Citrix Analytics

Machine translated content

Disclaimer

Contents

新機能

September 21, 2023

Citrix の目標は、Citrix Analytics のお客様に新機能や製品アップデートを提供することです。新しいリリースでは、より便利な機能をご利用いただけます。今すぐ更新してください。

このプロセスは、お客様向けのわかりやすいものになっています。最初の更新は、Citrix 内部サイトのみに適用され、その後徐々にお客様の環境に適用されます。アップデートを段階的に配信することで、製品の品質を確保し、可用性を最大限に高めることができます。

Citrix Analytics には、次の製品または製品があります。新機能と製品アップデートについては、各製品に固有の新機能記事を参照してください。

- Citrix Analytics for Security
- Citrix Analytics for Performance

このリリースノートでは、Citrix Analytics プラットフォーム固有の新機能と製品アップデートについて説明します。

2023 年 **9** 月 **21** 日

PowerShell スクリプトを使用して **StoreFront** のオンボーディングを簡素化

前提条件の確認、SStoreFront のインストール、構成のプロセスを自動化する新しい **PowerShell** スクリプトが導入されました。お客様は、StoreFront の管理者モードでこのスクリプトを実行して、オンボーディング、デボーディング、セルフチェックの実行、トラブルシューティング、および Citrix Analytics Service GUI へのオンボーディングが成功したかどうかの確認を行う必要があります。

詳しくは、「StoreFront 展開環境への接続」を参照してください。

2023 年 **8** 月 **28** 日

マイクロアプリサービス（サポート終了）

Citrix マイクロアプリサービスはサポート終了となり、ユーザーは利用できなくなりました。

2023 年 **8** 月 **1** 日

シトリックスアナリティクス**-**使用状況 **(**サポート終了**)**

Citrix Usage Analytics はサポート終了となり、ユーザーは利用できなくなりました。

2023 年 2 月 23 日

解決された問題

Citrix Virtual Apps and Desktops 2112 がリリースされる前は、Citrix Analytics は、Citrix Director から接続され、Citrix Cloud に最近登録されたオンプレミスサイトを検出できませんでした。そのため、これらの接続済みサイトは、[**Virtual Apps and Desktops-**監視] サイトカードには表示されません。この問題は現在修正されています。[CAS-63132]

2022 年 9 月 28 日

アラート通知用 **webhook**

Webhook を使用して、受信 Webhook URL が設定されている任意のサードパーティアプリケーションに Citrix Analytics のアラート通知を送信できます。Webhook は、サービスプロバイダーアプリケーションとコンシューマーアプリケーション間のリアルタイムメッセージングを可能にする HTTP コールバックです。アラート通知はリアルタイムで送信されるため、イベントが発生すると通知されます。詳細については、「アラート通知用ウェブフック」を参照してください。

2022 年 9 月 8 日

CSV エクスポートのエクスポート制限が増加しました

CSV 形式へのエクスポート機能を使用してエクスポートできる行数の上限が、10,000 行から 100 K 行に引き上げられました。詳細については、「CSV ファイルへのイベントのエクスポート」を参照してください。

2022 年 8 月 18 日

修正された問題

- アプリとデスクトップのセルフサービス検索で、**Workspace** アプリのバージョン値がダウンロードされた **CSV** ファイルでは **NA**（利用不可）として入力されましたが、ページビューでは使用できました。この問題は修正されました。[CAS-70361]

2022 年 8 月 10 日

サイト集約なしの **StoreFront** オンボーディング

StoreFront のサイトアグリゲーションの依存関係は、アプリとデスクトップ**-Workspace** アプリサイトカードから削除されました。サイトアグリゲーションにサイトを追加していない場合でも、ワークスペースアプリケーション

に［**Connect Storefront Deployment** ］オプションが表示されます。詳細については、「Citrix Virtual Apps and Desktops のデータソース」を参照してください。

2022 年 4 月 5 日

「**Secure Workspace Access**」が「**Secure Private Access**」に改名

Analytics ダッシュボードとレポートで、すべての **Secure Workspace Access** ラベルが、ブランド変更された製品名に合わせて **Secure Private Access** として更新されるようになりました。

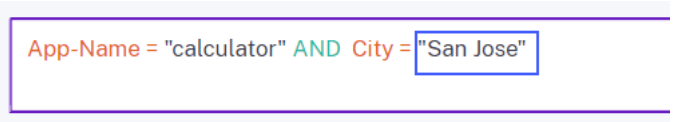
たとえば、[データソース] ページと [セルフサービス検索] ページでは、**[Secure Workspace Access]** ラベルの名前が [**Secure Private Access**] に変更されます。

2022 年 3 月 21 日

修正された問題

- [検索] ページで、検索クエリの前の条件にスペースで区切られたディメンション値が含まれている場合、ディメンションと演算子の自動候補は機能しません。

  たとえば、次のクエリでは、都市を`San Jose`として選択すると、自動候補が機能しなくなります。この問題は修正されました。[CAS-64126]

2022 年 2 月 10 日

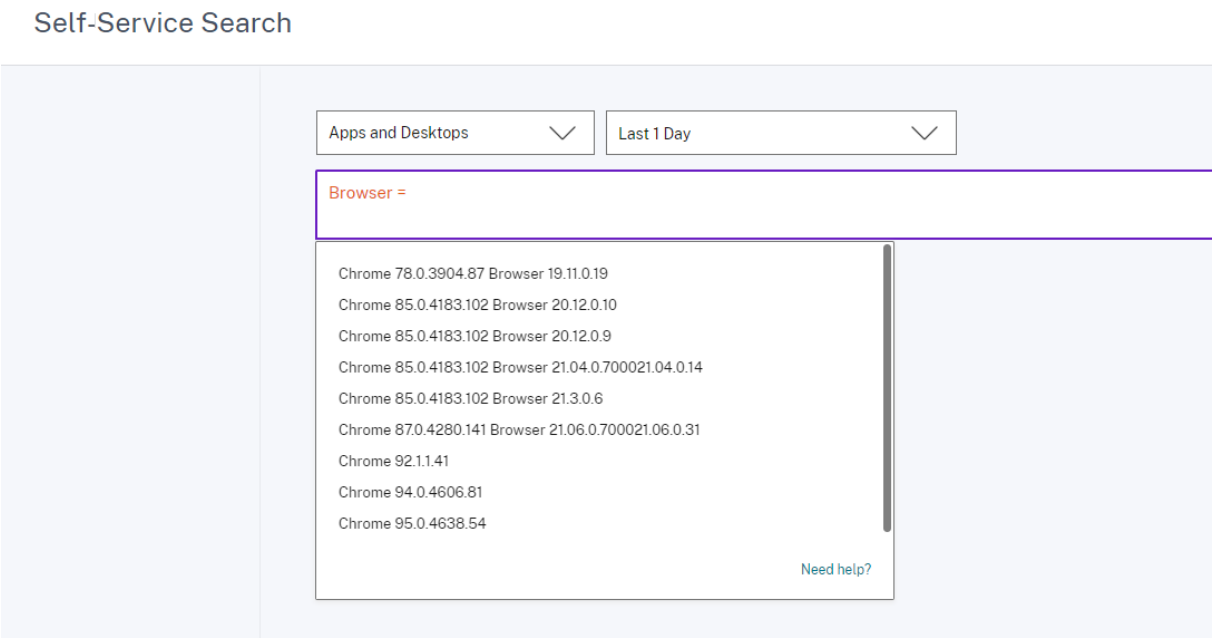
新機能

セルフサービス検索ボックスのディメンションの自動推奨値　セルフサービス検索ページで、検索ボックスでディメンションと有効な演算子を選択すると、ディメンションの値が自動的に表示されます。自動推奨リストから値を選択するか、ユースケースに応じて手動で値を入力します。値を入力すると、レコード内の一致する値が自動的に候補として表示されます。

ディメンションに推奨される値のリストは、データベースで事前定義されている (既知の値) か、履歴イベントに基づいています。

たとえば、ディメンション`Browser`と代入演算子を選択すると、既知の値が自動的に推奨されます。要件に応じて値を選択できます。

詳細については、「セルフサービス検索」を参照してください。



2021 年 12 月 20 日

新機能

アクセス制御の名前が「**Secure Workspace Access**」に変更されました　Analytics ダッシュボードとレポートでは、すべてのアクセス制御ラベルが **Secure Workspace Access** として更新され、ブランド変更された製品名に合わせられるようになりました。

たとえば、[データソース] ページと [セルフサービス検索] ページでは、[アクセス制御] ラベルの名前が [**Secure Workspace Access]** に変更されます。

2021 年 12 月 6 日

新機能

Citrix Analytics がアジア太平洋南部リージョンでサポートされるようになりました

- 組織を Citrix Cloud にオンボーディングして Citrix Analytics サービスを使用する際に、アジア太平洋南部をホームリージョンとして選択できるようになりました。詳細については、地理的考慮事項を参照してください。
- Citrix Analytics では、組織のユーザーイベントとメタデータをホームリージョンとして選択すると、アジア太平洋南部リージョンに保存されるようになりました。詳しくは、「データガバナンス」を参照してください。
- アジア太平洋南部リージョンのネットワーク要件については、「テクニカルセキュリティの概要」を参照してください。

- アジア太平洋南部リージョンでサポートされているデータソースについては、「データソース」を参照してください。

2021 年 8 月 19 日

新機能

IS EMPTY 演算子のサポート　セルフサービス検索では、条件で **IS EMPTY** 演算子を使用して、NULL または空のディメンションをチェックできるようになりました。

> 注:
>
> この演算子は、App-Name、Browser、Country などの文字列タイプのディメンションでのみ機能します。

詳細については、「セルフサービス検索」を参照してください。

2021 年 7 月 14 日

新機能

IS NOT EMPTY 演算子のサポート　セルフサービス検索では、クエリで **IS NOT EMPTY** 演算子を使用して、ディメンションが空ではない（空白ではない）ことをチェックできるようになりました。

> 注:
>
> この演算子は、App-Name、Browser、Country などの文字列タイプのディメンションでのみ機能します。

詳細については、「セルフサービス検索」を参照してください。

2021 年 6 月 07 日

非推奨の機能

Citrix Analytics デモ環境を削除しました　セキュリティ分析とパフォーマンス分析の [デモを試す] リンクが、[アナリティクス] の概要ページから削除されました。各製品のデモ環境にアクセスできなくなりました。Citrix Analytics 製品にアクセスする方法について詳しくは、「はじめに」を参照してください。

2021 年 5 月 18 日

新機能

! * 演算子と **!=** 演算子をサポート　検索クエリで、* 演算子と演算子を使用してユーザーイベントを検索できるようになりました。! = 例:

- 名前が「John」で始まらないすべてのユーザーイベントを検索するには、User-Name!= ジョン *
- 「Smith」という名前で終わらないすべてのユーザーイベントを検索するには、「User-Name!」というクエリを使用します。= * スミス

> 注
>
> 検索結果では大文字と小文字が区別されます。

詳細については、「セルフサービス検索」を参照してください。

セルフサービス検索ページでの検索バーエクスペリエンスの強化

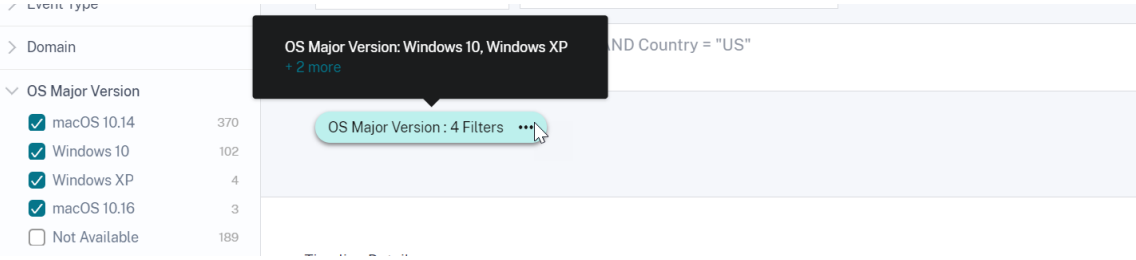
- 検索バーが複数行にわたる場合、クエリをよりよく表示できるようになりました。スクロールバーを使用して、複数行のクエリをスクロールします。以前は、複数行のクエリを表示することは困難でした。

- Safari ブラウザで検出されたカーソルジャンプの問題が修正されました。

詳細については、「セルフサービス検索」を参照してください。

セルフサービス検索でのチップビューの再設計

- 再設計されたチップは、選択した複数のファセットをよりよく見ることができます。



- チップをクリックして、要件に基づいてファセットを選択または選択解除します。

修正された問題

- Citrix Director では、[アナリティクスに移動] リンクが機能していません。この問題は、Citrix Cloud の欧州連合リージョンで組織にオンボーディングしたユーザーに発生しています。[CAS-50224]

2021 年 3 月 31 日

アプリとデスクトップの検索クエリに対する **IN** および **NOT IN** 演算子のサポート

[アプリとデスクトップ] ディメンション (`Device ID`、`DomainEvent-Type`、`User-Name`、および) では、次の演算子を使用できるようになりました。

- **IN**: ディメンションに複数の値を割り当てて、1 つ以上の値に関連するイベントを取得します。
- **NOT IN**: ディメンションに複数の値を割り当て、指定した値を含まないイベントを検索します。

> 注
>
> これらの演算子は、文字列値にのみ適用されます。

演算子について詳しくは、「セルフサービス検索」を参照してください。

2021 年 3 月 18 日

新機能

NOT LIKE (!~) 演算子のサポート　セルフサービス検索クエリでは、NOT LIKE (!~) 演算子。オペレータは、指定したマッチングパターンのユーザイベントをチェックします。これは、イベント文字列内の指定されたパターンを含まないイベントを返します。

たとえば、クエリ`User-Name !~ “John”`では、John、John Smith、または一致する名前「John」を含むユーザー以外のユーザーのイベントが表示されます。

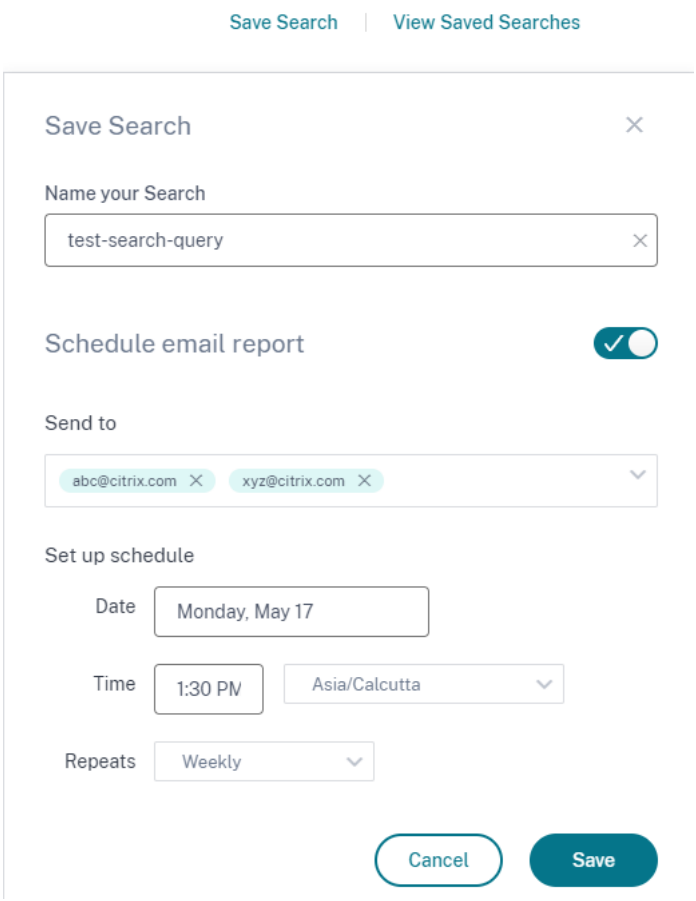
詳細については、「セルフサービス検索」を参照してください。

2021 年 2 月 23 日

新機能

検索クエリのメール配信をスケジュールする　セルフサービス検索ページでは、検索クエリの保存中に、保存した検索クエリのコピーとそれに対応するビジュアルサマリーレポートを自分や他のユーザーに送信する電子メール配信をスケジュールすることもできます。電子メールの送信を開始する日付、時刻、頻度（毎日、毎週、または毎月）を設定します。以前に保存した検索クエリの電子メール配信をスケジュールすることもできます。

詳細については、「セルフサービス検索」を参照してください。

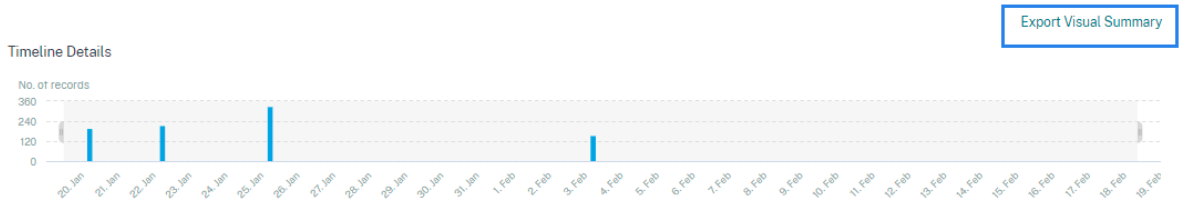


検索クエリのビジュアルサマリーをダウンロードする　セルフサービスページで、選択した期間の検索クエリのビジュアルサマリーレポートをダウンロードし、コピーを他のユーザーと共有できるようになりました。ビジュアルサマリーをエクスポートをクリックして、ビジュアルサマリーレポートを PDF としてダウンロードします。

