. Weitere Informationen finden Sie unter Richtlinien und Aktionen.
- Die kontinuierliche Überwachung des Benutzerverhaltens nach der ersten Authentifizierung gegenüber Unternehmensnetzwerken bietet umfassende Sicherheit und hervorragende Benutzererfahrung. Weitere Informationen finden Sie unter Fortlaufende Risikobewertung.

Dashboards

Details zum Verhalten von Benutzern oder Entitäten können Sie auf den folgenden Sicherheits-Dashboards anzeigen:

- Benutzer: Bietet Einblick in die Verhaltensmuster von Benutzern innerhalb einer Organisation.
- Benutzerzugriff: Fasst die Anzahl der riskanten Domänen zusammen, auf die zugegriffen wurde, und das Datenvolumen, das von den Benutzern in Ihrem Netzwerk hochgeladen und heruntergeladen wurde.

- App-Zugriff: Fasst die Details der Domänen, URLs und Apps zusammen, auf die Benutzer in Ihrem Netzwerk zugreifen.
- Access Assurance Location: Fasst die Zugriffsdetails und Anmeldedetails der Benutzer von Citrix Virtual Apps and Desktops und Citrix DaaS-Benutzern zusammen.
- Berichte: Erstellen Sie benutzerdefinierte Berichte basierend auf den Dimensionen und Metriken, die aus den eingebundenen Datenquellen verfügbar sind.

Nächste Schritte

- Systemanforderungen: Mindestanforderungen, die erfüllt sein müssen, bevor Sie beginnen.
- Datenquellen: Informieren Sie sich über die Produkte, die Analytics unterstützt.
- Data Governance: Wissen über die Erfassung, Speicherung und Aufbewahrung von Protokollen durch Analytics.
- Erste Schritte: So verwenden Sie Analytics in Ihrer Organisation.

Citrix Analytics for Performance (Leistungsanalyse)

September 22, 2023

Was ist Performance Analytics

Performance Analytics ist ein Citrix Analytics-Angebot, mit dem Sie wichtige Leistungsindikatoren Ihrer Apps- und Desktops-Umgebung verfolgen, aggregieren und visualisieren können.

- Performance Analytics fasst Leistungsmetriken der Website in einfach zu betrachtenden Dashboards für Benutzererlebnis und Infrastruktur zusammen. Mithilfe der Dashboards können Sie die Benutzererfahrung analysieren und die Nutzung Ihrer Apps- und Desktops-Websites optimieren.
- Performance Analytics unterstützt die Aggregation und Berichterstellung an mehreren Standorten. Es aggregiert Leistungsmetriken in Ihrer Cloud und in on-premises Setups. Daher können Sie Daten für alle Sites in Ihrer Umgebung auf einer einzigen Konsole anzeigen.
- Performance Analytics quantifiziert die Leistungsfaktoren der Benutzer und klassifiziert die Benutzer anhand dieser Faktoren. Es bietet umsetzbare Erkenntnisse zur Behebung von Fehlern, Bildschirmverzögerungen, verzögerten Sitzungsanmeldungen und anderen Leistungsindikatoren.

- Mit Performance Analytics können Sie Metriken suchen und filtern, um sie auf bestimmte Benutzer oder Sitzungen einzugrenzen, die mit Leistungsproblemen konfrontiert sind.

So verwenden Sie Performance Analytics

Benutzererlebnis-Dashboard

Das User Experience Dashboard zeigt die Leistung der Website in Bezug auf Faktoren wie die Reaktionsfähigkeit der Sitzung, die Dauer der Sitzungsanmeldung, Sitzungsfehler und Wiederverbindungen von Sitzungen an, die zusammen die Benutzererfahrung definieren.

Wenn Sie mehrere Benutzer virtueller Apps und Desktops in Ihrem Unternehmen unterstützen und gelegentlich Verzögerungen beim Starten von Apps oder Desktops auftreten, kann Ihnen die Metrik für die Anmeldedauer Einblicke in das Problem geben. Drilldowns können Ihnen helfen, die Faktoren zu identifizieren, die zu den Problemen führen.

Infrastruktur-Dashboard

Das Infrastruktur-Dashboard zeigt den Status und den Zustand der Computer an Ihrem Standort an. Bei gemeinsamer Verwendung können die Benutzer- und Infrastruktur-Dashboards Ihnen helfen, die Verfügbarkeit von Ressourcen proaktiv zu überprüfen und Leistungsengpässe auf den Websites zu identifizieren.

- Wenn Benutzer- oder Sitzungstrends einen Rückgang aufweisen, was auf eine Verringerung der Anzahl der auf der Site angemeldeten Benutzer oder Sitzungen hinweist, verwenden Sie diesen Indikator, um zu überprüfen, ob ein Hypervisor neu gestartet wurde oder die Anzahl der Computer nicht ausreicht.
- Wenn Sie mehrere Fälle sehen, in denen Sitzungen nicht gestartet werden, können Sie einen Drilldown durchführen, um die Ursache für den Fehler zu ermitteln. Es kann zu einem Mangel an Lizenzen oder Problemen bei der Verbindung der Maschine zum Delivery Controller kommen.

> **Hinweis:**
>
> Das**Infrastructure Analytics Dashboard** befindet sich derzeit in der Vorschau.

Mithilfe von Performance Analytics können Sie Probleme schnell analysieren, Fehler beheben und beheben sowie ein optimales Serviceniveau für Apps und Desktops aufrechterhalten.

Erste Schritte

Voraussetzungen

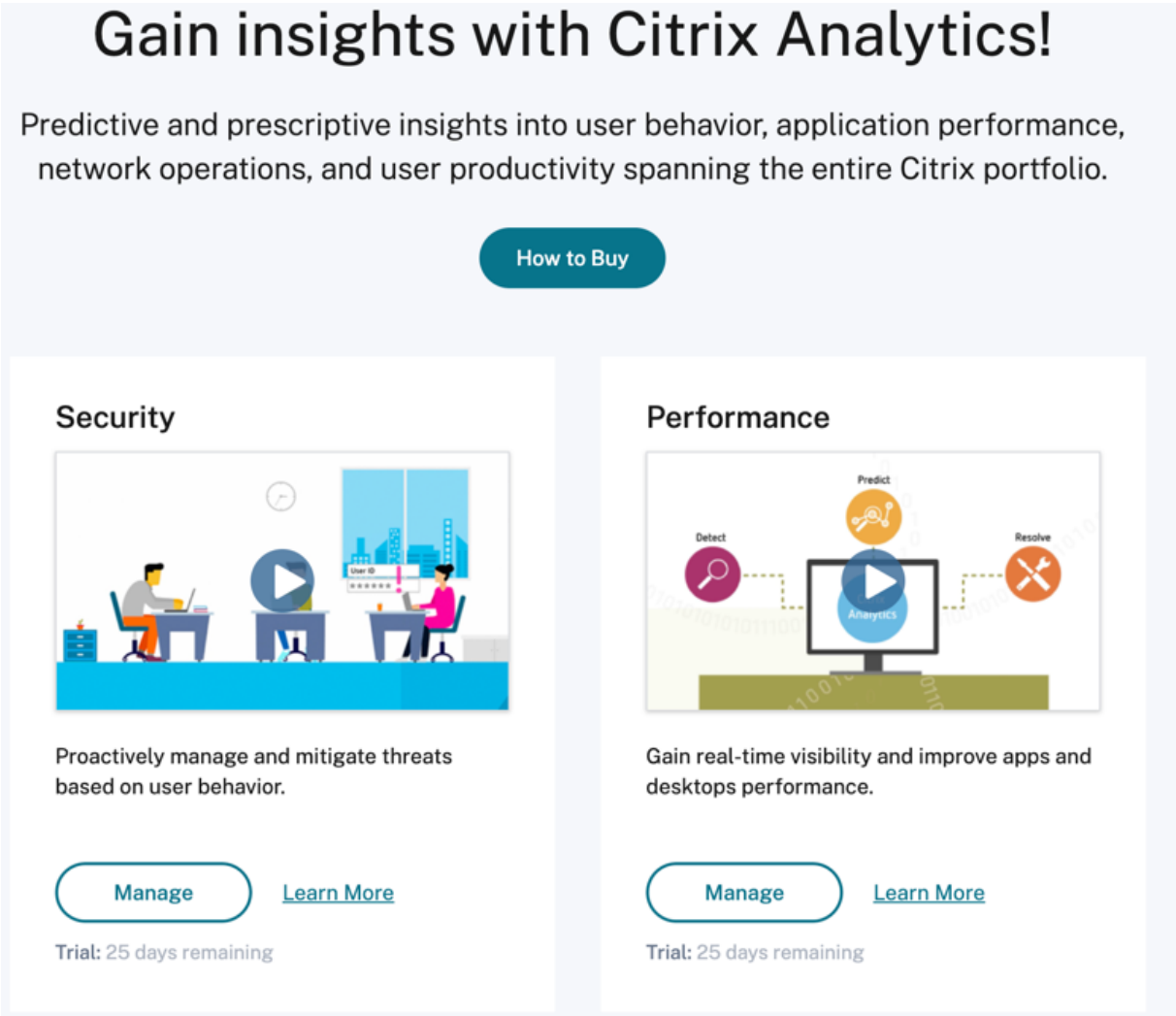
1. Prüfen Sie, ob Ihre Workstation über einen unterstützten Webbrowser verfügt, der im Artikel Unterstützte Browser aufgeführt ist. Informationen zu den Systemanforderungen finden Sie im Artikel Citrix Analytics Systemanforderungen .
2. Sie müssen über ein Citrix Cloud-Konto verfügen, um den Analytics-Dienst verwenden zu können. Ausführliche Anweisungen zum Erstellen eines Citrix Cloud-Kontos finden Sie unter Anmelden für Citrix Cloud. Gehen Sie zu https://citrix.cloud.com und melden Sie sich mit Ihrem Citrix Cloud-Konto an.
3. Citrix Analytics for Performance ist als abonnementbasiertes Angebot erhältlich, entweder als eigenständiges Angebot oder zusammen mit Citrix Analytics for Security gebündelt. Informationen zum Abonnieren von Citrix Analytics für Leistung finden Sie unter `https://www.citrix.com/products/citrix-analytics-performance.html)`.
4. Unterstützte Versionen von Datenquellen sind im Artikel Datenquellen verfügbar.
5. Citrix Profile Management muss auf allen Computern installiert sein.
6. Der End User Experience Monitoring (EUEM) -Dienst muss ausgeführt werden und die entsprechenden Richtlinien müssen auf allen Computern konfiguriert werden. Weitere Einzelheiten finden Sie unter Richtlinieneinstellungen für die Endbenutzer-Überwachung.
7. Die Richtlinie zur **VDA-Datenerfassung für Performance Analytics** muss auf Maschinen auf **Zulässig** festgelegt sein, damit der Überwachungsdienst maschinenbezogene Leistungsmetriken wie Bandbreiten- und Latenzstatistiken erfassen kann. Weitere Informationen finden Sie unter Richtlinien zum Sammeln von Daten für Performance Analytics.
8. Aktivieren Sie die Prozessüberwachungsrichtlinie von Citrix Studio, um auf der Registerkarte **Maschinenstatistiken > Prozess** einen Überblick über die Prozesse mit hohem Ressourcenverbrauch zu erhalten.
   Weitere Informationen finden Sie unter Prozessüberwachung aktivieren.
9. Stellen Sie sicher, dass von allen Endpunkten (oder Proxys, sofern diese konfiguriert sind) auf die folgenden URLs zugreifen können:

Endpunkt	Region der Vereinigten Staaten	Region der Europäischen Union	Asien-Pazifik Süd
Citrix Schlüsselregistrierung	`https://trust.citrixnetworkapi.net`	`https://trust.citrixnetworkapi.net`	`https://trust.citrixnetworkapi.net`

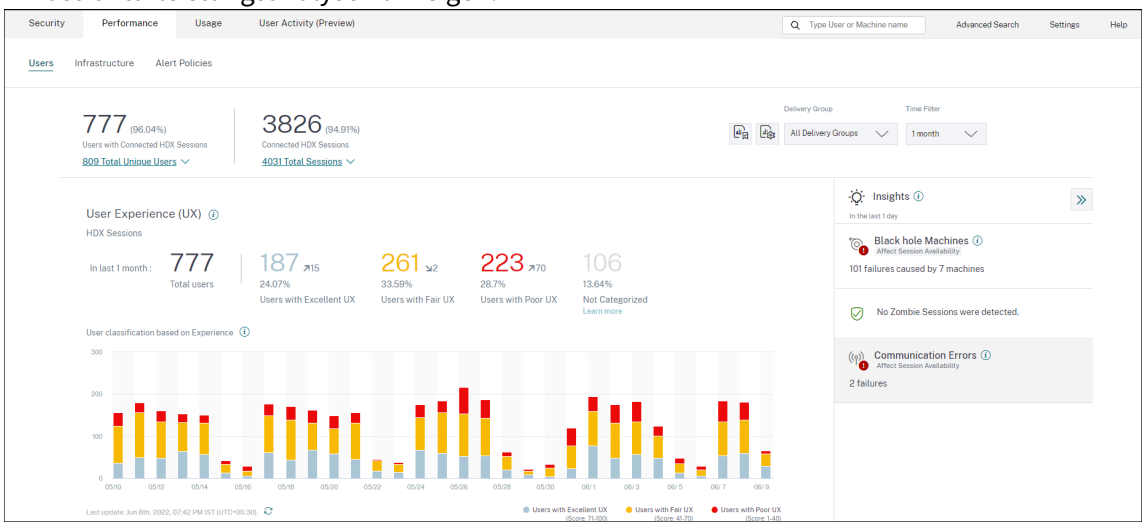
Endpunkt	Region der Vereinigten Staaten	Region der Europäischen Union	Asien-Pazifik Süd
Citrix Cloud	https://trust.citrixworkspacesapi.net	https://trust-eu.citrixworkspacesapi.net	https://trust-aps.citrixworkspacesapi.net
Citrix Analytics	https://api.was.cloud.com	https://api-eu.was.cloud.com	https://api-aps.was.cloud.com
Bulk-Upload	https://citrixanalyticseh-alias.servicebus.windows.net/	https://citrixanalyticsehec-alias.servicebus.windows.net/	https://citrixanalyticsehaps-alias.servicebus.windows.net/

Zugriff

1. Melden Sie sich bei Citrix Cloud an. Suchen Sie nach der Kachel Analytics Service und klicken Sie auf **Verwalten** Auf der Übersichtsseite werden die im Analytics-Portfolio verfügbaren Angebote angezeigt.
2. Klicken Sie im **Leistungsangebot** auf Testversion **anfordern**, um die Testversion des Angebots zu verwenden. Wenn Sie das Angebot von Citrix Analytics for Performance gekauft haben, klicken Sie stattdessen auf den Link **Verwalten** .



1. Citrix Analytics for Performance wird mit Dashboards geöffnet, die die Benutzererfahrungs- und Infrastrukturleistungsanalysen anzeigen.



Zugang von der Region Asien-Pazifik Süd Citrix Analytics for Performance ist jetzt automatisch für Testkunden und abonnementbasierte Kunden in der Region Asien-Pazifik-Süd (APS) integriert. Weitere Informationen zu den in Citrix Cloud unterstützten Regionen finden Sie unter Geografische Überlegungen.

Um von der APS-Region aus auf Performance Analytics zuzugreifen, wählen Sie die Region Asien-Pazifik Süd aus, während Sie Ihren Mandanten in Citrix Cloud integrieren. Melden Sie sich bei Citrix Cloud an und wählen Sie Ihren Mandanten in der APS-Region von Citrix Cloud aus. Verwenden Sie die URL `https://analytics-aps.cloud.com`, um auf Ihren Citrix Analytics Cloud Service zuzugreifen.

- Citrix Analytics for Performance speichert jetzt die Benutzerereignisse und Metadaten Ihrer Organisation in der Region Asien-Pazifik-Süd, wenn Sie sie als Ihre Heimatregion auswählen. Weitere Informationen finden Sie unter Data Governance.
- Informationen zu den Netzwerkanforderungen für die Region Asien-Pazifik Süd finden Sie unter Technische Sicherheit —Überblick.

Konfigurieren von Datenquellen

Sie können Performance Analytics verwenden, um on-premises oder Cloud-Sites zu überwachen. Sie können dieses Angebot unabhängig davon nutzen, ob Sie ein reiner On-Premise-Kunde, ein Cloud-Kunde oder ein Hybridkunde mit einer Mischung aus On-Premises- und Cloud-Sites sind.

Performance Analytics erkennt Ihren Citrix DaaS (früher Citrix Virtual Apps and Desktops Service) automatisch.
Wenn Sie ein On-Premise-Kunde sind,

- Integrieren Sie zuerst Ihre Citrix Virtual Apps and Desktops Sites in Performance Analytics.
- Um netzwerkbezogene Informationen zu Performance Analytics abzurufen, müssen Sie auch Ihr lokales NetScaler Gateway einbauen.

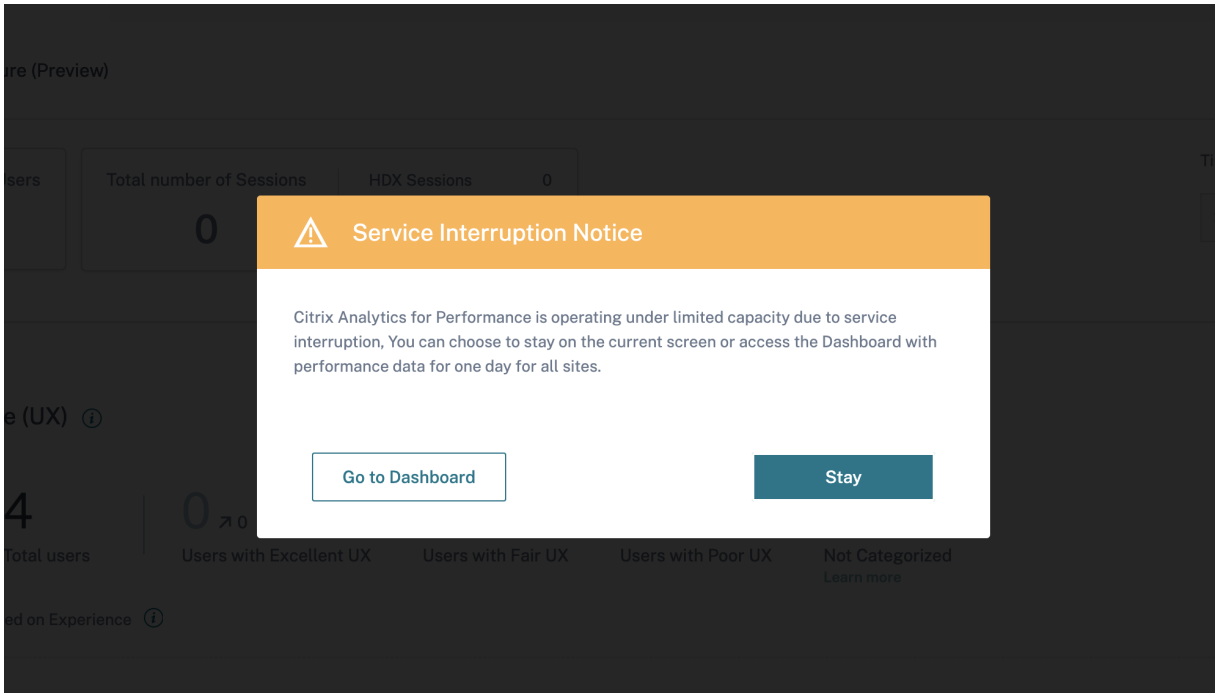
Konfigurieren Sie die erforderlichen Datenquellen wie im Artikel Datenquellen beschrieben.

