Citrix Analytics

Machine translated content

Disclaimer

Die offizielle Version dieses Inhalts ist auf Englisch. Für den einfachen Einstieg wird Teil des Inhalts der Citrix Dokumentation maschinell übersetzt. Citrix 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 Citrix 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 Citrix gegeben wird, dass das Produkt oder den Dienst mit der Dokumentation übereinstimmt, gilt nicht in dem Umfang, in dem diese Dokumentation maschinell übersetzt wurde. Citrix kann nicht für Schäden oder Probleme verantwortlich gemacht werden, die durch die Verwendung maschinell übersetzter Inhalte entstehen können.

Contents

Neue Features

June 17, 2021

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
- Citrix Analytics - Usage

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

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 darüber, wie Sie auf Citrix Analytics-Angebote zugreifen können, finden Sie unter Erste Schritte.

18. Mai 2021

Neue Features

Unterstützung für * operator mit! = Betreiber

In Ihrer Suchanfrage können Sie nun den Operator * mit dem! = Operator, 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: Username! = *Schmied

> **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 Suchanfrage Citrix Virtual Apps and Desktops

Mit den Dimensionen und Desktops von Citrix Virtual Apps and Desktops`User-Name` können Sie jetzt die folgenden Operatoren verwenden: `Device IDDomainEvent-Type`

- **IN** : Weisen Sie einer Dimension mehrere Werte zu, um die Ereignisse abzurufen, die sich auf einen oder mehrere Werte beziehen.

- **NICHT 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 Operatoren finden Sie unter Self-Service-Suche.

18. März 2021

Neue Features

Unterstützung für das NOT LIKE (! ~) Betreiber

Für die Self-Service-Suchanfrage können Sie jetzt das NOT LIKE (! ~) Betreiber. 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

Neue Features

Planen Sie die E-Mail-Zustellung für eine Suchanfrage

Auf der Self-Service-Suchseite können Sie beim Speichern einer Suchanfrage auch die E-Mail-Zustellung planen, um eine Kopie der gespeicherten Suchanfrage und des entsprechenden visuellen Zusammenfassungsberichts an sich selbst und andere Benutzer zu senden. Stellen Sie Datum, Uhrzeit und Häufigkeit ein - täglich, wöchentlich oder monatlich, um mit dem Senden von E-Mails 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

New 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 Citrix Gateway in der Region der Europäischen Union

Citrix Analytics unterstützt jetzt Citrix Gateway in der EU-Region. Weitere Informationen finden Sie unter Citrix Gateway Datenquelle.

09. Juli 2020

Veraltete Unterstützung

Microsoft Internet Explorer 11 wird 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.

June 02, 2020

Neue Features

Übersichtsseite und obere Leiste in Analytics neu gestaltet

Auf der Analytics-Übersichtsseite wird die Kachel **Usage** angezeigt, die die zuvor vorhandene Kachel **Operation**ersetzt. Außerdem wird die Kachel **Produktivität** von dieser Seite entfernt. Um die Übersichtsseite anzuzeigen, wählen Sie **Hilfe** > **Übersicht** .

In ähnlicher Weise ersetzt die Registerkarte **Usage** in der oberen Leiste die Registerkarte **Operations**. Weitere Informationen finden Sie unter Neue Funktionen für Citrix Analytics - Verwendung.

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 Sicherheits- oder Leistungsinformationen (oder beides) basierend auf dem von Ihnen abonnierten Angebot.

Sie können die folgenden Citrix Analytics Abonnementangebote erwerben:

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

Data Governance protokolliert Aktualisierungen

Neue Protokolle für die folgenden Datenquellen hinzugefügt:

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

Weitere Informationen finden Sie unter Daten-Governance.

Behobene Probleme

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

09 Jan 2020

Behobene Probleme

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

18. Dezember 2019

Behobene Probleme

In der **Analytics-Kachel** auf der **Citrix Cloud-Seite** wurde die Schaltfläche **Service 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 in Asien-Pazifik Süd

Citrix Analytics Plattform verarbeitet jetzt Benachrichtigungen vom Microapps-Dienst in der Region Asien-Pazifik-Süden. Datensätze, die Leistung,
Stabilität, Nutzung, Sicherheit und Support messen, werden jedoch aggregiert und in den USA gespeichert. Weitere Informationen finden Sie unter Daten-Governance.

> **Hinweis**
>
> Microapps Service wird als Teil von Citrix Workspace angeboten. Weitere Informationen finden Sie in der Dokumentation unter Mikroapps.

04. Dezember 2019

Behobene Probleme

Einige Benutzer in der Region Asien-Pazifik-Süd können sich nicht bei Citrix Analytics anmelden, obwohl sie sich bei Citrix Cloud angemeldet haben, indem sie die **Vereinigten Staaten** als Heimatregion auswählen. [CAS-27368]

22. November 2019

Neue Features

Übersichtsseite für Analytics neu gestaltet

Die Analytics-Übersichtsseite wurde neu gestaltet, um Zugriff auf alle Analytics-Angebote von dieser Seite 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** > **Übersicht** .

21. Oktober 2019

Neue Features

Technische Sicherheit

InÜbersicht über die technische Sicherheiterhalten Sie ein Verständnis der bewährten Sicherheitspraktiken im Zusammenhang mit Citrix Analytics. Dieses Dokument beschreibt den Datenfluss, den Datenschutz, die Netzwerkanforderungen und die Sicherheitszuständigkeiten, die bei der Verwendung von Citrix Analytics berücksichtigt werden müssen.

11. September 2019

Behobene Probleme

- Citrix Cloud kann Benutzer nicht zur regionsspezifischen Citrix Analytics Seite umleiten. [CAS-20559]

20. August 2019

Behobene Probleme

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

31. Juli 2019

Neue Features

Unterstützung für die Region der Europäischen Union

Citrix Analytics unterstützt jetzt die Region der Europäischen Union. Sie können die **Europäische Union** als Heimatregion auswählen, während Sie Ihre Organisation in Citrix Cloud einbinden und den Citrix Analytics Dienst verwenden. Citrix Analytics speichert die Benutzerereignisse und Metadaten für Ihre Organisation 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 korrekt geladen. [CAS-19867]

19. Juni 2019

Behobene Probleme

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

16. November 2018

Behobene Probleme

- Wenn Sie mit Internet Explorer Version 11.0 auf Citrix Analytics zugreifen, kann die **Citrix Cloud-Navigationsleiste** nicht geladen werden, und Sie können nicht auf das Hamburger Menü zugreifen.

10. Oktober 2018

Architektur- und Plattformverbesserungen

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

23. August 2018

Citrix Analytics ist ein Cloud-Service, der über Citrix Cloud bereitgestellt wird. Es sammelt Daten über alle Citrix Portfolioprodukte hinweg und bietet umsetzbare Erkenntnisse, sodass Administratoren Sicherheitsbedrohungen proaktiv umgehen, die App-Performance verbessern und den kontinuierlichen Betrieb unterstützen können. Derzeit bietet Citrix Analytics die folgenden Analyseangebote:

- **Security Analytics**: Sortiert und bietet Einblick in das Verhalten von Benutzern und Entitäten. Weitere Informationen finden Sie unter Sicherheitsanalysen.
- **Operations Analytics**: Sortiert und präsentiert Informationen über die Aktivitäten der Benutzer, z. B. besuchte Websites und die verbrauchte Bandbreite. Weitere Informationen finden Sie unter Operations Analytics.

Neue Produktnamen

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

Möglicherweise bemerken Sie neue Namen in unseren Produkten und Produktdokumentation. Dieses Rebranding ist das Ergebnis der Erweiterung des Citrix Portfolios und der Cloud-Strategie. Weitere Informationen zum einheitlichen Citrix Portfolio finden Sie unterCitrix product guide.

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 bestehende Kundenskripte zu verhindern.
- 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

June 17, 2021

In diesem Artikel werden die bekannten Probleme speziell für die Citrix Analytics Plattform erläutert. Informationen zu den für jedes Angebot spezifischen Themen finden Sie in den entsprechenden Artikeln zu Known issues: SicherheitLeistung, und Verwendung.

- Der Link **Demo Launch** for Citrix Analytics ist beim Zugriff auf Citrix Cloud mit Safari nicht verfügbar.

  Problemumgehung: Verwenden Sie einen anderen Webbrowser wie Google Chrome, Internet Explorer oder Microsoft Edge, oder greifen Siehttps://analytics-demo.cloud.comdirekt nach der Anmeldung bei Citrix Cloud auf die Demo-Anwendung zu. [CAS-24776]

Datenquellen

June 17, 2021

Datenquellen sind die Clouddienste und die lokalen Produkte, die Daten an Citrix Analytics senden. Citrix Analytics sammelt Daten aus den folgenden Datenquellen:

- **Citrix Datenquellen**. Citrix Cloud-Dienste und lokale 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. Dazu gehören auch Citrix ADC Instanzen, die Citrix Application Delivery Management (ADM) hinzugefügt wurden, und lokale Citrix Virtual Apps and Desktops, die Citrix Workspace hinzugefügt wurden.

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

Unterstützte Datenquellen

Je nach Citrix Analytics Angebot, das 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
- Von Citrix Analytics unterstützte Datenquellen - Verwendung

Daten-Governance

June 17, 2021

Dieser Abschnitt enthält Informationen zur Erfassung, Speicherung und Aufbewahrung von Protokollen durch den Citrix Analytics-Dienst. Alle groß geschriebenen Begriffe, die nicht im Abschnitt Definitionen definiert sind, haben die Bedeutung, die im Citrix Endbenutzerservicevertrag angegeben ist.

Citrix Analytics bietet Kunden Einblicke in die Aktivitäten ihrer Citrix Computing-Umgebung. Mit Citrix Analytics können Sicherheitsadministratoren die Protokolle auswählen, die sie überwachen möchten, und basierend auf der protokollierten Aktivität gezielte Aktionen ausführen. Mit diesen Erkenntnissen können Sicherheitsadministratoren den Zugriff auf ihre Computerumgebungen verwalten und Kundeninhalte in der Computerumgebung des Kunden schützen.

Datenresidenz

Citrix Analytics Protokolle werden getrennt von den Datenquellen verwaltet und in mehreren Microsoft Azure Cloud-Umgebungen zusammengefasst, die sich in den USA und der Europäischen Union befinden. Die Speicherung der Protokolle hängt von der Heimatregion ab, die die Citrix Cloud-Administratoren beim Onboarding ihrer Organisationen in Citrix Cloud ausgewählt haben. Wenn Sie beispielsweise beim Onboarding Ihrer Organisation 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 Erfassen von Kundendaten und Protokollen in Citrix Cloud Services und Geografische Überlegungen.

Datensammlung

Citrix Cloud-Services sind für die Übertragung von Protokollen an Citrix Analytics geeignet. Protokolle werden aus den folgenden Datenquellen gesammelt:

- Citrix Zugriffssteuerung
- Citrix ADC (lokal) zusammen mit Abonnement für Citrix Application Delivery Management
- Citrix Content Collaboration
- Citrix Endpoint Management
- Citrix Virtual Apps and Desktops (Dienst- und lokale Angebote)
- Microapps Service

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 lokale Citrix Virtual Apps and Desktops, bei denen Citrix Workspace konfiguriert ist.

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

Für den Microapps-Dienst kann der Administrator Citrix Analytics nicht explizit aktivieren, um die Protokolle zu analysieren und zu speichern. Die Protokolle werden nach der Konfiguration von Microapps an Citrix Analytics übertragen.

Datenkontrolle

Protokolle, die an Citrix Analytics gesendet werden, können vom Administrator jederzeit ein- oder ausgeschaltet werden.

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

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 für maximal 13 Monate oder 396 Tage in identifizierbarer Form aufbewahrt. Alle Protokolle und zugehörige Analysedaten wie Benutzerrisikoprofile, Details zur Bewer-

tung 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.

Anlage zur Sicherheit von Citrix Diensten

Detaillierte Informationen zu den für Citrix Analytics angewandten Sicherheitskontrollen, einschließlich Zugriff und Authentifizierung, Verwaltung von Sicherheitsprogrammen, Business Continuity und Incident-Management, sind in der Citrix Services Security Exhibit enthalten.

Definitionen

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

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

Indem Sie Ihre Daten in Citrix Analytics hochladen und die Funktionen von Citrix Analytics nutzen, stimmen Sie zu, dass Citrix technische, Benutzer- oder zugehörige Informationen über Ihre Citrix-Produkte und -Dienste sammelt, speichert, übermittelt, verwaltet, verarbeitet und verwendet.

Die von Citrix empfangenen Informationen werden jederzeit in Übereinstimmung mit der Datenschutzrichtlinie von Citrix behandelt, die unter folgender Adresse abgerufen werden kann: https://www.citrix.com/about/legal/privacy/.