レポートには、次の情報が含まれています。

- イベントに対して指定した検索クエリ。
- イベントに適用したファセット (フィルタ)。
- タイムラインチャート、棒グラフ、検索イベントのグラフなどの視覚的なサマリー。

詳細については、「セルフサービス検索」を参照してください。

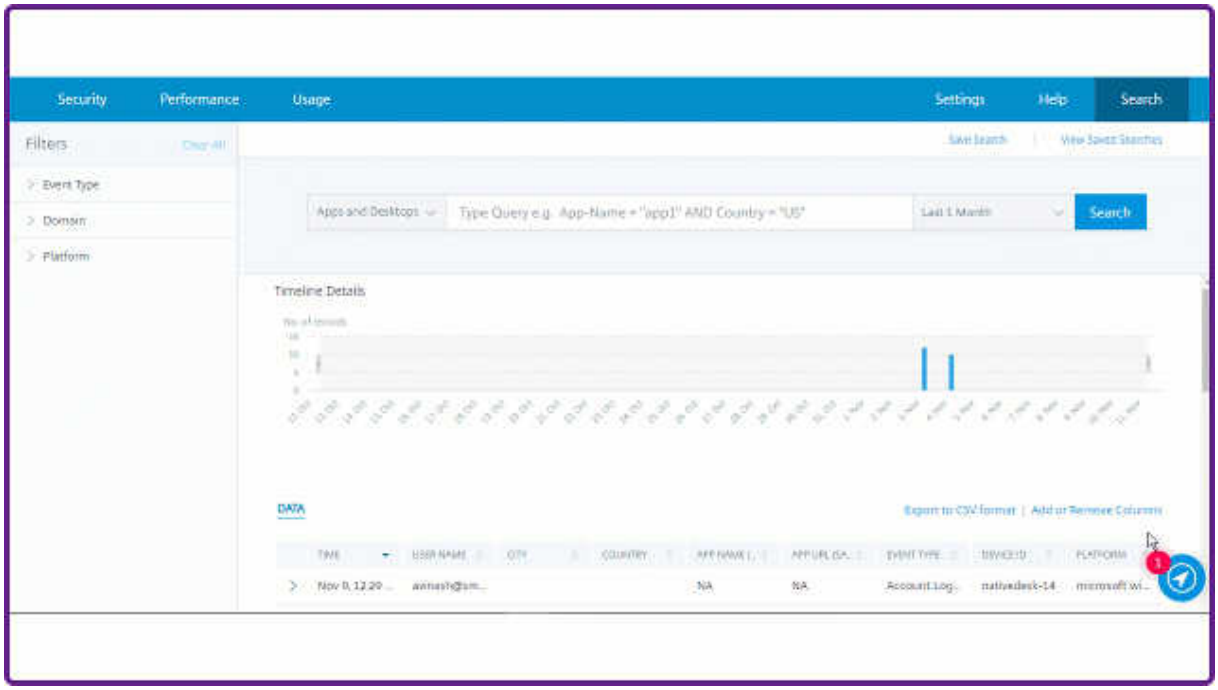


2020 年 11 月 12 日

新機能

セルフサービスクエリの保存　セルフサービスクエリを作成したら、後で使用するために保存できます。次のオプションは、クエリーとともに保存されます。

- 適用された検索フィルタ
- 選択したデータソースと期間



詳しくは、「セルフサービス検索を保存する方法」を参照してください。

2020 年 10 月 20 日

新機能

欧州連合リージョンでの **NetScaler Gateway** のサポート　Citrix Analytics は、EU リージョンで NetScaler Gateway をサポートするようになりました。詳しくは、「NetScaler Gateway データソース」を参照してください。

2020 年 **7** 月 **09** 日

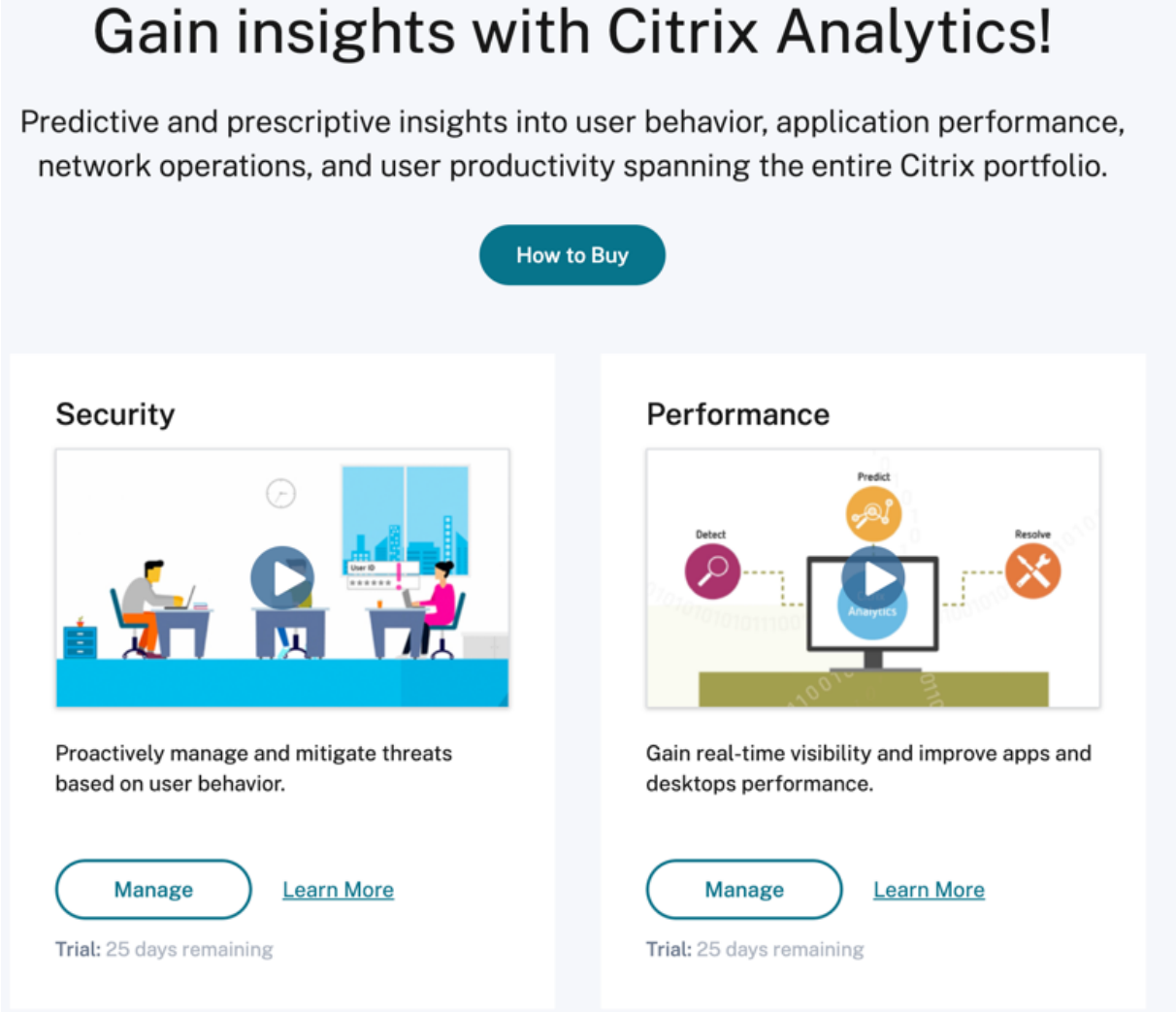
非推奨のサポート

Microsoft Internet Explorer 11 は、サポートされているブラウザーの一覧から削除されました。これは、ブラウザーで発生するセキュリティの脆弱性が原因です。サポートされているブラウザーの一覧については、「システム要件」を参照してください。

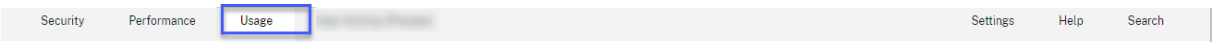
2020 年 **6** 月 **02** 日

新機能

Analytics の概要ページとトップバーのデザインを一新しました　Analytics の概要ページには、以前の オペレーション タイルに代わって 使用状況 タイルが表示されます。また、このページから 生産性 タイルが削除されます。概要ページを表示するには、［ヘルプ］>［概要］を選択します。



同様に、トップバーの［オペレーション］タブは ［使用状況］タブに置き換わります。



2020 年 2 月 20 日

新機能

Citrix Analytics サブスクリプションオファリング　ユーザーに柔軟な購入オプションを提供する Citrix は、サブスクリプションベースの 3 つの個別 Citrix Analytics 製品をご用意しました。Citrix Analytics は、サブスクライブするオファリングに応じて、独自のセキュリティまたはパフォーマンス（またはその両方）のインサイトを提供します。

次の Citrix Analytics サブスクリプションサービスを購入できます:

- Citrix Analytics for Security
- Citrix Analytics for Performance
- Citrix Analytics for Security および Performance（バンドル）

データガバナンスログの更新　次のデータソースの新しいログを追加しました:

- Citrix ID プロバイダー
- Citrix Gateway
- Secure Browser
- Microsoft Graph Security
- Microsoft Active Directory

詳しくは、「データガバナンス」を参照してください。

解決された問題

- Internet Explorer 11 では、セルフサービス検索が正確に機能しません。したがって、検索クエリを入力して検索操作を実行することはできません。[CAS-18657]

2020 年 1 月 09 日

解決された問題

- Citrix Analytics のチュートリアル機能は、欧州連合のホームリージョンのユーザーに対しては機能しません。[CAS-26297]

2019 年 12 月 18 日

解決された問題

Citrix Cloud ページの **Analytics** タイルが、［サービスの表示］ボタンを表示していました。このボタンは、ユーザーエクスペリエンスの向上を目的として、［管理］に変更されました。[CAS-27922]

2019 年 12 月 12 日

新機能

南アジア太平洋リージョンにおけるマイクロアプリサービスイベントのサポート　Citrix Analytics プラットフォームは、南アジア太平洋リージョンのマイクロアプリサービスからの通知を処理するようになりました。ただし、パフォーマンス、
安定性、使用状況、セキュリティ、およびサポートを測定するレコードは、米国で集計および保存されます。詳しくは、「データガバナンス」を参照してください。

> 注
>
> マイクロアプリサービスは、Citrix Workspace の一部として提供されています。詳しくは、「マイクロアプリ」ドキュメントを参照してください。

2019 年 12 月 04 日

解決された問題

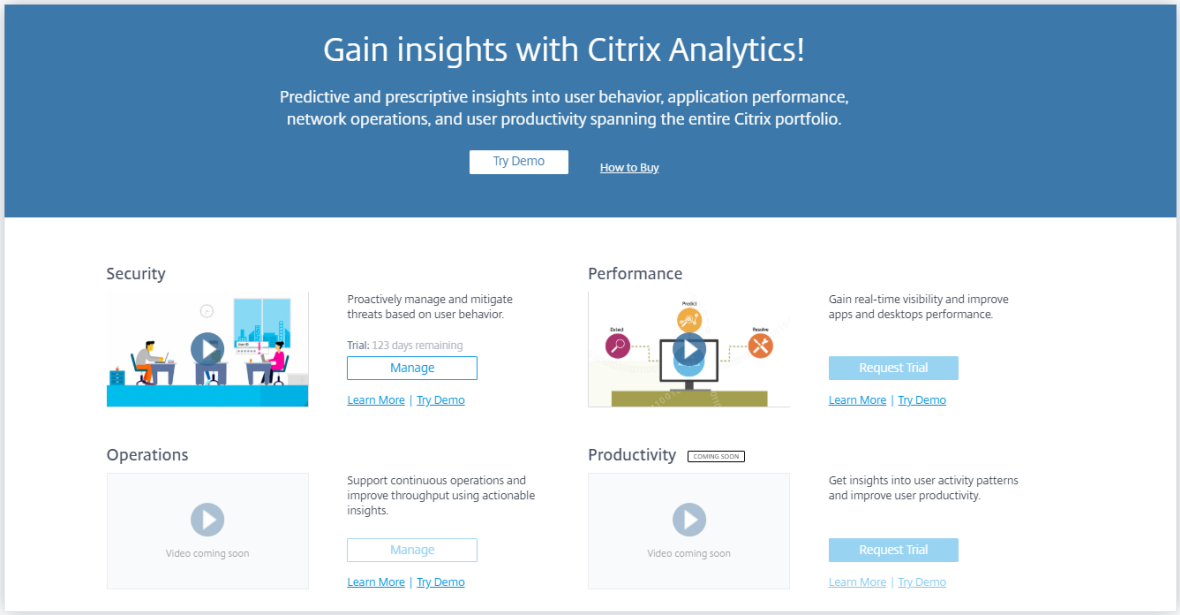
南アジア太平洋リージョンの一部のユーザーは、ホームリージョンとして米国を選択して Citrix Cloud にオンボーディングしていますが、Citrix Analytics にはサインインできません。[CAS-27368]

2019 年 11 月 22 日

新機能

Analytics の概要ページのデザインを一新しました　Analytics の概要ページのデザインが刷新され、このページからすべての Analytics オファリングにアクセスできるようになります。トライアルのリクエスト、デモの試行、または Analytics オファリングの管理を行うことができます。現在、セキュリティ分析と運用分析のみが一般に利用可能であり、したがってこのページでアクティブになっています。

概要ページを表示するには、［ヘルプ］>［概要］を選択します。



2019 年 10 月 21 日

新機能

セキュリティの技術概要　セキュリティの技術概要では、Citrix Analytics に関連するセキュリティのベストプラクティスの理解を助けます。このドキュメントでは、Citrix Analytics を使用するときに考慮する必要があるデータフロー、データ保護、ネットワーク要件、およびセキュリティの責任について説明します。

2019 年 9 月 11 日

解決された問題

- Citrix Cloud は、ユーザーをリージョン固有の Citrix Analytics ページにリダイレクトできません。[CAS-20559]

2019 年 8 月 20 日

解決された問題

- Citrix Analytics のチュートリアル機能は、Microsoft Edge および Safari ブラウザーで正確に読み込まれません。[CAS-20906]

2019 年 7 月 31 日

新機能

欧州連合のリージョンのサポート　Citrix Analytics は欧州連合リージョンをサポートするようになりました。組織を Citrix Cloud にオンボーディングし、Citrix Analytics サービスを使用するときに、欧州連合をホームリージョンとして選択できます。Citrix Analytics は、組織のユーザーイベントとメタデータを欧州連合リージョンに保存します。Citrix Cloud リージョンについて詳しくは、「地理的な考慮事項」を参照してください。

2019 年 6 月 26 日

解決された問題

- Citrix Analytics が、Internet Explorer 11 で正確に読み込まれません。[CAS-19867]

2019 年 6 月 19 日

解決された問題

- Citrix Analytics が、Microsoft Edge で正確に読み込まれません。[CAS-19930]

2018 年 11 月 16 日

解決された問題

- Internet Explorer バージョン 11.0 を使用して Citrix Analytics にアクセスしている場合、**Citrix Cloud** のナビゲーションバーが読み込まれず、ハンバーガーメニューにアクセスできなくなります。

2018 年 10 月 10 日

アーキテクチャとプラットフォームの強化

このリリースでは、パフォーマンス、スケール、監視、サポート性、セキュリティ、およびユーザーエクスペリエンスを強化するために、アーキテクチャとプラットフォームに複数の強化が行われました。

2018 年 8 月 23 日

Citrix Analytics は、Citrix Cloud を通じて提供される Cloud サービスです。Citrix ポートフォリオ製品全体のデータを収集し、実用的な洞察を提供し、管理者がセキュリティの脅威をプロアクティブに処理し、アプリケーション

のパフォーマンスを向上させ、継続的な運用をサポートできるようにします。現在、Citrix Analytics は次の分析機能を提供しています。

- セキュリティ分析: ユーザーとエンティティの動作を照合して可視化します。詳細については、「セキュリティ分析」を参照してください。
- **Operations Analytics**: 訪問した Web サイトや使用した帯域幅など、ユーザーのアクティビティに関する情報を照合して表示します。詳細については、「オペレーション分析」を参照してください。

新しい製品名

Citrix Analytics でサポートされている Citrix 製品は、Citrix の統合製品ポートフォリオの一部として名前が変更されました。

製品および製品ドキュメントに新しい名前が表示される場合があります。このブランド変更は、Citrix ポートフォリオとクラウド戦略の拡大の結果です。Citrix 統合ポートフォリオについて詳しくは、「Citrix 製品ガイド」を参照してください。
現在、製品と製品ドキュメントで移行作業が行われています。

- 製品内のコンテンツおよびドキュメントには、以前の名前が含まれている場合があります。たとえば、コンソールのテキスト、メッセージ、ディレクトリ名またはファイル名、スクリーンショット、図に以前の名前が含まれている場合があります。
- 一部の項目 (コマンドなど) は、既存のカスタマースクリプトを壊さないように、以前の名前を保持し続ける可能性があります。
- 関連する製品ドキュメントや、この製品のドキュメントからリンクされているその他のリソース（ビデオやブログの投稿など）には、以前の名前が含まれている場合があります。

既知の問題

September 21, 2023

この記事では、Citrix Analytics 製品（パフォーマンスとセキュリティ）全体に適用される既知の問題に焦点を当てています。

各サービス固有の問題については、対応する既知の問題の記事「[セキュリティとパフォーマンス](/ja-jp/performance-analytics/known-issues.html)」を参照してください。