> **Hinweis:**
>
> - Citrix Analytics for Performance sammelt und speichert Protokolle für Datenpunkte, wie in Protokolle für Citrix Analytics for Performanceaufgeführt.
> - Empfohlene Grenzwerte für den Dienst Citrix Analytics for Performance sind im Artikel Grenzwerte aufgeführt.

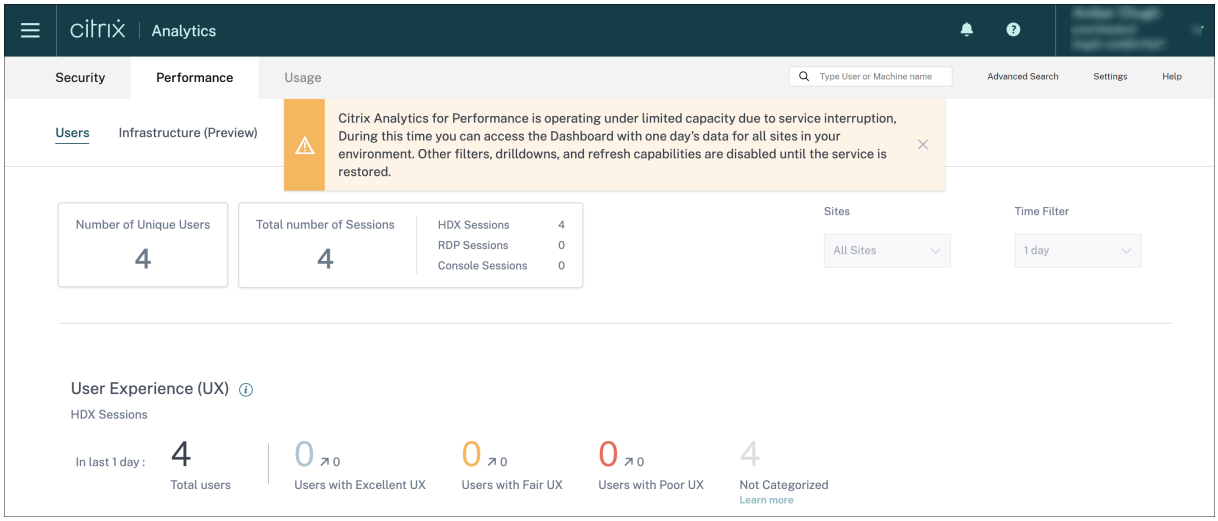
Servicekontinuität

Im Falle einer Dienstunterbrechung arbeitet Citrix Analytics for Performance mit einer begrenzten Kapazität.

Der Administrator kann wählen, ob er **bleiben** und die auf dem aktuellen Bildschirm verfügbaren Daten anzeigen oder in einem herabgestuften Modus **zum Dashboard gehen soll** .



Im herabgestuften Modus wird der Benutzer auf das Dashboard umgestellt, das Daten aller Websites für den letzten Tag enthält.
Alle Filter und Drilldowns werden deaktiviert, bis der Dienst in beiden Fällen wieder in den normalen Betrieb versetzt wird.



Dieses Update verbessert die Ausfallsicherheit des Produkts und hilft bei der Anpassung an das Service Level Agreement.

Problembehandlung bei Citrix Analytics für Sicherheit und Leistung

December 12, 2023

In diesem Abschnitt wird erläutert, wie Sie die folgenden Probleme beheben können, die bei der Verwendung von Citrix Analytics for Security auftreten können.

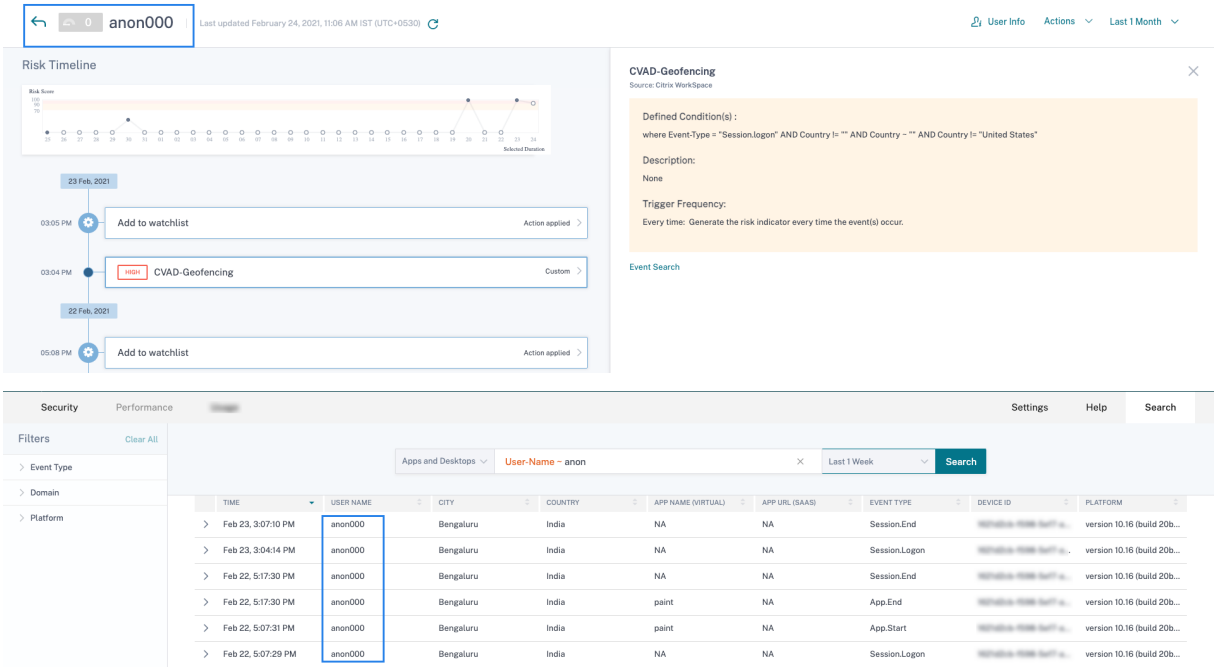
- Überprüfen Sie anonyme Benutzer als legitime Benutzer.
- Beheben Sie Probleme mit der Ereignisübertragung aus einer Datenquelle.
- Lösen Sie Virtual Apps and Desktops Desktop-Ereignisse, SaaS-Ereignisse aus und überprüfen Sie die Ereignisübertragung an Citrix Analytics for Security.
- DerSitzungsaufzeichnungsserver kann keine Verbindung herstellen.
- Konfigurationsprobleme mit dem Citrix Analytics-Add-On für Splunk

Überprüfen Sie die anonymen Benutzer als legitime Benutzer

August 19, 2022

Als Administrator stellen Sie möglicherweise fest, dass einige Citrix Virtual Apps and Desktops -Benutzer und Citrix DaaS-Benutzer (früher Citrix Virtual Apps and Desktops Service) in Citrix Analytics for Security als anonym angezeigt werden. Diese Benutzer werden als erkannte Benutzer identifiziert. Ihre Benutzernamen erscheinen jedoch als anonXYZ (wobei "XYZ"eine dreistellige Zahl darstellt) auf den folgenden Seiten:

- Benutzer
- Zeitleiste des Nutzers
- Riskante Benutzer
- Self-Service-Suche nach der Datenquelle Apps und Desktops



Wenn Sie solche Benutzer sehen, möchten Sie möglicherweise Folgendes wissen:

- Wer sind diese Benutzer?
- Sind diese Benutzer legitim oder böswillig?
- Wie überprüfe ich sie?
- Welche Aktionen muss ich für diese Benutzer anwenden?

In den folgenden Szenarien sehen Sie anonyme Benutzer in Ihrer Citrix IT-Umgebung:

- Wenn ein Benutzer eine veröffentlichte sichere Browser-App verwendet
- Wenn ein Benutzer einen nicht authentifizierten Store verwendet

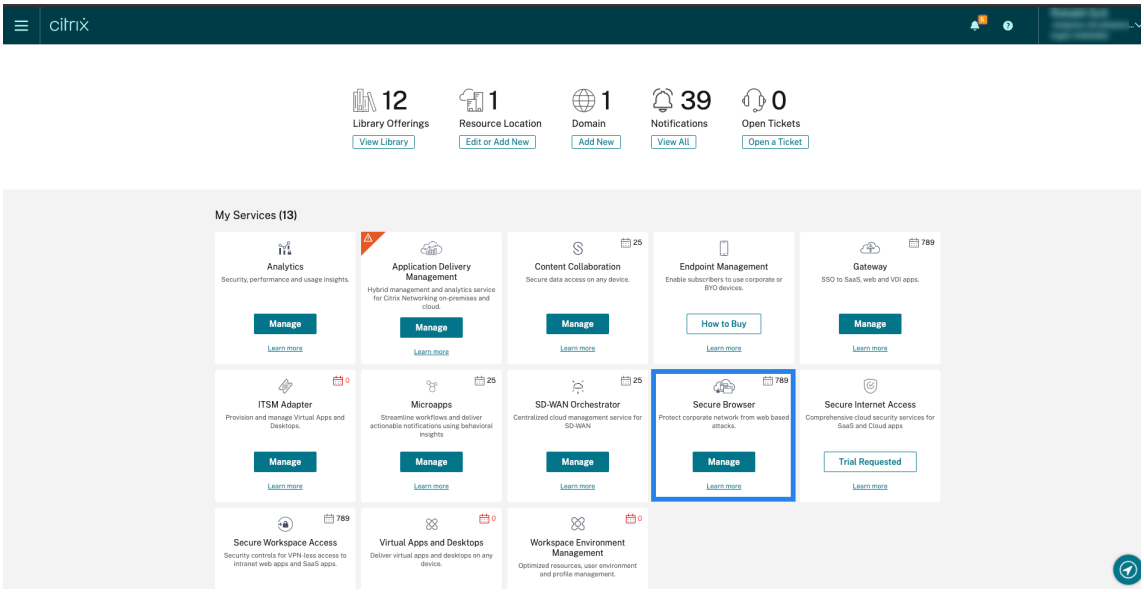
Benutzer verwendet veröffentlichte sichere Browser-Apps

Die sicheren Browser-Apps sind Web-Apps, die mit dem Citrix Secure Browser Service veröffentlicht werden. Diese Apps isolieren Ihre Webbrowser-Ereignisse und schützen Ihr Unternehmensnetzwerk vor browserbasierten Angriffen. Weitere Informationen finden Sie unter Secure Browser Service.

Die sicheren Browser-Apps verwenden die anonyme Sitzungsfunktion von Citrix DaaS.

So überprüfen Sie, ob Secure Browser in Ihrem Citrix Cloud-Konto konfiguriert ist:

1. Melden Sie sich bei Citrix Cloud an.
2. Klicken Sie auf der **Secure Browser**-Karte auf **Verwalten**.



3. Suchen Sie auf der Seite **Verwalten** nach veröffentlichten sicheren Browser-Apps.

Wenn ein Benutzer über Citrix Receiver für Websites über einen Webbrowser auf einen StoreFront-Store zugreift und die veröffentlichten sicheren Browser-Apps verwendet, ist die Identität des Benutzers ausgeblendet. Daher zeigt Citrix Analytics den Benutzer als anonym an.

Wenn ein Benutzer über eine Citrix Receiver- oder Citrix Workspace-App auf einen StoreFront-Store zugreift, die auf seinem Gerät installiert ist und die veröffentlichten sicheren Browser-Apps verwendet, zeigt Citrix Analytics den Benutzer als den im StoreFront angegebenen Benutzernamen an.

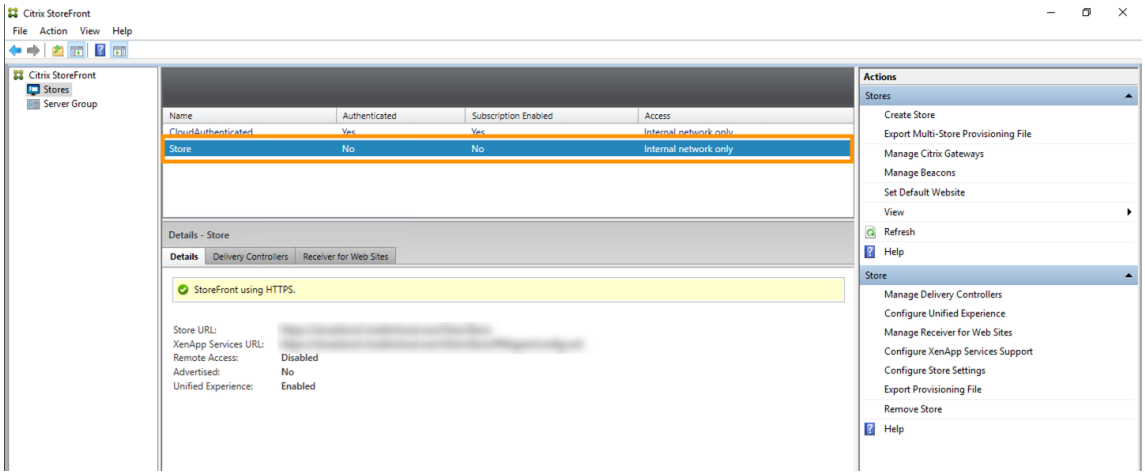
Sie können den Benutzer also als legitimen Benutzer Ihrer Organisation betrachten. Sie müssen keine Aktion anwenden, wenn dem Benutzer kein riskantes Verhalten zugeordnet ist.

Benutzer, der einen nicht authentifizierten Store verwendet

Der nicht authentifizierte Store ist eine Funktion von Citrix StoreFront und gilt für die Stores, die vom Kunden verwaltet werden. Diese Funktion unterstützt den Zugriff für nicht authentifizierte (anonyme) Benutzer.

So überprüfen Sie, ob Ihre Organisation über einen nicht authentifizierten Store verfügt:

1. Starten Sie Citrix Studio.
2. Klicken Sie auf **Stores**.
3. Überprüfen Sie für Ihre Geschäfte den Authentifizierungsstatus in der Spalte Authentifiziert.



Wenn ein Geschäft nicht authentifiziert ist und der Benutzer auf diesen nicht authentifizierten Speicher zugreift, bleibt die Benutzeridentität anonym. Daher zeigt Citrix Analytics den Benutzer als anonym an. Sie können diesen Benutzer als legitimen Benutzer Ihrer Organisation betrachten. Sie müssen keine Aktion anwenden, wenn dem Benutzer kein riskantes Verhalten zugeordnet ist.

Probleme mit der Ereignisübertragung aus einer Datenquelle beheben

April 12, 2024

Dieser Abschnitt hilft Ihnen bei der Behebung von Datenübertragungsproblemen in Citrix Analytics for Security. Wenn eine Datenquelle Benutzerereignisse nicht korrekt überträgt, können Probleme wie die Nicht-Erkennung von Benutzern und Risikoindikatoren auftreten.

Checkliste

Sequenz	Schecks
1	Haben Sie die richtige Berechtigung, Security Analytics zu nutzen?
2	Wird die Datenquelle in Ihrer Heimatregion unterstützt?

Sequenz	Schecks
3	Erfüllt Ihre Umgebung alle Systemanforderungen?
4	Sind alle entdeckten Datenquellen und die Datenverarbeitung in Analytics aktiviert?
5	Übertragen die Benutzeraktivitäten auf der Datenquelle Ereignisse genau an Analytics?
6	Werden die Ereignisse der virtuellen Apps und Desktops an Analytics übertragen?
7	Werden die Benutzerereignisse auf der Self-Service-Suchseite in Analytics angezeigt?
8	Werden die Benutzer von Analytics entdeckt?

Test 1 —Haben Sie die richtige Berechtigung, Security Analytics zu verwenden?

Citrix Analytics for Security ist ein abonnementbasiertes Angebot. Weitere Informationen finden Sie unter Erste Schritte.

Test 2- Wird die Datenquelle in Ihrer Heimatregion unterstützt?

Citrix Analytics for Security wird in den folgenden Home-Regionen unterstützt:

- Vereinigte Staaten (US)
- Europäische Union (EU)
- Asien-Pazifik Süd (APS)

Je nach Standort Ihrer Organisation können Sie sich in einer der Heimatregionen bei Citrix Cloud einbinden.

Bestimmte Datenquellen werden jedoch nicht in allen Heimatregionen unterstützt. Die Datenquellen sind die Produkte, von denen Citrix Analytics for Security Benutzerereignisse empfängt.

Wenn Ihr Unternehmen in einer Heimatregion, in der eine Datenquelle nicht unterstützt wird, in Citrix Cloud integriert ist, erhalten Sie keine Benutzerereignisse von der Datenquelle.

Verwenden Sie die folgende Tabelle, um die Datenquellen und die Regionen anzuzeigen, in denen sie unterstützt werden.

Datenquelle	Unterstützt in der US-Region	Unterstützt in der EU-Region	In der APS-Region unterstützt
Citrix Endpoint Management	Ja	Ja	Ja
NetScaler Gateway (on-premises)	Ja	Ja	Ja
Citrix Identitätsanbieter	Ja	Ja	Ja
Citrix Secure Browser	Ja	Ja	Ja
Citrix Secure Private Access	Ja	Nein	Nein
Citrix DaaS (früher Citrix Virtual Apps and Desktops Service)	Ja	Ja	Ja
Citrix Virtual Apps and Desktops on-premises	Ja	Ja	Ja
Microsoft Active Directory	Ja	Ja	Ja
Microsoft Graph Security	Ja	Ja	Ja

Test 3- Erfüllt Ihre Umgebung alle Systemanforderungen?