Anhang: gesammelte Protokolle

- Citrix Analytics für Sicherheitsprotokolle

- Citrix Analytics für Performance-Protokolle

Citrix Analytics für Sicherheitsprotokolle

- Allgemeine Protokolle
- Citrix Content Collaboration Protokolle
- Citrix Endpoint Management Dienstprotokolle
- Citrix Virtual Apps and Desktops Protokolle
- Citrix ADC Protokolle
- Citrix Virtual Apps and Desktops Standard für Azure-Protokolle
- Microapps Dienstprotokolle
- Citrix Identitätsanbieter-Protokolle
- Citrix Gateway Protokolle
- Protokolle des sicheren Browsers
- Microsoft Graph -Sicherheits-Protokolle
- Microsoft Active Directory Protokolle

Allgemeine Protokolle

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

- Header-Tasten
- Gerätekennung
- Identifizierung
- IP-Adresse
- Organisation
- Produkt
- Produktversion
- Systemzeit
- Mandantenkennung
- Typ
- Benutzer: E-Mail, ID, SAM-Kontoname, Domäne, UPN
- Version

Citrix Content Collaboration Protokolle

Die Citrix Content Collaboration Protokolle enthalten die folgenden Datenpunkte:

- Konto-ID
- Kontoinformationen: API Control Plane, App Control Plane, Subdomain
- Add On Name
- Zusätzliche Bandbreite
- Zusätzliche Bandbreitenrate
- Zusätzlicher Speicherplatz
- Zusätzliche Speicherplatzrate
- Zusätzliche Benutzerrate
- Zusätzliche Benutzer
- Address1
- Address2
- Name des erweiterten benutzerdefinierten Branding Ordners
- Alias-ID
- App-Code
- Zugeordnete Ordnervorlagen-ID
- Bandbreite max.
- Basisbandbreite
- Basisabrechnungssatz
- Basisspeicherplatz
- Basisbenutzer
- Fakturierungskontaktnummer
- Abrechnungszyklus
- Abrechnungssatz
- Abrechnungsart
- Branding Styles
- Heruntergeladene Bytes
- Bytes gesamt

- Cc Absender
- Ort
- Kundeninformationen: Ort, Client-IP, Steuerungsebene, Land, OAuth-Client-ID, Betriebssystem, Werkzeuganzeigename, Werkzeugname, Werkzeugversion
- Clientname
- Firma
- Firmenname
- Komponentenname
- Konnektortyp
- Kontakte: Vorname, Werte, Kontakt-ID, E-Mail
- Kontext: Ressourcen-ID, Ressourcentyp
- Kopierte Datei-ID
- Land
- Erstellt von
- Erstellungsdatum
- Ersteller-ID
- Standard-Zonen-ID
- Endgültig gelöscht
- Beschreibung
- Ziel: Dateipfad, übergeordnete ID, Pfad, Zonen-ID
- Speicherplatzbeschränkung
- Max. Speicherplatz
- DLP-Status
- Nach Service herunterladen
- Download-ID
- E-Mail-Adressen: Vorname, Werte
- Verschlüsselungsrate
- Endzeit
- Entity-ID
- Ereignis-ID

- Ereigniszeit
- E-Mail des Ereignisbenutzers
- Ereignisbenutzer-ID
- Ereignisse: Arbeitsvorgangsname, Ressourcentyp
- Ablaufdatum
- Fields: Account Id, Account Information Type, API Control Plane, App Control Plane, Subdomain, Approval Context Type, Approval Id, Approval Step Id, Approval Step Status, Is Linked to Approval Step, Bytes Downloaded, Client Information Type, City, Client IP, Control Plane, Country, OAuth Client ID, Operating System, Tool Display Name, Tool Name, Tool Version, Completed Step Id, Connector Type, Created By Type, Created By Email Address, Created By First Name, Created By Id, Created By Last Name, Due, End Time Event User Id, File Extension, File Id, File Name, File Path, File Size, Form Id, Last Ping Back, Name, Next Step Id, Participant Type, Participant Role, Participant Status, Participant User Id, Recipient Type, Recipient Op Name, Recipient Email Address, Recipient First Name, Recipient Id, Recipient Last Name, Role Type, Role Initiators Type, Role Initiators Op Name, Role Initiators Email Address, Role Initiators First Name, Role Initiators Id, Role Initiators Last Name, Role Instance Manager Type, Role Instance Manager Op Name, Role Instance Manager Email Address, Role Instance Manager First Name, Role Instance Manager Id, Role Instance Manager Last Name, Role Template Manager Type, Role Template Manager Op Name, Role Template Manager Email Address, Role Template Manager First Name, Role Template Manager Id, Role Template Manager Last Name, Role View Report Type, Role View Report Op Name, Role View Report Email Address, Role View Report First Name, Role View Report Id, Role View Report Last Name, Routing Key Type, Routing Key Account Id, Routing Key Component Name, Routing Key File Extension, Routing Key File Id, Routing Key File Name, Routing Key Form Id, Routing Key Operation Name, Routing Key Product Name, Routing Key Resource Type, Routing Key Storage Center Id, Routing Key Submission Id, Routing Key Template Id, Routing Key Workflow Id, Routing Key Zone Id, Routing Key Zone Version, Server Name, Start Time, State, Step Data Type, Step Data File Id, Step Data Status, Step Data Step Type, Steps Completed, Steps Remaining, Steps Type, Steps Approvers Type, Steps Approvers Email Address, Steps Approvers First Name, Steps Approvers Id, Steps Approvers Last Name, Steps Days To Complete, Steps Sequential, Steps Step Id, Steps To Type, Steps To Email Address, Steps To First Name, Steps To Id, Steps To Last Name, Steps Viewers Type, Steps Viewers Email Address, Steps Viewers First Name, Steps Viewers Id, Steps Viewers Last Name, Steps Viewers Name, Storage Center Id, Stream Id, Submission Id, Templated Id,Trigger Type, Trigger Folder Ids, Trigger Form Id, User Id, Workflow Type, Workflow Id, Workflow Initiator Type, Workflow Initiator User Id, Workflow Name, Workflow Template Id, Workflow Trigger Resource Id, Workflow Trigger Type, Workflow Initiator Info User Id, Workflow Status, Workflow Type, Zone Id, Zone Services, Zone Version
- Dateierweiterung

- Datei-ID
- Dateiname
- Dateipfad
- Dateigröße
- Dateigröße Bytes
- Vorname
- Ordner-ID
- Ordnername
- Gewährungstypen
- Gruppen-ID
- Hat Verschlüsselung
- Hat mehrere Versionen
- Hat Power Tools
- Hash
- Integration OAuth-Client-ID
- Typ des Integrationsanbieters
- IRM-Klassifikations-ID
- Bestätigt
- Ist deaktiviert
- Ist Mitarbeiter
- Ist kostenlose Testversion
- Wird freigegeben
- Ist Vorlagenbesitz
- Ist nur Ansicht
- Artikelerweiterung
- Artikelerweiterungen
- Letzter beliebiger Login
- Nachname
- Sperre ID

- Schlosstyp
- Logo-URL
- Max. Downloads
- Methode
- Name
- Neue Stream-ID
- Anzahl der Lizenzen
- Anzahl der bezahlten Lizenzen
- OAuth-Client-ID
- Alte Stream-ID
- Vorgangsname
- Besitzer-ID
- Übergeordnete ID
- Path
- Telefon
- Planname
- Track planen
- Power Tools Rate
- Preis pro Lizenz
- Primäre E-Mail
- Primäre Subdomain
- Produktcode
- Produktname
- Empfänger-ID
- Empfänger-IDs
- URIs umleiten
- Erforderliches Login
- Erforderliche Benutzerinformationen
- Ressourcentyp

- Root-Item-ID
- Routing-Schlüssel: Konto-ID, Add On Name, App-Code, Komponentenname, Connector-Typ, Entity-ID, Datei-ID, Ordner-ID, Gruppen-ID, Integration-Provider-Typ, OAuth-Client-ID, Vorgangsname, übergeordnete ID, Produktname, Ressourcentyp, Freigabe-ID, Daten-ID, Benutzer-ID, Version, Zonen-ID
- Bereich
- Semantischer Pfad
- Servername
- Freigabe-ID
- Informationen teilen: Alias-ID, Ersteller-ID, Freigabe-ID, Teile-Untertyp-ID
- Teiltyp-ID freigeben
- Freigabeart
- Einzelversion
- Startzeit
- Status
- Name des Speichercenters
- Stream-ID
- Subdomains: Operationsname, Werte
- Abonnierte Ressourcen-ID
- Abonnierter Ressourcentyp
- Steuergebietscode
- Titel
- Aktualisierungsdatum
- Upload-ID
- URL-Pfad
- Erweiterte benutzerdefinierte Branding verwenden
- Benutzer-E-Mail
- Benutzer-ID
- Max. Benutzer
- Benutzerrollen: Vorname, Werte

- Version
- Webhook-Abonnement-ID
- Webhook-URL
- Zippen
- Zonen-ID

Citrix Endpoint Management Dienstprotokolle

Die Citrix Endpoint Management Dienstprotokolle enthalten die folgenden Datenpunkte:

- Richtlinientreue
- Unternehmenseigentum
- Geräte-ID
- Gerätemodell
- Gerätetyp
- Geo Breitengrad
- Geo-Längengrad
- Hostname
- IMEI
- IP-Adresse
- Jailbreak
- Letzte Aktivität
- Verwaltungsmodus
- Betriebssystem
- Betriebssystemversion
- Plattforminformationen
- Grund
- Seriennummer
- Betreut

Citrix Virtual Apps and Desktops Protokolle

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

- App-Name
- Browser
- Details: Formatgröße, Formattyp, Initiator, Ergebnis
- Geräte-ID
- Gerätetyp
- Dateiname
- Dateipfad
- Dateigröße
- Jailbreak
- Auftragsdetails: Dateiname, Format, Größe
- Ort: Geschätzter, Breitengrad, Längengrad
- Lange CMD-Linie
- Moduldateipfad
- Vorgang
- Betriebssystem
- Zusätzliche Informationen zur Plattform
- Druckername
- SaaS-App-Name
- Sitzungsdomäne
- Name des Sitzungsservers
- Names des Sitzungsbenutzers
- Sitzungs-GUID
- Zeitstempel
- Zeitzone: Verzerrung, DST, Name
- Typ
- URL
- Benutzeragent

Citrix ADC Protokolle

Die Citrix ADC Protokolle enthalten die folgenden Datenpunkte:

- Container
- Dateien
- Format
- Typ

Citrix Virtual Apps and Desktops Standard für Azure-Protokolle

Die Citrix Virtual Apps and Desktops Standard for Azure-Protokolle enthalten die folgenden Datenpunkte:

- App-Name
- Browser
- Details: Formatgröße, Formattyp, Initiator, Ergebnis
- Geräte-ID
- Gerätetyp
- Dateiname
- Dateipfad
- Dateigröße
- Jailbreak
- Auftragsdetails: Dateiname, Format, Größe
- Ort: Geschätzter, Breitengrad, Längengrad
- Lange CMD-Linie
- Moduldateipfad
- Vorgang
- Betriebssystem
- Zusätzliche Informationen zur Plattform
- Druckername
- SaaS-App-Name
- Sitzungsdomäne
- Name des Sitzungsservers

- Names des Sitzungsbenutzers
- Sitzungs-GUID
- Zeitstempel
- Zeitzone: Verzerrung, DST, Name
- Typ
- URL
- Benutzeragent

Microapps Dienstprotokolle

- Mikroappname
- Microapp-ID
- Benachrichtigungsname
- Benachrichtigungs-ID
- Benachrichtigungspriorität
- Integration (App) ID
- Integration (App) UUID
- Name der Integration (App)
- Integration (App) Klasse
- Kanal
- Benutzerempfänger/Erstellen-E-Mail
- Benutzerempfänger/Erstellende OID
- Benutzer-Citrix Kunden-ID
- Benutzerliste der Abonnenten
- Gruppenempfänger OID
- Aktions-ID
- Aktionstyp
- Aktionszeitstempel
- Aktionsdauer
- Aktionsergebnis

- Action-Substantiv
- Aktionsverb
- Seite/Karte ID
- Seite/Karte UUID
- Seite/Kartentitel
- Seiten-/Karten-Entität
- Seite/Karte RecordID
- Ereignis-ID
- Ereignis-UUID
- Ereignistitel
- Event-Typ
- Ereignis-Kanal
- Ereignisentität
- Schaltflächen-ID
- Schaltflächen-UUID
- Schaltflächentitel
- Durchschnittliche Dauer des Data Integration Provider-API-Aufrufs
- Datenintegrationsanbieter-API-Aufruf-Spitzenrate
- API-Anrufrate für Datenintegrationsanbieter
- API-Aufrufe des Datenintegrationsanbieters insgesamt
- API-Aufrufdauer des Datenintegrationsanbieters
- API-Aufrufergebnis des Datenintegrationsanbieters