- **Gateway-New IP** からの初回アクセスインジケータは、初回ログイン時に Gateway 経由でサービスまたはアプリケーションにアクセスするユーザに対してトリガーされます。[CAS-57963]

データソース

September 21, 2023

データソースは、Citrix Analytics にデータを送信するクラウドサービスとオンプレミス製品です。

Citrix Analytics は、次のデータソースからデータを収集します。

- **Citrix** データソース。Citrix Analytics にデータを送信する Citrix Cloud サービスおよびオンプレミス製品。Citrix Analytics は、Citrix Cloud アカウントに関連付けられている Content Collaboration や Endpoint Management などの Citrix Cloud サービスを自動的に検出します。

  Citrix Gateway や Citrix Virtual Apps and Desktops などのオンプレミス製品の場合、Citrix Analytics に接続するには一連の構成を実行する必要があります。たとえば、オンプレミスの Gateway インスタンスをアプリケーションデリバリ管理に追加する必要があります。また、オンプレミスの Virtual Apps and Desktops サイトを Workspace に追加するか、StoreFront サーバーを構成する必要があります。
- 外部データソース。Citrix Analytics と統合できる MicroMicrosoft Graph セキュリティ、Microsoft Active Directory などのサードパーティ製アプリケーション。Citrix Analytics は、統合が成功すると、これらの外部データソースからデータを収集します。

サポートされているデータソース

使用している Citrix Analytics 製品によって、データソースは異なります。各オファリングでサポートされるデータソースを確認するには、次の記事を参照してください。

- Citrix Analytics for Security でサポートされているデータソース
- パフォーマンス向け Citrix Analytics でサポートされているデータソース

Citrix Gateway、Citrix DaaS（以前の Citrix Virtual Apps and Desktops s サービス）、および Citrix Virtual Apps and Desktops s のデータソースは、セキュリティ向け Citrix Analytics と Performance 向け Citrix Analytics for Performance の両方のサービスでサポートされています。両方のオファリングに適用できるオンボーディング手順については、次の記事を参照してください。

- NetScaler Gateway データソース
- Citrix Virtual Apps and Desktops データソース

NetScaler Gateway データソース

April 12, 2024

Gateway データソースは、環境内のオンプレミスの NetScaler Gateway インスタンスを表します。Citrix Analytics は、NetScaler ADM サービスに追加された NetScaler Application Delivery Management（ADM）エージェントと Gateway インスタンスを自動的に検出します。

ユーザーが Gateway 経由でサービスまたはアプリケーションにアクセスすると、Citrix Analytics はユーザーアクセスイベントをリアルタイムで受信します 。ユーザーイベントは、セキュリティ上の脅威を検出するために処理されます。

この記事では、NetScaler Gateway を Citrix Analytics に追加する手順について説明します。これらの手順は、Citrix Analytics for Performance と Citrix Analytics for Security の両方の製品に適用されます。

前提条件

- Citrix Cloud で提供される NetScaler ADM を購読します。NetScaler ADM の使用を開始する方法については、「はじめに」を参照してください。
- Citrix ADM ライセンスを確認しました。Citrix ADM ライセンスについて詳しくは、「ライセンス」を参照してください。
- システム要件を確認し 、要件を満たしていることを確認します。

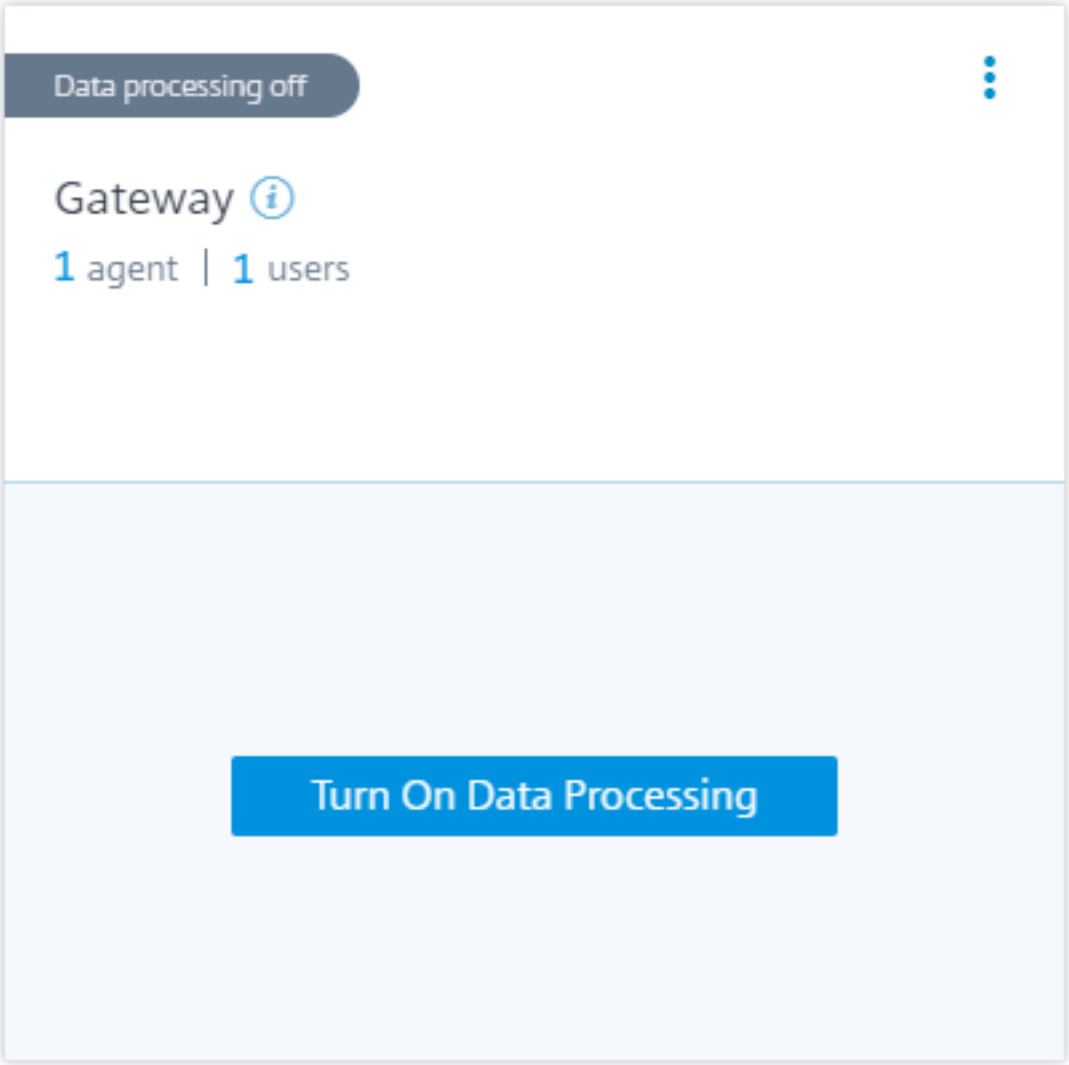
NetScaler ADM に追加されたゲートウェイデータソース

Citrix Analytics ADM サービスにすでに追加されている NetScaler ADM エージェントと NetScaler Gateway インスタンスを自動的に検出します。

データソースを表示するには:

トップバーで、[設定] > [データソース] をクリックします。提供内容に応じて、[セキュリティ] または [パフォーマンス] のいずれかを選択して Gateway サイトカードを表示します。

検出されたエージェントとユーザが Gateway サイトカードに表示されます。Citrix Analytics がこのデータソースのデータの処理を開始できるようにするには、［データ処理を有効にする］をクリックします。

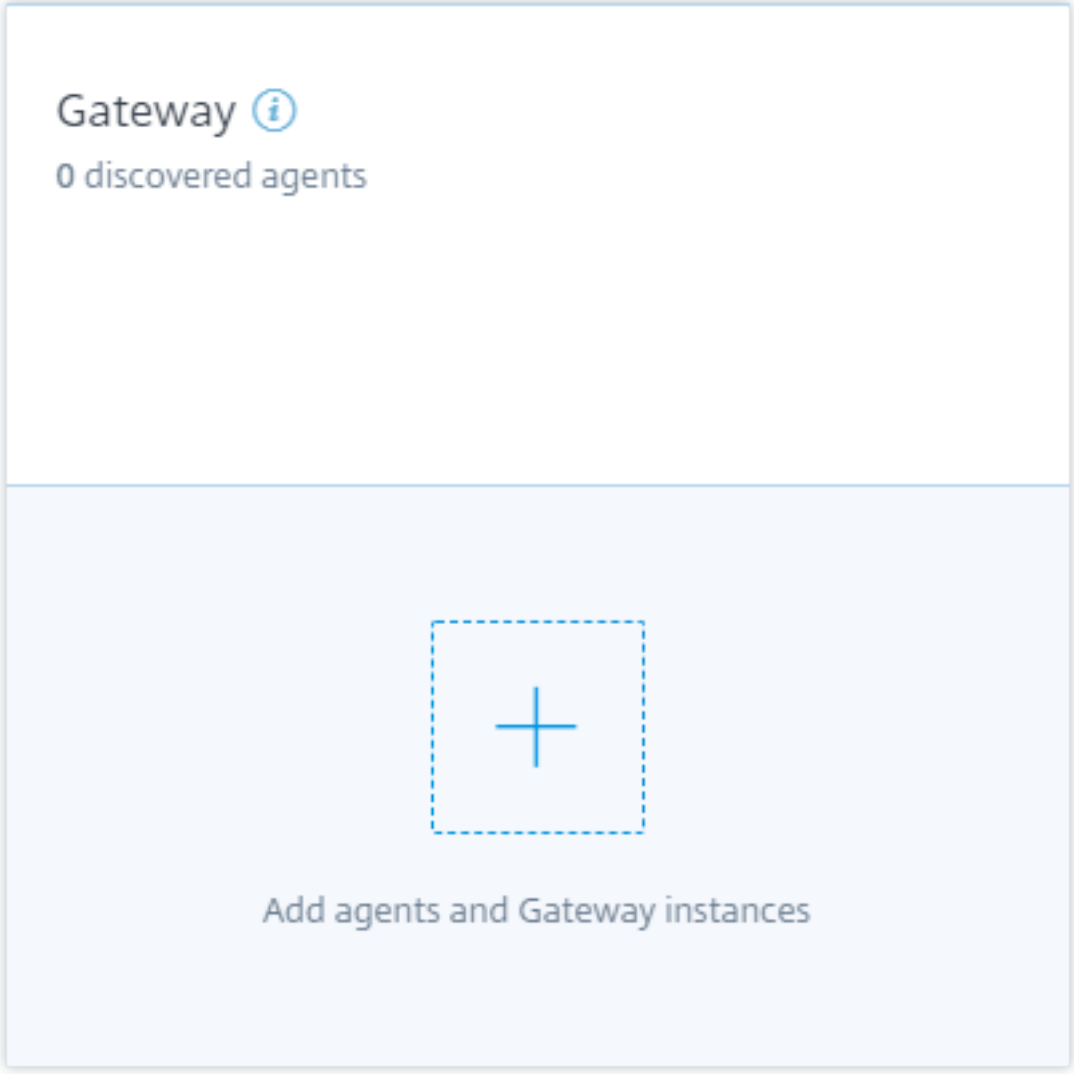


受信したイベントを表示できます。

Citrix ADM サービスでまだ有効になっていない場合は、「仮想サーバーで分析を有効にする統合プロセス」を参照してください。

NetScaler ADM に追加されないゲートウェイデータソース

Citrix **ADM** エージェントと **NetScaler Gateway** インスタンスが **NetScaler ADM** サービスに追加されていない場合、**Gateway** サイトカードには検出されたエージェントが **0** 件表示されます。



エージェントと Gateway インスタンスを検出するには、次の手順を実行します。

1. NetScaler ADM Service サブスクリプションをすでに持っている場合は、サイトカードの [**+**] をクリックしてエージェントと Gateway インスタンスを追加します。
2. NetScaler ADM サービスのサブスクリプションがない場合は、サブスクリプションする必要があります。Citrix Cloud アカウントに移動し、次の操作を行います。
   a) [利用可能なサービス] で、[アプリケーションデリバリ管理**]** タイルの **[**管理] をクリックします。
   b) 画面の指示に従って、NetScaler ADM の Express アカウントを作成します。詳細については、NetScaler ADM のドキュメントの「はじめに 」を参照してください。
   c) Express アカウントを作成したら、Analytics に戻り、[設定**] > [**データソース**] > [**セキュリティ**]** の順にクリックします。
   d) Gateway サイトカードで [**+**] をクリックして、エージェントと Gateway インスタンスを追加します。

3. 次のページで、[はじめに] をクリックします。

4. 次のタスクを実行します。

   - NetScaler ADM エージェントをインストールする
   - Gateway インスタンスを追加する
   - 仮想サーバーで Analytics を有効にする

前提条件

- **NetScaler ADM** エージェントのインストール要件：データセンターでは、Citrix Hypervisor、VMware ESXi、Microsoft Hyper-V、および Linux KVM サーバーにエージェントをインストールできます。

  次の表に、ハイパーバイザーがエージェントに提供する必要のある仮想コンピューティングリソースの一覧を示します。

Component	条件
RAM	8 GB (パフォーマンスを向上させるには 32 GB を推奨)
仮想 CPU	4 (パフォーマンス向上のため 8 個の仮想 CPU を推奨)
記憶域	120 GB
仮想ネットワークインターフェイス	1
スループット	1Gbps

- ポート要件：NetScaler ADM エージェントが NetScaler Gateway インスタンスと通信するために、次のポートが開いていることを確認します。

種類	ポート	説明
TCP	80/443	エージェントから NetScaler Gateway インスタンスへの NITRO 通信用
TCP	22	エージェントから NetScaler Gateway インスタンスへの SSH 通信用。
UDP	4739	NetScaler Gateway からエージェントへの AppFlow 通信の場合
ICMP	予約されているポートなし	エージェントから NetScaler Gateway インスタンスへのネットワーク到達可能性を検出するため。
SNMP	161, 162	NetScaler Gateway インスタンスからエージェントに SNMP イベントを受信します。
Syslog	514	NetScaler Gateway インスタンスからエージェントで syslog メッセージを受信するには。
TCP	5557	NetScaler Gateway インスタンスからエージェントへのログストリーム通信用。

NetScaler ADM エージェントと Citrix Analytics 間の通信では、次のポートが開いていることを確認してください。

種類	ポート	説明
TCP	443	エージェントと NetScaler Application Delivery Management サービス間の NITRO 通信用。

NetScaler ADM エージェントと Citrix Analytics 間の通信では、次のエンドポイントがホワイトリストに登録されていることを確認します。

エンドポイント	米国リージョン	EU リージョン
Event Hub	https://cas-eh-ns-alias.servicebus.windows.net/	https://cas-eh-ns-eu-alias.servicebus.windows.net/

エージェントのインストールとセットアップ

ネットワーク環境に NetScaler ADM サービスエージェントをインストールして構成し、Analytics とデータセンター内の Gateway インスタンス間の通信を可能にします。

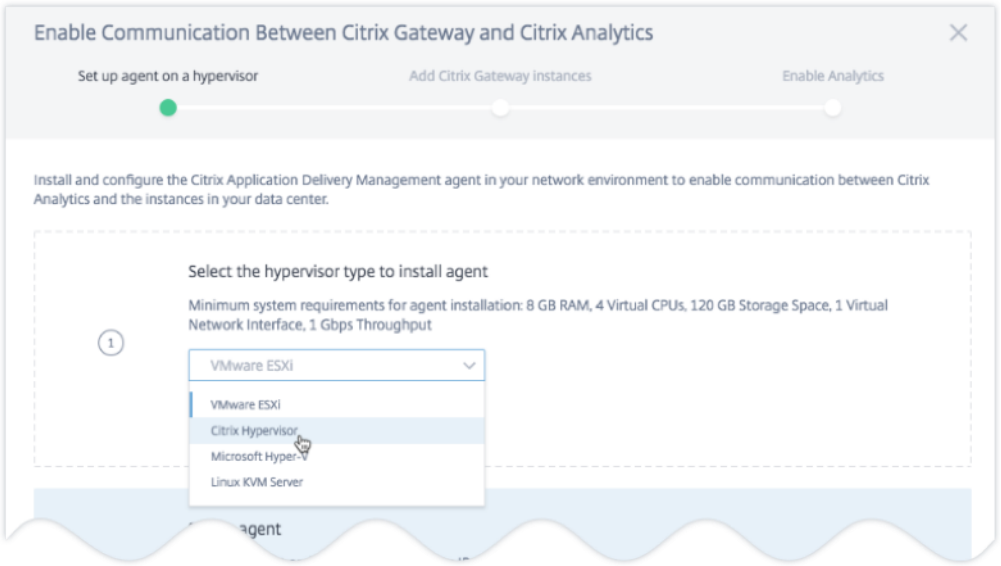
エンタープライズデータセンターの次のハイパーバイザーにエージェントをインストールできます。