Citrix Analytics kann einige Minuten benötigen, um die Benutzerereignisse aus den Datenquellen zu empfangen. Wenn auf den Sitekarten der Datenquelle keine Benutzerereignisse angezeigt werden, stellen Sie sicher, dass Ihre Umgebung die Voraussetzungen und Systemanforderungenerfüllt.

Voraussetzungen

1. Alle Ihre Citrix Cloud-Abonnements müssen aktiv sein. Stellen Sie auf der Citrix Cloud-Seite sicher, dass alle Citrix Cloud-Dienste aktiv sind.
2. Wenn Sie on-premises verwenden Citrix Virtual Apps and Desktops, müssen Sie Ihre Sites zu Citrix Workspace hinzufügen und die Site-Aggregation konfigurieren. Citrix Analytics erkennt automatisch die Sites, die Citrix Workspace hinzugefügt wurden. Weitere Informationen finden Sie unter Aggregieren on-premises virtueller Apps und Desktops in Arbeitsbereichen.
3. Wenn Sie eine StoreFront-Bereitstellung für Ihre Sites verwenden, konfigurieren Sie Ihre StoreFront-Server so, dass die Citrix Workspace-App Benutzerereignisse an Citrix Analytics

senden kann. Stellen Sie sicher, dass die StoreFront-Version 1906 oder höher ist. Wenn Sie den StoreFront-Server nicht konfigurieren, empfängt Citrix Analytics keine Benutzerereignisse von on-premises Citrix Virtual Apps and Desktops. Informationen zum Konfigurieren der StoreFront-Bereitstellung finden Sie im Citrix Analytics Service Analytics-Dienstartikel in der StoreFront-Dokumentation.

4. Die Citrix Virtual Apps and Desktops-Benutzer und Citrix DaaS-Benutzer müssen die angegebene Version der Citrix Workspace-Apps oder Citrix Receiver auf ihren Endpunkten verwenden. Andernfalls erhält Analytics die Benutzerereignisse nicht von den Benutzerendpunkten. Die Liste der unterstützten Versionen der Citrix Workspace-App oder Citrix Receiver ist in Citrix Virtual Apps and Desktops und der Citrix DaaS-Datenquelleverfügbar.
5. Um die Benutzerereignisse aus einer veröffentlichten Secure Browser-Sitzung zu empfangen, aktivieren Sie die Einstellung **Hostname Tracking** im Secure Browser. Diese Einstellung ist standardmäßig deaktiviert. Weitere Informationen finden Sie unter Verwalten veröffentlichter sicherer Browser.
6. Integrieren Sie Ihre Datenquellen wie in den folgenden Artikeln erwähnt:
   - Citrix Endpoint Management-Datenquelle
   - Citrix Gateway-Datenquelle
   - Citrix Secure Private Access-Datenquelle
   - Citrix Virtual Apps and Desktops und Citrix DaaS-Datenquelle
   - Microsoft Active Directory-Integration
   - Integration von Microsoft Graph Security

Test 4- Sind alle entdeckten Datenquellen und die Datenverarbeitung in Analytics aktiviert?

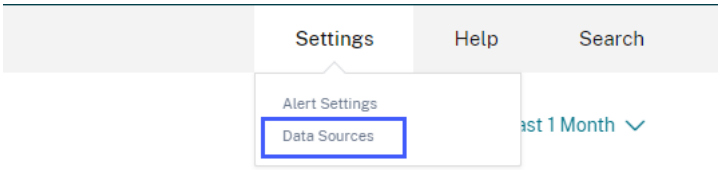
Stellen Sie sicher, dass alle Ihre Datenquellen erkannt werden und Sie die Datenverarbeitung für sie aktiviert haben. Wenn Sie die Datenverarbeitung für eine Datenquelle nicht aktivieren, werden die Benutzer, die die Datenquelle verwenden, nicht erkannt. Diese Situation könnte ein potenzielles Sicherheitsrisiko darstellen.

Durch die Aktivierung der Datenverarbeitung wird sichergestellt, dass Citrix Analytics Ihre Benutzerereignisse verarbeitet. Ereignisse werden nur an Citrix Analytics gesendet, wenn die Benutzer die Datenquelle aktiv verwenden.

> **Hinweis**
>
> Citrix Analytics zieht nicht aktiv Daten aus Ihrer Umgebung.

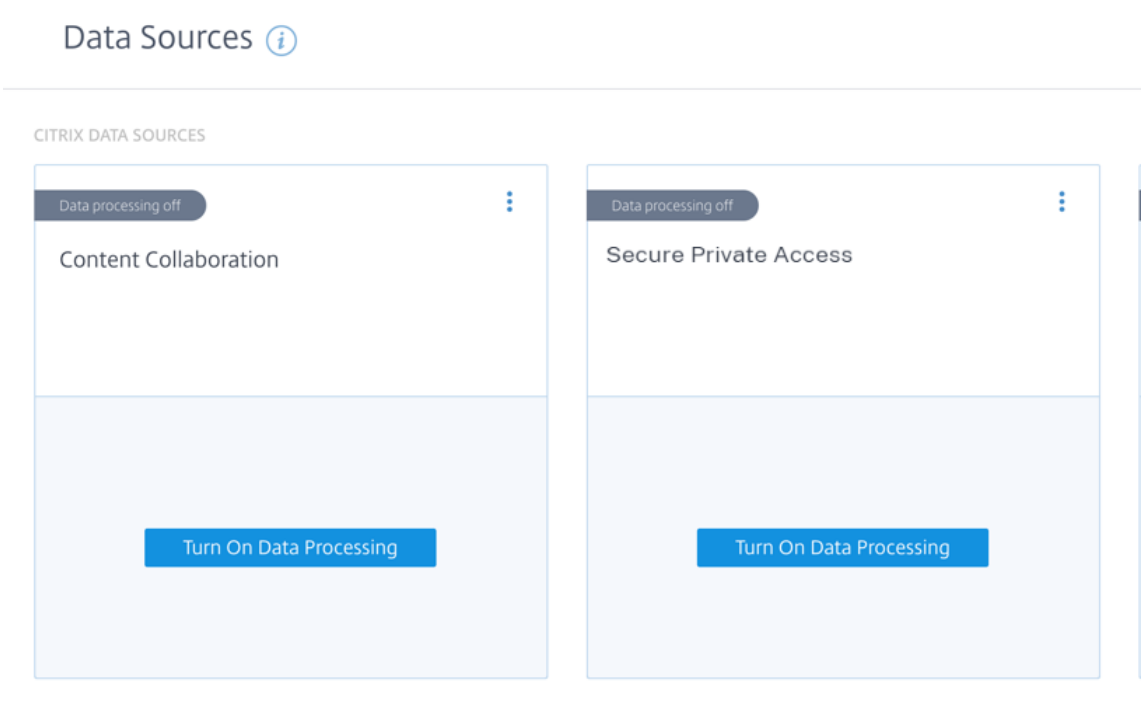
Gehen Sie wie folgt vor, um Ihre Datenquellen zu ermitteln und Analysen zu ermöglichen:

1. Klicken Sie auf **Einstellungen** > **Datenquellen** > **Sicherheit**, um die erkannten Datenquellen anzuzeigen. Citrix Analytics erkennt automatisch die Datenquellen, die Sie für Ihr Citrix Cloud-Konto abonniert haben.

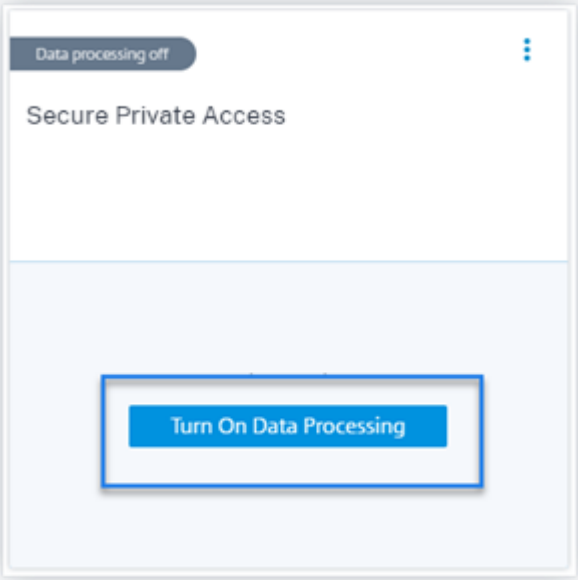


2. Auf der Seite **Datenquellen** werden die erkannten Datenquellen als Sitekarten angezeigt. Standardmäßig ist die Datenverarbeitung ausgeschaltet.

> **Wichtig**
>
> Citrix Analytics verarbeitet Ihre Daten, nachdem Sie Ihre Einwilligung erteilt haben.



3. Klicken Sie **auf der Sitekarte, für die Citrix Analytics Ereignisse verarbeiten soll, auf Datenverarbeitung einschalten** . Klicken Sie beispielsweise auf der Citrix Secure Private Access-Sitekarte auf **Datenverarbeitung einschalten**.



4. Nachdem Sie die Datenverarbeitung aktiviert haben, verarbeitet Citrix Analytics die Ereignisse für die Datenquelle. Der Status der Site Card ändert sich in Datenverarbeitung. Sie können die Anzahl der Benutzer und die empfangenen Ereignisse basierend auf dem ausgewählten Zeitraum anzeigen.

5. Befolgen Sie für alle erkannten Datenquellen die unter Erste Schritte angegebenen Schritte, um die Analyse zu aktivieren.

Test 5- Übertragen die Benutzeraktivitäten auf der Datenquelle Ereignisse genau an Analytics?

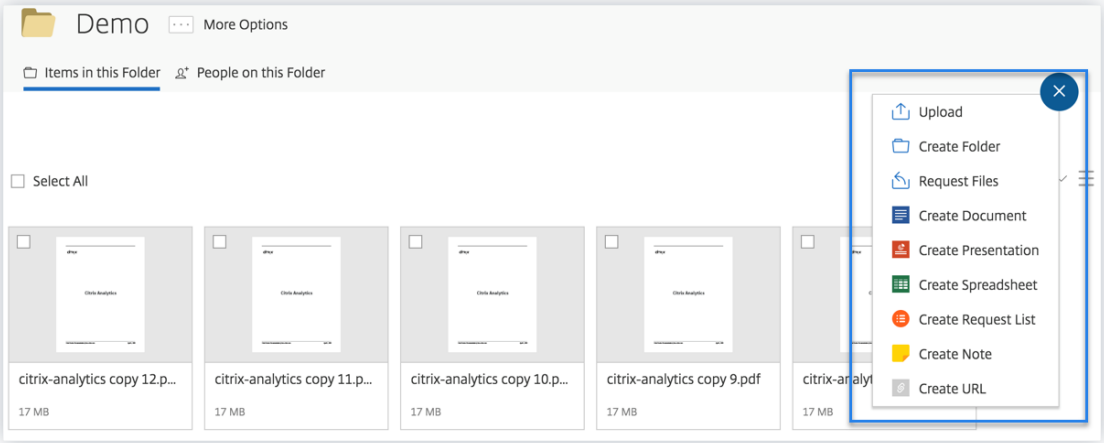
Citrix Analytics empfängt Benutzerereignisse aus den Datenquellen, wenn die Benutzer die Datenquellen aktiv verwenden. Die Benutzer müssen einige Aktivitäten an der Datenquelle ausführen, um Ereignisse zu generieren. Um beispielsweise Ereignisse aus der Apps and Desktops-Datenquelle zu empfangen, müssen die Apps and Desktops-Benutzer einige Dateien teilen, hochladen oder herunterladen.

> **Hinweis**
>
> Citrix Analytics zieht nicht aktiv Daten aus Ihrer Umgebung.

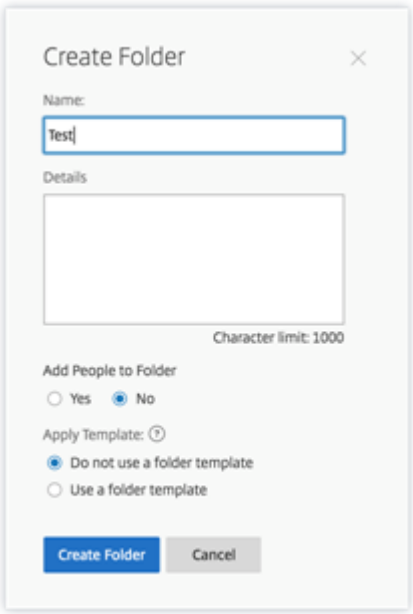
Wenn Sie in Citrix Analytics keine Benutzerereignisse für Ihre Datenquelle sehen, besteht eine hohe Wahrscheinlichkeit, dass die Benutzer zu diesem Zeitpunkt nicht aktiv sind.

Führen Sie die folgende Aktivität aus, um zu überprüfen, ob Citrix Analytics die Benutzerereignisse korrekt empfängt. Diese Aktivität verwendet die Citrix Apps and Desktops-Datenquelle. Sie können eine ähnliche Aktivität mit anderen Citrix Produkten (Datenquellen) basierend auf Ihrem Abonnement ausführen.

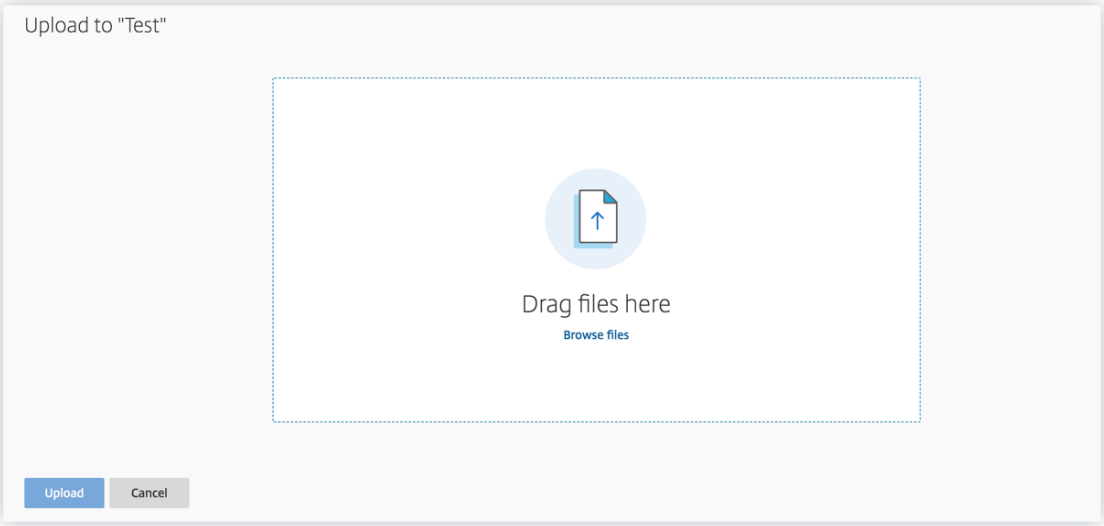
1. Melden Sie sich beim Citrix Apps and Desktops Service an.
2. Führen Sie einige übliche Benutzeraktivitäten aus, z. B. Ordner erstellen, Dateien herunterladen, Dateien hochladen oder Dateien löschen.



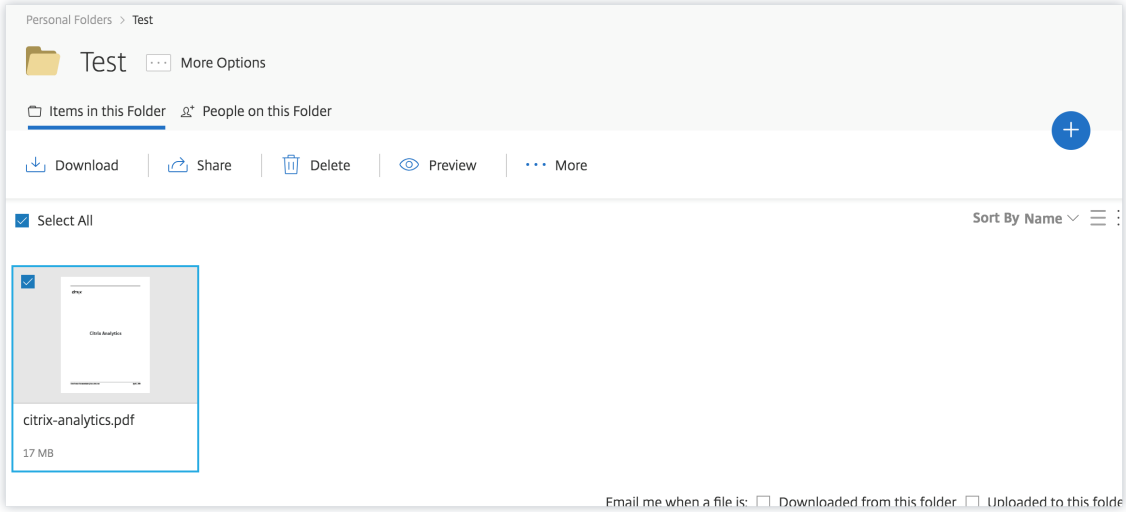
3. Erstellen Sie beispielsweise einen Testordner.



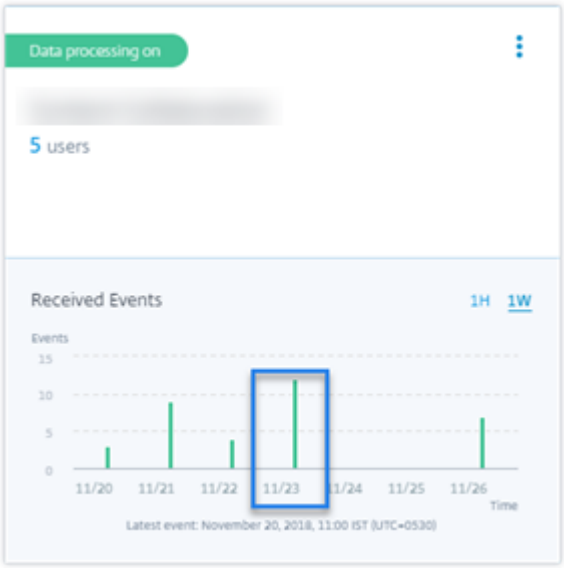
4. Laden Sie einige lokale Dateien hoch.



5. Löschen Sie einige Dateien im Ordner.



6. Kehren Sie zu Citrix Analytics zurück und sehen Sie sich die Seitenkarte **Apps and Desktops** auf der Datenquellenseite an. Citrix Analytics empfängt die Benutzerereignisse von der Apps and Desktops-Datenquelle und zeigt sie auf der Sitekarte an.