Citrix Identitätsanbieter-Protokolle

- Benutzeranmeldung:
  - Authentifizierungsdomänen: Name, Produkt, IdP-Typ, IdP-Anzeigename
    - IdP-Eigenschaften: App, Authentifizierungs-Typ, Kunden-ID, Client-ID, Verzeichnis, Aussteller, Logo, Ressourcen, TID
    - Erweiterungen:

        - Arbeitsbereich: Hintergrundfarbe, Kopfzeilenlogo, Anmeldelogo, Linkfarbe, Textfarbe, StoreFront Domänen
        - ShareFile: Kunden-ID, Kunden-Geo
        - Langlebige Token: Aktiviert, Ablauftyp, absolute Ablaufsekunde, gleitende Ablaufsekunde
    - Authentifizierungsergebnis: Benutzername, Fehlermeldung
    - Anmeldenachricht: Client-ID, Client-Name
    - Benutzeranspruch: AMR, Zugriffstoken Hash, Aud, Authentifizierungszeit, CIP-Cred, Auth Alias, Auth Domains, Gruppen, Produkt, Systemaliase, E-Mail, E-Mail verifiziert, Exp, Familienname, Vorname, IAT, IdP, ISS, Gebietsschema, Name, NBF, SID, Sub
        - Authentifizierungs-Aliasansprüche: Name, Wert
        - Verzeichniskontext: Domäne, Forrest, Identitätsanbieter, Mandanten-ID
        - Benutzer: Kunden, E-Mail, OID, SID, UPN
        - Zusätzliche IdP-Felder: Azure AD OID, Azure AD TID
- Benutzerabmeldung: Client-ID, Client-Name, Nonce, Sub-ID
- Client-Update: Aktion, Client-ID, Client-Name

Citrix Gateway Protokolle

- Transaktionsereignisse:
    - 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

- Metrik-Ereignisse:
  - 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

Protokolle des sicheren Browsers

- Anwendungsbeitrag:
  - Protokolle vor der veröffentlichten Anwendung: Authentifizierung, Browser, Änderungs-ID, Erstellt, Kundenname, Ziel-URL, E-Tag, Gateway-Service-Produkt-ID, Sitzungs-ID, Legacy-Icon, Anwendungsname, Richtlinien, ID der veröffentlichten Anwendung, Region, Ressourcenzone, Ressourcenzonen-ID, Abonnement, Zeitüberschreitung im Leerlauf, Sitzung Warnung bei Leerlaufzeitüberschreitung, Wasserzeichen, Positivliste Extern, Positivliste Intern, Positivliste Redirect
  - Protokolle nach der veröffentlichten Anwendung: Authentifizierung, Browser, Änderungs-ID, Erstellt, Kundenname, Ziel, E-Tag, Gateway-Service-Produkt-ID, Sitzungs-ID, Legacy-Icon, Anwendungsname, Richtlinien, ID der veröffentlichten Anwendung, Region, Ressourcenzone, Ressourcenzonen-ID, Abonnement, Timeout für Sitzung im Leerlauf, Sitzung im Leerlauf Zeitüberschreitungswarnung, Wasserzeichen, Externe URL der Positivliste, interne URL der Positivliste, URL für die Weiterleitung der Positivliste
- Anwendung löschen:
  - Protokolle vor der veröffentlichten Anwendung: Authentifizierung, Browser, Änderungs-ID, Erstellt, Kundenname, Ziel-URL, E-Tag, Gateway-Service-Produkt-ID, Sitzungs-ID, Legacy-Icon, Anwendungsname, Richtlinien, ID der veröffentlichten Anwendung, Region, Ressourcenzone, Ressourcenzonen-ID, Abonnement, Zeitüberschreitung im Leerlauf,

Sitzung Warnung bei Leerlaufzeitüberschreitung, Wasserzeichen, Positivliste Extern, Positivliste Intern, Positivliste Redirect

- Protokolle nach der veröffentlichten Anwendung: Authentifizierung, Browser, Änderungs-ID, Erstellt, Kundenname, Ziel, E-Tag, Gateway-Service-Produkt-ID, Sitzungs-ID, Legacy-Icon, Anwendungsname, Richtlinien, ID der veröffentlichten Anwendung, Region, Ressourcenzone, Ressourcenzonen-ID, Abonnement, Timeout für Sitzung im Leerlauf, Sitzung im Leerlauf Zeitüberschreitungswarnung, Wasserzeichen, Externe URL der Positivliste, interne URL der Positivliste, URL für die Weiterleitung der Positivliste

- Anwendungsupdate:
  - Protokolle vor der veröffentlichten Anwendung: Authentifizierung, Browser, Änderungs-ID, Erstellt, Kundenname, Ziel-URL, E-Tag, Gateway-Service-Produkt-ID, Sitzungs-ID, Legacy-Icon, Anwendungsname, Richtlinien, ID der veröffentlichten Anwendung, Region, Ressourcenzone, Ressourcenzonen-ID, Abonnement, Zeitüberschreitung im Leerlauf, Sitzung Warnung bei Leerlaufzeitüberschreitung, Wasserzeichen, Positivliste Extern, Positivliste Intern, Positivliste Redirect
  - Protokolle nach der veröffentlichten Anwendung: Authentifizierung, Browser, Änderungs-ID, Erstellt, Kundenname, Ziel, E-Tag, Gateway-Service-Produkt-ID, Sitzungs-ID, Legacy-Icon, Anwendungsname, Richtlinien, ID der veröffentlichten Anwendung, Region, Ressourcenzone, Ressourcenzonen-ID, Abonnement, Timeout für Sitzung im Leerlauf, Sitzung im Leerlauf Zeitüberschreitungswarnung, Wasserzeichen, Externe URL der Positivliste, interne URL der Positivliste, URL für die Weiterleitung der Positivliste

- Berechtigung Erstellen:
  - Protokolle vor der Anspruchserstellung: Genehmigt, Kunden-ID, Data-Aufbewahrungstage, Enddatum, Kulanzzeitraum Tage, Sitzungs-ID, Produkt-SKU, Menge, Seriennummern, Startdatum, Status, Typ
  - Protokolle nach der Erstellung der Berechtigung: Genehmigt, Kunden-ID, Data-Aufbewahrungstage, Enddatum, Kulanzzeitraum Tage, Sitzungs-ID, Produkt-SKU, Menge, Seriennummern, Startdatum, Status, Typ

- Berechtigungsaktualisierung:
  - Protokolle vor der Berechtigungsaktualisierung: Genehmigt, Kunden-ID, Data-Aufbewahrungstage, Enddatum, Kulanzzeitraum Tage, Sitzungs-ID, Produkt-SKU, Menge, Seriennummern, Startdatum, Status, Typ
  - Protokolle nach der Berechtigungsaktualisierung: Genehmigt, Kunden-ID, Data-Aufbewahrungstage, Enddatum, Kulanzzeitraum Tage, Sitzungs-ID, Produkt-SKU, Menge, Seriennummern, Startdatum, Status, Typ

- Sitzungszugriffshost: Host akzeptieren, Client-IP, Datum Uhrzeit, Host, Sitzung, Benutzername

- Sitzung verbinden:
  - Protokolle vor der Sitzungsverbindung: Anwendungs-ID, Anwendungsname, Browser, Erstellt, Kunden-ID, Dauer, Sitzungs-ID, IP-Adresse, Zuletzt aktualisiert, Startquelle, Benutzername
  - Protokolle nach der Sitzungsverbindung: Anwendungs-ID, Anwendungsname, Browser, Erstellt, Kunden-ID, Dauer, Sitzungs-ID, IP-Adresse, Zuletzt aktualisiert, Startquelle, Benutzername
- Sitzungsstart:
  - Protokolle vor dem Sitzungsstart: Anwendungs-ID, Anwendungsname, Browser, Erstellt, Kunden-ID, Dauer, Sitzungs-ID, IP-Adresse, Zuletzt aktualisiert, Startquelle, Benutzername
  - Protokolle nach dem Sitzungsstart: Anwendungs-ID, Anwendungsname, Browser, Erstellt, Kunden-ID, Dauer, Sitzungs-ID, IP-Adresse, Zuletzt aktualisiert, Startquelle, Benutzername
- Session Tick:
  - Protokolle vor der Sitzung: Anwendungs-ID, Anwendungsname, Browser, Erstellt, Kunden-ID, Dauer, Sitzungs-ID, IP-Adresse, Zuletzt aktualisiert, Startquelle, Benutzername
  - Protokolle nach dem Sitzungskreuz: Anwendungs-ID, Anwendungsname, Browser, Erstellt, Kunden-ID, Dauer, Sitzungs-ID, IP-Adresse, Zuletzt aktualisiert, Startquelle, Benutzername

Microsoft Graph -Sicherheits-Protokolle

- Mandanten-ID
- Benutzer-ID
- Kennung des Indikators
- Indikator UUID
- Ereigniszeit
- Zeit erstellen
- Kategorie der Warnung
- Anmelde-Speicherort
- Anmelde-IP
- Anmeldetyp

- Typ des Benutzerkontos
- Händler-Informationen
- Informationen zum Anbieter-Anbieter
- Status von Sicherheitsanfälligkeiten
- Schweregrad der Schwachstelle

Microsoft Active Directory Protokolle

- Mandanten-ID
- Zeit sammeln
- Typ
- Verzeichniskontext
- Gruppen
- Identität
- Benutzertyp
- Kontoname
- Anzahl fehlerhafter Kennwörter
- Ort
- Allgemeiner Name
- Firma
- Land
- Tage bis zum Ablauf des Kennworts
- Abteilung
- Beschreibung
- Anzeigename
- Distinguished Name
- E-Mail
- Fax-Nummer
- Vorname
- Gruppe Kategorie

- Gruppen-Geltungsbereich
- Telefon (privat)
- Initialen
- IP-Telefon
- Ist Konto aktiviert
- Ist Konto gesperrt
- Ist Sicherheitsgruppe
- Nachname
- Vorgesetzte(r)
- Mitglied von
- Mobiltelefon
- Pager
- Kennwort läuft nie ab
- Name des physischen Bereitstellungsbüros
- Postamt Box
- Postleitzahl
- Primäre Gruppen-ID
- Status
- Straße
- Titel
- Benutzerkontensteuerung
- Liste der Benutzergruppen
- Benutzerprinzipalname
- Telefon (Firma)

Citrix Analytics für Performance-Protokolle

- actionid
- actionreason
- actiontype

- adminfolder
- agentversion
- allocationtype
- applicationid
- applicationname
- applicationpath
- applicationtype
- applicationversion
- associateduserfullnames
- associatedusername
- associatedusernames
- associateduserupns
- authenticationduration
- autoreconnectcount
- autoreconnecttype
- 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
- instancecount
- interactiveenddate
- interactivestartdate
- ipaddress
- isassigned
- isinmaintenancemode
- ismachinephysical
- ispendingupdate
- ispreparing
- isremotepc
- issecureica
- lastderegisteredcode

- launchedviahostname
- launchedviaipaddress
- lifecyclestate
- 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
- Netzwerk
- networkindex
- ostype
- path
- percentcpu
- persistentuserchanges
- powerstate
- processname
- profileloadenddate
- profileloadstartdate
- protocol
- provisioningschemeid
- provisioningtype
- publishedname
- registrationstate
- serversessionvalidatedate
- sessioncount
- sessionend
- sessionid
- sessionidlesince
- sessionindex
- sessionkey
- sessionstart
- sessionstate
- sessionsupport
- sessiontype
- sid

- siteid
- sitename
- startdate
- totalmemory
- triggerinterval
- triggerlevel
- triggerperiod
- triggervalue
- usedmemory
- userid
- username
- usersid
- vdalogonduration
- version
- vmstartenddate
- vmstartstartdate
- windowsconnectionsetting

Technische Sicherheit

June 17, 2021

Der Analytics-Service, der in Citrix Cloud gehostet wird, sammelt Daten über Citrix Portfolioprodukte und Drittanbieterprodukte. Diese Produkte werden als Datenquellen bezeichnet. Citrix Analytics unterstützt sowohl Cloud- als auch lokale 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 lokalen Datenquellen erfordern jedoch eine zusätzliche Konfiguration, um in Analytics integriert zu werden. Beispielsweise müssen Sie Ihre lokalen Citrix Virtual Apps and Desktops Sites zu Citrix Workspace hinzufügen, bevor Analytics die Sites erkennen kann. Ähnlich erfordert das lokale Citrix

Gateway die Konfiguration eines Citrix ADM Agenten. Weitere Informationen zum Aktivieren von Analytics für die Datenquellen finden Sie unter Aktivieren von Analytics auf Citrix Datenquellen.