- Citrix Hypervisor
- VMware ESXi
- Microsoft Hyper-V
- Linux KVM サーバー

エージェントをインストールしてセットアップするには、次の手順に従います。

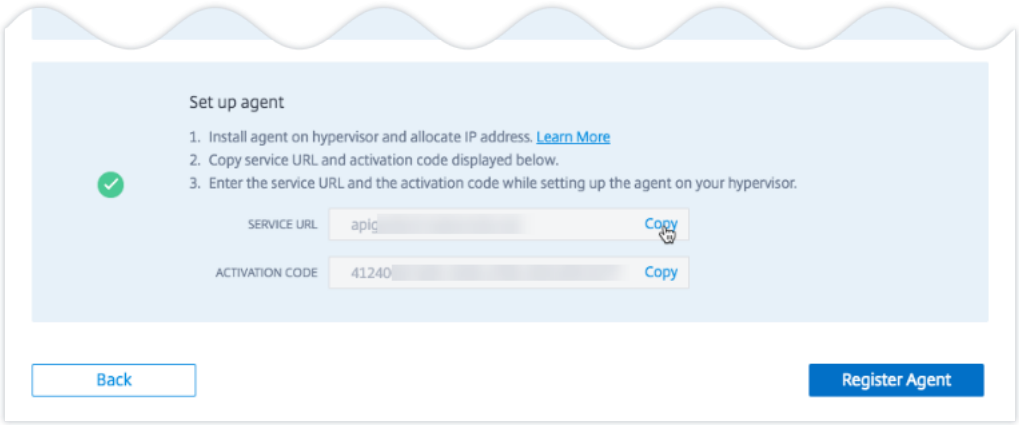
1. エージェントイメージをダウンロードします。

   [ハイパーバイザーでエージェントをセットアップする] ページでハイパーバイザーを選択し、[イメージのダウンロード] をクリックして、エージェントイメージをローカルシステムにダウンロードします。



2. サービス URL とアクティベーションコードをコピーします。

次の図に示すように、サービス URL とアクティベーションコードが生成され、UI に表示されます。(この処理には数秒かかる場合があります)。エージェントは、サービス URL を使用してサービスを検索し、アクティベーションコードを使用してサービスに登録します。ハイパーバイザーにエージェントをインストールするときに、サービス URL とアクティベーションコードを入力します。

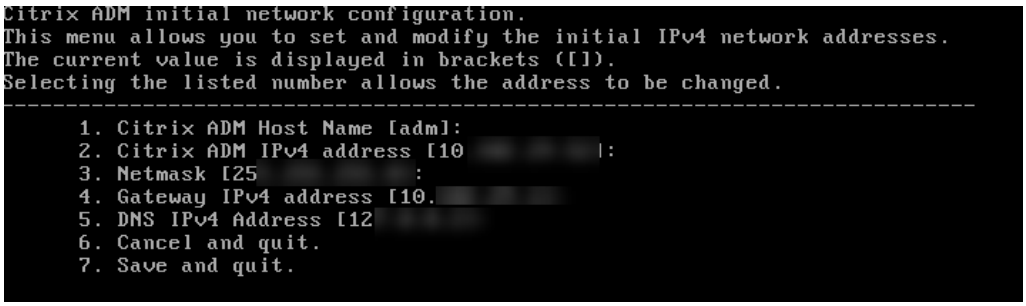


3. エージェントをハイパーバイザーにインストールします。

> 注:
>
> エージェントのインストールを開始する前に、次の点を確認してください。
>
> - ハイパーバイザーがエージェントごとに提供する必要のある仮想コンピューティングリソースがある。RAM: 8 GB、vCPU: 4、ストレージ容量:120 GB、仮想ネットワークインターフェイス:1、スループット:1 Gbps
> - エージェントへのインターネットアクセスを許可するように DNS を設定します。

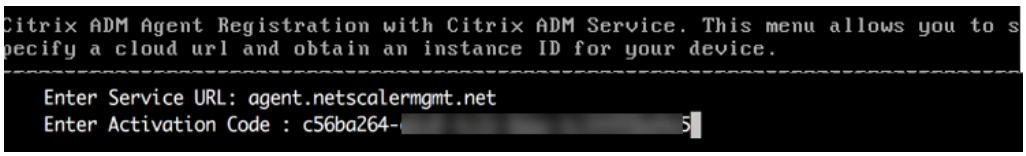
- Citrix Hypervisor で、次の手順を実行します。

  a) エージェントイメージファイルをハイパーバイザーにインポートします。[**Console**] タブから、次の例に示すように、初期ネットワーク構成オプションを構成します。



  間違った値を入力した場合、または値を変更する場合は、デフォルトの認証情報 `nsrecover/nsroot`を使用してシェルプロンプトにログオンします。その後、コマンド`networkconfig`を実行します。

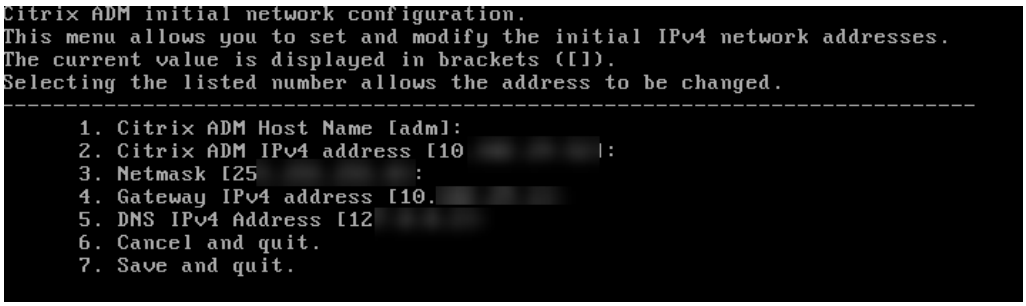
  b) エージェントイメージのダウンロード中に保存したサービス **URL** とアクティベーションコードを入力します。



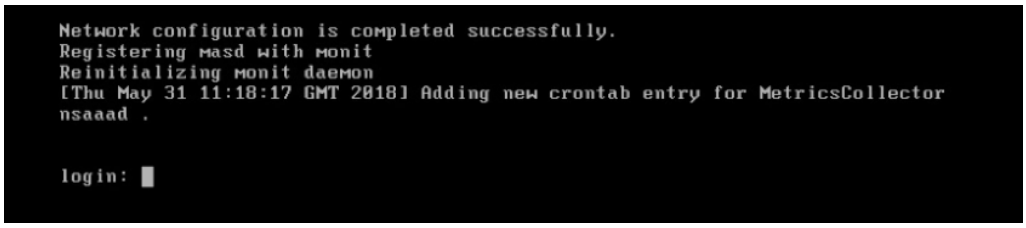
サービス URL またはアクティベーションコードを誤って入力した場合は、エージェントのシェルプロンプトにログオンし、スクリプト: を実行します。`deployment_type.py`。このスクリプトを使用すると、サービス URL とアクティベーションコードを再入力できます。

- VMware ESXi ハイパーバイザーで、次の手順を実行します。

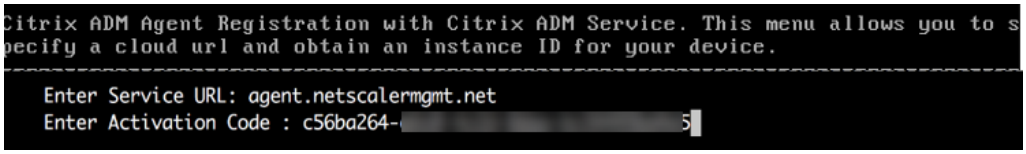
  a) エージェントイメージファイルをハイパーバイザーにインポートします。[**Console**] タブから、次の例に示すように、初期ネットワーク構成オプションを構成します。



  b) ネットワークを構成した後、プロンプトが表示されたら、デフォルトの認証情報`nsrecover`/`nsroot`を使用してエージェントのシェルプロンプトにログオンします。



  c) **/mps** ディレクトリに移動してスクリプトを実行し、エージェントイメージのダウンロード時に保存したサービス **URL** とアクティベーションコードを入力します。

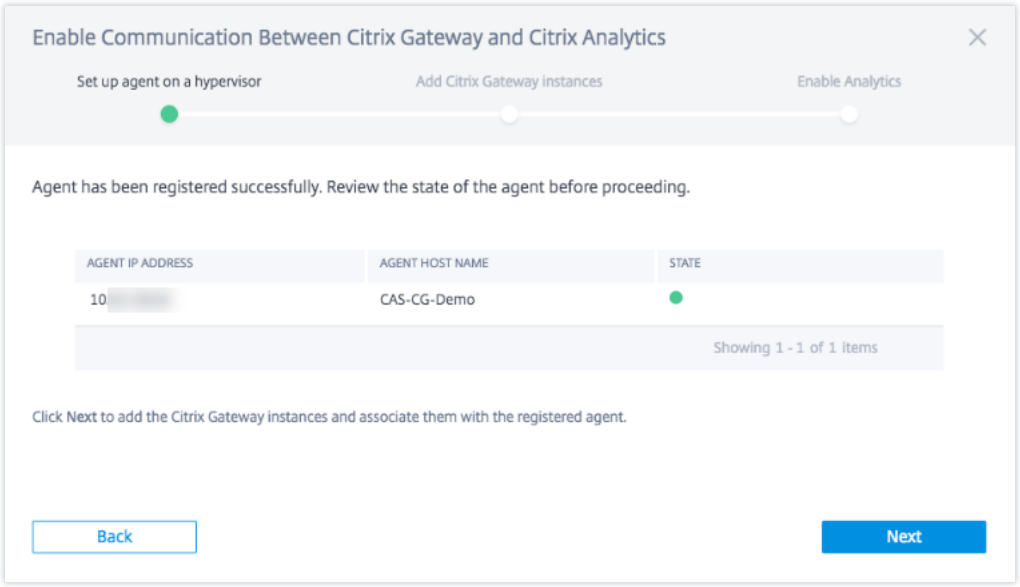


> 注:
>
> 同じイメージファイルを使用して、複数のエージェントをインストールできます。ただし、複数のエージェントで同じアクティベーションコードを使用することはできません。新しいアクティベーションコ

> ードを生成するには、Citrix Analytics にアクセスし、ハイパーバイザーの手順でセットアップエージェントで［イメージのダウンロード］をもう一度クリックします。新しいアクティベーションコードが生成されます。

4. エージェントを登録します。

   エージェントの登録に成功すると、エージェントは再起動してインストールプロセスを完了します。エージェントが再起動したら、Citrix Analytics にアクセスして［エージェントの登録］をクリックし、エージェントのステータスを確認します。

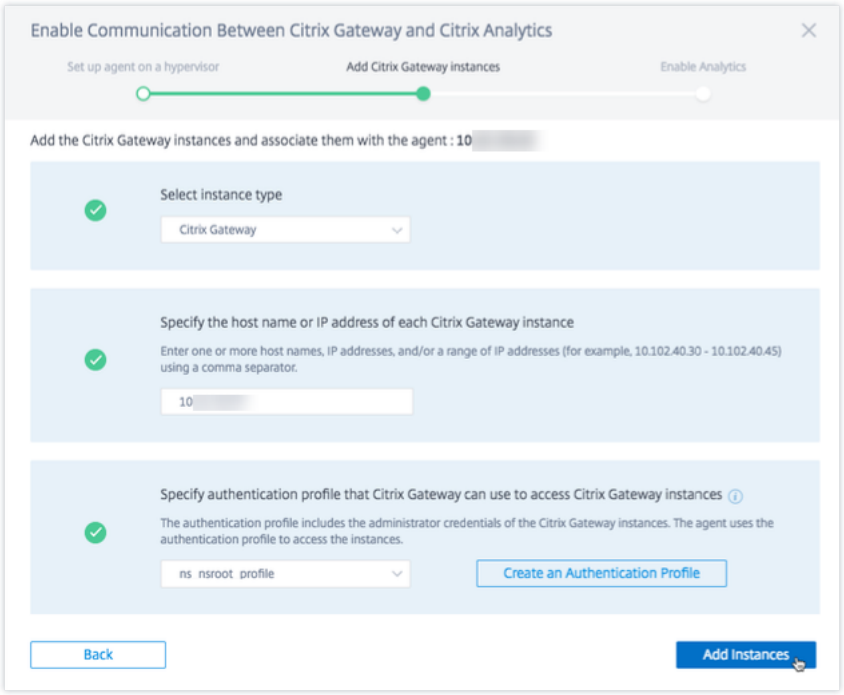


   エージェントのステータスが UP 状態になり、横に緑色のドットが表示されている場合は、[**Next**] をクリックしてサービスへのインスタンスの追加を開始します。

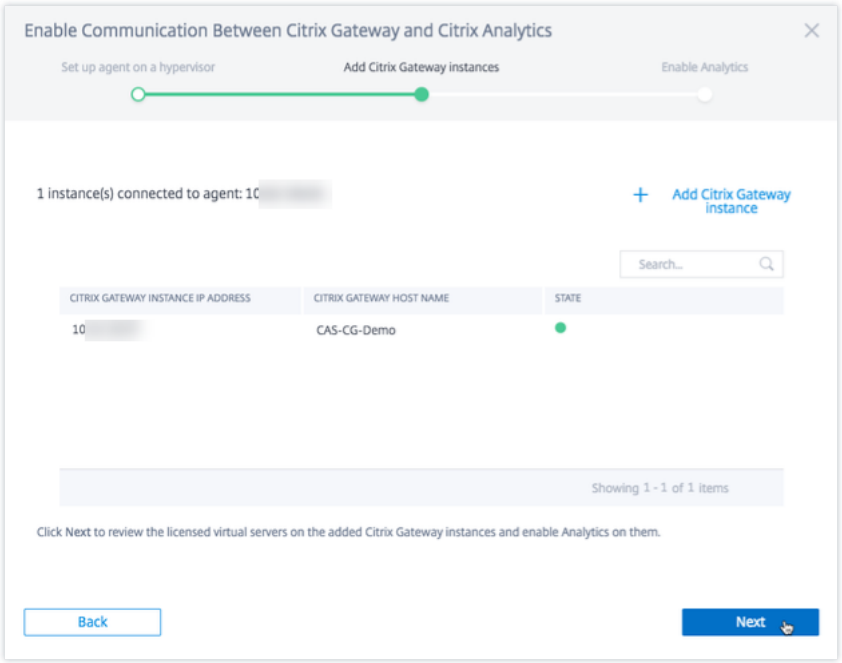
NetScaler Gateway インスタンスの追加

インスタンスとは、Citrix Analytics のデータソースである NetScaler Gateway アプライアンスまたは仮想アプライアンスのことです。

1. ［**NetScaler Gateway** インスタンスの追加］ページでインスタンスタイプを選択し、検出する Gateway インスタンスのホスト名、IP アドレス、または IP アドレスの範囲を指定します。
2. エージェントが Gateway インスタンスにアクセスするために使用できる認証プロファイルを作成します。このプロファイルは、Gateway インスタンスの管理者認証情報です。次に、[インスタンスの追加] をクリックします。



インスタンスを追加すると、正常に検出されたインスタンスの数を確認できます。インスタンスを追加するには、[**NetScaler Gateway** インスタンスの追加] をクリックします。



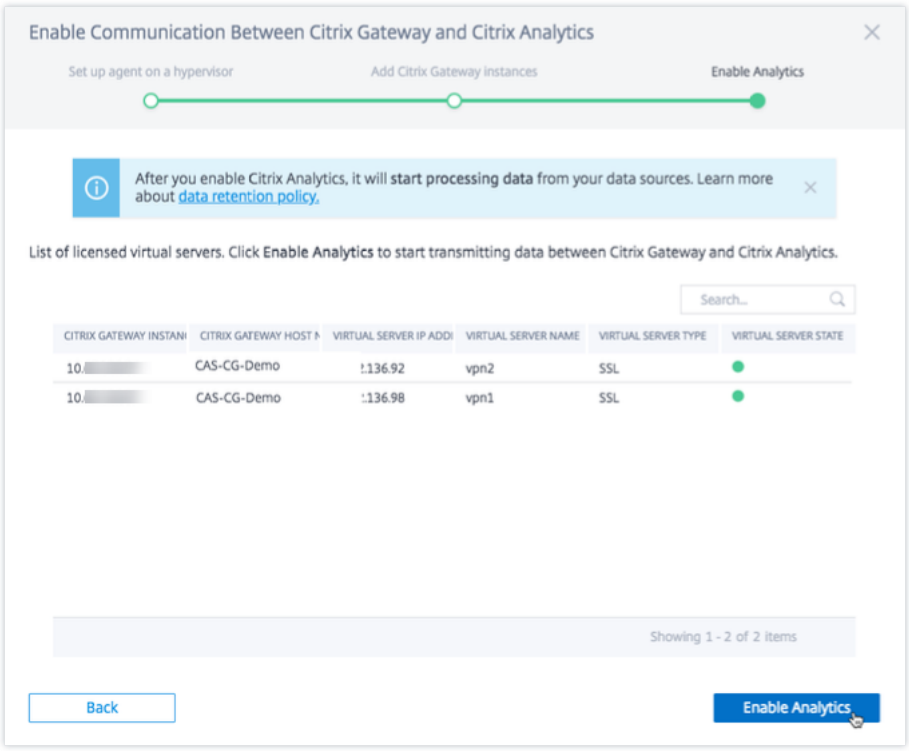
[次へ] をクリックして分析を有効にします。

分析を有効にする

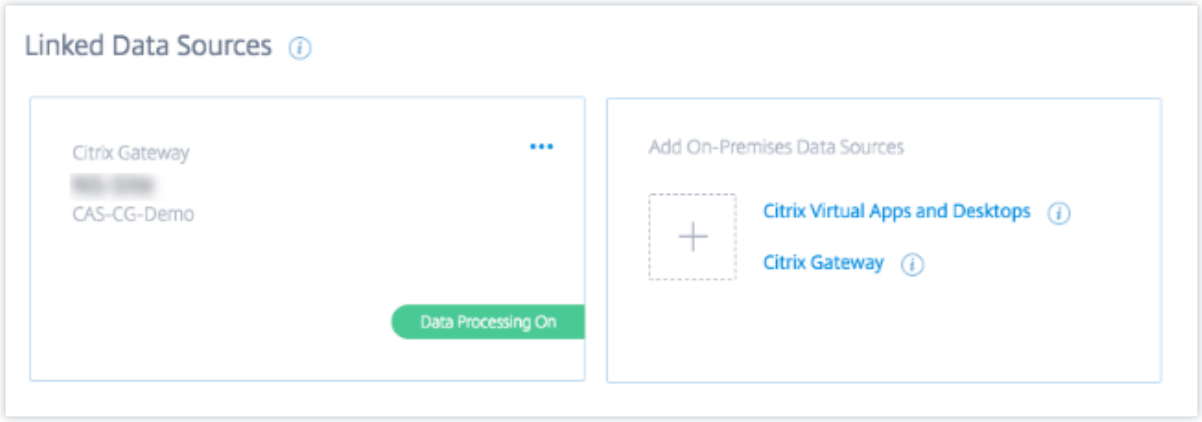
Citrix Analytics は、追加された NetScaler Gateway インスタンス上でライセンスされた仮想サーバーを自動的に検出します。検出されたすべての仮想サーバーで分析を有効にします。