Test 6: Werden die Ereignisse der virtuellen Apps und Desktops an Analytics übertragen?

Einige Versionen der Citrix Workspace-App oder des Citrix Receiver-Clients senden Benutzerereignisse nicht an Citrix Analytics. Wenn Benutzer virtuelle Apps und Desktops über diese Clients starten, erkennt Citrix Analytics die Benutzer erst, wenn sie die unterstützten Ereignisse ausführen.

Beispielsweise sendet die Citrix Workspace-App für Linux 2006 oder höher die ***SaaS App Launch*** - und ***SaaS App End-Ereignisse*** nicht an Citrix Analytics. Ein Benutzer, der eine SaaS-App mit der Citrix Workspace-App für Linux startet, wird in Citrix Analytics nicht erkannt.

Unterstützte Ereignisse

In der folgenden Tabelle können Sie die Benutzerereignisse überprüfen, die von jeder Clientversion unterstützt werden.

- **Ja**—Das Ereignis wird vom Client an Citrix Analytics gesendet.
- **Nein**—Das Ereignis wird vom Client nicht an Citrix Analytics gesendet.
- **NA**—Das Ereignis gilt nicht für den Kunden.

Ereignis	Workspace-App für Windows 1907 oder höher	Workspace-App für Mac 1910.2 oder höher	Workspace-App für Linux 2006 oder höher	Arbeitsbereich-App für Android - Aktuelle Version in Google Play verfügbar	Workspace-App für iOS — neueste Version im Apple App Store verfügbar	Workspace-App für Chrome — Aktuelle Version im Chrome Web Store verfügbar	Workspace-App für HTML5 2007 oder höher
Konto Logon	Ja	Ja	Ja	Ja	Ja	Nein	Nein
Sitzungs-Anmeldung	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Sitzungsstart	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Ende der Sitzung	Ja	Ja	Ja	Ja	Ja	Ja	Ja
App-Start	Ja	Ja	Ja	Nein	Ja	Ja	Ja
App-Ende	Ja	Ja	Ja	Nein	Ja	Ja	Ja
Datei Herunter-laden	Ja	Ja	Ja	Nein	Nein	Ja	Ja
Drucken	Nein	Ja	Ja	Nein	Nein	Ja	Ja
SaaS App starten	Ja	Ja	Nein	Nein	Nein	Nein	Nein
SaaS App Ende	Ja	Ja	Nein	Nein	Nein	Nein	Nein

Ereignis	Workspace-App für Windows 1907 oder höher	Workspace-App für Mac 1910.2 oder höher	Workspace-App für Linux 2006 oder höher	Arbeitsbereich-App für Android - Aktuelle Version in Google Play verfügbar	Workspace-App für iOS — neueste Version im Apple App Store verfügbar	Workspace-App für Chrome — Aktuelle Version im Chrome Web Store verfügbar	Workspace-App für HTML5 2007 oder höher
SaaS App URL-Navigation	Ja	Ja	Nein	Nein	Nein	Nein	Nein
Zugriff auf SaaS App Zwischen-ablage	Ja	Ja	Nein	Nein	Nein	Nein	Nein
SaaS App Datei herunter-laden	Ja	Ja	Nein	Nein	Nein	Nein	Nein
SaaS App Datei drucken	Ja	Ja	Nein	Nein	Nein	Nein	Nein

Basierend auf dem Übertragungsstatus des Ereignisses können folgende Probleme auftreten:

- Wenn Benutzer eine Verbindung mit ihren Clients zu Citrix Virtual Apps and Desktops oder Citrix DaaS herstellen, werden die Benutzer möglicherweise erst in Citrix Analytics erkannt, wenn sie ein unterstütztes Ereignis (Aktivität) ausführen. Betrachten Sie beispielsweise zwei Benutzerereignisse - App Start und SaaS App Launch. Citrix Analytics, ein Benutzer, der die Citrix Workspace-App für iOS verwendet, empfängt das App Start-Ereignis, aber nicht das SaaS App Launch-Ereignis. Wenn der Benutzer also virtuelle Apps startet, wird das App Start-Ereignis an Citrix Analytics übertragen und der Benutzer wird erkannt. Wenn der Benutzer jedoch eine SaaS-App startet, erhält Citrix Analytics das SaaS App Launch-Ereignis nicht und der Benutzer wird nicht erkannt. Informationen zu entdeckten Benutzern finden Sie unter Entdeckte Benutzer.
- Ereignisse, die auf der Tabelle mit **Nein** gekennzeichnet sind, werden auf der Self-Service-

Suchseite nicht angezeigt. Informationen zur Verwendung der Self-Service-Seite finden Sie unter Informationen zur Self-Service-Suche.

Empfehlung

Um die maximalen Vorteile von Analytics zu nutzen, empfiehlt Citrix Folgendes:

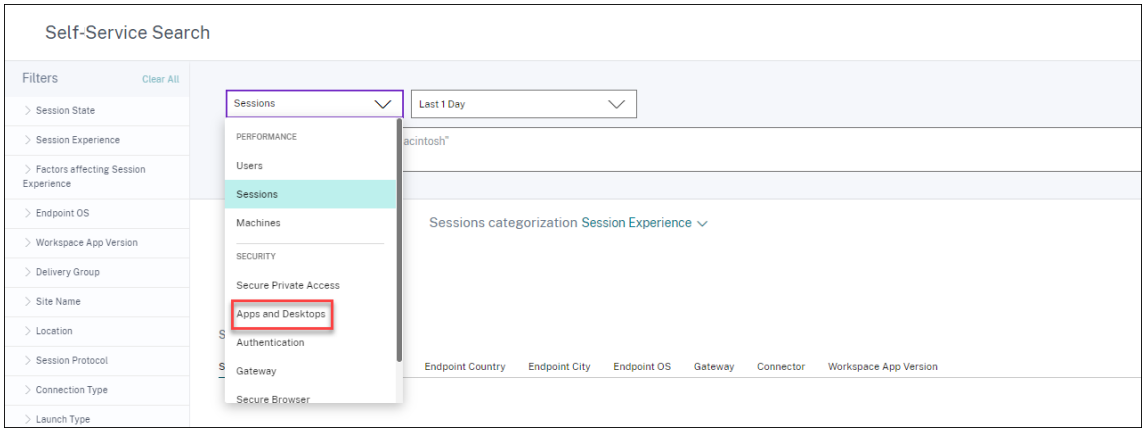
- **Windows-Benutzer**: Stellen Sie mit der Citrix Workspace-App für Windows 1907 oder höher eine Verbindung zu Citrix Virtual Apps and Desktops von Citrix und Citrix DaaS her.
- **Mac-Benutzer**: Stellen Sie mithilfe der Citrix Workspace-App für Mac 1910.2 oder höher eine Verbindung zu Citrix Virtual Apps and Desktops von Citrix und Citrix DaaS her.

Test 7- Werden die Benutzerereignisse auf der Self-Service-Suchseite in Analytics angezeigt?

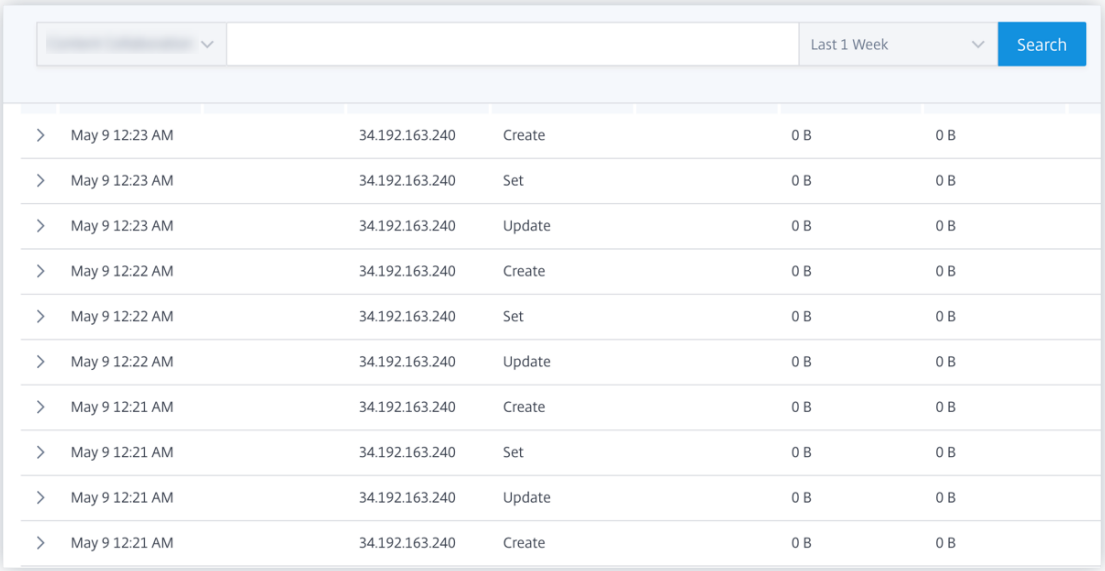
Führen Sie diese letzte Überprüfung durch, um sicherzustellen, dass die Ereignisse korrekt an Citrix Analytics übertragen werden.

1. Klicken Sie in der oberen Leiste auf **Erweiterte Suche**, um zur Self-Service-Suchseite zu gelangen.

2. Wählen Sie die Datenquelle aus, um die entsprechende Suchseite und die Ereignisse anzuzeigen.



3. Um die mit den Apps and Desktops-Ereignissen verknüpften Daten anzuzeigen, wählen Sie **Apps and Desktops** aus der Liste aus, wählen Sie den Zeitraum aus, und klicken Sie dann auf **Suchen**.



Weitere Informationen finden Sie unter Self-Service-Suche.

Test 8- Werden die Benutzer von Analytics entdeckt?

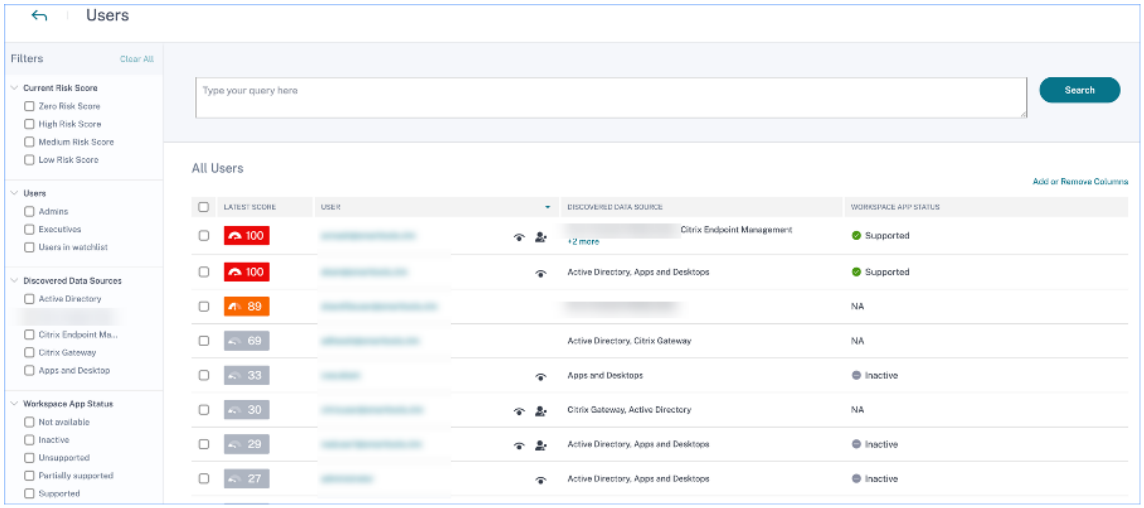
Wenn Ereignisse an Citrix Analytics fließen, werden die Benutzer, die die Ereignisse generieren, erkannt und im **Benutzer-Dashboard** angezeigt. Dieser Vorgang dauert normalerweise etwa ein paar Minuten, bis Sie sie im Dashboard anzeigen können.

1. Klicken Sie im **Benutzer-Dashboard** auf den Link **Erkannte Benutzer**, um die vollständige Liste der von Citrix Analytics erkannten Benutzer anzuzeigen.

2. Auf der Seite **Benutzer** wird die Liste aller Benutzer angezeigt, die in den letzten 31 Tagen entdeckt wurden. Wählen Sie den Zeitraum aus, in dem die Vorkommen der Risikoindikatoren angezeigt werden sollen.

> **Hinweis:**
>
> Wenn Sie versuchen, einen höheren Wert als 31 Tage festzulegen, zeigt das System eine Fehlermeldung an, die besagt: **Ungültiger Datumsbereich. Der maximal zulässige**

> **Zeitraum zwischen dem Start- und Enddatum beträgt 31 Tage.**



Wenn Ereignisse erfolgreich übertragen werden, funktioniert Ihre Citrix Analytics-Umgebung wie erwartet. Risikoindikatoren werden generiert, wenn Anomalien festgestellt werden.

Virtual Apps and Desktops-Ereignisse, SaaS-Ereignisse auslösen und Ereignisübertragung überprüfen

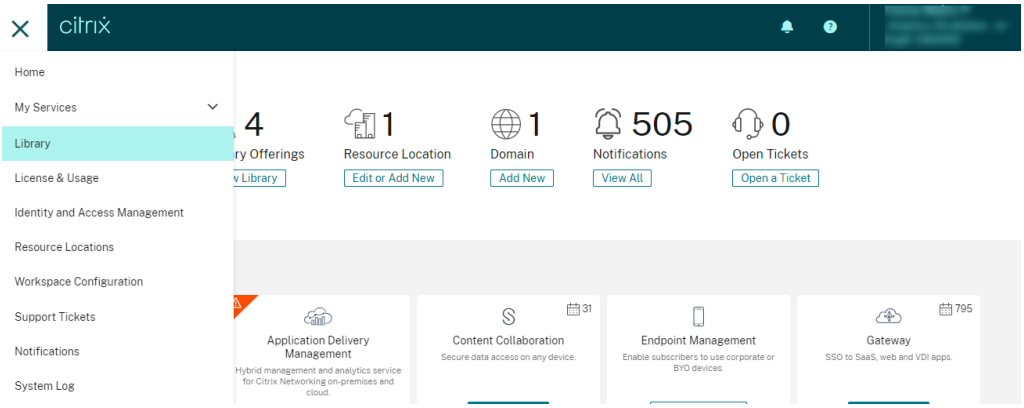
April 12, 2024

In diesem Abschnitt werden die Verfahren zum Auslösen von Apps- und Desktops-Ereignissen und SaaS-Ereignissen beschrieben und überprüft, ob Citrix Analytics for Security diese Benutzerereignisse aktiv empfängt.

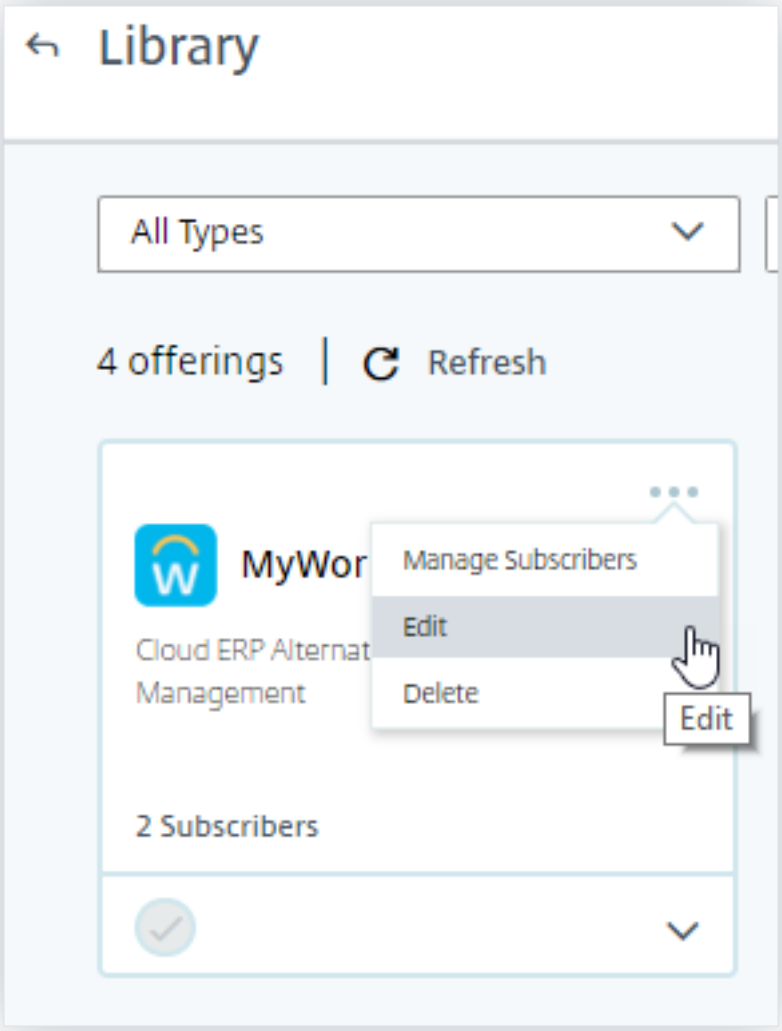
Voraussetzungen

- Wenn Sie lokal verwenden Citrix Virtual Apps and Desktops, binden Sie Ihre on-premises Sites in Citrix Analytics ein und aktivieren Sie die Datenverarbeitung von der Sitekarte aus. Wenn Sie Citrix DaaS (früher Citrix Virtual Apps and Desktops Service) verwenden, aktivieren Sie die Datenverarbeitung direkt von der Sitekarte. Weitere Informationen finden Sie unter Citrix Virtual Apps and Desktops und Citrix DaaS-Datenquelle.
- Verwenden Sie die richtigen Versionen der Citrix Workspace-App oder Citrix Receiver auf den Endpunktgeräten der Benutzer, damit die Ereignisse korrekt an Citrix Analytics gesendet werden. Weitere Informationen finden Sie unter Citrix Virtual Apps and Desktops und Citrix DaaS-Datenquelle.