Sie können einige Drittanbieterprodukte wie Microsoft Graph Security und Microsoft Active Directory mit Analytics integrieren. Weitere Informationen finden Sie in den folgenden Themen:

- Analytics für Microsoft Graph Security aktivieren
- Analytics in Microsoft Active Directory integrieren

Citrix Analytics kann auch Risikoinformationen an eine Kunden-eigene Splunk-Umgebung senden. Diese Integration erfordert die Bereitstellung und Konfiguration von **Citrix Analytics Add-on 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 werden. 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 unterDaten-Governance.

Netzwerkanforderungen

- **Anforderungen an Citrix Cloud-Dienste**: Um die Citrix Cloud-Dienste verwenden zu können, müssen Sie über den HTTPS-Port 443 eine Verbindung zu den erforderlichen Citrix Adressen herstellen können. Weitere Informationen finden Sie unter Anforderungen an die Internetverbindung.
- **Citrix Analytics Anforderungen**: Überprüfen Sie die,Systemanforderungenbevor Sie Analytics verwenden. Zusätzlich zu den Citrix Cloud-Anforderungen müssen auf die folgenden Endpunktadressen über den HTTPS-Port 443 zugegriffen werden, um den Analytics-Dienst verwenden zu können.

Endpunkt	USA Region	EU-Region
Admin-Benutzeroberfläche	`https://analytics.cloud.com`	`https://analytics-eu.cloud.com`
Admin-Benutzeroberfläche (Demosite)	`https://analytics-demo.cloud.com`	Nicht verfügbar
API Micro-Services	`https://api.analytics.cloud.com`	`https://api.analytics-eu.cloud.com`
Öffentliche IP abrufen	`https://locus.analytics.cloud.com/`	`https://locus.analytics.cloud.com/`

Endpunkt	USA Region	EU-Region
Event Hub (Gilt nicht für Citrix ADM-Agent)	`https://citrixanalyticseh-alias.servicebus.windows.net/`	`https://citrixanalyticseheu-alias.servicebus.windows.net/`
Ereignis-Hub (für Citrix ADM-Agent)	`https://cas-eh-ns-alias.servicebus.windows.net/`	`https://cas-eh-ns-eu-alias.servicebus.windows.net/`
Bulk-Upload	`https://casstoragebulk.blob.core.windows.net`	`https://casstorebulkeu.blob.core.windows.net`

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

- **Citrix Cloud Connector Installation**: Einige Datenquellen wie Citrix Endpoint Management, Citrix Virtual Apps and Desktops und Microsoft Active Directory erfordern die Installation eines Citrix Cloud Connector am Ressourcenstandort. Der Citrix Cloud Connector ist ein Kommunikationskanal zwischen Citrix Cloud und Ihren Ressourcenstandorten. Nach der Installation von Citrix Cloud Connector müssen Sie die Webproxyeinstellungen konfigurieren. Weitere Informationen finden Sie unter Konfiguration von Cloud Connector-Proxy und Firewall.
- **Citrix Analytics Endpunkt für Splunk**: Um Analytics in Ihre Splunk Umgebung zu integrieren, müssen Sie das **Citrix Analytics Add-On für Splunk**konfigurieren. Das Add-on stellt eine Verbindung mit den folgenden Endpunkten in Citrix Analytics her:

Endpunkt	USA Region	EU-Region
Kafka Broker	`casnb-0.citrix.com:9094`	`casnb-eu-0.citrix.com:9094`
	`casnb-1.citrix.com:9094`	`casnb-eu-1.citrix.com:9094`
	`casnb-2.citrix.com:9094`	`casnb-eu-2.citrix.com:9094`

Identitäts- und Zugriffsverwaltung

- Um auf 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 erwähntIdentitäts- und Zugriffsverwaltung.
- Citrix Analytics unterstützt delegierte Administratorberechtigungen. Sie können einem Benutzer eine schreibgeschützte Administratorberechtigung zur Verwaltung von Analytics in Ihrem Unternehmen zuweisen. Weitere Informationen finden Sie unter Delegierte Administratoren.

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 und den Regionen der Europäischen Union. Der Speicherort hängt von der Heimatregion ab, die die Citrix Cloud-Administratoren beim Onboarding ihrer Organisationen in Citrix Cloud ausgewählt haben. Weitere Informationen finden Sie in den folgenden Themen:

- Geographische Erwägungen
- Daten-Governance

Datenschutz

Citrix Analytics empfängt Daten aus den abonnierten Citrix Cloud-Datenquellen, lokalen Datenquellen und den Drittanbieterprodukten. Analytics verarbeitet die empfangenen Daten nur, wenn der Kunde eine Citrix Cloud-Berechtigung hat und der Analytics-Administrator die Datenverarbeitung für jede der abonnierten Datenquellen explizit aktiviert hat.

Citrix Analytics schützt die Daten der Kunden mit den folgenden Sicherheitsmaßnahmen:

- Citrix Cloud-Authentifizierung für die Analytics-Benutzer. Weitere Informationen finden Sie unter Identitäts- und Zugriffsverwaltung.
- Mandantenbasierte Datenzugriffskontrollen, die von der Datendienst- und Datenzugriffsebene erzwungen werden.
- Starke Datenisolierung pro Kunde oder Mandant in allen Data Stores im Data Lake und Data Warehouse.
- TLS-verschlüsselte Datenübertragung zwischen den verschiedenen Micro-Services und Data Stores, anwendbar für die öffentlichen Endpunkte (APTS/Inputs/Outputs) der Plattform und innerhalb der Plattform.

- Hohe Standards in TLS-Endpunkten. TLS 1.0 und TLS 1.1 sind deaktiviert.
- Verschlüsselte Datenspeicherung mit Verschlüsselungsschlüsseln und Geheimnissen, die in den entsprechenden Schlüsseltresoren gespeichert werden.
- Starke Benutzerverwaltungszugriffskontrollen für Servicebetriebe und Support bei gleichzeitigem Schutz der Kundenprotokolle.
- Schwachstellensuche, Erkennung von Eindringlingen, Anti-Malware, Rootkit-Scans, die zusammen mit Azure Security Center verwendet werden.

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

- Lizenzvereinbarung
- Citrix Datenschutzrichtlinie
- Citrix Datenverarbeitungsvertrag
- Citrix Services Security Exhibit
- Citrix Cloud Services: Umgang mit Kundeninhalten und Protokollen
- Citrix Datenschutz- und Compliance-Informationen

Sicherheitsverantwortung

Citrix Zuständigkeit

Citrix ist verantwortlich für die Sicherung aller Infrastruktur und Daten in den von Citrix verwalteten Cloud-Umgebungen, in denen Citrix Analytics gehostet wird. Citrix ist verantwortlich für die Anwendung regelmäßiger Software-Updates und Patches in der Cloud-Umgebung, um Sicherheitslücken zu beheben.

Kundenverantwortung

Citrix Kunden sind für die Sicherung ihrer Datenquellen, Richtlinienerzwingungspunkte und SIEM-Systeme (Security Information and Event Management) verantwortlich, die in Citrix Analytics integriert sind. Dazu gehören:

- On-Premise-Datenquellen, die im Besitz von Kunden sind 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 verwenden, um Ereignisse aus Citrix Analytics zu lesen.

- Vom Kunden bereitgestellte Administratoranmeldeinformationen für die Verwaltung von Citrix Cloud-Diensten, einschließlich Citrix Analytics.
- Benutzereigene Administratorkonten, die E-Mails oder Benachrichtigungen von Citrix Cloud-Diensten empfangen.
- Vom Kunden bereitgestellte Administratoranmeldeinformationen für die Bereitstellung und Integration der Agents wie Citrix ADM Agents, Analytics-Richtlinienagent. Der Zugriff auf diese Agents muss eingeschränkt werden, da die Schlüssel lokal für die Kommunikation mit Citrix Analytics gespeichert werden.
- Citrix Analytics generierte Anmeldeinformationen für die Konfiguration von **Citrix Analytics Add-on für Splunk**.
- Endbenutzergeräte, die unter Windows, Mac, Android und iOS ausgeführt werden, um eine Verbindung mit 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
- Citrix Workspace-Plattform
- Technische Sicherheitsübersicht für Citrix Virtual Apps and Desktops Service
- Sicherheitsüberlegungen für lokale Citrix Virtual Apps and Desktops
- Sichern der StoreFront-Bereitstellung
- Technische Sicherheitsübersicht für Citrix Endpoint Management
- Technische Sicherheitsübersicht für Citrix Content Collaboration
- Dokumentation des Zugriffskontrolldienstes
- Leitfaden zur sicheren Bereitstellung für Citrix ADC
- Citrix ADM -Systemanforderungen

Systemanforderungen

June 17, 2021

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

Citrix Analytics Abonnements

Sie müssen über gültige Abonnements verfügen, um die folgenden Analytics-Produkte verwenden zu können:

- Citrix Analytics für Sicherheit
- Citrix Analytics für Leistung
- Citrix Analytics - Usage

Weitere Informationen finden Sie unter Citrix Cloud Services.

Anforderungen an Datenquellen

Bei den Datenquellen handelt es sich um Produkte, die Ereignisse an Citrix Analytics senden. Abhängig von den von Ihnen verwendeten Citrix Analytics Angeboten unterscheiden sich 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
- Von Citrix Analytics unterstützte Datenquellen - Verwendung

Unterstützte Browser

Um auf Citrix Analytics zuzugreifen, muss Ihre Workstation 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

Erste Schritte

June 17, 2021

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 zunächst ein Citrix Cloud-Konto erstellen oder einem vorhandenen Konto beitreten, das von einer anderen Person in Ihrer Organisation erstellt wurde. Ausführliche Prozesse und Anweisungen zum Vorgehen finden Sie unter Registrieren Sie sich für Citrix Cloud.

Schritt 2: Zugriff auf Analytics erhalten

Sie können auf Analytics auf eine der folgenden Arten zugreifen:

- **Fordern Sie eine Testversion Citrix Analytics Angebote an**. Klicken Sie nach der Anmeldung bei Citrix Cloud im Abschnitt **Verfügbare Dienste** auf der **Analytics**-Kachel auf **Verwalten**, um die Analytics-Übersichtsseite anzuzeigen.

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

  - Klicken Sie für Sicherheitsanalysen und Leistungsanalysen 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 verwenden. Weitere Informationen zu Serviceverfahren finden Sie unter Citrix Cloud Service - Testversionen.
  - Usage Analytics ist kostenlos mit folgenden Produkten und Paketen erhältlich:
    - Citrix Content Collaboration
    - Citrix Workspace Pakete - Standard, Premium und Premium Plus

    Wenn Sie über eines dieser Abonnements verfügen, können Sie das Usage Analytics-Angebot verwenden und die grundlegenden Nutzungsberichte der Citrix Produkte anzeigen. Sie müssen keine Testversion anfordern, um dieses Angebot nutzen zu können.

  Auf der Seite Citrix Cloud wird die **Analytics**-Kachel in den Abschnitt **Meine Dienste** verschoben.

- **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 Add-On-Service mit den Citrix Workspace-Paketen Workspace Standard, Workspace Premium und Workspace Premium Plus angeboten. Weitere Informationen finden Sie unter Citrix Cloud Services.

Schritt 3: Analytics verwalten

Für Security Analytics und Performance Analytics, nachdem Sie über die erforderlichen Abonnements verfügen oder für den Zugriff auf die Testversion berechtigt sind, auf der Übersichtsseite Analytics die Schaltfläche **Testversion anfordern** für das Angebot Änderungen in **Verwalten** . Klicken Sie auf **Verwalten**, um das dem jeweiligen Angebot entsprechende Benutzer-Dashboard anzuzeigen.

Klicken Sie für Usage Analytics auf **Erste Schritte** oder **Verwalten**, um die Verwendungs-Dashboards für Ihr Citrix Produkt anzuzeigen.

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

Weitere Informationen zu den einzelnen Analytics-Angeboten finden Sie unter

- Citrix Analytics für Sicherheit
- Citrix Analytics für Leistung
- Citrix Analytics - Usage

Finden Sie Ihren Weg

February 22, 2021

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

Obere Leiste

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

Menü “Einstellungen”

Navigieren Sie im Menü **Einstellungen** zu derIndikatoren und Richtlinien Seite oder derDatenquellen Seite.