デフォルトでは、**[Analytics** の有効化] ページには、Gateway インスタンスからライセンスされた仮想サーバーがすべて表示されます。ライセンスされた仮想サーバーの一覧を確認し、[**Analytics** を有効にする] をクリックして、仮想サーバーで分析を有効にします。

> 注
>
> 仮想サーバがページに表示されるまで、約 10 分かかる場合があります。



サイトカードのステータスが [データ処理オン] に変わります。受信したイベントを表示できます。



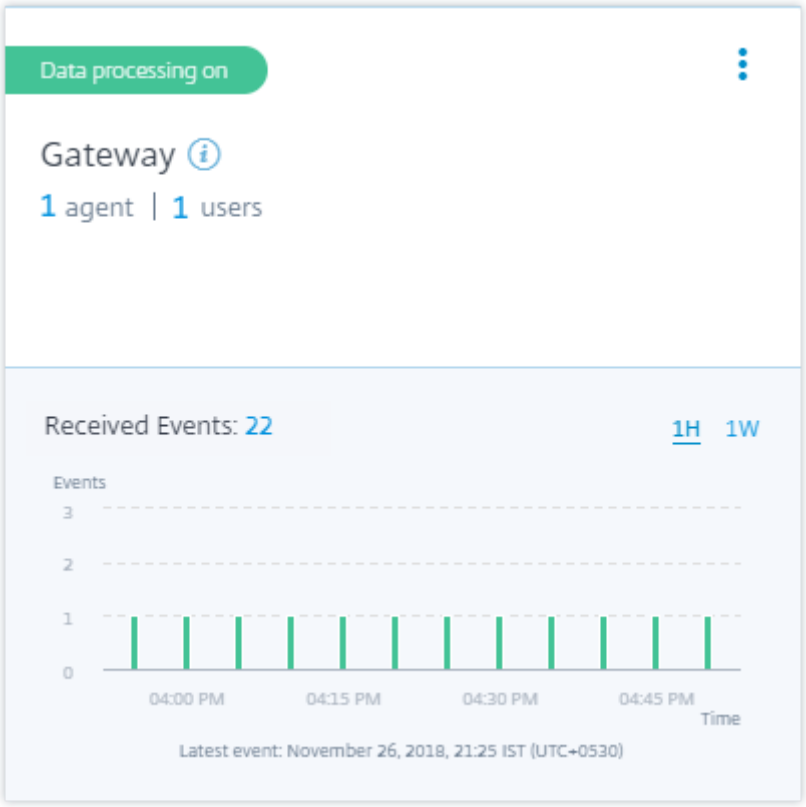
オンボーディング動画を見る

以下の動画は、Gateway インスタンスをオンボーディングする手順を示しています。

これは埋め込みビデオです。リンクをクリックしてビデオを見る

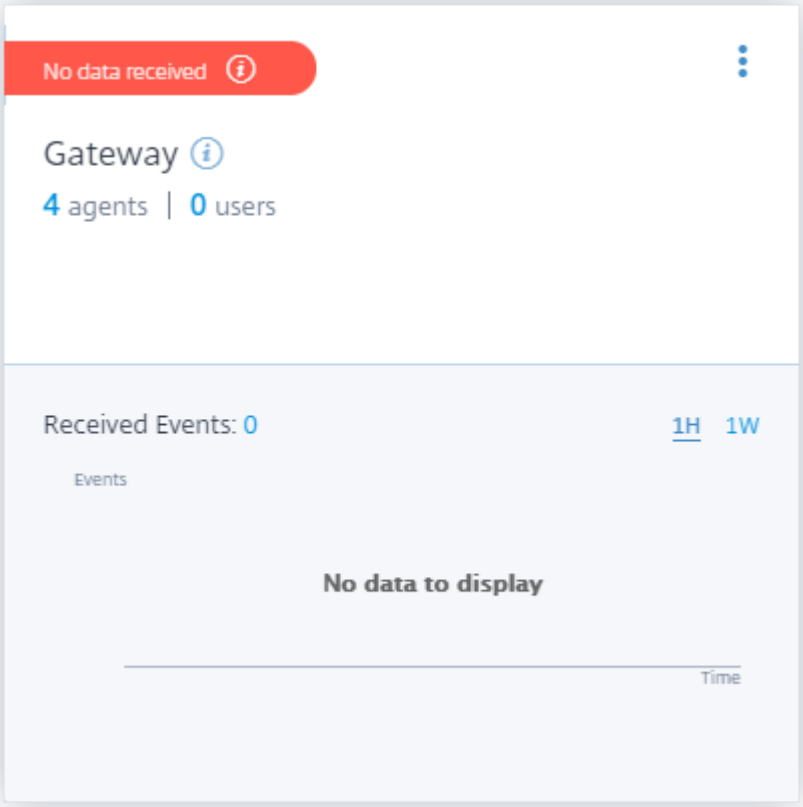
受信したイベント、ユーザ、およびエージェントの表示

サイトカードには、Gateway ユーザー、NetScaler ADM エージェント、およびデータソースから過去 1 時間に受信したイベントの数が表示されます。これはデフォルトの時間選択です。また、1 週 (**1W**) を選択してデータを表示することもできます。[Users] ページに表示するユーザー数をクリックします。エージェントの数をクリックすると、NetScaler Gateway インスタンスとエージェントが表示されます。



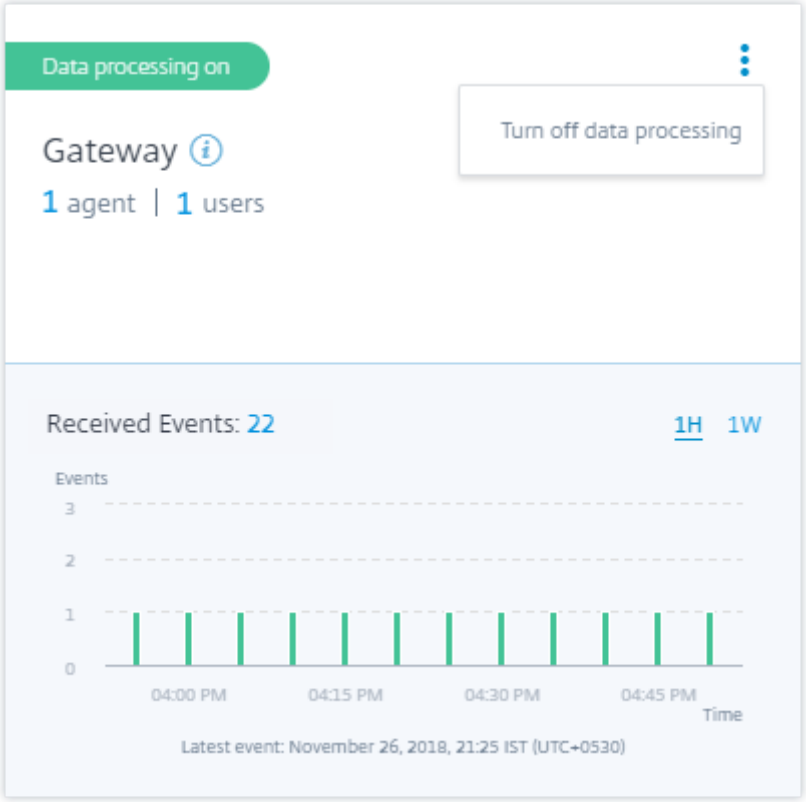
データ処理を有効にすると、サイトカードに [データを受信していません] ステータスが表示される場合があります。このステータスは、次の 2 つの理由で表示されます:

1. 初めてデータ処理をオンにした場合、イベントが Citrix Analytics のイベントハブに到達するまでに時間がかかります。Citrix Analytics がイベントを受信すると、ステータスが **Data processing on** に変わります。しばらくしてもステータスが変わらない場合は、[データソース] ページを更新します。
2. アナリティクスは、過去 1 時間の間にデータソースからイベントを受信していません。

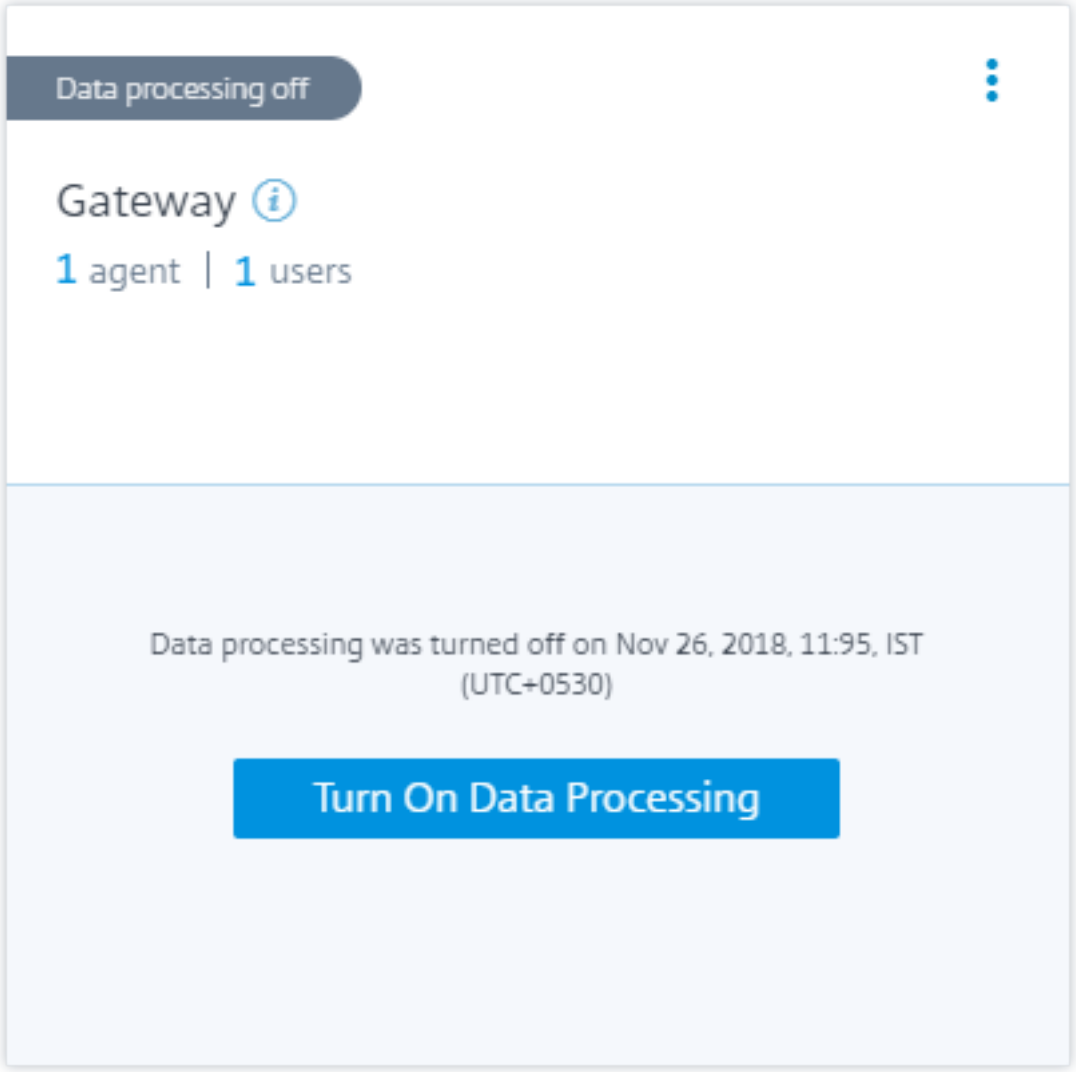


データ処理のオンとオフを切り替える

データ処理を停止するには、サイトカードの縦の省略記号 (⋮) をクリックし、[データ処理をオフにする] をクリックします。Citrix Analytics は、このデータソースに対するデータの処理を停止します。

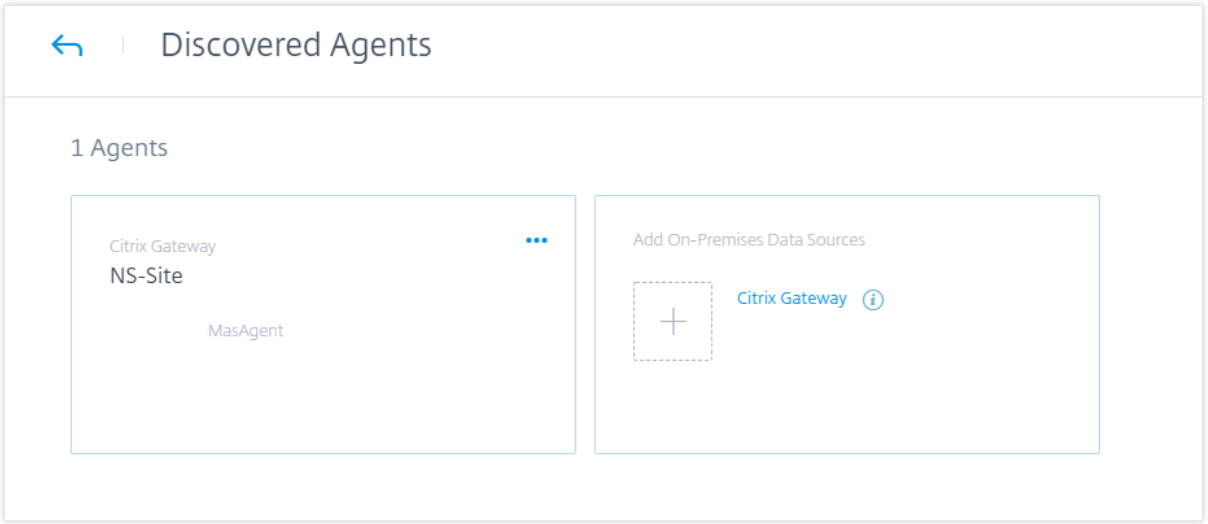


データ処理を再度有効にするには、[データ処理をオンにする] をクリックします。



Gateway インスタンスを追加する

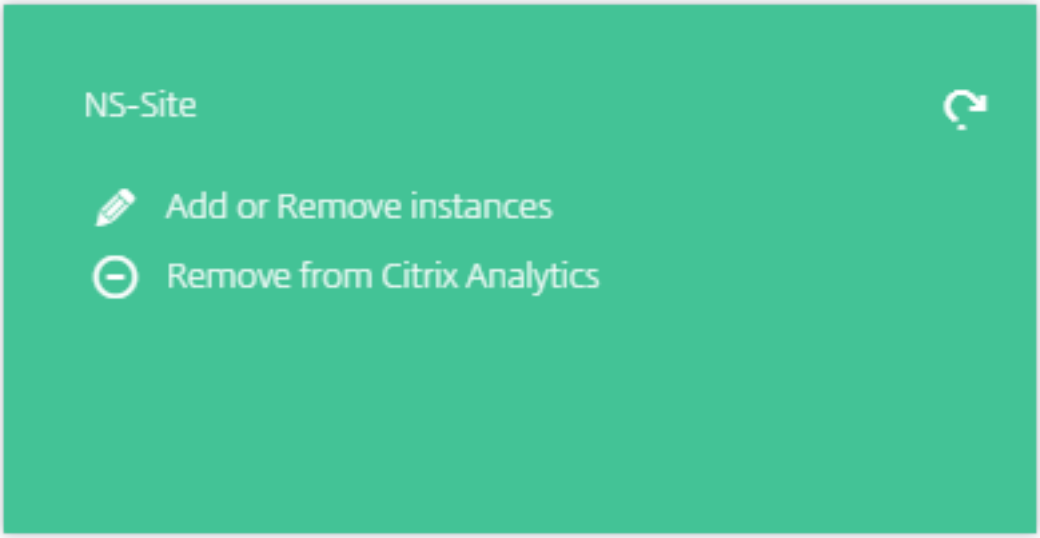
Gateway インスタンスを追加する場合は、Gateway サイトカードのエージェント数をクリックして [検出されたエージェント] ページを表示します。[オンプレミスデータソースの追加] タイルで [**NetScaler Gateway**] をクリックします。