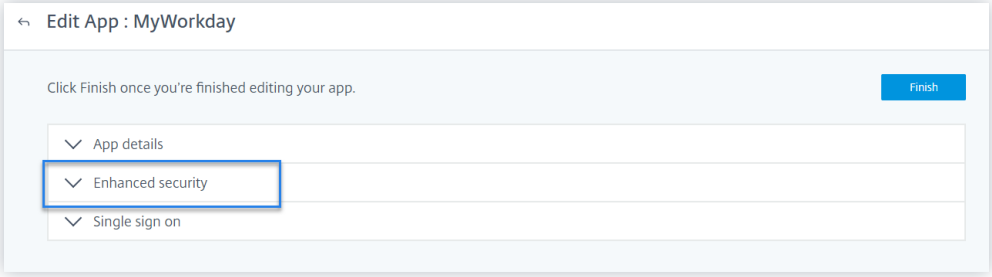
- Stellen Sie vor dem Auslösen des Druckereignisses von Ihrem virtuellen Desktop aus sicher, dass ein Drucker in Ihrer Apps- und Desktopumgebung konfiguriert und bereitgestellt ist. Weitere Informationen zum Verwalten eines Druckers finden Sie unter Drucken.
- Um SaaS-Ereignisse wie SaaS App Launch, SaaS-App-URL-Navigation und SaaS-App-Dateidownload auszulösen, müssen Sie eine konfigurierte SaaS-App aus Workspace verwenden. Zu den häufig verwendeten SaaS-Apps gehören Salesforce, Workday, Concur und GoTo Meeting.
  - Wenn keine konfigurierten SaaS-Apps vorhanden sind, müssen Sie eine SaaS-App konfigurieren und veröffentlichen. Weitere Informationen finden Sie unter Unterstützung für Software-as-a-Service-Apps. Stellen Sie beim Konfigurieren einer SaaS-App sicher, dass die folgenden Sicherheitsoptionen deaktiviert sind:
    - Zugriff auf Zwischenablage einschränken
    - Drucken einschränken
    - Navigation einschränken
    - Herunterladen einschränken
  - Wenn Sie eine bereits konfigurierte SaaS-App aus Ihrem Workspace verwenden möchten, um die Ereignisse auszulösen, stellen Sie sicher, dass die angegebenen erweiterten Sicherheitsoptionen für die SaaS-App deaktiviert sind:
    1. Gehen Sie zu Ihrem Citrix Cloud-Konto und wählen Sie **Bibliothek**aus.



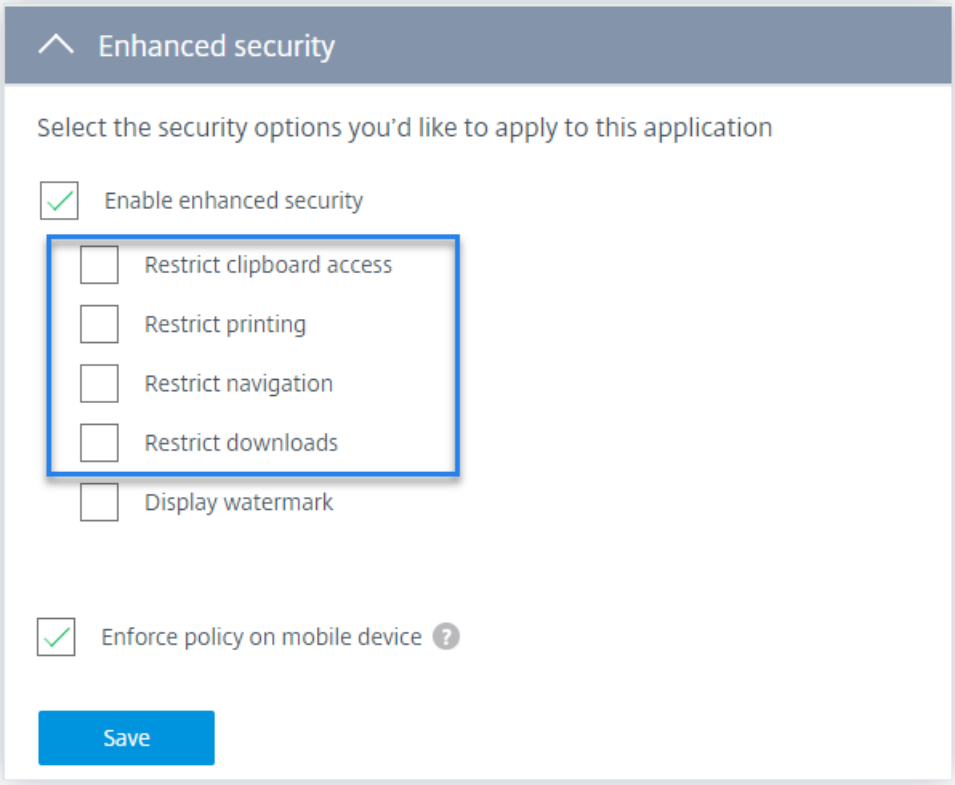
    2. Identifizieren Sie auf der Seite **Bibliothek** die SaaS-App, die Sie zur Überprüfung der Ereignisse verwenden möchten. Zum Beispiel Workday.
    3. Klicken Sie auf die Ellipsen und wählen Sie **Bearbeiten**aus.



4. Klicken Sie auf der Seite **App bearbeiten** auf den Abwärtspfeil für Verbesserte Sicherheit.



5. Stellen Sie sicher, dass die folgenden Sicherheitsoptionen nicht ausgewählt sind.



Bekanntes Problem

Wenige Versionen der Citrix Workspace-App und Citrix Receiver senden einige Ereignisse nicht an Citrix Analytics. Daher kann Citrix Analytics keine Erkenntnisse liefern und Risikoindikatoren für diese Ereignisse generieren. Weitere Informationen zu dem Problem und seiner Problemumgehung finden Sie im bekannten Problem —CAS-16151.

Prozedur

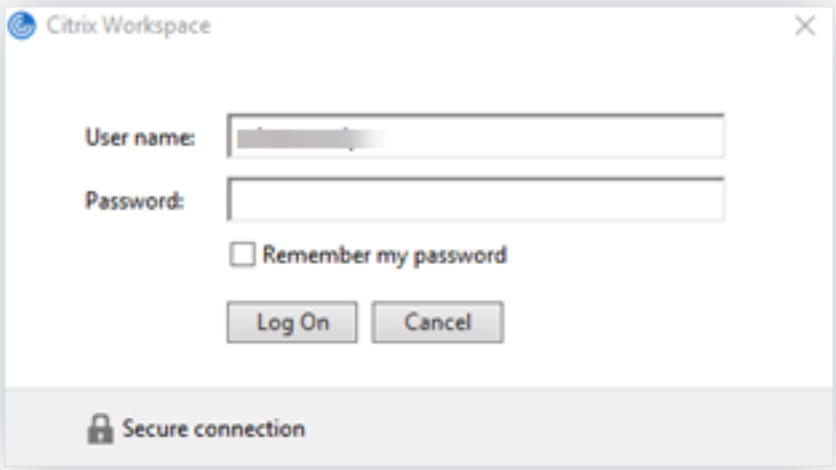
Führen Sie nacheinander die folgenden Schritte aus, um die Ereignisse in Ihrer Apps- und Desktopumgebung auszulösen und sicherzustellen, dass Citrix Analytics for Security diese Ereignisse aktiv empfängt.

> **Hinweis**
>
> - Es kann einige Zeit dauern, bis die Ereignisse Citrix Analytics erreichen. Aktualisieren Sie die Citrix Analytics-Seite, wenn Sie die ausgelösten Ereignisse nicht sehen.
> - Für das Auslösen der SaaS-Ereignisse verwendet dieses Verfahren die Workday-App als

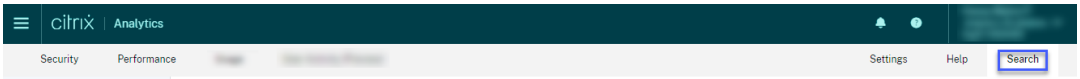
> Beispiel. Sie können alle konfigurierten SaaS-Apps aus Ihrem Workspace verwenden, um die SaaS-Ereignisse auszulösen.

- **Konto Logon**

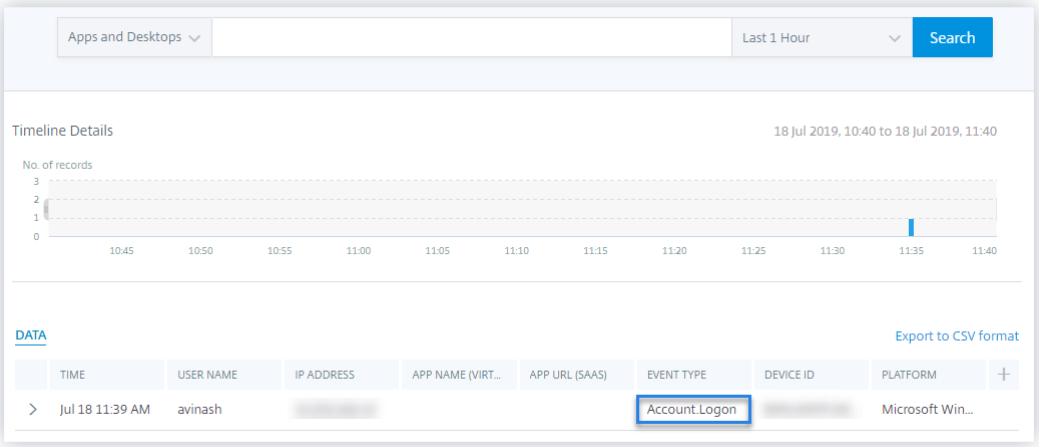
  1. Starten Sie die Citrix Workspace-App oder Citrix Receiver, um auf Workspace oder Store-Front zuzugreifen.
  2. Geben Sie Ihre Anmeldeinformationen ein, um sich bei der Citrix Workspace-App oder Citrix Receiver anzumelden.



  3. Gehen Sie zu Citrix Analytics.
  4. Klicken Sie auf **Suchen** und wählen Sie **Apps und Desktops** aus der Liste aus.

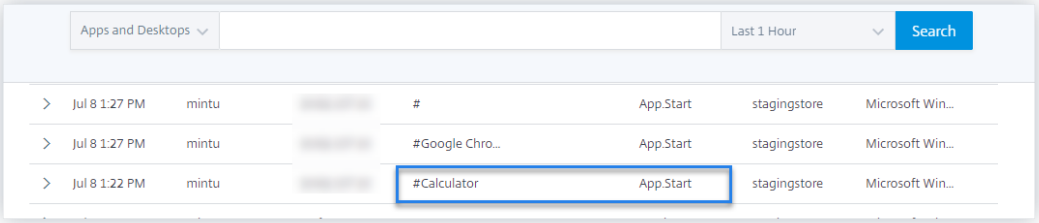


  5. Zeigen Sie auf der Suchseite die Daten für das **Account.Logon-Ereignis an** . Erweitern Sie die Zeile, um die Ereignisdetails anzuzeigen.



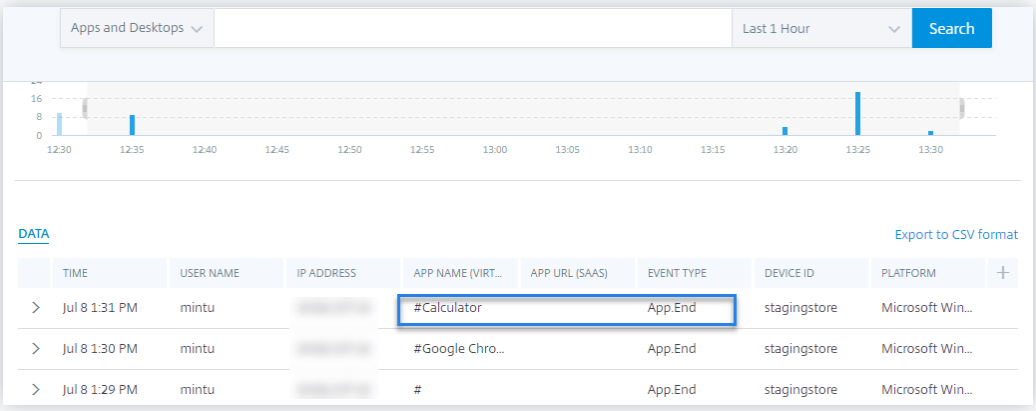
- **App-Start**

  1. Starten Sie die Citrix Workspace-App oder Citrix Receiver, um auf Workspace oder Store-Front zuzugreifen.
  2. Starten Sie eine Anwendung wie den Taschenrechner.
  3. Gehen Sie zu Citrix Analytics.
  4. Klicken Sie auf **Suchen** und wählen Sie **Apps und Desktops** aus.
  5. Zeigen Sie auf der Suchseite die Daten für die **App.Start-Ereignisdaten** an. Erweitern Sie die Zeile, um die Ereignisdetails anzuzeigen.



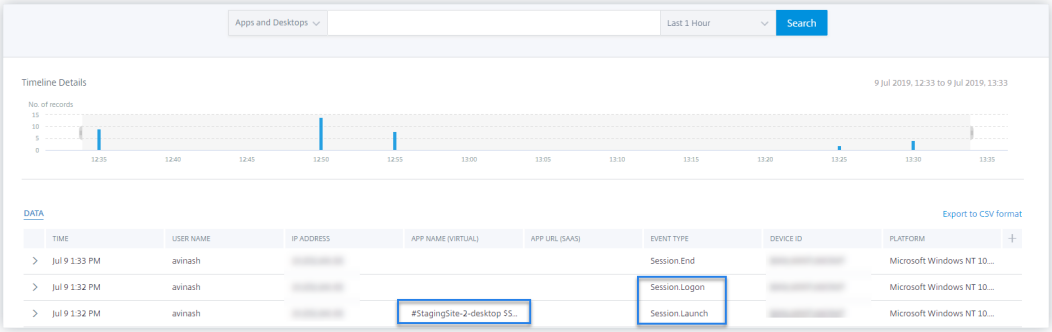
- **App-Ende**

  1. Schließen Sie den Taschenrechner, den Sie bereits in Ihrem Workspace oder StoreFront gestartet haben.
  2. Gehen Sie zu Citrix Analytics.
  3. Klicken Sie auf **Suchen** und wählen Sie **Apps und Desktops** aus.
  4. Zeigen Sie auf der Suchseite die Daten für die **App.End-Ereignisdaten** an. Erweitern Sie die Zeile, um die Ereignisdetails anzuzeigen.



- **Sitzungsanmeldung und Sitzungsstart**

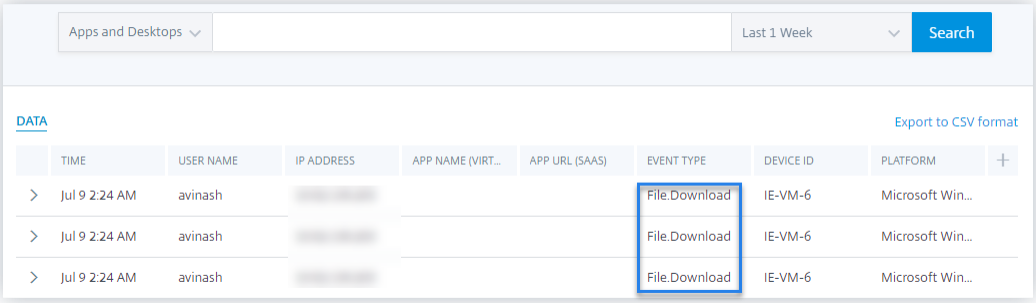
  1. Starten Sie die Citrix Workspace-App oder Citrix Receiver, um auf Workspace oder Store-Front zuzugreifen.
  2. Starten Sie Ihren virtuellen Desktop.
  3. Gehen Sie zu Citrix Analytics.
  4. Klicken Sie auf **Suchen** und wählen Sie **Apps und Desktops** aus.
  5. Zeigen Sie auf der Suchseite die Daten für die Ereignisse **Session.Logon** und **Session.Launch** an. Erweitern Sie die Zeile, um die Ereignisdetails anzuzeigen.



- **Datei Herunterladen**

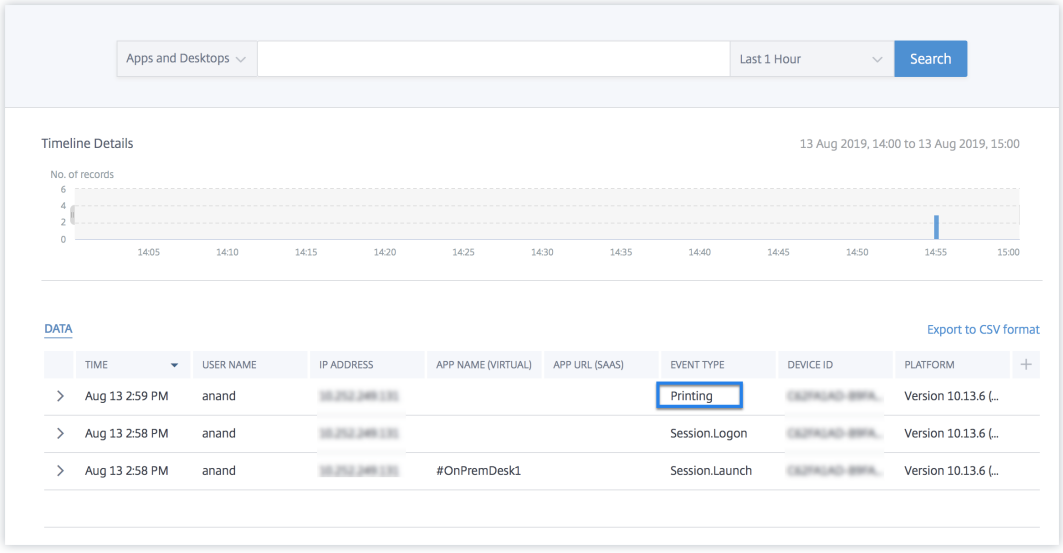
  1. Starten Sie die Citrix Workspace-App oder Citrix Receiver, um auf Workspace oder Store-Front zuzugreifen.
  2. Starten Sie Ihren virtuellen Desktop.
  3. Kopieren Sie eine Datei von Ihrem virtuellen Desktop auf Ihren lokalen Computer.
  4. Gehen Sie zu Citrix Analytics.
  5. Klicken Sie auf **Suchen** und wählen Sie **Apps und Desktops** aus.

6. Zeigen Sie auf der Suchseite die Daten für das **File.Download-Ereignis** an. Erweitern Sie die Zeile, um die Ereignisdetails anzuzeigen.