Menü “Hilfe”

Entdecken Sie weitere Datenquellen

Ermitteln Sie neu hinzugefügte Datenquellen oder zuvor gelöschte Datenquellen.

Audit-Protokoll

Navigieren Sie zur Seite “Überwachungsprotokoll”, auf der alle in Analytics generierten Ereignisse aufgelistet werden.

Self-Service-Suche

June 17, 2021

Was ist Self-Service-Suche?

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

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

- Zugriffssteuerung
- Authentifizierung
- Content Collaboration
- Gateway
- Secure Browser
- Virtual Apps and Desktops
- Performance-Benutzer und -Sitzungen

Außerdem können Sie 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 Self-Service-Suche zu

Sie können auf die Self-Service-Suche zugreifen, indem Sie die folgenden Optionen verwenden:

- **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 über die obere Leiste

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

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 über die Risikozeitleiste des Benutzers

Verwenden Sie diese Option, wenn Sie die Benutzerereignisse anzeigen möchten, die einem Risikoindikator zugeordnet 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 (für die der Risikoindikator ausgelöst wird) auf der Self-Service-Suchseite zugeordnet sind.

Weitere Informationen zum Zeitplan für das Benutzerrisiko finden Sie unter Risiko-Timeline.

So verwenden Sie die Self-Service-Suche

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

- Facetten, um Ihre Ereignisse zu filtern.
- Suchfeld, um Ihre Abfrage einzugeben und Ereignisse zu filtern.
- Zeitauswahl, um den Zeitraum auszuwählen.
- Zeitleistendetails, um die Ereignisdiagramme anzuzeigen.
- Ereignisdaten, um die Ereignisse anzuzeigen.
- In CSV-Format exportieren, um Ihre Suchereignisse als CSV-Datei herunterzuladen.

- Visuelle Zusammenfassung exportieren um den visuellen Zusammenfassungsbericht Ihrer Suchanfrage herunterzuladen.
- Mehrspaltige Sortierung um die Events 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 Access Control-Datenquelle sind beispielsweise Reputation, Aktionen, Standort und Kategoriegruppe. Während die Facetten für Virtual 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 der Suchabfrage im Suchfeld zum Filtern von Ereignissen

Wenn Sie den Cursor in das Suchfeld platzieren, zeigt das Suchfeld eine Liste der Dimensionen basierend auf den Benutzerereignissen an. Diese Dimensionen variieren je nach Datenquelle. Verwenden Sie die Dimensionen und das Gültige Betreiber, um Ihre Suchkriterien zu definieren und nach den erforderlichen Ereignissen zu suchen.

Beispielsweise erhalten Sie bei der Self-Service-Suche nach Zugriff die folgenden Dimensionen für die Zugriffsereignisse. Verwenden Sie die Dimensionen, um Ihre Abfrage einzugeben, wählen Sie den Zeitraum aus und klicken Sie dann auf **Suchen**.

Unterstützte Betreiber bei Suchanfrage

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

Operator	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.

Operator	Beschreibung	Beispiel	Ausgabe
~	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.
UND	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.

Operator	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 dem Operator = und dem! = Betreiber. 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 nicht mit John beginnen.

Operator	Beschreibung	Beispiel	Ausgabe
		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 Citrix Virtual Apps and Desktops- `Device ID`, `DomainEvent-Type`, und verwenden `User-Name`. Dieser Operator ist nur für die String-Werte anwendbar.	Benutzername IN (John, Kevin)	Finde alle Veranstaltungen im Zusammenhang mit John oder Kevin.

Operator	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 Citrix Virtual Apps and Desktops- `Device ID`, `DomainEvent-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.

> **Hinweis**
>
> Verwenden Sie für den Operator NOT **EQUAL** bei der Eingabe 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 zwischen Groß- und Kleinschreibung

Weitere Informationen zum Angeben der Suchabfrage für die Datenquelle finden Sie im Self-Service-Suchartikel für die Datenquelle, die weiter oben in diesem Artikel erwähnt wird.

Wählen Sie die Zeit für die Anzeige des Ereignisses aus

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

Anzeigen der Timeline-Details

Die Zeitleiste bietet eine grafische Darstellung der Benutzerereignisse für den ausgewählten Zeitraum. Verschieben Sie die Selektorbalken, um den Zeitbereich auszuwählen und die Ereignisse anzuzeigen, die dem ausgewählten Zeitraum entsprechen.

Die Abbildung zeigt Details der Zeitachse für Zugriffsdaten.

Die Veranstaltung anzeigen

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

Die Abbildung zeigt die Details zu den Zugriffsdaten des Benutzers.

Spalten hinzufügen oder entfernen

Sie können Spalten entweder aus der Ereignistabelle hinzufügen oder entfernen, um die entsprechenden Datenpunkte ein- oder auszublenden. Gehen Sie wie folgt vor:

1. Klicken Sie auf **Spalten hinzufügen oder entfernen**.
2. Wählen Sie die Datenelemente aus der Liste aus oder heben Sie die Auswahl 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 aufheben, wird die Spalte **TIME** aus der Ereignistabelle entfernt. Um den Zeitdatensatz anzuzeigen, erweitern Sie die Ereigniszeile für einen Benutzer.

Exportieren der 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.

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 Zusammenfassungsbericht der Datenquellen wie Virtual Apps and Desktops, Sessions herunterladen, wo Daten als Zeitleistendetails und Balkendiagramme angezeigt werden. 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 stellen die Werte verschiedener Datenelemente wie Benutzername, Datum und Uhrzeit sowie URL dar. Diese Datenelemente unterscheiden sich je nach den ausgewählten Datenquellen.

Um eine mehrspaltige Sortierung durchzuführen, gehen Sie folgendermaßen vor:

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 andere Spalte aus der Liste “ **Dann nach** “ aus.
6. Wählen Sie die Sortierreihenfolge - 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 **Apply**.
8. Wenn Sie die vorangehenden 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 für die Access Control-Ereignisse. Die Ereignisse werden nach Zeit (in letzter zur ältesten Reihenfolge) und dann nach URL (in alphabetischer Reihenfolge) sortiert.

Alternativ können Sie eine mehrspaltige Sortierung mit der **Umschalttaste** durchführen. Drücken Sie die **Umschalttaste** und klicken Sie auf die Spaltentitel, 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

So speichern Sie eine Self-Service-Abfrage:

1. Wählen Sie die erforderliche Datenquelle und die 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 zum Speichern der benutzerdefinierten Abfrage an.

   > **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 Sie eine E-Mail für eine Suchanfrage.
7. Klicken Sie auf **Speichern**.

So zeigen Sie die gespeicherten Suchenan:

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 Suchanfrage aus, die Sie gespeichert haben.
3. Klicken Sie auf **gespeicherte Suche entfernen**.

So ändern Sie eine gespeicherte Suche:

1. **Klicken Sie auf Gespeicherte Suchen**
2. Klicken Sie auf den Namen der Suchanfrage, 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, überschreiben die geänderten Suchdaten die vorhandenen Suchdaten.

> **Hinweis**
>
> - Nur ein Abfragebesitzer kann seine gespeicherten Suchen 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 Virtual Apps and Desktops, Sitzungen, in denen Daten als Zeitleistendetails und Balkendiagramme angezeigt werden, planen. 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.

Citrix Analytics für Sicherheit (Security Analytics)

June 5, 2020

Mit dem Vorteil der Arbeit von überall, zu jeder Zeit und jedem Gerät in jedem Netzwerk, werden sensible Unternehmensdaten mehr offengelegt, als wenn Benutzer nur von einem isolierten Firmenbüro aus gearbeitet haben. Bösartige Benutzer haben eine große Angriffsfläche zum Ziel. IT-Teams haben die Aufgabe, eine hervorragende Benutzererfahrung zu bieten, ohne die Sicherheit zu beeinträchtigen. Citrix Analytics for Security kann diese Lücke mit Fokus auf Benutzersicherheit schließen.

Was ist Security Analytics?

Citrix Analytics for Security bewertet kontinuierlich das Verhalten von Citrix Virtual Apps and Desktops Benutzern und Citrix Workspace Benutzern und wendet Aktionen zum Schutz vertraulicher Unternehmensinformationen an. Die Aggregation und Korrelation von Daten über Netzwerke, virtualisierte Anwendungen und Desktops hinweg sowie Tools zur Zusammenarbeit mit Inhalten ermöglicht die Gewinnung wertvoller Erkenntnisse und gezielterer Aktionen zur Bewältigung von Sicherheitsbedrohungen für Benutzer. Außerdem unterstützt maschinelles Lernen hochgradig prädiktive Ansätze zur Identifizierung böswilliger Benutzer.

Funktionen

- Optimierte Einblicke aus Citrix Produkten und Partnerintegrationen. Weitere Informationen.
- Einfach zu bedienende Dashboards bieten eine vollständige Ansicht des Benutzerverhaltens. Weitere Informationen.

- Erkennen und verringern Sie böswillige Benutzerverhalten mithilfe von maschinellem Lernen und angepassten Richtlinien mit automatisierten Aktionen. Weitere Informationen.
- Die kontinuierliche Überwachung des Benutzerverhaltens nach der erstmaligen Authentifizierung in Unternehmensnetzwerken gewährleistet eine gute Sicherheit und eine hervorragende Benutzererfahrung. Weitere Informationen.

Dashboards

Sie können Details zum Benutzer- oder Entitätsverhalten in den folgenden Sicherheits-Dashboards anzeigen:

- Benutzer: Bietet Einblick in Benutzerverhaltensmuster in einer Organisation.
- Benutzerzugriff: Fasst die Anzahl der riskanten Domänen zusammen, auf die zugegriffen wird, und die Menge der Daten, die von den Benutzern in Ihrem Netzwerk hochgeladen und heruntergeladen werden.
- App-Zugriff: Fasst die Details der Domänen, URLs und Apps auf die Benutzer in Ihrem Netzwerk zugreifen.
- Links teilen: Fasst die Details der Muster der Freigabelinks in einer Organisation zusammen.
- Berichte: Auf dieser Seite können Sie benutzerdefinierte Berichte basierend auf den Dimensionen und Metriken erstellen, die aus den onboarded Datenquellen verfügbar sind.

So geht’s weiter

- Systemanforderungen: Mindestanforderungen, die vor dem Start erfüllt werden müssen.
- Datenquellen: Erfahren Sie mehr über die von Analytics unterstützten Produkte.
- Daten-Governance: Erfahren Sie mehr über die Erfassung, Speicherung und Aufbewahrung von Protokollen durch Analytics.
- Erste Schritte: So starten Sie mit der Verwendung von Analytics in Ihrer Organisation.

Citrix Analytics für Performance (Performance Analytics)

June 17, 2021

Was ist Performance-Analytics

Performance Analytics ist ein Citrix Analytics s-Service-Angebot (CAS), mit dem Sie wichtige Leistungsindikatoren Ihrer Citrix Virtual Apps and Desktops verfolgen, aggregieren und visualisieren können.

Im Großen und Ganzen

- Performance Analytics fasst Site-Performance-Metriken in einfach zu bedienenden Dashboards für User Experience und Infrastructure zusammen. Sie helfen Ihnen dabei, die Benutzererfahrung zu analysieren und die Nutzung Ihrer Citrix Virtual Apps and Desktops -Sites zu optimieren.
- Performance Analytics unterstützt Aggregation und Reporting von mehreren Standorten. Sie aggregiert Performance-Metriken für Ihre Cloud- und lokale Setups. Daher können Sie Daten für alle Sites in Ihrer Umgebung in einer einzigen Konsole anzeigen.
- Performance Analytics quantifiziert die Benutzerleistungsfaktoren und klassifiziert die Benutzer anhand dieser Faktoren. Es bietet umsetzbare Erkenntnisse zur Fehlerbehebung, Bildschirmverzögerungen, verzögerte Sitzungsanmeldungen und andere Leistungsindikatoren.
- Mit Performance Analytics können Sie Metriken suchen und filtern, um bestimmte Benutzer oder Sitzungen mit Leistungsproblemen einzuschränken.

So verwenden Sie Performance Analytics

Benutzererlebnis-Dashboard

Das Benutzererlebnis-Dashboard zeigt die Siteleistung in Bezug auf Faktoren wie Sitzungsreaktionszeit, Sitzungsanmeldedauer, Sitzungsfehler und Sitzungsreverbindungen, die gemeinsam die Benutzererfahrung definieren.

Wenn Sie mehrere Benutzer virtueller Apps und Desktops in Ihrer Organisation unterstützen und gelegentlich Verzögerungen beim Starten von Apps oder Desktops auftreten, erhalten Sie mithilfe der Kennzahl für die Anmeldedauer Einblicke in das Problem. Drill-Down kann Ihnen helfen, die Faktoren zu identifizieren, die zu den Problemen führen.