データソースを管理

エージェントにインスタンスを追加したり、エージェントに関連付けられているインスタンスを削除したりすることもできます。エージェントとそれに関連付けられているインスタンスを Citrix Analytics から削除することもできます。

エージェントサイトカードを裏返して、次のいずれかの操作を行います。



- インスタンスを追加または削除する。エージェントに Gateway インスタンスを追加し、それらのインスタンスに設定されている仮想サーバーで Analytics を有効にすることができます。エージェントに追加されたインスタンスを削除することもできます。インスタンスをエージェントから切り離すと、Citrix Analytics はそのインスタンスと通信できません。
- **Citrix Analytics** から削除します。エージェントサイトを削除すると、Citrix Analytics はそのエージェン

トに関連付けられているインスタンスからのデータの収集を停止します。ただし、保存期間中は、以前に処理されたすべてのデータを利用できます。

Citrix Virtual Apps and Desktops データソース

April 12, 2024

この記事では、StoreFront を使用してオンプレミスの CitrixVirtual Apps and Desktops サイトを Citrix Analytics に接続する手順について説明します。この記事に記載されているオンボーディング手順は、パフォーマンス向け Citrix Analytics（パフォーマンス分析）とセキュリティ向け Citrix Analytics（セキュリティ分析）の両方に適用されます。

各オファリングに固有のオンボーディング手順については、次の記事を参照してください。

- Citrix Analytics for Performance によるオンプレミスの CitrixVirtual Apps and Desktops サイトの構成
- Citrix Analytics for Security 用の Citrix Virtual Apps and Desktops および Citrix DaaS データソースの設定

StoreFront を使用した Citrix Virtual Apps and Desktops のオンプレミスサイトのオンボーディング

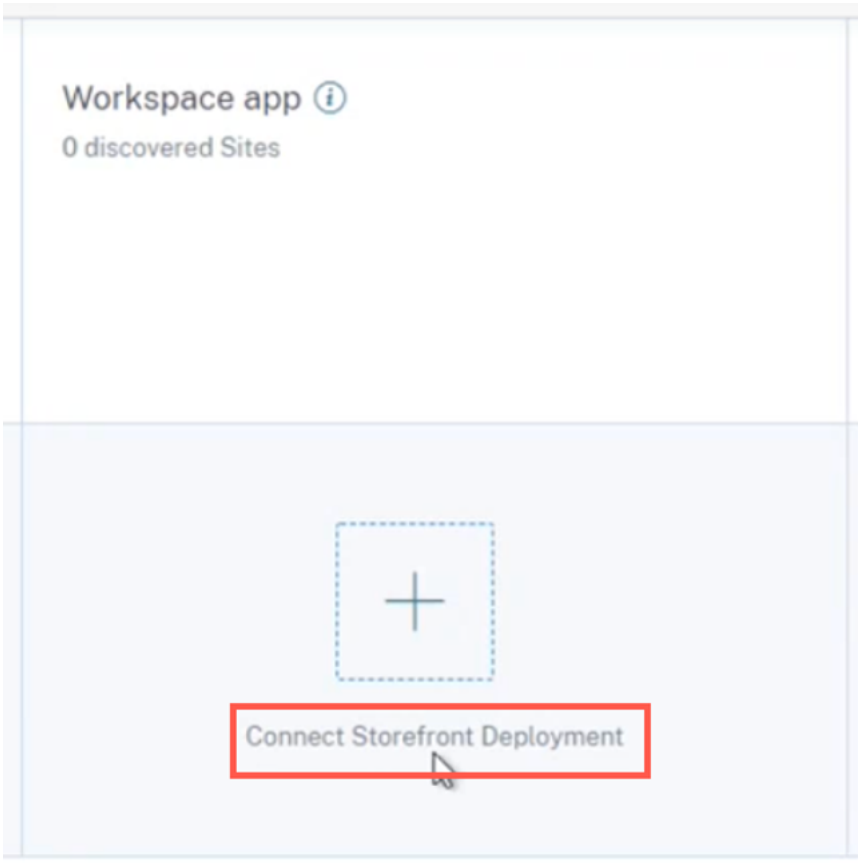
組織でオンプレミスの StoreFront 展開環境を使用している場合は、Citrix Workspace アプリが Citrix Analytics にイベントを送信できるように StoreFront サーバーを構成する必要があります。Citrix Analytics はイベントを処理して、Citrix IT インフラストラクチャのパフォーマンスとユーザー行動に関する実用的な洞察を提供します。

Citrix Analytics 用に StoreFront 展開環境を構成する方法について詳しくは、StoreFront ドキュメントの「Citrix Analytics サービス」を参照してください。

以前は、Citrix Apps and Desktops のオンプレミスサイトを使用しているお客様は、サイトアグリゲーションを使用してオンプレミスサイトを Citrix Analytics for Security and Performance にオンボーディングする必要がありました。

サイトの集約に依存することなく、Citrix Apps and Desktops のオンプレミスサイトをオンボーディングできるようになりました。

サイトアグリゲーションにサイトを追加していない場合でも、ワークスペースアプリケーションに［**Connect Storefront Deployment**］オプションが表示されます。



前提条件

開始する前に、次のことを確認してください。

- StoreFront のバージョンは 1906 以降である必要があります。
- StoreFront 展開環境では、次のアドレスに接続できる必要があります。
  - https://*.cloud.com
  - https://api.analytics.cloud.com
- StoreFront 展開環境では、アウトバウンドインターネット接続用にポート 443 が開いている必要があります。ネットワーク上のプロキシサーバーは、Citrix Analytics とのこの通信を許可する必要があります。
- StoreFront 展開環境が、Web プロキシを使用してインターネットに接続する Web サーバー上でホストされている場合は、各ストアのプロキシをアウトバウンドトラフィックを許可するように手動で構成する必要があります。StoreFront は、ホスト Web サーバーのプロキシ設定を自動的には使用しません。詳しくは、「HTTP プロキシを使用する Web サーバーでホストされる StoreFront 展開環境の構成」を参照してください。
- StoreFront 展開環境には、次のいずれかのクライアントを使用してアクセスする必要があります。
  - HTML5 互換ブラウザーの Web サイト用の Citrix Receiver。

> 注
>
> HTML5 ユーザーの場合、CitrixVirtual Apps and Desktops は、StoreFront で特定の構成が有効になっているときにイベントを起動できます。構成手順について詳しくは、HTML5 向け Citrix Workspace アプリのドキュメントの「インストール」の記事を参照してください。印刷関連のイベントの場合、StoreFront で追加のポリシーを構成する必要があります。詳しくは、HTML5 向け Citrix Workspace アプリのドキュメントの「PDF 印刷」を参照してください。

  - Citrix Workspace アプリ 1907 以降の Windows 版。
  - Linux 以降の Citrix Workspace アプリ 2006。
  - Mac 版以降の Citrix Workspace アプリ 2006

- Citrix Virtual Apps and Desktops 7 1912 LTSR を使用している場合、サポートされている StoreFront のバージョンは 1912 です。

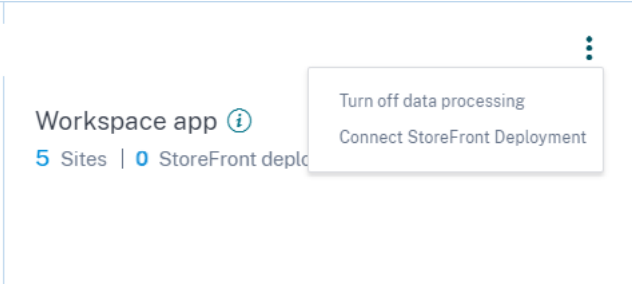
StoreFront 展開環境に接続する

以下の方法で StoreFront デプロイメントに接続できます。

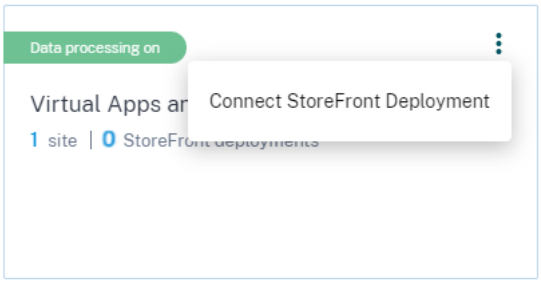
- アプリとデスクトップ—**Workspace** アプリサイトカードとアプリとデスクトップ—監視サイトカードの使用
- レコメンデーションパネルの使用

アプリとデスクトップ—**Workspace** アプリサイトカードとアプリとデスクトップ—監視サイトカードを使用して接続

1. [設定] > [データソース] > [セキュリティ] に移動します。[アプリとデスクトップ-**Workspace**] アプリサイトカードで、縦方向の省略記号（⋮）をクリックし、[**StoreFront** 展開環境の接続] を選択します。

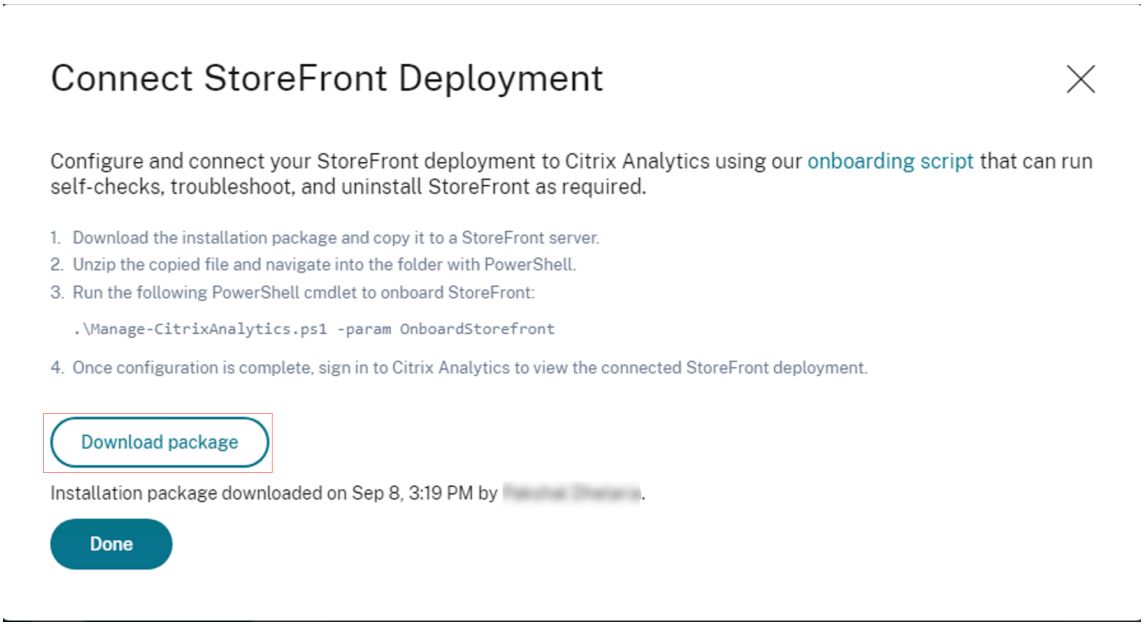


2. [設定] > [データソース] > [パフォーマンス] に移動します。[アプリとデスクトップ-監視] サイトカードで、縦方向の省略記号（⋮）をクリックし、[**StoreFront** 展開環境の接続] を選択します。



StoreFront オンボーディングウィザードまたは **StoreFront** デプロイメントへの接続ポップアップが表示されます。

3. 「パッケージをダウンロード」をクリックします。



> 注
>
> このファイルには機密情報が含まれています。ファイルを安全な場所に保存します。

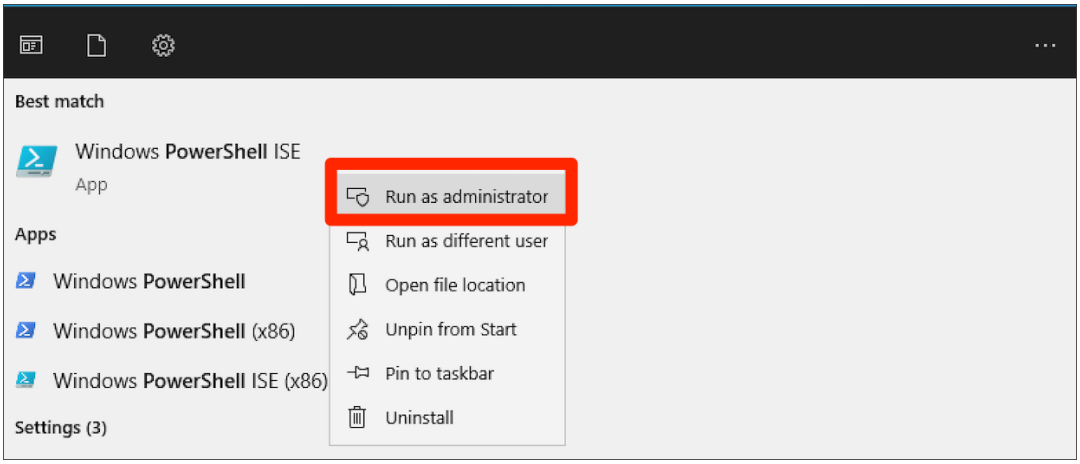
4. StoreFront デプロイメントを構成するには、

   a) インストールパッケージを StoreFront サーバーにコピーします。

   b) コピーしたファイルを解凍し、PowerShell 内のフォルダーに移動します。

   c) StoreFront をオンボーディングするには、管理者として次のコマンドを実行する必要があります。

   .\Manage-CitrixAnalytics.ps1 –param OnboardStorefront



その他のオプションやパラメーターについては、「PowerShell スクリプト 」セクションを参照してください。

d) StoreFront サーバーを開き、PowerShell スクリプトを実行します。

e) OnboardStoreFront を実行しても StoreFront サイトが Citrix Analytics Service GUI に表示されない場合は、iisreset コマンドを実行してください。

f) Citrix Analytics Service GUI にログインし、クラスター ID がスクリプトによってコンソールに記録されたものと一致するかどうかを確認します。

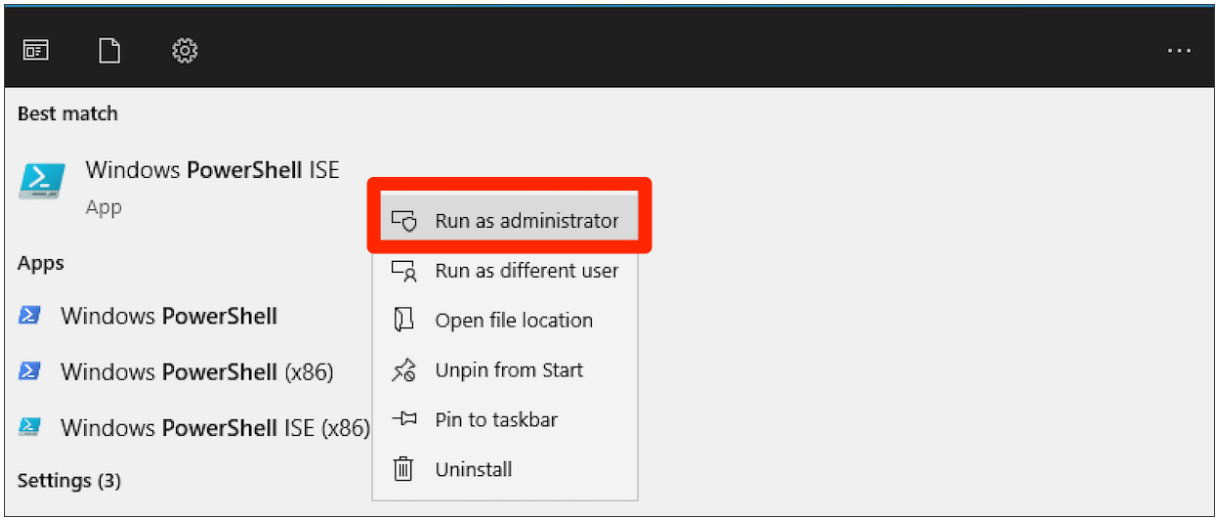
g) 構成が完了したら、Citrix Analytics にログインして、接続されている StoreFront 展開環境を表示します。

5. 設定が成功したら、[完了] をクリックします。

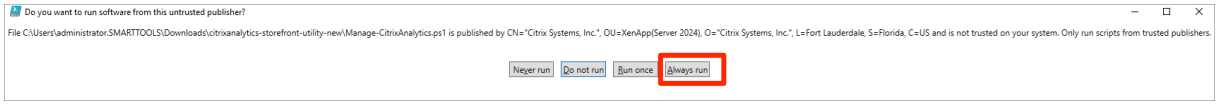
6. ［データ処理を有効にする］をクリックして、Citrix Analytics でデータを処理できるようにします。

PowerShell スクリプト

Citrix Analytics サービスへの StoreFront のオンボーディングプロセスを簡素化するために、新しい PowerShell スクリプトが導入されました。この PowerShell スクリプトは、前提条件の確認、インストール、および StoreFront の構成プロセスを自動化します。PowerShell スクリプトは管理者モードで実行する必要があります。



お客様は、StoreFront でこの PowerShell スクリプトを実行して、オンボーディング、デボーディング、セルフチェックの実行、トラブルシューティング、および Citrix Analytics Service GUI へのオンボーディングが成功したかどうかの検証を行うことができます。顧客が初めてスクリプトを実行すると、発行者に確認を求めるセキュリティ警告メッセージが表示されます。発行元が信頼できる場合は、「常に実行」オプションを選択します。