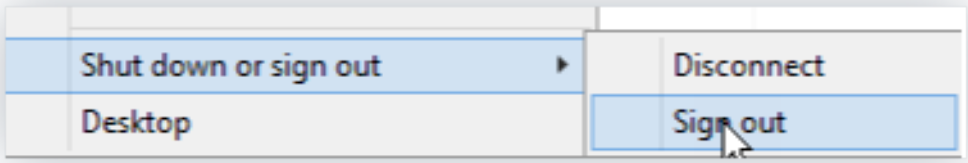
- **Drucken**

1. Starten Sie Citrix Workspace-App oder Citrix Receiver, um auf Workspace zuzugreifen
2. Starten Sie Ihren virtuellen Desktop.
3. Drucken Sie ein Dokument mit einem Drucker, der mit Ihrem virtuellen Desktop konfiguriert ist.
4. Gehen Sie zu Citrix Analytics.
5. Klicken Sie auf **Suchen** und wählen Sie **Apps und Desktops** aus.
6. Zeigen Sie auf der Seite Suchen die Daten für das **Druckereignis** an. Erweitern Sie die Zeile, um die Ereignisdetails anzuzeigen.

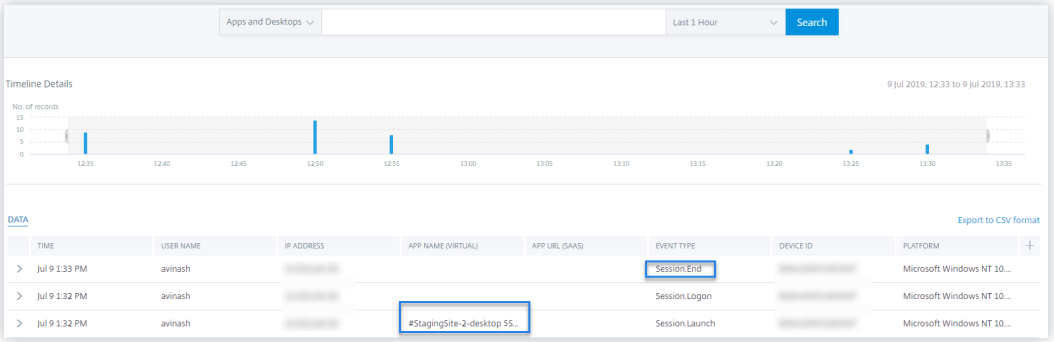


- **Ende der Sitzung**

1. Melden Sie sich von Ihrem virtuellen Desktop aus ab. Wenn Sie beispielsweise einen virtuellen Windows-Desktop verwenden, wählen Sie die Option **Abmelden** .



2. Gehen Sie zu Citrix Analytics.
3. Klicken Sie auf **Suchen** und wählen Sie **Apps und Desktops** aus.
4. Zeigen Sie auf der Suchseite die Daten für das **Session.End-Ereignis** an. Erweitern Sie die Zeile, um die Ereignisdetails anzuzeigen.

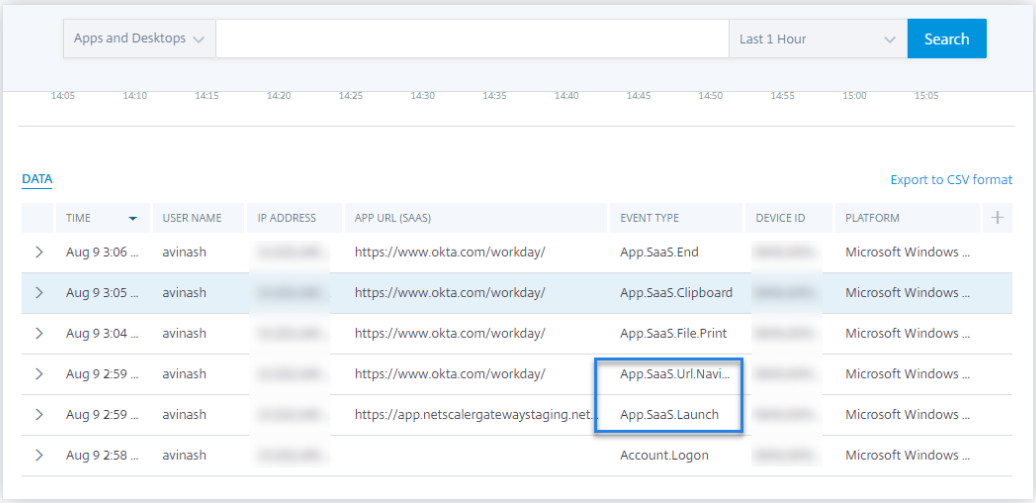


- **SaaS-App-Start und SaaS-App-URL-Navigation**

1. Starten Sie die Citrix Workspace-App oder Citrix Receiver, um auf Workspace oder Store-Front zuzugreifen.
2. Starten Sie eine SaaS-Anwendung wie Workday und warten Sie, bis die Workday-Seite geladen wurde. Navigieren Sie in Workday auf den Webseiten.

> **Hinweis**
>
> Stellen Sie sicher, dass die Option **Navigation einschränken** im Abschnitt Verbesserte Sicherheit deaktiviert ist. Weitere Informationen finden Sie unter **Voraussetzungen**.

3. Gehen Sie zu Citrix Analytics.
4. Klicken Sie auf **Suchen** und wählen Sie **Apps und Desktops** aus.
5. Zeigen Sie auf der **Suchseite** die Daten für die Ereignisse **App.SaaS.Launch** und **App.SaaS.URL.Navigation** an. Erweitern Sie die Zeile, um die Ereignisdetails anzuzeigen.

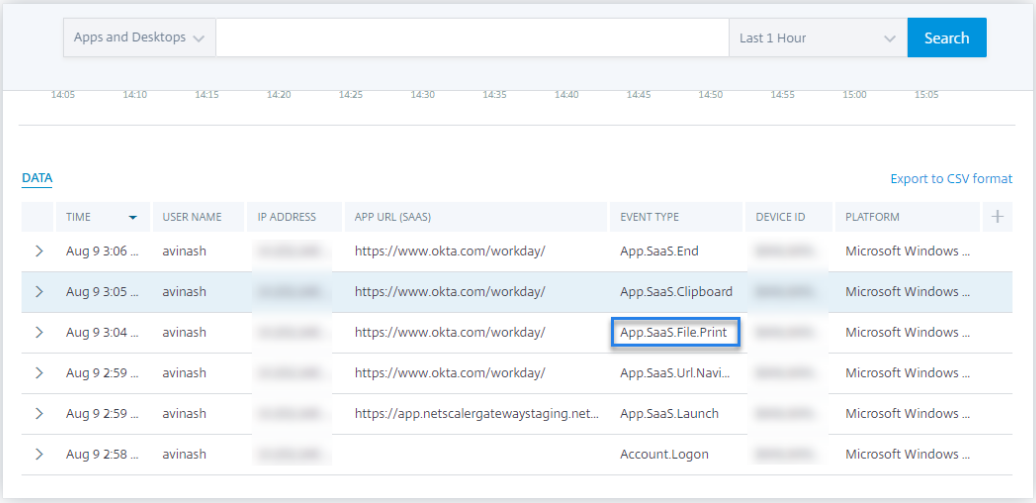


- **SaaS App Datei drucken**

  1. Drucken Sie die Workday-Seite, die Sie gerade anzeigen.

     > **Hinweis**
     >
     > Stellen Sie sicher, dass die Option **Drucken einschränken** im Abschnitt Verbesserte Sicherheit deaktiviert ist. Weitere Informationen finden Sie in den **Voraussetzungen**.

  2. Gehen Sie zu Citrix Analytics.
  3. Klicken Sie auf **Suchen** und wählen Sie **Apps und Desktops** aus.
  4. Zeigen Sie auf der Suchseite die Daten für das Ereignis **app.saas.File.print** an. Erweitern Sie die Zeile, um die Ereignisdetails anzuzeigen.

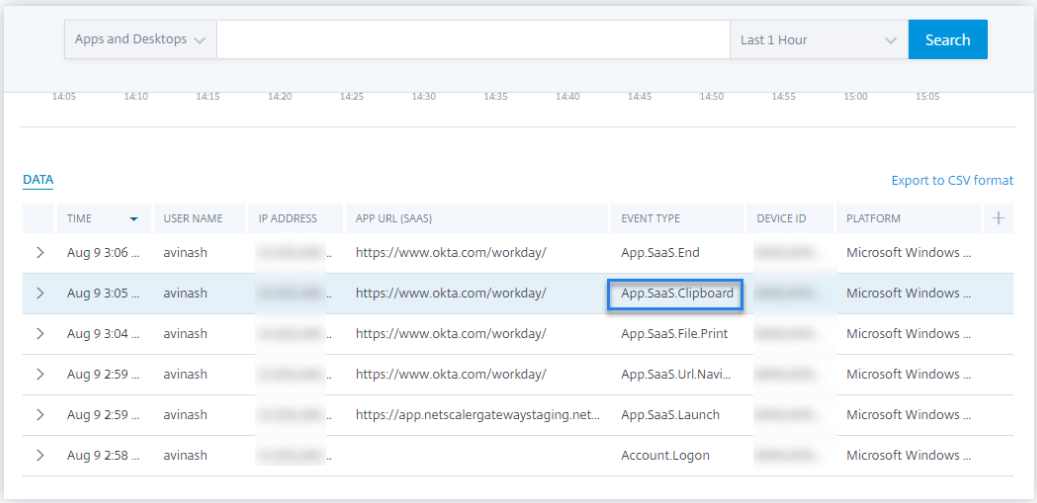


- **Zugriff auf SaaS App Zwischenablage**

1. Kopieren Sie auf der Workday-Seite Text in die Zwischenablage Ihres Systems.

> **Hinweis**
>
> Stellen Sie sicher, dass die Option **Zugriff auf die Zwischenablage beschränken** im Abschnitt Verbesserte Sicherheit deaktiviert ist. Weitere Informationen finden Sie in den **Voraussetzungen**.

2. Gehen Sie zu Citrix Analytics.
3. Klicken Sie auf **Suchen** und wählen Sie **Apps und Desktops** aus.
4. Zeigen Sie auf der Suchseite die Daten für das **app.saas.Clipboard-Ereignis an** . Erweitern Sie die Zeile, um die Ereignisdetails anzuzeigen.

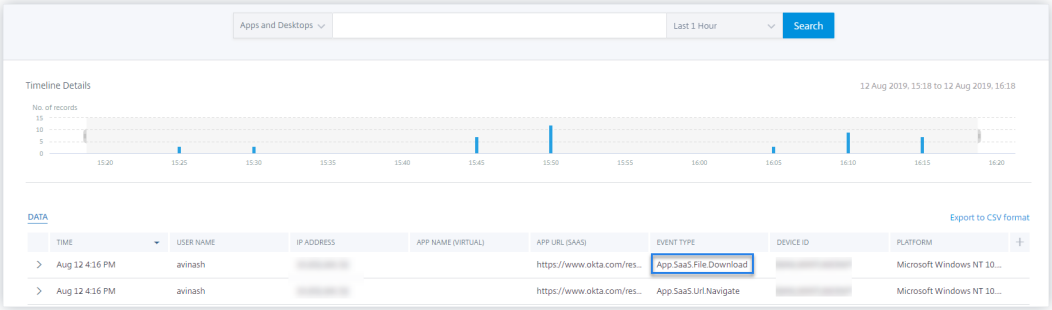


- **SaaS App Datei herunterladen**

1. Suchen Sie auf der Workday-Seite nach einem öffentlichen Dokument wie Whitepaper, und laden Sie das Dokument herunter.

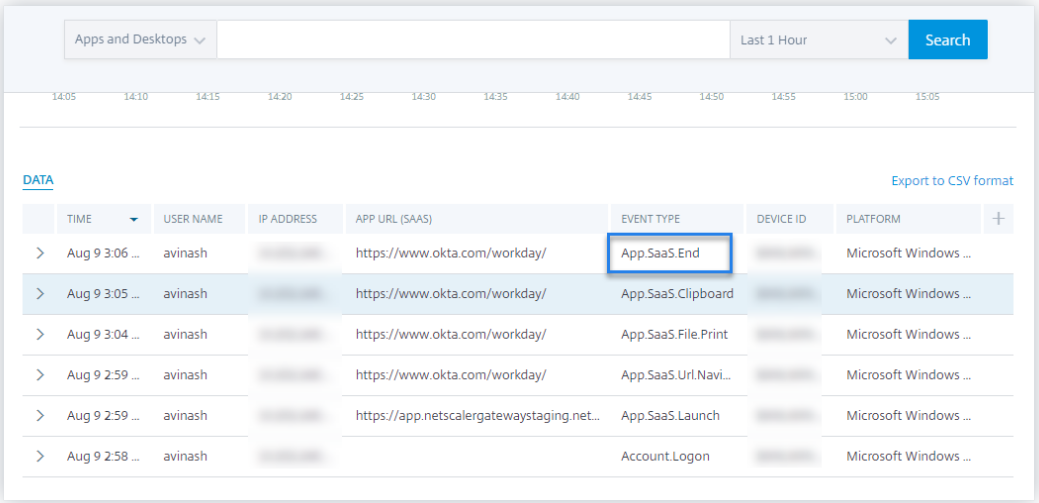
> **Hinweis**
>
> Stellen Sie sicher, dass die Option **Downloads einschränken** im Abschnitt Verbesserte Sicherheit deaktiviert ist. Weitere Informationen finden Sie in den **Voraussetzungen**.

2. Gehen Sie zu Citrix Analytics.
3. Klicken Sie auf Suchen und wählen Sie **Apps und Desktops**aus.
4. Zeigen Sie auf der Seite Suchen die Daten für das Ereignis **app.saas.File.Download** an. Erweitern Sie die Zeile, um die Ereignisdetails anzuzeigen.



- **SaaS App Ende**

  1. Schließen Sie die Workday-Seite.
  2. Gehen Sie zu Citrix Analytics.
  3. Klicken Sie auf **Suchen** und wählen Sie **Apps und Desktops** aus.
  4. Zeigen Sie auf der Suchseite die Daten für das Ereignis **app.saas.end** an. Erweitern Sie die Zeile, um die Ereignisdetails anzuzeigen.



- **VDA.Drucken**

  Voraussetzungen

  Bevor Sie das Druckereignis auslösen, lesen Sie den Abschnitt Drucktelemetrie für Citrix DaaS aktivieren.

  Führen Sie die folgenden Aktionen aus, um ein Druckereignis auszulösen:

  1. Öffnen Sie ein Textdokument mit Notepad oder einer anderen App, in der das Drucken zulässig ist.
  2. Klicken Sie auf **Datei > Drucken** oder drücken Sie **Strg+P**.

3. Wählen Sie unter Drucker auswählen den gewünschten Drucker aus, klicken Sie auf **Übernehmen** und dann auf "Drucken".

- **VDA.Zwischenablage**

  Voraussetzungen

  Bevor Sie das Druckereignis auslösen, lesen Sie den Abschnitt Telemetrie in der Zwischenablage für Citrix DaaS aktivieren.

  Gehen Sie wie folgt vor, um ein Zwischenablage-Ereignis auszulösen:

  1. Öffnen Sie ein Textdokument mit Notepad oder einem beliebigen Texteditor.
  2. Wählen Sie den zu kopierenden Inhalt aus.
  3. Klicken Sie mit der rechten Maustaste auf Kopieren oder drücken Sie Strg+C.

Konfigurierter Sitzungsaufzeichnungsserver kann keine Verbindung herstellen

July 12, 2022

Ihr Sitzungsaufzeichnungsserver kann nach der Konfigurationkeine Verbindung zu Citrix Analytics herstellen. Daher wird der konfigurierte Server nicht auf der Sitekarte der **Sitzungsaufzeichnung** angezeigt.

Gehen Sie wie folgt vor, um dieses Problem zu beheben:

1. Führen Sie auf Ihrem konfigurierten Sitzungsaufzeichnungsserver den folgenden PowerShell-Befehl aus, um die Client-Maschinen-Identifizierung (CMID) zu überprüfen

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

2. Wenn CMID leer ist, fügen Sie die folgenden Registrierungsdateien in den angegebenen Pfaden hinzu.

Name	Registrierungspfad	Schlüsseltyp	Wert
AuditorUniqueID	Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\	Zeichenfolge	Geben Sie Ihre UUID ein.
EnableCASUseAuditorUniqueID	Computer\HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/SmartAuditor/Server/	REG_DWORD	1

3. Starten Sie die folgenden Dienste neu:
    - Analysedienst der Citrix Sitzungsaufzeichnung
    - Speichermanager der Citrix Sitzungsaufzeichnung

Konfigurationsprobleme mit dem Citrix Analytics-Add-On für Splunk

July 12, 2022

Citrix Analytics-Zusatzeinstellungen sind nicht verfügbar

Nachdem Sie das Citrix Analytics Add-on für Splunk in Ihrer Splunk Forwarder- oder Splunk Standalone-Umgebung installiert haben, werden die **Citrix Analytics-Add-on-Einstellungen** unter **Einstellungen > Dateneingaben**nicht angezeigt.

Grund

Dieses Problem tritt auf, wenn Sie das Citrix Analytics Add-on für Splunk in einer nicht unterstützten Splunk-Umgebung installieren.

Fixes

Installieren Sie das Citrix Analytics-Add-on für Splunk in einer unterstützten Splunk-Umgebung. Informationen zu den unterstützten Versionen finden Sie unter Splunk-Integration.

Keine Daten in Splunk-Dashboards verfügbar

Nach der Installation und Konfiguration des Citrix Analytics Add-ons für Splunk in Ihrer Splunk Forwarder- oder Splunk Standalone-Umgebung werden in Ihren Splunk-Dashboards keine Daten von Citrix Analytics angezeigt.

Schecks

Um das Problem zu beheben, überprüfen Sie Folgendes in Ihrer Splunk Forwarder- oder Splunk Standalone-Umgebung:

1. Stellen Sie sicher, dass die Voraussetzungen für die Splunk-Integration erfüllt sind.
2. Gehen Sie zu **Einstellungen > Dateneingaben > Citrix Analytics Add-on**. Stellen Sie sicher, dass die Citrix Analytics-Konfigurationsdetails verfügbar sind.
3. Wenn die Konfigurationsdetails verfügbar sind, führen Sie die folgende Abfrage aus, um die Protokolle auf Fehler im Zusammenhang mit dem Citrix Analytics-Add-on für Splunk zu überprüfen:

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

4. Wenn Sie keine Fehler finden, funktioniert das Citrix Analytics-Add-On für Splunk wie erwartet. Wenn Sie Fehler in den Protokollen finden, kann dies an einem der folgenden Gründe liegen:

   - Es konnte keine Verbindung zwischen Ihrer Splunk-Umgebung und Citrix Analytics Kafka-Endpunkten hergestellt werden. Dieses Problem könnte auf die Firewall-Einstellungen zurückzuführen sein.