Infrastruktur-Dashboard

Das Infrastruktur-Dashboard zeigt den Status und die Integrität der VDAs in Ihrer Site an. Die Dashboards für Benutzer und Infrastruktur können Ihnen dabei helfen, die Verfügbarkeit von Ressourcen proaktiv zu überprüfen und Performance-Engpässe auf den Websites zu identifizieren.

- Wenn Benutzer- oder Sitzungstrends ein Absinken aufweisen, was auf eine Verringerung der Anzahl der an der Site angemeldeten Benutzer oder Sitzungen hinweist, verwenden Sie diesen

Indikator, um zu überprüfen, ob ein Hypervisor neu gestartet wurde oder die Anzahl der VDAs nicht ausreicht.

- Wenn mehrere Fälle angezeigt werden, in denen Sitzungen nicht gestartet werden, führen Sie einen Drilldown durch, um die Ursache für den Fehler zu ermitteln. Es kann zu einem Mangel an Lizenzen oder Problemen mit der VDA-Verbindung zum Delivery Controller kommen.

> **Hinweis:**
>
> **Infrastructure Analytics Dashboard** befindet sich derzeit unter Vorschau.

Mit Performance Analytics können Sie Probleme schnell analysieren, beheben und beheben und ein optimales Service-Level für Apps und Desktops aufrechterhalten.

Informationen zu den Systemanforderungen finden Sie imCitrix Analytics -SystemanforderungenArtikel.

Citrix Analytics for Performance sammelt und speichert Protokolle für Datenpunkte, wie in aufgeführtProtokolle, die für Citrix Analytics for Performance gesammelt wurden.

Voraussetzungen

Citrix Analytics for Performance ist als abonnementbasiertes Angebot verfügbar, entweder als eigenständiges Angebot oder als Paket mit Citrix Analytics for Security. Informationen zum Abonnieren von Citrix Analytics for Performance finden Sie unter `https://www.citrix.com/products/citrix-analytics-performance.html)`.

1. Überprüfen Sie, ob Ihre Workstation über einen unterstützten Webbrowser verfügt, der im Unterstützte Browser Artikel aufgeführt ist.
2. Sie benötigen ein Citrix Cloud-Konto, um den Analytics-Dienst verwenden zu können. Ausführliche Anweisungen zum Erstellen eines Citrix Cloud-Kontos finden Sie unterRegistrieren Sie sich für Citrix Cloud. Gehen Sie zuhttps://citrix.cloud.comund melden Sie sich mit Ihrem Citrix Cloud-Konto an.
3. Performance Analytics erfordert, dass Citrix Profile Management auf den Rechnern installiert ist.
4. Stellen Sie sicher, dass die erforderlichen Datenquellen wie im folgenden Abschnitt konfiguriert sind.

Konfigurieren von Datenquellen

Sie können Performance Analytics verwenden, um lokale oder Cloud-Sites zu überwachen. Sie können dieses Angebot verwenden, unabhängig davon, ob Sie ein reiner On-Premise-Kunde, ein Cloud-Kunde oder ein Hybrid-Kunde mit einer Mischung aus lokalen und Cloud-Sites sind. Die von Performance Analytics unterstützten Datenquellen sind in dem Datenquellen Artikel aufgeführt.

Sie können den Status von Cloud-Datenquellen, die für Performance Analytics relevant sind, über den **Citrix Analytics Service > Einstellungen > Datenquellen > Leistung**überprüfen.

> **Hinweis:**
>
> Performance Analytics erkennt automatisch Ihren Citrix Virtual Apps and Desktops Cloud-Dienst.
>
> Wenn Sie ein On-Premises-Kunde sind,
>
> - Machen Sie erst ein Onboarding Ihrer Citrix Virtual Apps and Desktops Desktop-Sites in Performance Analytics.
> - Um netzwerkbezogene Informationen zu Performance Analytics zu erhalten, müssen Sie auch ein Onboarding für Ihr on-premises Citrix Gateway durchführen.

Konfigurieren von on-premises Citrix Virtual Apps and Desktops Sites

Konfigurieren Sie zunächst Ihre on-premises Citrix Virtual Apps and Desktops Sites mit Performance Analytics mit Ihrer On-Premises-Director-Konsole. Die Konfiguration hilft Performance Analytics, die erforderlichen Metriken aus Ihrer Umgebung zu erhalten.

Die Versionen von Virtual Apps and Desktops Komponenten, die für die Konfiguration mit Citrix Analytics for Performance unterstützt werden, lauten wie folgt:

- Delivery Controller Version 1909 und höher
- Director Version 1909 und höher
- Maschinenversion 7.15 LTSR und höher
- Citrix Workspace-App Version 1909 und höher für Chrome, HTML5, Linux, Mac, Windows und Windows (Store). (Citrix Workspace-App für iOS und Android werden nicht unterstützt).

Weitere Hinweise zum Onboarding-Prozess finden Sie unter Konfigurieren von lokalen CVAD-Sites mit Citrix Analytics für Performance.

Konfigurieren von lokalen Citrix StoreFront

Wenn Ihre Organisation eine lokale StoreFront Bereitstellung verwendet, können Sie Ihre StoreFront-Server so konfigurieren, dass die Citrix Workspace-App Ereignisse an Citrix Analytics senden kann. Führen Sie die Schritte aus, wie unter Onboarding von Virtual Apps and Desktops-Sites mit StoreFront beschrieben.

Konfigurieren des lokalen Citrix Gateway

Damit Performance Analytics netzwerkbezogene Statistiken aus Ihrer lokalen Umgebung abrufen kann, müssen Sie Ihr lokales Citrix Gateway mit dem Citrix Application Delivery Management (ADM) Service in Citrix Cloud konfigurieren. Citrix Gateway -Versionen 12.1.x.x und höher werden unterstützt.

1. Stellen Sie sicher, dass Sie den Citrix ADM Dienst abonniert haben.
2. Registrieren Sie Ihr lokales Citrix Gateway beim Citrix ADM Dienst. Folgen Sie den Anweisungen im Citrix ADM-Artikel Erste Schritte.
3. Konfigurieren Sie HDX-Insights auf Citrix Gateway. Befolgen Sie die imHDX InsightArtikel beschriebenen Anweisungen.
4. Erweiterte Analysen aktivieren. Folgen Sie den Anweisungen im Artikel Erweiterte Analysen.

Zusammenfassung der Datenquellen

Datenquelle	Voraussetzung	Onboarding	Wertschöpfung
On-Prem Gateway	Citrix Gateway-Versionen 12.1.x.x und höher, ADM Service und HDX Insights-Abonnement	Onboard Gateway mit ADM Service	Session Responsiveness (Latency) breakdown
StoreFront	StoreFront-Version 1906 und höher	Onboarding von Virtual Apps and Desktops-Sites mit StoreFront	Endpoint Location, Failure Insights: Kommunikationsfehler, Fehlgeschlagene Sitzungen: Endpunkt-Betriebssystem, Workspace-App-Version, Startstatus des Benutzers beendet
CVAD Cloud Service - Überwachung	Citrix Cloud-Lizenz, CVAD-Service-Abonnement	Automatisch erkannt	Funktionen für Leistungsanalysen
CVAD on-prem - Director	CVAD-Abonnement mit Director Version 1909 und höher	3-stufiger Onboarding-Prozess von Director	Funktionen für Leistungsanalysen

So greifen Sie auf Performance Analytics zu

1. Suchen Sie nach der Analytics-Dienstkachel, 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** .

.

3. Citrix Analytics for Performance wird mit Dashboards geöffnet, die die User Experience und Infrastructure Performance Analytics anzeigen.

Nutzungsanalysen

June 17, 2021

> **Hinweis**
>
> Das Angebot von Usage Analytics befindet sich in der Vorschau.

Citrix Analytics — Usage (Usage Analytics) bietet Einblicke in die grundlegenden Nutzungsdaten Ihrer Citrix Produkte. Sie erhalten einen Überblick darüber, wie Benutzer mit den verschiedenen Citrix Produkten interagieren, die in Ihrer Organisation verwendet werden. Die Nutzungsdaten helfen Ihnen, die Benutzerakzeptanz und das Engagement eines Produkts zu verstehen. In den **Usage** Dashboards können Sie anhand der folgenden Metriken ermitteln, wie die Citrix Produkte verwendet werden und einen Mehrwert für Ihre Benutzer hinzufügen:

- Benutzermetriken wie aktive Verwendungen
- Produktnutzungsmetriken wie Top-Domains, auf die zugegriffen wird, verwendete Anwendungen und Data-Download-Volumen

Dashboards

Sie können die folgenden Dashboards verwenden, um die Nutzungsdaten anzuzeigen:

- Content Collaboration - Stellt die grundlegenden Nutzungsdaten des Citrix Content Collaboration Service bereit.
- Mikroapps - Stellt die grundlegenden Nutzungsdaten des Citrix Workspace Dienstes bereit.
- SaaS und Web-Apps - Stellt die grundlegenden Nutzungsdaten von Webanwendungen und SaaS-Anwendungen bereit, auf die über den Citrix Access Control-Dienst zugegriffen wird.

Wie kaufe ich Citrix Analytics - Verwendung

Citrix Analytics - Die Nutzung ist kostenlos verfügbar und in den folgenden Citrix Produkten enthalten. Um dieses Analytics-Angebot nutzen zu können, müssen Sie eines der Produkte oder Pakete kaufen:

- Citrix Content Collaboration
- Citrix Workspace Pakete - Standard, Premium und Premium Plus

So geht’s weiter

- Systemanforderungen: Mindestanforderungen, die vor dem Start erfüllt werden müssen.
- Datenquellen: Erfahren Sie mehr über die von Analytics unterstützten Produkte.
- Daten-Governance: Erfahren Sie mehr über die Erfassung, Speicherung und Aufbewahrung von Protokollen durch Analytics.
- Erste Schritte: So starten Sie mit der Verwendung von Analytics in Ihrer Organisation.

Problembehandlung für Citrix Analytics für die Sicherheit

June 17, 2021

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 von Problemen mit der Ereignisübertragung aus einer Datenquelle.
- Lösen Sie Ereignisse Virtual Apps and Desktops, SaaS-Ereignisse und Überprüfung der Ereignisübertragung an Citrix Analytics for Security aus.

Überprüfen Sie die anonymen Benutzer als legitime Benutzer

June 17, 2021

Als Administrator stellen Sie möglicherweise fest, dass einige Benutzer von Citrix Virtual Apps and Desktops in Citrix Analytics 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 des Citrix Virtual Apps and Desktops Service.

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.

Beheben von Problemen mit der Ereignisübertragung aus einer Datenquelle

June 17, 2021

Dieser Abschnitt hilft Ihnen bei der Behebung von Problemen bei der Datenübertragung in Citrix Analytics for Security. Wenn eine Datenquelle Benutzerereignisse nicht genau überträgt, können Probleme wie die Nichterkennung von Benutzern und Risikoindikatoren auftreten.

Checkliste

Sequenz	Prüfen
1	Befindet sich Ihre Organisation in einer unterstützten geografischen Region - USA, Europäische Union oder Asien-Pazifik Süd?
2	Haben Sie die richtige Berechtigung, Security Analytics zu verwenden?
3	Erfüllt Ihre Umgebung alle Systemanforderungen?
4	Sind alle entdeckten Datenquellen und die Datenverarbeitung in Analytics aktiviert?
5	Übertragen die Benutzeraktivitäten in der Datenquelle Ereignisse genau an Analytics?
6	Werden die Ereignisse virtueller Apps und Desktops an Analytics übertragen?
7	Werden die Benutzerereignisse auf der Self-Service-Suchseite in Analytics angezeigt?

Sequenz	Prüfen
8	Werden die Benutzer von Analytics entdeckt?

Prüfen 1- Befindet sich Ihre Organisation in einer unterstützten geografischen Region?

Wenn in Citrix Analytics keine Benutzerereignisse angezeigt werden, wurde Ihre Organisation möglicherweise in einer Privatregion eingebaut, die derzeit nicht unterstützt wird. Citrix Analytics empfängt keine Ereignisse aus den nicht unterstützten Regionen.

Um Citrix Analytics verwenden zu können, müssen Sie entweder **USA** oder **Europäische Union** als Heimatregion für Ihre Organisation auswählen. Wenn sich Ihre Organisation in der Region Asien-Pazifik Süd befindet, müssen Sie die Region **USA** auswählen, um Ihre Organisation zu unterstützen. Weitere Informationen finden Sie unter Geografische Überlegungen.

So überprüfen Sie die Citrix Cloud-Region, in der Ihre Organisation integriert ist:

Wählen Sie in Ihrem Citrix Cloud-Konto **Kontoeinstellungen** > **Unternehmenskonto** aus.