     Korrekturen: Wenden Sie sich an Ihren Netzwerkadministrator, um dieses Problem zu beheben.

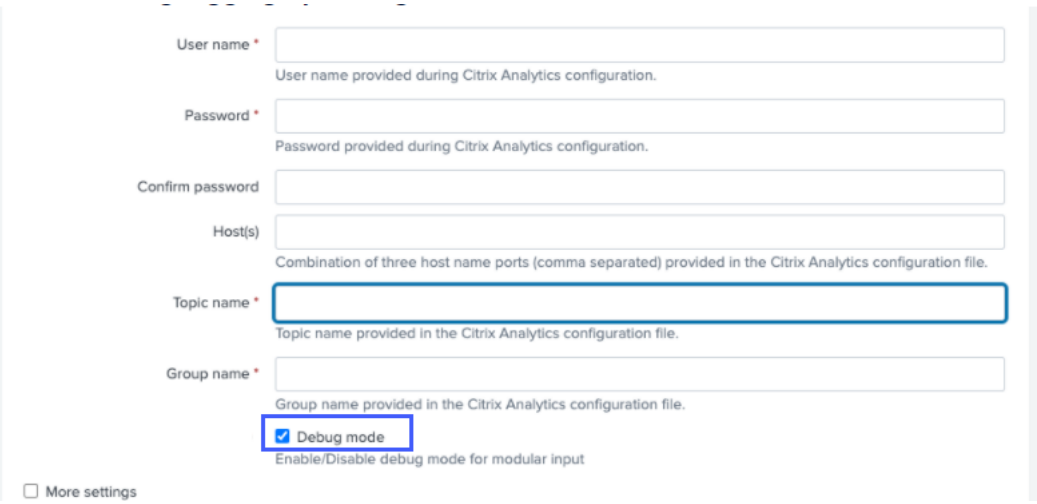
   - Falsche Konfigurationsdetails unter **Einstellungen > Dateneingaben > Citrix Analytics Add-on**.

     Korrekturen: Stellen Sie sicher, dass die Citrix Analytics-Konfigurationsdetails wie Benutzername, Kennwort, Host-Endpunkte, Thema und Benutzergruppe gemäß der Citrix Analytics-Konfigurationsdatei korrekt eingegeben werden. Weitere Informationen finden Sie unter Konfigurieren des Citrix Analytics-Add-ons für Splunk.

5. Wenn Sie die Ursache des Problems in den vorhergehenden Protokollen nicht finden können und weitere Untersuchungen durchführen möchten:

   a) Aktivieren Sie den **Debug-Modusunter Einstellungen > Dateneingaben > Citrix Analytics Add-on**.

   > Hinweis
   >
   > Standardmäßig ist der **Debug-Modus** deaktiviert. Durch die Aktivierung dieses Modus werden zu viele Protokolle generiert. Verwenden Sie diese Option also nur bei Bedarf und deaktivieren Sie sie, nachdem Sie Ihre Debugging-Aufgabe abgeschlossen haben.



   b) Suchen Sie die generierten Debug-Protokolle an folgendem Ort und überprüfen Sie, ob Fehler auftreten:

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

   c) (Optional) Verwenden Sie das Debug-Skript `splunk cmd python cas_siem_consumer_debug.py`, das mit dem Citrix Analytics-Add-on für Splunk verfügbar ist. Dieses Skript generiert eine Protokolldatei, die die Details Ihrer Splunk-Umgebung und die Konnektivitätsprüfungen enthält. Sie können die Details verwenden, um das Problem zu debuggen. Führen Sie das Script mit dem folgenden Befehl aus:

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


Fehlermeldung

In den Protokollen im Zusammenhang mit dem Citrix Analytics-Add-on für Splunk wird möglicherweise der folgende Fehler angezeigt:

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

Dieser Fehler ist entweder auf ein Problem mit der Netzwerkkonnektivität oder auf ein Authentifizierungsproblem zurückzuführen.

Um das Problem zu debuggen:

1. Aktivieren Sie in Ihrer Splunk Forwarder- oder Splunk Standalone-Umgebung den **Debug-Modus**, um die Debug-Protokolle abzurufen. Beziehen Sie sich auf den vorherigen Schritt 5.a.
2. Führen Sie die folgende Abfrage aus, um Authentifizierungsprobleme in den Debug-Protokollen zu finden:

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

3. Wenn Sie in den Debug-Protokollen keine Authentifizierungsprobleme finden, ist der Fehler auf ein Problem mit der Netzwerkkonnektivität zurückzuführen.
4. Suchen und beheben Sie das Problem, indem Sie Telnet oder das im vorherigen Schritt 5.c erwähnte Debug-Skript verwenden.

Das Add-on-Upgrade schlägt von einer Version vor 2.0.0 fehl

Wenn Sie in Ihrer Splunk Forwarder- oder Splunk Standalone-Umgebung das Citrix Analytics-Add-On für Splunk von einer Version vor 2.0.0 auf die neueste Version aktualisieren, schlägt das Upgrade fehl.

Fixes

1. Löschen Sie die folgenden Dateien und Ordner im Ordner `/bin` des Citrix Analytics-Add-ons für Splunk-Installationsordner:
   - `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. Starten Sie Ihre Splunk Forwarder- oder Splunk Standalone-Umgebung neu.

StoreFront-Server kann nicht mit Citrix Analytics verbunden werden

January 4, 2023

Nach dem Importieren der Konfigurationseinstellungen von Citrix Analytics auf Ihren StoreFront-Server kann der StoreFront-Server keine Verbindung zu Citrix Analytics herstellen.

Informationen zum Importieren von Konfigurationseinstellungen auf einen StoreFront-Server finden Sie unter Integrieren von Websites Virtual Apps and Desktops mit StoreFront.

Der CAS-Onboarding-Assistent hilft bei der Überprüfung und Behebung der in diesem Artikel beschriebenen Probleme. Weitere Informationen finden Sie unter Onboarding-Assistent für Citrix Analytics Service (CAS).

Gehen Sie wie folgt vor, um das Problem zu beheben:

1. Pingen Sie auf dem StoreFront-Server die regionsspezifischen Endpunkte von Citrix Analytics, um die Konnektivität zwischen dem StoreFront-Server und dem Citrix Analytics-Server zu testen. Stellen Sie außerdem sicher, dass die Voraussetzungen erfüllt sind.

   > **Hinweis**
   >
   > Auf Ihrem StoreFront-Server können Sie die Konnektivität testen, indem Sie die regionsspezifischen Endpunkte direkt anpingen oder einen Webbrowser öffnen und auf die regionsspezifischen Endpunkte zugreifen.

2. Aktivieren Sie die ausführliche Protokollierung im StoreFront-Server, um die Protokolle zu verfolgen. Weitere Informationen zur ausführlichen Protokollierung finden Sie im Artikel CTX139592.
3. Öffnen Sie den Internetinformationsdienste-Manager (IIS) und überprüfen Sie Folgendes:
   - Wenn sich die StoreFront-Site unter der IIS-Standardsite befindet, startet IIS die StoreFront-Site neu.
   - Wenn sich die StoreFront-Site in anderen Treibern befindet oder nicht unter der Standard-Site, öffnen Sie das Befehlsfenster und geben Sie ein `iisreset`.

4. Führen Sie folgenden Befehl aus, um die Citrix Analytics-Einstellungen zu importieren:

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

5. Führen Sie den folgenden Befehl aus, um die importierten Einstellungen zu überprüfen:

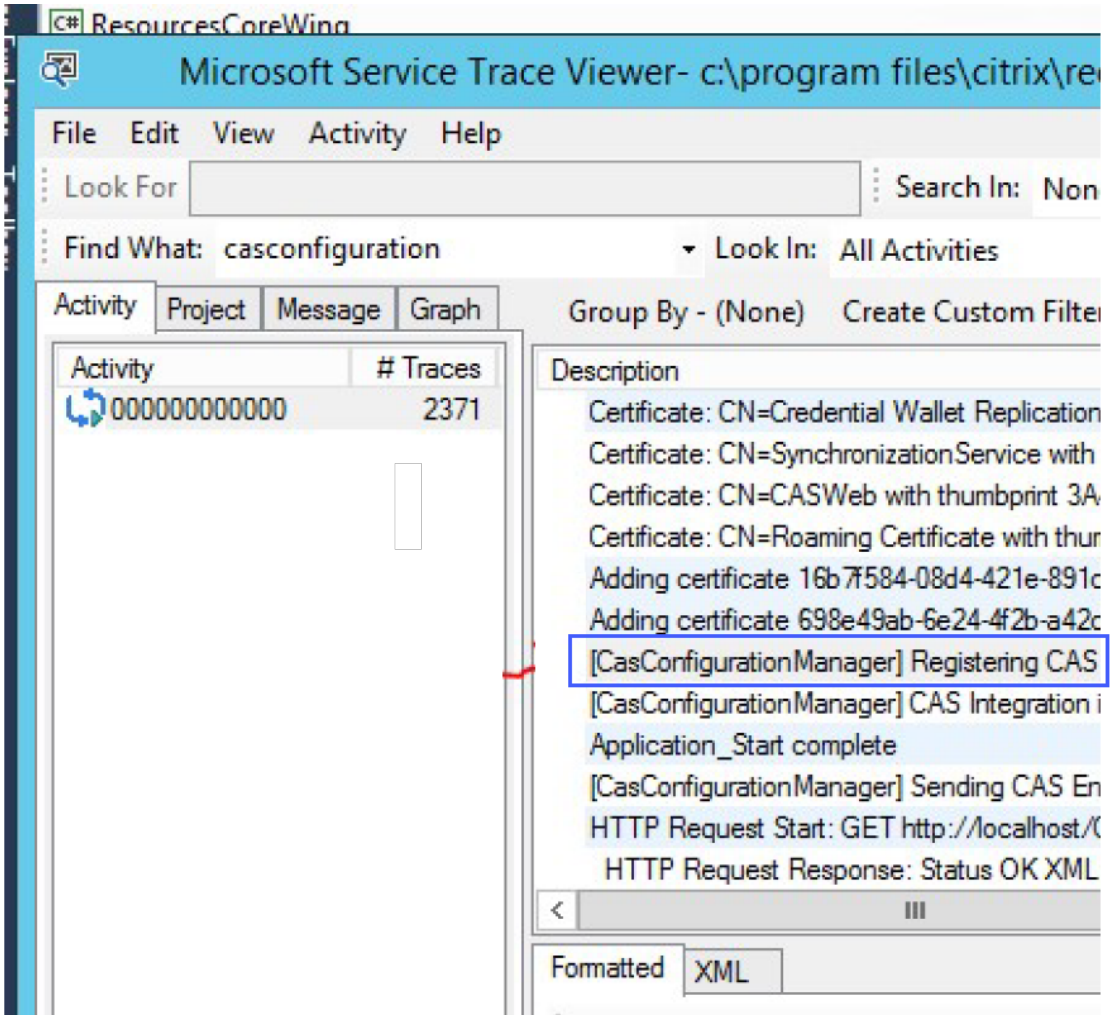
```
Get-STFCasConfiguration
```

6. Wenn sich die StoreFront-Site in anderen Treibern befindet oder nicht unter der Standard-Site, öffnen Sie das Befehlsfenster. Geben Sie `iisreset` ein, damit die StoreFront-Site Citrix Analytics-Einstellungen
7. Rufen Sie die ausführlichen StoreFront-Protokolldateien von folgendem Speicherort ab:

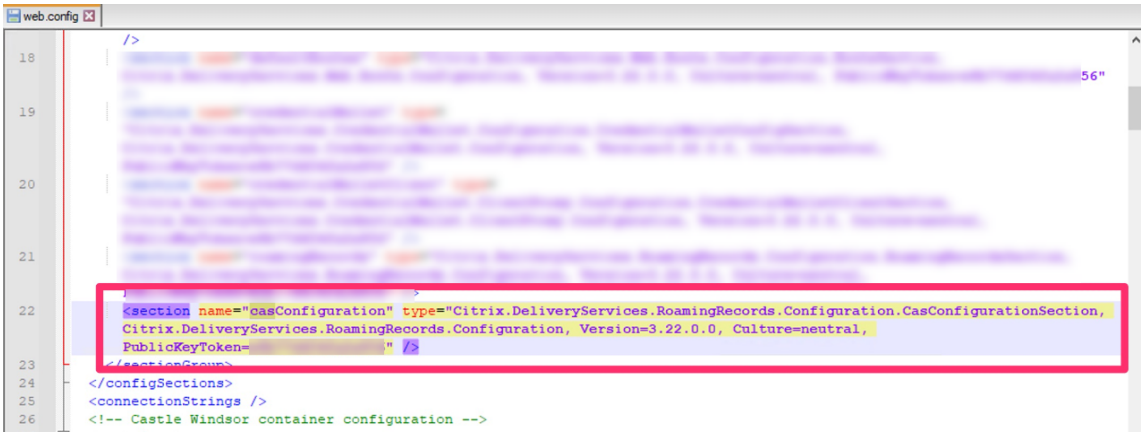
```
C:\Program Files\Citrix\Receiver StoreFront\Admin\trace
```

   Unter dem oben genannten Speicherort finden Sie mehrere svclog-Dateien, die in der Ereignisanzeige geöffnet werden können.

8. Verwenden Sie den Microsoft Service Trace Viewer, um die folgenden Protokolle zu öffnen:
   - StoreFront-Protokolle
   - Ausführliche Protokolle der Roaming-Site
9. Stellen Sie in den Protokollen sicher, dass die Abschnitte **CasConfigurationManager** und Citrix Analytics-Serverinformationen verfügbar sind.



10. Wenn die Abschnitte von CasConfigurationManager nicht verfügbar sind, öffnen Sie die Datei web.config für die Roaming-Site, die Sie unter `roaming site\folder` finden.
11. Suchen Sie in der Datei `web.config` den Abschnitt **casConfiguration** und stellen Sie sicher, dass die Citrix Analytics-Serverinformationen verfügbar sind.



12. Stellen Sie auf den Windows Server-Computern, auf denen der StoreFront-Server installiert ist,

Folgendes sicher:

- Der TLS 1.2 Client ist aktiviert.
- Mindestens eine der folgenden Verschlüsselungssammlungen ist aktiviert:
  - `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`

Informationen zum Konfigurieren der TLS-Verschlüsselungssammlungsreihenfolge finden Sie in der Microsoft-Dokumentation.

13. Wenn Sie Windows Server 2012-Computer verwenden, stellen Sie sicher, dass Diffie-Hellman Exchange (ECDHE/DHE) aktiviert ist.
14. Stellen Sie sicher, dass die Windows Server-Computer, auf denen der StoreFront-Server installiert ist, die in der Microsoft-Dokumentationgenannten Registrierungseinstellungen enthalten müssen.

> **WICHTIG**
>
> Aktualisieren Sie die TLS/SSL-Verschlüsselungssammlungen mithilfe von Gruppenrichtlinien. Ändern Sie die TLS/SSL-Verschlüsselungssammlungen nicht manuell. Weitere Informationen zur Verwendung von Gruppenrichtlinien finden Sie in der Microsoft-Dokumentation.

Beispielsweise müssen die folgenden Registrierungseinstellungen auf Ihrem Windows Server-Computer verfügbar sein:

TLS 1.2 Kunde:

```
[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-->
```

Diffie-Hellman-KEAs:

```
[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-->
```

AES-128/AES-256-Verschlüsselungen:

```
[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-->
```

SHA256/SHA384-Hashes:

```
[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-->
```

Häufig gestellte Fragen

November 16, 2023

Datenquelle

Was ist eine Datenquelle?

Datenquellen sind Dienste und Produkte von Citrix, die Daten an Citrix Analytics senden.

Weitere Informationen: Datenquelle

Wie füge ich eine Datenquelle hinzu?

Nachdem Sie sich bei Citrix Analytics angemeldet haben, wählen Sie auf dem **Begrüßungsbildschirm** die Option **Erste Schritte** aus, um Citrix Analytics eine Datenquelle hinzuzufügen. Alternativ können Sie auch eine Datenquelle hinzufügen, indem Sie zu **Einstellungen > Datenquellen** navigieren.

NetScaler ADM Agent

Was sind die Mindestanforderungen an Ressourcen, um einen Agenten auf einem Hypervisor on-premises zu installieren?

8 GB RAM, 4 virtuelle CPU, 120 GB Speicher, 1 virtuelle Netzwerkschnittstellen, 1 Gbit/s Durchsatz

Muss ich NetScaler ADM Agenten während der Bereitstellung einen zusätzlichen Datenträger zuweisen?

Nein, Sie müssen keinen zusätzlichen Datenträger hinzufügen. Der Agent wird nur als Vermittler zwischen Citrix Analytics und den Instanzen in Ihrem Unternehmensrechenzentrum verwendet. Es werden keine Bestands- oder Analysedaten gespeichert, für die ein zusätzlicher Datenträger erforderlich wäre.

Was sind die Standardanmeldeinformationen für die Anmeldung bei einem Agenten?

Die Standardanmeldeinformationen für die Anmeldung am Agenten lauten `nsrecover`/`nsroot`. Dadurch werden Sie an der Shell-Eingabeaufforderung des Agenten angemeldet.

Wie ändere ich die Netzwerkeinstellungen eines Agenten, wenn ich einen falschen Wert eingegeben habe?

Melden Sie sich bei der Agent-Konsole auf Ihrem Hypervisor an, greifen Sie mit den Anmeldeinformationen `nsrecover`/`nsroot`auf die Shell-Eingabeaufforderung zu. Führen Sie dann den Befehl aus `networkconfig`.

Warum benötige ich eine Service-URL und einen Aktivierungscode?

Der Agent verwendet die Dienst-URL, um den Dienst zu finden, und den Aktivierungscode, um den Agenten beim Dienst zu registrieren.

Wie kann ich die Dienst-URL erneut eingeben, wenn ich sie in der Agent-Konsole falsch eingegeben habe?

Melden Sie sich mit den Anmeldeinformationen `nsrecover`/an der Shell-Eingabeaufforderung des Agenten an`nsroot`, und geben Sie dann: ein `deployment_type.py`. Mit diesem Skript können Sie die Service-URL und den Aktivierungscode erneut eingeben.

Wie erhalte ich einen neuen Aktivierungscode?

Sie können einen neuen Aktivierungscode vom NetScaler ADM Service erhalten. Melden Sie sich beim NetScaler ADM Service an und navigieren Sie zu **Netzwerke > Agenten**. Wählen Sie auf der Seite **Agenten** in der Liste **Aktion auswählen** die Option **Aktivierungscode generieren** aus.

Kann ich meinen Aktivierungscode mit mehreren Agents wiederverwenden?

Nein, das geht nicht.

Wie viele NetScaler ADM Agents muss ich installieren?

Die Anzahl der Agents hängt von der Anzahl der verwalteten Instanzen in einem Rechenzentrum und dem Gesamtdurchsatz ab. Citrix empfiehlt, mindestens einen Agent für jedes Datencenter zu installieren.

Wie installiere ich mehrere NetScaler ADM Agents?

Klicken Sie auf der Seite Datenquellen auf das Pluszeichen (+) neben NetScaler Gateway, und befolgen Sie die Anweisungen zum Installieren eines anderen Agents.

Alternativ können Sie auf die NetScaler ADM-GUI zugreifen und zu Netzwerke > Agenten navigieren und auf **Agent einrichten** klicken, um mehrere Agents zu installieren.

Kann ich zwei Agenten in einem Hochverfügbarkeits-Setup installieren?

Nein, das geht nicht.

Was mache ich, wenn meine Agentregistrierung fehlschlägt?

- Stellen Sie sicher, dass Ihr Agent Zugriff auf das Internet hat (DNS konfigurieren).
- Stellen Sie sicher, dass Sie den Aktivierungscode korrekt kopiert haben.
- Stellen Sie sicher, dass Sie die Service-URL korrekt eingegeben haben.
- Stellen Sie sicher, dass die erforderlichen Ports geöffnet sind.

Die Registrierung war erfolgreich, aber woher weiß ich, ob der Agent gut läuft?

Sie können Folgendes tun, um zu überprüfen, ob der Agent einwandfrei läuft:

- Nachdem der Agent erfolgreich registriert wurde, greifen Sie auf NetScaler ADM zu und navigieren Sie zu **Netzwerke > Agenten**. Sie können die erkannten Agenten auf dieser Seite anzeigen. Wenn der Agent einwandfrei läuft, wird der Status durch ein grünes Symbol angezeigt. Wenn es nicht ausgeführt wird, wird der Status durch ein rotes Symbol angezeigt.
- Melden Sie sich bei der Shell-Eingabeaufforderung des Agenten an und führen Sie die folgenden Befehle aus: `ps -ax | grep masps -ax | grep ulfd` Stellen Sie sicher, dass die folgenden Prozesse ausgeführt werden.

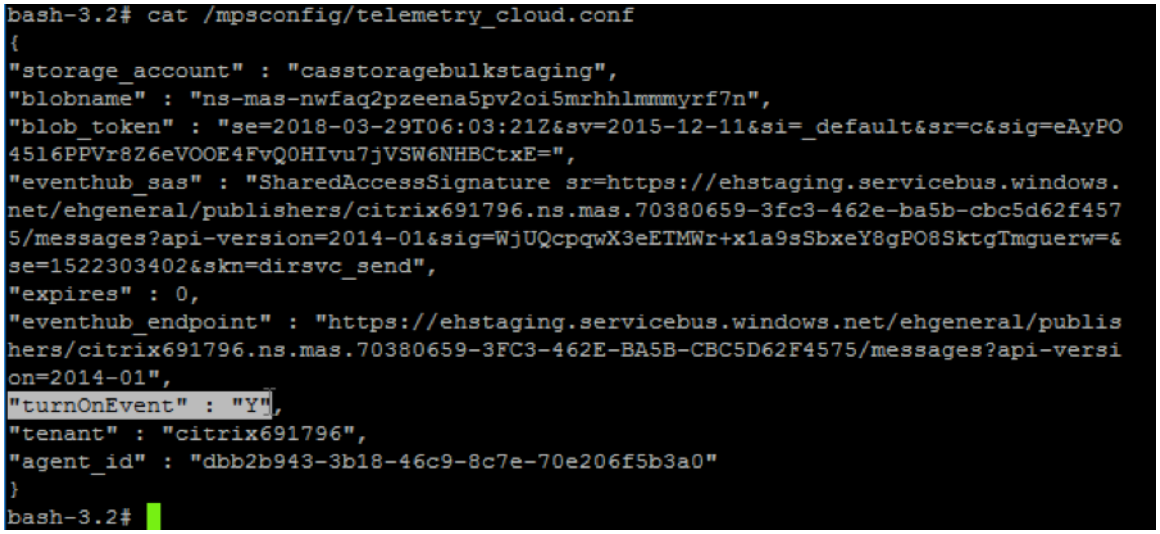
- Wenn einer der Prozesse nicht ausgeführt wird, führen Sie den Befehl **masd restart** aus. Dies kann einige Zeit dauern, um alle Daemons zu starten (etwa 1 Minute).
- Stellen Sie sicher, dass `agent.conf` nach erfolgreicher Registrierung des Agents in `/mpsconfig` erstellt wurde.

Onboarding von Citrix Gateway-Instanzen

Citrix Gateway-Instanzen werden zu Citrix Analytics hinzugefügt, aber woher weiß ich, ob Analytics auf dem Agent aktiviert ist?

Sie können anhand der Shell-Eingabeaufforderung des Agenten überprüfen, ob Analytics auf dem Agent aktiviert ist. Wenn Analytics erfolgreich auf dem Agenten aktiviert wurde, wird der Parameter `turnOnEvent` in der Datei `/mpsconfig/telemetry_cloud.conf` auf `Y`gesetzt.

Melden Sie sich bei der Shell-Eingabeaufforderung des Agents an und führen Sie den folgenden Befehl aus: cat `/mpsconfig/telemetry_cloud.conf` und überprüfen Sie den Wert des Parameters `turnOnEvent`.



Ich habe versehentlich den NetScaler Gateway-Onboardingassistenten geschlossen. Muss ich meine Konfiguration von Anfang an starten?

Nein. Citrix Analytics speichert den Fortschritt und zeigt die unvollständige Konfiguration als Kachel auf der Seite **Datenquellen > Einstellungen** an. Klicken Sie auf **Setup fortsetzen**, um die Konfiguration abzuschließen.

Onboarding der Website für Virtual Apps and Desktops

Wie schalte ich die Datenverarbeitung aus?

Wenn Sie die Datenverarbeitung von Ihrer Site zu Citrix Analytics vorübergehend deaktivieren möchten, klicken Sie einfach auf die **Sitekarte** und dann auf **Datenverarbeitung deaktivieren**.

Wenn ich meine Site zu Workspace hinzufüge und auf "STA testen"klicke, schlägt der Test fehl. Welche Schritte sind erforderlich?

Möglicherweise liegt ein Verbindungsproblem zwischen Ihrem NetScaler Gateway und Cloud Connectors vor. Informationen zur Fehlerbehebung finden Sie unter CTX232517 im Citrix Support Knowledge Center.

Wo erhalte ich Hilfe zu Citrix Analytics?

Im Diskussionsforum von Citrix Analytics unter https://discussions.citrix.com/forum/1710-citrix-analytics/ können Sie Fragen stellen und sich mit Experten von Citrix Analytics in Verbindung setzen.

Um am Forum teilzunehmen, müssen Sie sich mit Ihrer Citrix ID anmelden.

Zugangssicherung —Geolocation

Wie werden Geolokalisierungsdetails von Analytics abgeleitet?

Citrix Analytics verwendet die IP-Adresse des Geräts, von dem aus der Workspace Client gestartet wird. Citrix Analytics nutzt einen Drittanbieter für IP-Geolokalisierungsdaten, um den Standort eines Benutzers aus seiner IP-Adresse abzuleiten. Wenn Sie eine Sitzungsanmeldung durchführen, wird Ihr Standort (IPv4-Adresse) in ein Land oder eine Stadt aufgelöst, und die Zuordnung wird regelmäßig aktualisiert. Unternehmen können diese nach Ländern definierten Standorte verwenden, um Zugriffsmuster zu überwachen, von denen aus sie keine Geschäfte tätigen.

Wie hoch ist die Genauigkeit bei der Ableitung des Standorts eines Benutzers?

Citrix Analytics nutzt einen Drittanbieter für IP-Geolokalisierungsdaten, um den Standort eines Benutzers aus seiner IP-Adresse abzuleiten. GeoIP-Dienste können die meiste Zeit in der richtigen Stadt oder am richtigen Ort aufgelöst werden, GeoIP-Suchen sind jedoch nie vollständig korrekt. Manchmal kann sich der für einen Benutzer angezeigte Standort von seinem genauen Standort des Zugriffs unterscheiden.

Basierend auf der Dokumentation von IP GeoPointliegt der Abdeckungsgrad bei etwa 99,99% der weltweit zugewiesenen IP-Adressen (IPv4-routingfähige IP-Adressen). In Bezug auf die Standortgenauigkeit begleitet es jedes der wesentlichen Standortfelder (Land, Bundesland, Stadt, Postleitzahl) mit einem Konfidenzfaktor.

In welchen Fällen ist die Standortbestimmung ungenau?

Die Genauigkeit der Geolokalisierungsdaten hängt davon ab, wie das Gerät eine Verbindung zum Internet herstellt. Ein Gerät kann eine Verbindung zum Internet herstellen über:

- Mobile Gateways
- VPN oder Hosting-Einrichtung
- Regionaler oder internationaler Proxy-/Anonymisierserver

In solchen Fällen sind Geolokalisierungsdaten unabhängig von der Verwendung der Software des IP-Geolocation-Anbieters nicht genau.

Was sind die unterstützten Versionen der Citrix Workspace-App?

Es gibt Mindestversionen der Citrix Workspace-App, die für das Betriebssystem erforderlich sind, um das **IP-Adressattribut** an Citrix Analytics for Security zu senden. Weitere Informationen finden Sie in der Matrixtabelle oder in den als nicht verfügbar identifizierten Standorten .

In welchen Fällen erhalten wir keine geologischen Details?

Einzelheiten zur Geolocation finden Sie im Abschnitt Als nicht verfügbar identifizierte Standorte .

Welchen Geolocation-Dienst verwendet Citrix Analytics, um den Standort eines Benutzers zu melden? Wie melde ich einen falschen Standort für eine IP?

Citrix Analytics verwendet dateibasierte Geolocation-Dienste von Neustar, um Geolokalisierungsdaten für eingehende Zugriffe bereitzustellen. Es verfügt über eine öffentlich zugängliche IP-Korrekturseite, auf der Sie eine Korrekturanforderung selbst einreichen können. Sobald ein Korrekturantrag eingereicht wurde, wird der Antrag von Neustar auf Richtigkeit geprüft und bearbeitet.

Der GeoIP-Anbieter hilft dabei, so genaue Informationen wie möglich anzuzeigen. Leider kann es Fälle geben, in denen die GeoIP-Daten aufgrund der angeborenen Natur von GeoIP ungenau sind.

Glossar der Begriffe

April 12, 2024

- **Aktionen**: Geschlossene Reaktionen auf verdächtige Ereignisse. Es werden Maßnahmen angewendet, um zukünftige anomale Ereignisse zu verhindern. Weitere Informationen.
- **Cloud Access Security Broker (CASB)**: Lokaler oder Cloud-basierter Durchsetzungspunkt für Sicherheitsrichtlinien zwischen Cloud-Dienstnutzern und Cloud-Dienstanbietern. CASBs kombinieren und integrieren Sicherheitsrichtlinien des Unternehmens, wenn auf Cloud-basierte Ressourcen zugegriffen wird. Sie helfen Unternehmen auch dabei, die Sicherheitskontrollen ihrer on-premises Infrastruktur auf die Cloud auszudehnen.
- **Citrix ADC (Application Delivery Controller)**: Netzwerkgerät, das sich in einem Rechenzentrum befindet, das sich strategisch zwischen der Firewall und einem oder mehreren Anwendungsservern befindet. Behandelt den Lastausgleich zwischen Servern und optimiert die Endbenutzerleistung und Sicherheit für Unternehmensanwendungen. Weitere Informationen

- **Citrix ADM (Application Delivery Management)**: Zentralisierte Netzwerkverwaltungs-, Analyse- und Orchestrierungslösung. Von einer einzigen Plattform aus können Administratoren Netzwerkdienste für skalierbare Anwendungsarchitekturen anzeigen, automatisieren und verwalten. Weitere Informationen
- **Citrix ADM Agent**: Proxy, der die Kommunikation zwischen Citrix ADM und den verwalteten Instanzen in einem Rechenzentrum ermöglicht. Weitere Informationen
- **Citrix Analytics**: Cloud-Dienst, der Daten über Dienste und Produkte hinweg (on-premises und in der Cloud) sammelt und umsetzbare Erkenntnisse generiert, sodass Administratoren proaktiv mit Sicherheitsbedrohungen von Benutzern und Anwendungen umgehen, die App-Leistung verbessern und den kontinuierlichen Betrieb unterstützen können. Weitere Informationen
- **Citrix Cloud**: Plattform, die über den Citrix Cloud Connector in jeder Cloud oder Infrastruktur (on-premises, Public Cloud, Private Cloud oder Hybrid Cloud) eine Verbindung zu Ressourcen herstellt. Weitere Informationen
- **NetScaler Gateway**: Konsolidierte RAS-Lösung, die die RAS-Infrastruktur konsolidiert, um Single Sign-On für alle Anwendungen zu ermöglichen, ob in einem Rechenzentrum, in der Cloud oder als SaaS bereitgestellt. Erfahren Sie mehr.
- **Citrix Hypervisor**: Virtualisierungsverwaltungsplattform, optimiert für Anwendungs-, Desktop- und Servervirtualisierungsinfrastrukturen. Weitere Informationen
- **Citrix Workspace App** (früher bekannt als Citrix Receiver): Clientsoftware, die nahtlosen, sicheren Zugriff auf Anwendungen, Desktops und Daten von jedem Gerät, einschließlich Smartphones, Tablets, PCs und Macs, bietet. Weitere Informationen
- **DLP (Data Loss Prevention)**: Lösung, die eine Reihe von Technologien und Prüfmethoden beschreibt, um in einem Objekt enthaltene Informationen wie Datei, E-Mail, Paket, Anwendung oder Datenspeicher zu klassifizieren. Das Objekt kann sich auch im Speicher, in Verwendung oder über ein Netzwerk befinden. DLP-Tools können Richtlinien wie Protokollieren, Berichten, Klassifizieren, Verschieben, Kennzeichnen und Verschlüsseln dynamisch anwenden. DLP-Tools können auch Schutzmaßnahmen zur Verwaltung von Unternehmensdatenrechten anwenden. Weitere Informationen
- **DNS (Domain Name System)**: Netzwerkdienst, der verwendet wird, um Internet-Domänennamen zu finden und sie in Internetprotokolladressen (IP) zu übersetzen. DNS ordnet die von Benutzern bereitgestellten Website-Namen ihren entsprechenden IP-Adressen zu, die von Computern bereitgestellt werden, um eine Website unabhängig vom physischen Standort der Entitäten zu finden.
- **Datenverarbeitung**: Methode zur Verarbeitung von Daten aus einer Datenquelle zu Citrix Analytics. Weitere Informationen

- **Datenquelle**: Produkt oder Dienst, der Daten an Citrix Analytics sendet. Eine Datenquelle kann intern oder extern sein. [Erfahren Sie mehr] /en-us/citrix-analytics/data-sources.html).
- **Datenexport**: Produkt oder Dienst, der Daten von Citrix Analytics empfängt und Erkenntnisse liefert. Weitere Informationen
- **Erkannte Benutzer**: Gesamtzahl der Benutzer in einer Organisation, die Datenquellen verwenden. Weitere Informationen
- **FQDN (vollqualifizierter Domänenname)**: Vollständiger Domänenname für internen (StoreFront) und externen (Citrix ADC) Zugriff.
- **Maschinelles Lernen**: Art der Datenanalysetechnologie, die Wissen extrahiert, ohne explizit dafür programmiert zu werden. Daten aus einer Vielzahl potenzieller Quellen wie Anwendungen, Sensoren, Netzwerken, Geräten und Geräten werden in ein System für maschinelles Lernen eingespeist. Das System verwendet die Daten und wendet Algorithmen an, um eine eigene Logik aufzubauen, um ein Problem zu lösen, Erkenntnisse abzuleiten oder eine Vorhersage zu treffen.
- **Microsoft Graph Security**: Gateway, das Kundensicherheit und Unternehmensdaten miteinander verbindet. Bietet einfach zu überprüfende Warnungen und Behebungsoptionen, wenn eine Maßnahme ergriffen werden muss. Weitere Informationen
- **Leistungsanalyse**: Dienst, der Einblick in die Details der Benutzersitzung in einer Organisation bietet. Weitere Informationen
- **Richtlinie**: Eine Reihe von Bedingungen, die erfüllt sein müssen, damit eine Aktion auf das Risikoprofil eines Benutzers angewendet werden kann. Weitere Informationen
- **Risikoindikator**: Kennzahl, die Informationen über das Ausmaß des Risikos des Unternehmens zu einem bestimmten Zeitpunkt liefert. Weitere Informationen
- **Risikobewertung**: Dynamischer Wert, der das aggregierte Risiko angibt, das ein Benutzer oder eine Entität für eine IT-Infrastruktur über einen vorab festgelegten Überwachungszeitraum darstellt. Weitere Informationen
- **Risikozeitplan**: Aufzeichnung des riskanten Verhaltens eines Benutzers oder einer Entität, sodass Administratoren ein Risikoprofil untersuchen und die Datennutzung, Gerätenutzung, Anwendungsnutzung und Standortnutzung verstehen können. Weitere Informationen
- **Riskanter Benutzer**: Benutzer, der riskant gehandelt hat oder riskantes Verhalten gezeigt hat. Weitere Informationen
- **Sicherheitsanalyse**: Erweiterte Analyse von Daten, die verwendet werden, um überzeugende Sicherheitsergebnisse wie Sicherheitsüberwachung und Bedrohungssuche zu erzielen. Weitere Informationen

- **Sicherer privater Zugriff**: Service, der die Integration von Single Sign-On, Remote-Zugriff und Inhaltsüberprüfung in einer einzigen Lösung für die End-to-End-Zugriffskontrolle ermöglicht. Weitere Informationen.
- **Splunk**: SIEM-Software (Security Information and Event Management), die intelligente Daten von Citrix Analytics empfängt und Einblicke in die potenziellen Geschäftsrisiken liefert. Weitere Informationen.
- **UBA (User Behavior Analytics)**: Baselining von Benutzeraktivitäten und -verhalten in Kombination mit Peer-Group-Analysen, um potenzielle Eindringlinge und böswillige Aktivitäten zu erkennen.
- **Watchlist**: Liste der Benutzer oder Entitäten, die Administratoren auf verdächtige Aktivitäten überwachen möchten. Weitere Informationen.