Unterstützte Datenquellen basierend auf ihren Standorten

Citrix Analytics unterstützt die folgenden Datenquellen basierend auf ihren geografischen Regionen. Datenquellen sind die Produkte, die Daten an Analytics senden. Weitere Informationen finden Sie unter Datenquellen.

Datenquelle	In der US-Region unterstützt	In der EU-Region unterstützt
Citrix Zugriffssteuerung	Ja	Nein
Citrix Content Collaboration	Ja	Ja
Citrix Endpoint Management	Ja	Ja
Citrix Gateway	Ja	Ja
Citrix Virtual Apps and Desktops Service	Ja	Ja
Citrix Virtual Apps and Desktops lokal	Ja	Ja
Citrix Secure Browser	Ja	Ja
Microsoft Active Directory	Ja	Ja
Microsoft Graph Security	Ja	Ja
Splunk	Ja	Ja

Test 2- Haben Sie die richtige Berechtigung, Security Analytics zu verwenden?

Citrix Analytics for Security ist ein abonnementbasiertes Angebot. Sie können entweder eine begrenzte Testversion verwenden oder ein Abonnement erwerben, um dieses Angebot zu nutzen. Weitere Informationen finden Sie unter Erste Schritte.

Check 3- Erfüllt Ihre Umgebung alle Systemanforderungen?

Citrix Analytics kann einige Minuten dauern, bis die Benutzerereignisse aus den Datenquellen empfangen werden. Wenn keine Benutzerereignisse auf den Datenquellen-Sitekarten angezeigt werden, stellen Sie sicher, dass Ihre Umgebung die Voraussetzungen erfüllt und die Systemanforderungen.

Voraussetzungen

1. Alle Ihre Citrix Cloud-Abonnements müssen aktiv sein. Stellen Sie auf der Seite Citrix Cloud sicher, dass alle Citrix Cloud-Dienste aktiv sind.
2. Wenn Sie lokale Citrix Virtual Apps and Desktops verwenden, 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 von on-premises bereitgestellten virtuellen Apps und Desktops in Workspaces.
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, kann Citrix Analytics Benutzerereignisse von Citrix Virtual Apps and Desktops nicht empfangen. Informationen zum Konfigurieren der StoreFront Bereitstellung finden Sie im Citrix Analytics-Dienst Artikel in der StoreFront-Dokumentation.
4. Führen Sie Ihre Datenquellen ein, wie in den folgenden Artikeln erwähnt:
    - Citrix Access Control-Datenquelle
    - Citrix Content Collaboration Datenquelle
    - Citrix Endpoint Management Datenquelle
    - Citrix Gateway Datenquelle
    - Citrix Virtual Apps and Desktops Datenquelle
    - Integration von Microsoft Active Directory
    - Integration von Microsoft Graph Security

5. Citrix Virtual Apps and Desktops s-Benutzer müssen die angegebene Version von Citrix Workspace-Apps oder Citrix Receiver an ihren Endpunkten verwenden. Andernfalls erhält Analytics die Benutzerereignisse nicht von den Endpunkten des Benutzers. Die Liste der unterstützten Versionen der Citrix Workspace App oder Citrix Receiver ist in verfügbar Citrix Virtual Apps and Desktops Datenquelle.

Überprüfen Sie 4- Sind alle Datenquellen entdeckt 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 dann an Citrix Analytics gesendet, wenn die Benutzer die Datenquelle aktiv verwenden.

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

Gehen Sie folgendermaßen vor, um Ihre Datenquellen zu ermitteln und Analysen zu aktivieren:

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 deaktiviert.

   > **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 aktivieren** . Klicken Sie beispielsweise auf der Sitekarte der Zugriffskontrolle **auf Datenverarbeitung aktivieren**.
4. Nachdem Sie die Datenverarbeitung aktiviert haben, verarbeitet Citrix Analytics die Ereignisse für die Datenquelle. Der Status der Sitekarte ändert sich in Datenverarbeitung am. 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 angegebenen Schritte, Erste Schritte um Analysen zu aktivieren.

Überprüfen Sie 5- Übertragen die Benutzeraktivitäten in 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 für die Datenquelle ausführen, um Ereignisse zu generieren. Um beispielsweise Ereignisse aus der Content Collaboration Datenquelle zu empfangen, müssen die Content Collaboration Benutzer einige Dateien freigeben, hochladen oder herunterladen.

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

Wenn in Citrix Analytics für Ihre Datenquelle keine Benutzerereignisse angezeigt werden, besteht eine hohe Wahrscheinlichkeit, dass die Benutzer in diesem Moment nicht aktiv sind.

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

1. Melden Sie sich beim Citrix Content Collaboration Service an.
2. Führen Sie einige übliche Benutzeraktivitäten wie 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. Gehen Sie zurück zu Citrix Analytics, und zeigen Sie auf der Seite “Datenquelle” die Seite **Content Collaboration** an. Citrix Analytics empfängt die Benutzerereignisse aus der Content Collaboration Datenquelle und wird auf der Sitekarte angezeigt.

Check 6: Werden die Ereignisse virtueller 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 Ereignisse ***SaaS App Launch*** und ***SaaS App End*** nicht an Citrix Analytics. Ein Benutzer, der eine SaaS-App mit der Citrix Workspace-App für Linux startet, wird in Citrix Analytics nicht entdeckt.

Unterstützte Ereignisse

In der folgenden Tabelle können Sie die Benutzerereignisse überprüfen, die von den einzelnen Clientversionen 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 Client.

Ereignis	Workspace-App für Windows 1907 oder höher	Workspace-App für Mac 1910.2 oder höher	Workspace-App für Linux 2006 oder höher	Workspace-App für Android - Die neueste Version ist in Google Play verfügbar	Workspace-App für iOS - Neueste Version im Apple App Store erhältlich	Workspace-App für Chrome - Neueste Version im Chrome Web Store erhältlich	Workspace-App für HTML5 2007 oder höher
Kontoanme	Ja	Ja	Ja	Ja	Ja	Nein	Nein
Sitzungsanmeldung	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Sitzungssta	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
Dateidownl	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
SaaS-App-URL-Navigation	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	Workspace-App für Android - Die neueste Version ist in Google Play verfügbar	Workspace-App für iOS - Neueste Version im Apple App Store erhältlich	Workspace-App für Chrome - Neueste Version im Chrome Web Store erhältlich	Workspace-App für HTML5 2007 oder höher
SaaS-App-Zwischenablage Zugriff	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

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

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

Führen Sie diese abschließende Prüfung durch, um sicherzustellen, dass die Ereignisse genau an Citrix Analytics übertragen werden.

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

2. Wählen Sie die Datenquelle aus, um die entsprechende Suchseite und die Ereignisse anzuzeigen.
3. Um die Daten anzuzeigen, die den Ereignissen der Content Collaboration zugeordnet sind, wählen Sie **Content Collaboration** aus der Liste aus, wählen Sie den Zeitraum aus, und klicken Sie dann auf **Suchen**.

Weitere Informationen finden Sie unter Self-Service-Suche.

Check 8- Werden die Benutzer von Analytics entdeckt?

Wenn Ereignisse an Citrix Analytics weitergeleitet werden, werden die Benutzer, die die Ereignisse generieren, erkannt und im Dashboard **Benutzer** angezeigt. Dieser Vorgang dauert in der Regel etwa einige Minuten, bevor Sie sie auf dem Dashboard anzeigen können.

1. Klicken Sie im Dashboard **Benutzer** auf den Link **Ermittelte 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 13 Monaten entdeckt wurden. Wählen Sie den Zeitraum aus, in dem die Risikoindikatorvorkommen angezeigt werden sollen.

Wenn Ereignisse erfolgreich übertragen werden, wird Ihre Citrix Analytics Umgebung erwartungsgemäß ausgeführt. Risikoindikatoren werden generiert, wenn Anomalien festgestellt werden.

Lösen Sie Ereignisse Virtual Apps and Desktops, SaaS-Ereignisse und Überprüfung der Ereignisübertragung an Citrix Analytics for Security aus

June 17, 2021

In diesem Abschnitt werden die Verfahren zum Auslösen Virtual Apps and Desktops sowie SaaS-Ereignisse beschrieben und überprüft, ob Citrix Analytics diese Benutzerereignisse aktiv empfängt.

Voraussetzungen

- Stellen Sie Citrix Virtual Apps and Desktops in Citrix Analytics ein, und aktivieren Sie dann die Datenverarbeitung. Weitere Informationen finden Sie unter Citrix Virtual Apps and Desktops Datenquelle.
- Verwenden Sie die richtigen Versionen der Citrix Workspace-App oder Citrix Receiver auf den Endpunktgeräten der Benutzer, damit die Ereignisse genau an Citrix Analytics gesendet werden. Weitere Informationen finden Sie unter Citrix Virtual Apps and Desktops Datenquelle.

- Stellen Sie vor dem Auslösen des Druckereignisses von Ihrem virtuellen Desktop sicher, dass ein Drucker in der Citrix Virtual Apps and Desktops-Umgebung konfiguriert und bereitgestellt wird. Weitere Informationen zum Verwalten eines Druckers finden Sie unter Drucken.
- Zum Auslösen der SaaS-Ereignisse wie SaaS-App Launch, SaaS-App-URL-Navigation und SaaS-App-Datei-Download müssen Sie eine konfigurierte SaaS-App aus Workspace verwenden. Häufig verwendete SaaS-Apps umfassen Salesforce, Workday, Concur, GoTo Meeting.
  - Wenn keine konfigurierten SaaS-Apps vorhanden sind, müssen Sie eine SaaS-App konfigurieren und veröffentlichen. Weitere Informationen finden Sie unterSupport for 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
    * Download 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. Geben Sie auf der Seite **Bibliothek** die SaaS-App an, die Sie zum Überprüfen der Ereignisse verwenden möchten. Beispiel: Workday.
    3. Klicken Sie auf die Auslassungspunkte 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

Einige 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 zum Problem und seiner Problemumgehung finden Sie im bekannten Probleme-CAS-16151.

Prozedur

Führen Sie die folgenden Schritte nacheinander aus, um die Ereignisse in Ihrer Citrix Virtual Apps and Desktops-Bereitstellung auszulösen, und überprüfen Sie, ob Citrix Analytics diese Ereignisse aktiv

empfängt.

> **Hinweis**
>
> - Die Ereignisse können einige Zeit in Anspruch nehmen, bis Citrix Analytics erreicht wird. Aktualisieren Sie die Seite Citrix Analytics, wenn die ausgelösten Ereignisse nicht angezeigt werden.
> - Zum Auslösen der SaaS-Ereignisse wird in diesem Verfahren die Workday-App als Beispiel verwendet. Sie können alle konfigurierten SaaS-Apps aus Ihrem Workspace verwenden, um die SaaS-Ereignisse auszulösen.

- **Kontoanmeldung**
  1. Starten Sie die Citrix Workspace-App oder Citrix Receiver, um auf Ihren Workspace oder StoreFront 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 Ihren Workspace oder StoreFront zuzugreifen.
  2. Starten Sie eine Anwendung wie den Rechner.
  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 Rechner, 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 Ihren Workspace oder StoreFront 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.
- **Dateidownload**
  1. Starten Sie die Citrix Workspace-App oder Citrix Receiver, um auf Ihren Workspace oder StoreFront 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 die 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 ab. Wenn Sie beispielsweise einen virtuellen Windows-Desktop verwenden, wählen Sie die Option **Abmelden aus** .
  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 Ihren Workspace oder StoreFront zuzugreifen.
2. Starten Sie eine SaaS-Anwendung wie Workday und warten Sie, bis die Workday-Seite geladen wurde. Navigieren Sie durch die Webseiten in Workday.

   > **Hinweis**
   >
   > Stellen Sie sicher, dass die Option **Navigieren einschränken** im Abschnitt Erweiterte 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 Seite “Workday”, die Sie gerade anzeigen.

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

- **SaaS-App-Zwischenablage Zugriff**

1. Kopieren Sie auf der Seite “Workday” Text in die Systemzwischenablage.

   > **Hinweis**
   >
   > Stellen Sie sicher, dass die Option **Zugriff auf die Zwischenablage einschränken** im Abschnitt Erweiterte Sicherheit deaktiviert ist. Weitere Informationen finden Sie unter 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.clipboard an** . Erweitern Sie die Zeile, um die Ereignisdetails anzuzeigen.

- **SaaS-App-Datei herunterladen**

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

> **Hinweis**
>
> Stellen Sie sicher, dass die Option **Downloads einschränken** im Abschnitt Erweiterte Sicherheit deaktiviert ist. Weitere Informationen finden Sie unter 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 Seite “Workday”.
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.

FAQ

June 17, 2021

Datenquelle

Was ist eine Datenquelle?

Datenquellen sind Citrix Services und Produkte, 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 Erste Schritte aus, um Citrix Analytics eine Datenquelle hinzuzufügen. Alternativ können Sie auch eine Datenquelle hinzufügen, indem Sie zu **Einstellungen > Datenquellen**navigieren.

Citrix ADM Agent

Was sind die minimalen Ressourcenanforderungen, um einen Agenten auf einem Hypervisor lokal zu installieren?

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

Muss ich Citrix 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 Enterprise-Rechenzentrum verwendet. Es werden keine Bestands- oder Analysedaten gespeichert, für die ein zusätzlicher Datenträger erforderlich wäre.

Was sind die Standardanmeldeinformationen, um sich bei einem Agenten anzumelden?

Die Standardanmeldeinformationen für die Anmeldung am Agent lautet`nsrecover`/`nsroot`. Dies meldet Sie an der Shell-Eingabeaufforderung des Agenten an.

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 mithilfe der Anmeldeinformationen`nsrecover`/auf die Shell-Eingabeaufforderung zu`nsroot`, und führen Sie 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 Service-URL erneut eingeben, wenn ich sie falsch in der Agent-Konsole eingegeben habe?

Melden Sie sich mit den Anmeldeinformationen`nsrecover`/an der Shell-Eingabeaufforderung des Agenten an`nsroot`, und geben Sie dann Folgendes 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 Citrix ADM Dienst abrufen. Melden Sie sich beim Citrix ADM Dienst an, und navigieren Sie zu **Netzwerke > Agents**. Wählen Sie auf der Seite **Agents** aus der Liste **Aktion auswählen** die Option **Aktivierungscode generieren** aus.

Kann ich meinen Aktivierungscode mit mehreren Agenten wiederverwenden?

Nein, das geht nicht.

Wie viele Citrix ADM Agenten muss ich installieren?

Die Anzahl der Agenten hängt von der Anzahl der verwalteten Instanzen in einem Rechenzentrum und vom Gesamtdurchsatz ab. Citrix empfiehlt, mindestens einen Agenten für jedes Rechenzentrum zu installieren.

Wie installiere ich mehrere Citrix ADM Agents?

Klicken Sie auf der Seite Datenquellen auf das Pluszeichen (+) neben Citrix Gateway, und folgen Sie den Anweisungen zum Installieren eines anderen Agents.

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

Kann ich zwei Agenten in einem Hochverfügbarkeits-Setup installieren?

Nein, das geht nicht.

Was mache ich, wenn meine Agentenregistrierung 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 ist 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 Citrix ADM zu und navigieren zu **Netzwerken > Agents**. 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 an der Shell Prompt des Agenten an und führen Sie die folgenden Befehle aus:`ps -ax | grep mas` und`ps -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, bis alle Daemons gestartet werden (1 Minute oder so).
- Stellen Sie sicher,`agent.conf` dass`/mpsconfig` nach erfolgreicher Registrierung des Agenten in erstellt wurde.

Onboarding von Citrix Gateway Instanzen

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

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

Melden Sie sich an der Shell-Eingabeaufforderung des Agenten 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 Citrix Gateway Onboarding-Assistenten 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 Virtual Apps and Desktops-Site

Kann ich weitere Agents auf Delivery Controllern für Citrix Analytics hinzufügen?

- Ja, ja. Durch das Hinzufügen weiterer Agents wird eine hohe Verfügbarkeit für Ihre Site gewährleistet. Citrix Analytics kann das Benutzerverhalten weiterhin analysieren, falls einer Ihrer Delivery Controller

nicht verfügbar ist.

So fügen Sie weitere Agenten hinzu:

1. Klicken Sie auf die Sitekarte und dann auf **Sitedetails anzeigen**. Citrix Analytics zeigt eine Liste der verfügbaren Delivery Controller in Ihrer Site an.
2. Klicken Sie auf **Agent installieren** für die Delivery Controller, die Sie hinzufügen möchten. Nach Abschluss der Installation ändert sich der Agent-Status in "online".

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 Citrix Gateway und Cloud Connectors vor. Informationen zur Problembehandlung finden Sie im Citrix Support Knowledge Center: CTX232517.

Wo erhalte ich Hilfe zu Citrix Analytics?

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

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

Glossar der Begriffe

June 17, 2021

- **Zugriffskontrolle**: Service, der die Integration von Single Sign-On, Remote-Zugriff und Content-Inspection in eine einzige Lösung für die End-to-End-Zugriffskontrolle ermöglicht. Weitere Informationen.
- **Aktionen**: Geschlossene Schleifenantworten auf verdächtige Ereignisse. Es werden Maßnahmen angewendet, um das Auftreten zukünftiger anomaler Ereignisse zu verhindern. Weitere Informationen.

- **Cloud Access Security Broker (CASB)**: Erzwingungspunkt für lokale oder cloudbasierte Sicherheitsrichtlinien zwischen Clouddienstnutzern und Clouddienstanbietern. CASB kombinieren und interagieren Unternehmenssicherheitsrichtlinien, wenn auf cloudbasierte Ressourcen zugegriffen werden kann. Darüber hinaus unterstützen sie Unternehmen dabei, die Sicherheitskontrollen ihrer lokalen Infrastruktur auf die Cloud auszuweiten.
- **Citrix ADC (Application Delivery Controller)**: Netzwerkgerät, das sich in einem Rechenzentrum befindet und strategisch zwischen der Firewall und einem oder mehreren Anwendungsservern befindet. Behandelt den Lastenausgleich zwischen Servern und optimiert die Endbenutzerleistung und Sicherheit für Unternehmensanwendungen. Weitere Informationen.
- **Citrix ADM (Application Delivery Management)**: Zentralisierte Netzwerkmanagement-, Analyse- und Orchestrierungslösung. Über eine einzige Plattform können Administratoren Netzwerkdienste für Scale-Out-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**: Clouddienst, der Daten über Services und Produkte hinweg sammelt (lokal und in der Cloud) und umsetzbare Erkenntnisse generiert. Administratoren können Sicherheitsbedrohungen von Benutzern und Anwendungen proaktiv umgehen, die App-Performance verbessern und den kontinuierlichen Betrieb unterstützen. Weitere Informationen.
- **Citrix Cloud**: Plattform, die über den Citrix Cloud Connector in jeder Cloud oder Infrastruktur (lokal, Public Cloud, Private Cloud oder Hybrid Cloud) eine Verbindung zu Ressourcen herstellt. Weitere Informationen.
- **Citrix Gateway**: Konsolidierte RAS-Lösung, die die RAS-Infrastruktur konsolidiert, um Single Sign-On für alle Anwendungen bereitzustellen, egal ob in einem Rechenzentrum, in der Cloud oder als SaaS bereitgestellt. Weitere Informationen.
- **Citrix Hypervisor**: Virtualisierungsmanagement-Plattform, optimiert für Anwendungs-, Desktop- und Servervirtualisierungsinfrastrukturen. Weitere Informationen.
- **Citrix Workspace-App** (früher Citrix Receiver genannt): Clientsoftware, die nahtlosen und sicheren Zugriff auf Anwendungen, Desktops und Daten von jedem Gerät, einschließlich Smartphones, Tablets, PCs und Macs, ermöglicht. Weitere Informationen.
- **DLP (Data Loss Prevention)**: Lösung, die eine Reihe von Technologien und Inspektionstechniken beschreibt, um Informationen in einem Objekt wie Datei, E-Mail, Paket, Anwendung oder Datenspeicher zu klassifizieren. Außerdem kann sich das Objekt im Speicher befinden, wird verwendet oder über ein Netzwerk hinweg. DLP-Tools können Richtlinien dynamisch anwenden, z. B. protokollieren, melden, klassifizieren, verschieben, kennzeichnen und verschlüsseln. DLP-Tools können auch Schutz für das Management von Unternehmensdatenrechten anwenden. Weitere Informationen.

- **DNS (Domain Name System)**: Netzwerkdienst, der verwendet wird, um Internet-Domainnamen zu finden und sie in IP-Adressen zu übersetzen. DNS ordnet Website-Namen, die Benutzer angeben, den entsprechenden IP-Adressen, die Maschinen bereitstellen, zu, um unabhängig vom physischen Standort der Entitäten eine Website zu finden.
- **Datenverarbeitung**: Methode zur Verarbeitung von Daten von einer Datenquelle zu Citrix Analytics. Weitere Informationen.
- **Datenquelle**: Produkt oder Service, der Daten an Citrix Analytics sendet. Eine Datenquelle kann intern oder extern sein. [Weitere Informationen]/en-us/citrix-analytics/data-sources.html) verwendet werden.
- **Datenexport**: Produkt oder Service, der Daten von Citrix Analytics empfängt und Erkenntnisse liefert. Weitere Informationen.
- **Ermittelte Benutzer**: Gesamtzahl der Benutzer in einer Organisation, die Datenquellen verwenden. Weitere Informationen.
- **FQDN (Fully Qualified Domain Name)**: Vollständiger Domänenname für internen (StoreFront) und externen (Citrix ADC) Zugriff.
- **Machine Learning**: Art der Datenanalyse-Technologie, die Wissen extrahiert, ohne explizit dafür programmiert zu werden. Daten aus einer Vielzahl von potenziellen Quellen wie Anwendungen, Sensoren, Netzwerken, Geräten und Appliances werden in ein maschinelles Lernsystem eingespeist. Das System verwendet die Daten und wendet Algorithmen an, um eine eigene Logik zu erstellen, um ein Problem zu lösen, Einblicke abzuleiten oder eine Vorhersage zu erstellen.
- **Microsoft Graph Security**: Gateway, das Kundensicherheit und Organisationsdaten verbindet. Bietet einfach zu überprüfende Warnungen und Korrekturoptionen, wenn eine Aktion ausgeführt werden muss. Weitere Informationen.
- **Performance Analytics**: Service, der Einblick in Benutzersitzungsdetails in einer Organisation bietet. Weitere Informationen.
- **Richtlinie**: Eine Reihe von Bedingungen, die erfüllt sein müssen, damit eine Aktion auf das Risikoprofil eines Benutzers angewendet wird. Weitere Informationen.
- **Risikoindikator**: Metrik, die Informationen über die Höhe der Risikoposition für ein Geschäftsrisiko bereitstellt, die die Organisation zu einem bestimmten Zeitpunkt hat. Weitere Informationen.
- **Risikobewertung**: Dynamischer Wert, der das aggregierte Risiko angibt, das ein Benutzer oder ein Unternehmen für eine IT-Infrastruktur innerhalb eines vorher festgelegten Überwachungszeitraums darstellt. Weitere Informationen.
- **Risikozeitleiste**: Aufzeichnung des riskanten Verhaltens eines Benutzers oder einer Entität, mit dem Administratoren ein Risikoprofil untersuchen und die Datenverwendung, die

Gerätenutzung, die Anwendungsnutzung und die Standortnutzung verstehen können. Weitere Informationen.

- **Riskant user**: Benutzer, der riskant gehandelt hat oder riskantes Verhalten präsentiert hat. Weitere Informationen.
- **Sicherheitsanalyse**: Erweiterte Analyse von Daten, die verwendet werden, um überzeugende Sicherheitsergebnisse wie Sicherheitsüberwachung, Bedrohungsjagd usw. zu erzielen. Weitere Informationen.
- **Splunk**: SIEM-Software (Security Information and Event Management), die intelligente Daten von Citrix Analytics empfängt und Einblicke in potenzielle Geschäftsrisiken bietet. Weitere Informationen.
- **UBA (User Behavior Analytics)**: Prozess des Baselinings der Benutzeraktivität und -verhaltens in Kombination mit Peer-Group-Analyse, um potenzielle Eindringlinge und bösartige Aktivitäten zu erkennen.
- **Usage Analytics**: Bietet Einblick in die grundlegenden Nutzungsmetriken Ihrer Citrix Produkte wie Access Control, Content Collaboration und Microapps. Weitere Informationen.
- **Agent für Virtual Apps und Desktops**: Ein Richtlinienagent, der erforderlich ist, um Aktionen und Richtlinien auf die von lokalen Sites empfangenen Ereignisse anzuwenden. Laden Sie die Agentendatei von der Analytics-Benutzeroberfläche herunter und installieren Sie diesen Agenten auf einem Delivery Controller für Ihre lokale Site. Der Agent ermöglicht Ihrer Site die Kommunikation mit Citrix Analytics auf dem HTTPS-Port 443. Weitere Informationen.
- **Watchlist**: Liste der Benutzer oder Entitäten, die Administratoren auf verdächtige Aktivitäten überwachen möchten. Weitere Informationen.

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States