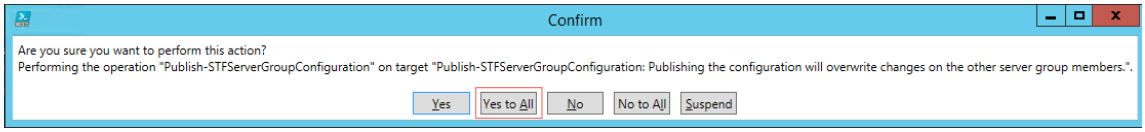
PowerShell スクリプトは、**StoreFront Configuration.json** ファイル、いくつかの **CCauth**、および **dll** ファイルとともに、**StoreFrontDeployment** の接続ページで **zip** ファイル形式で入手できます。PowerShell スクリプトログは、ダウンロードフォルダーの cas-logs ファイルに保存されます。

PowerShell スクリプトは、以下のパラメーターをサポートしています。

- **SelfCheck**: **SelfCheck** パラメーターを使用して、StoreFront オンボーディングの前提条件が満たされていることを検証します。StoreFront のインストール、必要なバージョン、アウトバウンド接続、cURL Analytics サーバーのネットワーク接続、インターネット接続、サーバーグループ構成、および既存の Citrix Analytics Service 構成をチェックします。以下のコマンドを使用してセルフチェックを実行します。

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

- **OnboardStoreFront**: **OnboardStoreFront** パラメーターは、セルフチェックをすばやく実行して、Citrix Analytics サービス構成のセットアップ準備が整っていることを確認します。セットアップの準備が整うと、Citrix Analytics Service の構成がインポートされ、変更がサーバーグループ内の他のサーバーに公開されます。サーバーグループの場合、PublishConfiguration コマンドはスクリプトから自動的に実行され、StoreFront 構成をその StoStoreFront 内のすべてのサーバーに公開します。`PublishConfiguration` アクションを確認するポップアップが表示されます。「すべてはい」ボタンを選択します。



構成の公開が正常に完了すると、スクリプトは Citrix Analytics Service API を呼び出して、StoreFront が Citrix Analytics サービス GUI にオンボーディングされているかどうかを確認します。この API を呼び出すには、認証用の秘密鍵が必要です。この秘密鍵を生成するには、CCAuth ファイルと dll ファイル、およびダウンロードした JSON ファイルにある認証情報が必要です。

> 注:
>
> StoreFront のオンボーディングプロセスが完了すると、StoreFront が Citrix Analytics サービスの GUI に表示されるまでに 2〜5 分かかる場合があります。StoreFront サイトが Citrix Analytics サービスの GUI に表示されない場合は、IISRESET を実行してインターネットインフォメーションサービスをリセットする必要があります。

次のコマンドを使用して **OnBoardStoreFront** を実行します。

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

- **IsOnBoarded**: **IsOnBoarded** パラメーターは、**StoreFront** が **Citrix Analytics** サービス **GUI** にオンボーディングされているかどうかを確認するために使用されます。スクリプトは終了するまで 1 分間待機しますが、オンボーディングが成功してから StoreFront が GUI に表示されるまでに最大 5 分かかることがあります。確認するには、このコマンドを実行する必要があります。このコマンドには、CCAuth ファイルと dll ファイルとの依存関係もあります。以下のコマンドを使用して **ISonBoarded** を実行します。

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

- トラブルシューティング: 5 分待っても Citrix Analytics Service GUI に StoreFront サイトが表示されない場合は、IISRESET を実行してインターネットインフォメーションサービスをリセットする必要があります。それでも StoreFront サイトが GUI に表示されない場合は、トラブルシューティングパラメーターを使用してください。接続に関する問題のトラブルシューティングやログの収集に役立ちます。次のコマンドを使用してトラブルシューティングを実行します。

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

  トラブルシューティングパラメータは、次の 2 つのユースケースに役立ちます。

  - ユースケース **1**: CurlAnalytics が失敗したかどうかのセルフチェックの一環として、ファイアウォールルールが作成されます。このファイアウォールルールは 443 ポートを開き、Analytics への接続を確認します。そうでない場合は、Analytics サーバーにアクセスできず、スクリプトはここから終了します。Citrix Analytics サービスへの接続が復元されたら、スクリプトを再実行します。
  - ユースケース **2**: cURL が正常に実行されても StoreFront サイトが GUI に反映されない場合、管理者はDebugView のダウンロードから DebugView ツールの zip ファイルをダウンロードし、解凍してダウンロードフォルダーに配置する必要があります。PowerShell スクリプトは、Citrix Analytics サービスがすでに構成されている場合、まずアンインストールします。Verbose ロギングを有効にしま

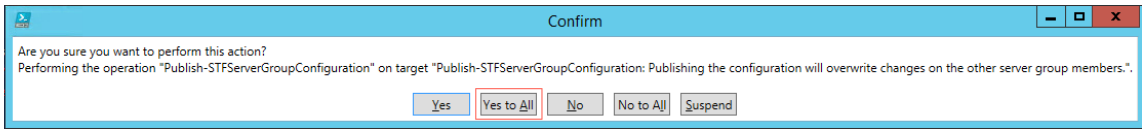
す。次に、DebugView ツールを起動し、Citrix Analytics サービスを再インストールします。最後に、DebugView を停止し、詳細ログを無効にします。

デバッグビューログはキャプチャして Citrix スサポートと共有できます。Citrix 管理者はさらにデバッグを行い、問題の特定と解決を試みます。ログは生成され、DebugView フォルダー内にログファイルとして保存されます。

次の 3 つのログファイルを Citrix 管理者と共有する必要があります。

- デバッグビューログファイル (ダウンロード\ デバッグビュー\ ログ)
- StoreFront ログファイル (C:\Program Files\ Citrix\ Receiver StoreFront\ Admin\ trace)
- CAS ログファイル。これらのログはスクリプトの実行の一部として生成され、[ダウンロード**] > [cas-logs**] フォルダーに保存されます。

サーバーグループの場合、スクリプトが StoreFront のデボードまたはオンボードを試みると、`PublishConfiguration` コマンドが自動的に実行されます。PublishConfiguration コマンドは、その StoreFront 内のすべてのサーバーに StoreFront 構成を公開するのに役立ちます。このアクションを確認するポップアップが表示されます。「すべてはい」ボタンを選択します。

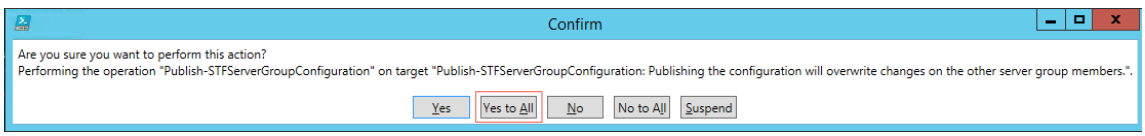


- **DeboardStoreFront**: DeboardStoreFront パラメーターは、Citrix Analytics サービスから StoreFront サーバーをデボーディングするために使用されます。次のコマンドを使用して DeBoardStoreFront を実行します。

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

PowerShell スクリプトは、まずすべての Citrix Analytics Service 構成を StoreFront から削除し、削除が正常に完了したことを確認します。次に、ServerGroup が存在するかどうかを確認し、構成を公開して、削除された構成がすべての StoreFront に公開されるようにします。最後に、「ボード上のサイトの削除」を呼び出します。サイトが Citrix Analytics Service GUI から削除されていない場合は、StoreFront 展開を使用して StoreFront サイトを手動で削除し、StoreFront 展開環境のワークスペースアプリケーションサイトカードから StoreFront サイトを手動で削除する必要があります。

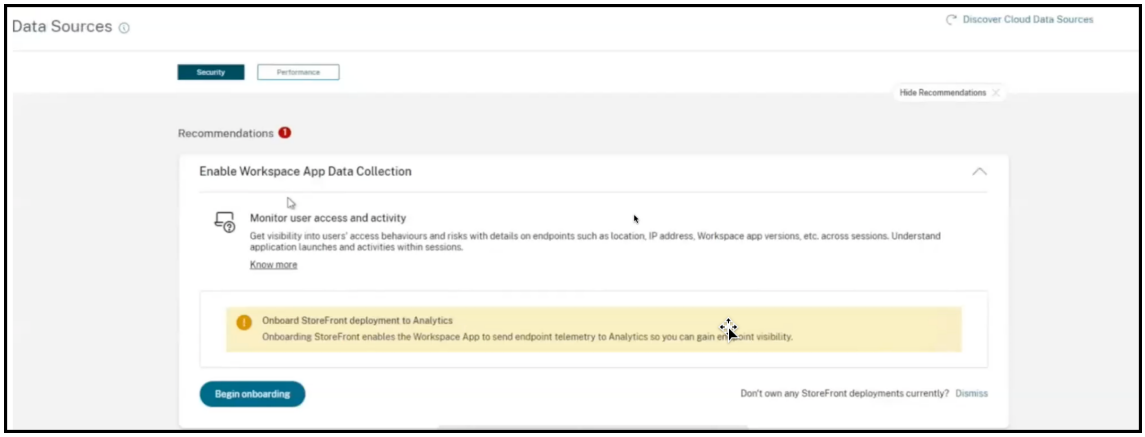
サーバーグループの場合、PublishConfiguration コマンドはスクリプトから自動的に実行され、StoreFront 構成をその StoStoreFront 内のすべてのサーバーに公開します。このアクションを確認するポップアップが表示されます。「すべてはい」ボタンを選択します。



レコメンデーションパネルを使用して接続

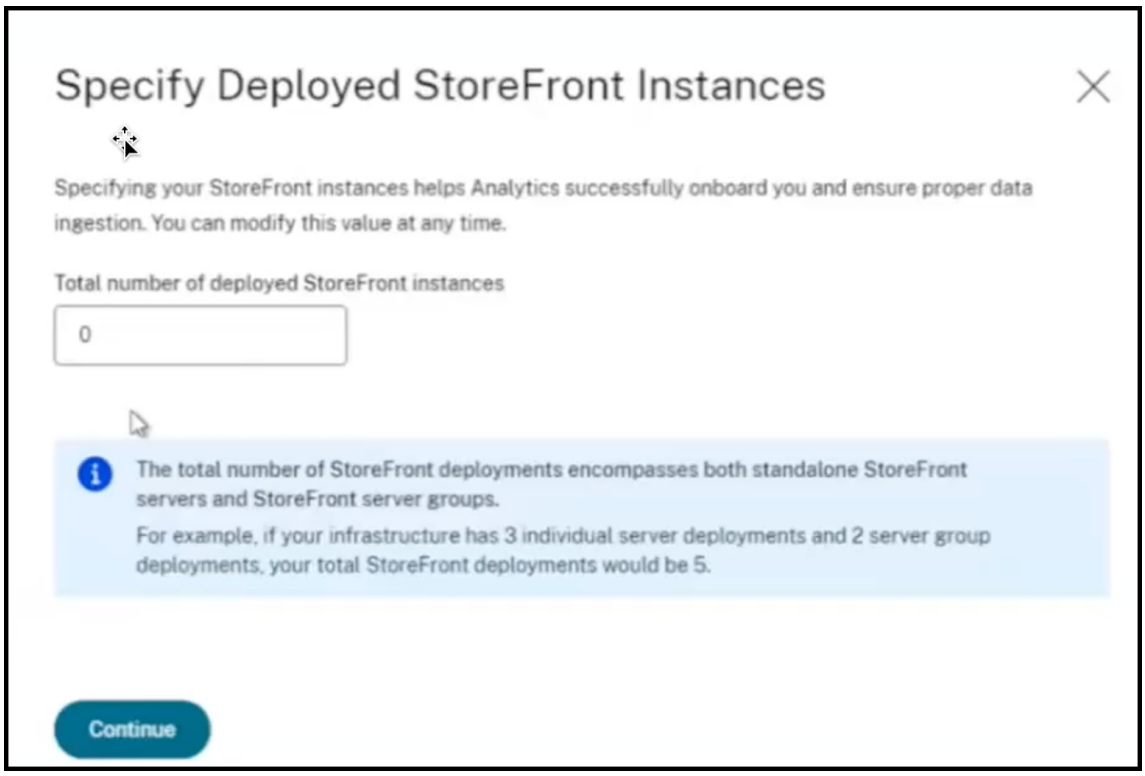
データソースページのレコメンデーションパネルは、データソースをオンボーディングすることの重要性についてユーザーに教えます。これにより、ユーザーはデータソースを簡単にオンボーディングできます。また、使用可能なすべてのデータソースを確認してオンボーディングしたことを確認するオプションも提供されます。

1. Security Analytics サービスを使用している場合は、[設定] **>** [データソース] **>** [セキュリティ] を選択します。
2. パフォーマンス分析サービスを使用している場合は、[設定] **>** [データソース] **>** [パフォーマンス] に移動します。
3. **[**** データソース] ページの [推奨事項] パネルに表示される情報と推奨事項を確認して、Storefront の展開を開始します。**



> 注
>
> StoreFront データソースをオンボーディングすると、Workspace アプリはエンドポイントの可視性に関するテレメトリデータを Analytics に送信できます。

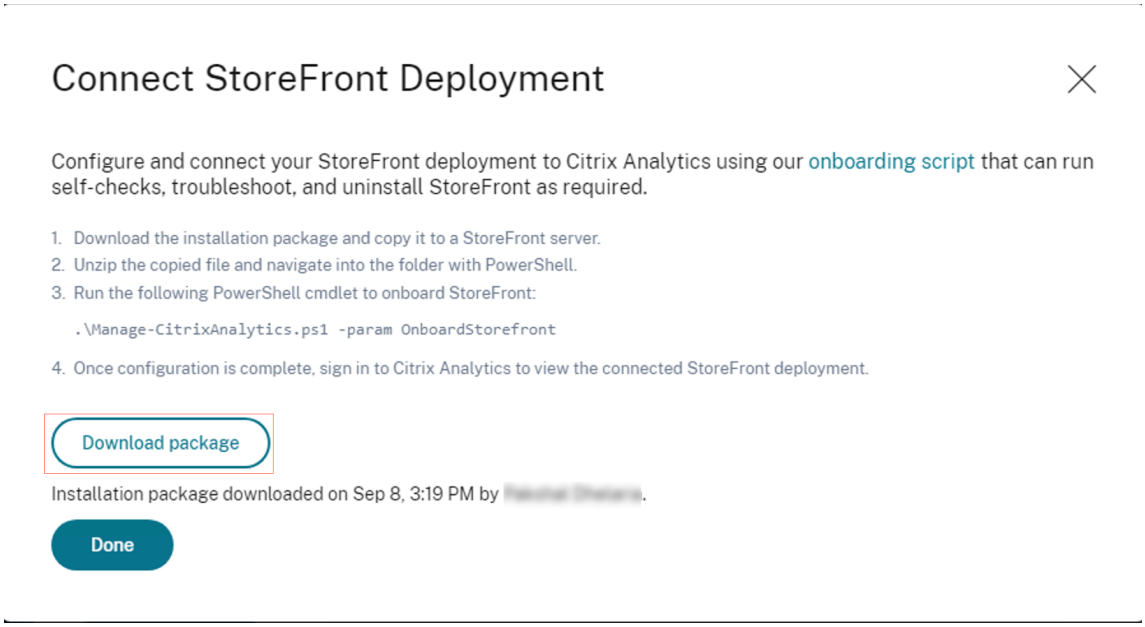
4. 「オンボーディングを開始」をクリックします。「デプロイされた **StoreFront** インスタンスの指定」ページが表示されます。



5. Analytics がデータソースを正常にオンボーディングできるように、デプロイされた **StoreFront** インスタンスの総数を指定します。

   > 注:
   >
   > デプロイされた **StoreFront** インスタンスの総数は **StoreFront** グループの総数であり、個々の StoreFront サーバーの数ではありません。

6. ［続行］をクリックします。StoreFront オンボーディングウィザードまたは **StoreFront** デプロイメントへの接続ポップアップが表示されます。
7. ［**StoreFront** 展開環境の接続］ページで、［パッケージのダウンロード］をクリックしてインストールパッケージをダウンロードします。



> メモ
>
> このファイルには機密情報が含まれています。ファイルを安全な場所に保存します。
>
> 1 つのパッケージをダウンロードして、1 つの StoreFront グループのオンボーディングにのみ使用できます。StoreFront グループが複数ある場合は、StoreFront グループごとにパッケージを個別にダウンロードする必要があります。1 つのパッケージを使用して 1 つの StoreFront グループのオンボーディングが終了したら、そのパッケージを再度ダウンロードして、次の StoreFront グループのオンボーディングを続行します。
>
> 何らかの問題により、1 つのパッケージを使用して 2 日以内に StoreFront のオンボーディングが正しく完了しない場合は、2 日後に新しいパッケージを再ダウンロードする必要があります。2 日以内に正常にオンボーディングされないと、パッケージ内のキーの有効期限が切れてしまうためです。

8. StoreFront デプロイメントを構成するには、

   a) インストールパッケージを StoreFront サーバーにコピーします。

   b) コピーしたファイルを解凍し、PowerShell 内のフォルダーに移動します。

   c) 次のコマンドを実行して StoreFront をオンボードします。

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

   d) StoreFront サーバーを開き、PowerShell スクリプトを実行します。

   e) StoreFront サイトが Citrix Analytics Service GUI に表示されない場合は、次のコマンドを実行します:

   ```
   Execute iisreset
   ```

   f) PowerShell スクリプトで使用可能なクラスタ ID を記録して確認します。

g) 構成が完了したら、Citrix Analytics にログインして、接続されている StoreFront 展開環境を表示します。

9. 設定が成功したら、[完了] をクリックします。

推奨パネルからオンボーディングする場合、システムは Citrix Analytics サービスにオンボーディングした StoreFront 展開環境の数を取得します。推奨パネルが表示され、オンボードされた StoreFront 展開を確認できます。「レコメンデーション」パネルでメッセージを確認し、「完了としてマーク」をクリックします。

> 注
>
> レコメンデーションパネルとメッセージは、宣言されたすべての Storefront デプロイがオンボーディングされた場合にのみ消えます。

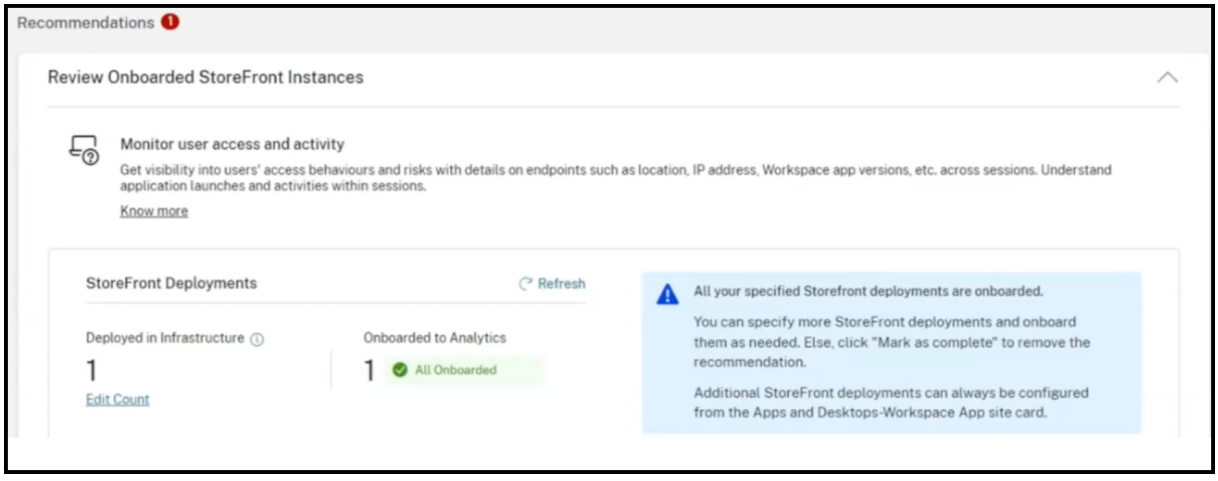
1. ［データ処理を有効にする］をクリックして、Citrix Analytics でデータを処理できるようにします。

レコメンデーションパネルを確認

推奨パネルでは、宣言された StoreFront 展開の数と、登録された StoreFront 展開環境の数を比較できます。

宣言された StoreFront 展開環境の数がオンボーディングされた StoreFront 展開環境の数と同じ場合は、すべての StoreFront 展開環境がオンボーディングされたことを示す **All Onboarded** メッセージが表示されます。「レコメンデーション」パネルでメッセージを確認し、「完了としてマーク」をクリックします。

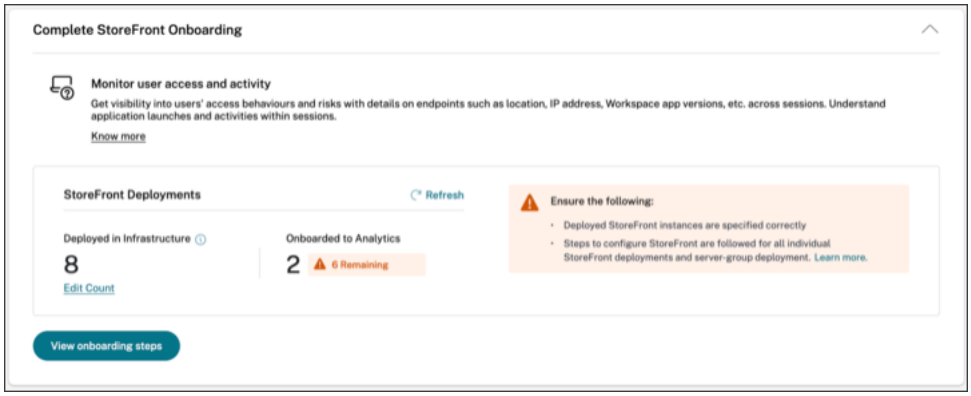
> 注
>
> さらに多くの StoreFront 展開環境をオンボーディングする場合は、［オンボーディング手順を表示］をクリックすると、StoreFront オンボーディングウィザードまたは［**StoreFront** 展開環境への接続］ポップアップが再び表示されます。



宣言された StoreFront 展開の数がオンボードされた StoreFront 展開の数より少ない場合は、［数を編集］をクリックすると、［展開された **StoreFront** インスタンスの指定］ページが表示されます。次に、デプロイされた **StoreFront** インスタンスの総数を入力して、［続行］をクリックします。StoreFront オンボーディングウィザー

ドまたは **StoreFront** デプロイメントへの接続ポップアップが再び表示されます。手順に従って、さらに多くの StoreFront デプロイメントをオンボーディングしてください。

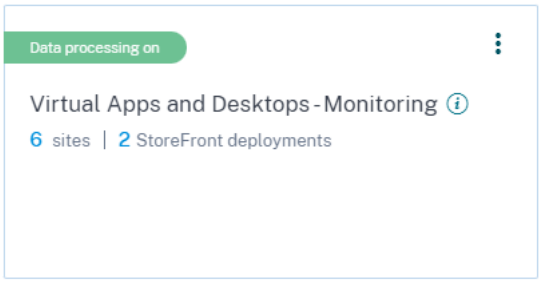
> 注:
>
> デプロイされた **StoreFront** インスタンスの総数は **StoreFront** グループの総数であり、個々の StoreFront サーバーの数ではありません。



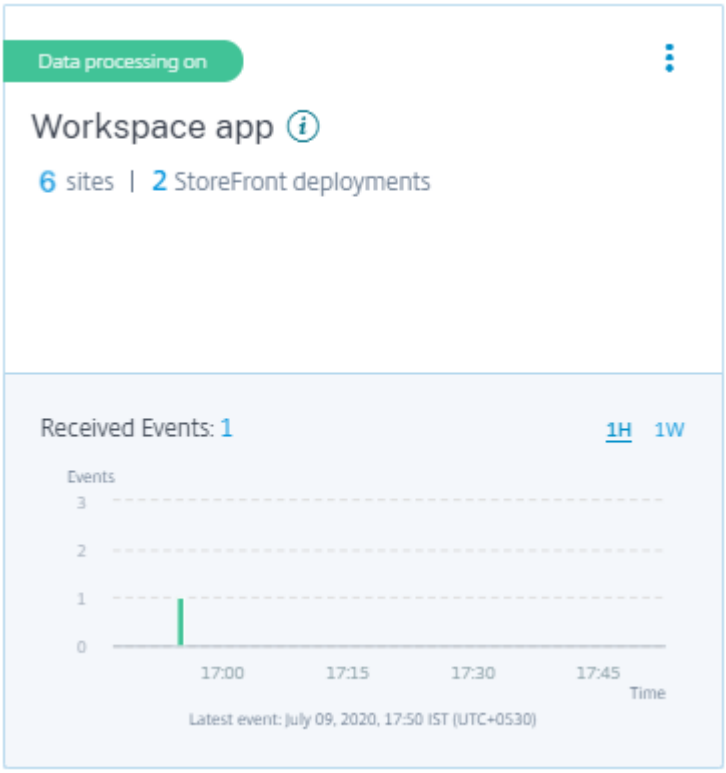
接続されている **StoreFront** 展開環境の表示

StoreFront 展開環境は、正常に構成された場合にのみサイトカードに表示されます。サイトカードには、Citrix Analytics との接続が確立されている StoreFront 展開環境の数が表示されます。

- パフォーマンス分析オファリングを使用している場合、[アプリとデスクトップ-監視] サイトカードに次の情報が表示されます。

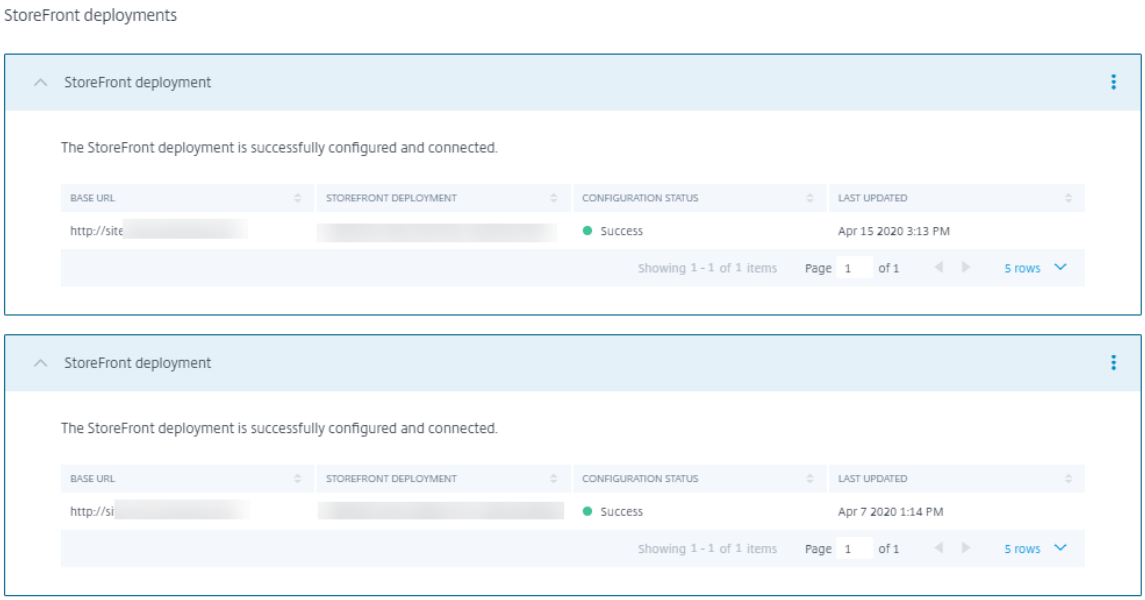


- Security Analytics サービスを使用している場合、**Workspace** アプリサイトカードに次の情報が表示されます。



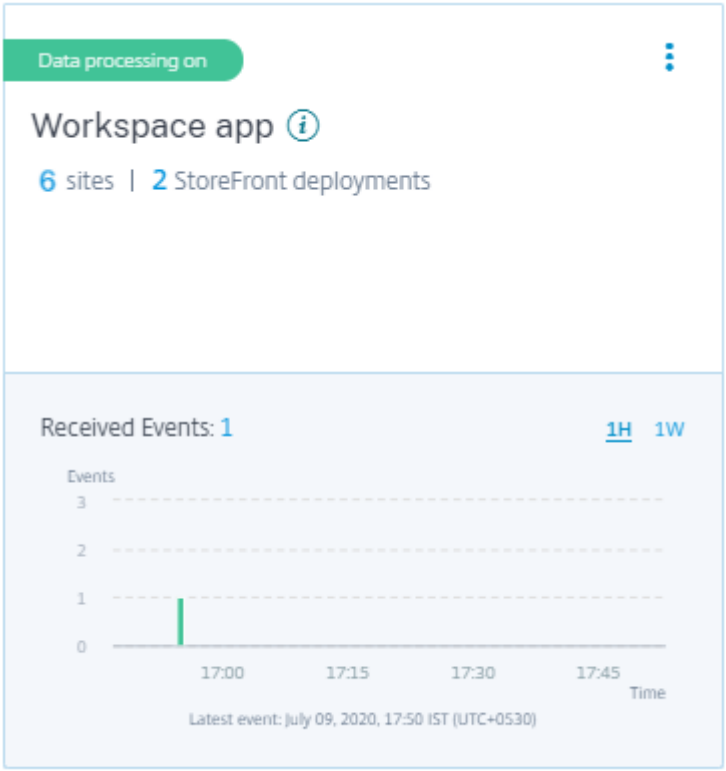
サイトカード上の StoreFront 展開環境の数をクリックして、サーバーグループを表示します。

各 StoreFront 展開は、ベース URL とサーバーグループ ID によって表されます。



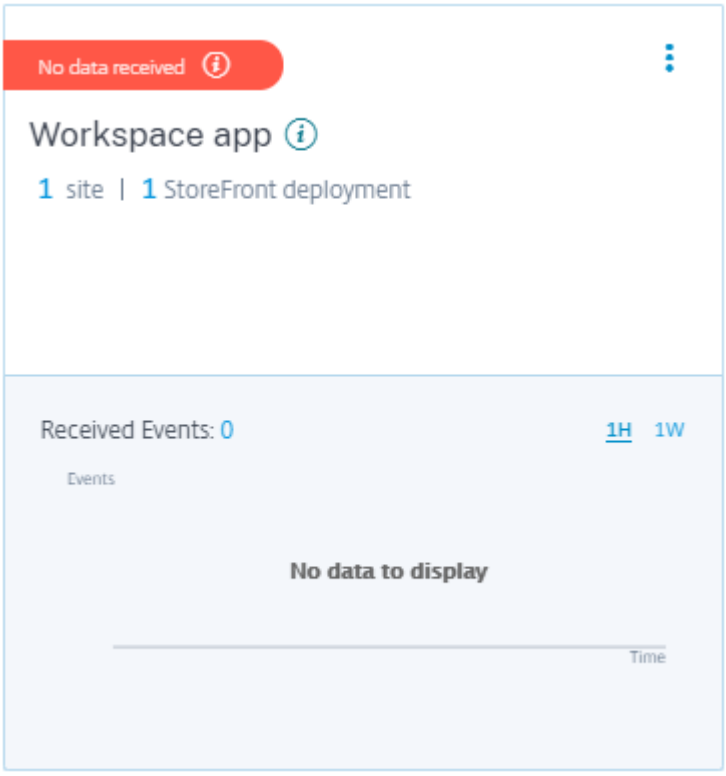
Security Analytics オファリングを使用している場合、受信したイベントに関する次の情報もサイトカードに表示されます。

- 過去 1 時間に StoreFront 展開環境から受信したイベント。これはデフォルトの時間選択です。1 週間（1 W）を選択して、データを表示することもできます。受信したイベントの数をクリックすると、セルフサービス検索ページにイベントが表示されます 。



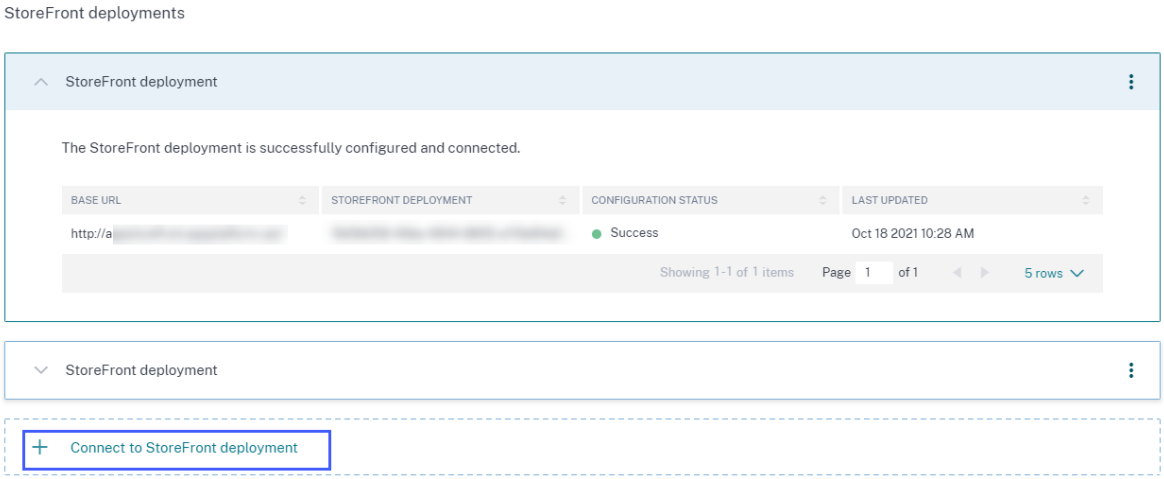
- データ処理を有効にすると、サイトカードに [データを受信していません] ステータスが表示される場合があります。このステータスは、次の 2 つの理由で表示されます:

  1. 初めてデータ処理をオンにした場合、イベントが Citrix Analytics のイベントハブに到達するまでに時間がかかります。Citrix Analytics がイベントを受信すると、ステータスが **Data processing on** に変わります。しばらくしてもステータスが変わらない場合は、[データソース] ページを更新します。
  2. Citrix Analytics は、過去 1 時間にデータソースからイベントを受信していません。



StoreFront 展開環境を追加または削除する

StoreFront 展開環境を追加するには、[**StoreFront** 展開環境] セクションの [StoreFront 展開環境への接続 **] をクリックします。構成ファイルをダウンロードし、手順に従って StoreFront 展開環境を構成します。



構成済みの StoreFront 展開環境からのイベント送信を停止し、Citrix Analytics から削除するには:

1. Citrix Analytics から削除する StoreFront 展開環境に移動します。次のコマンドを実行して、StoreFront サーバーから構成設定を削除します。


```
Remove-STFCasConfiguration
```

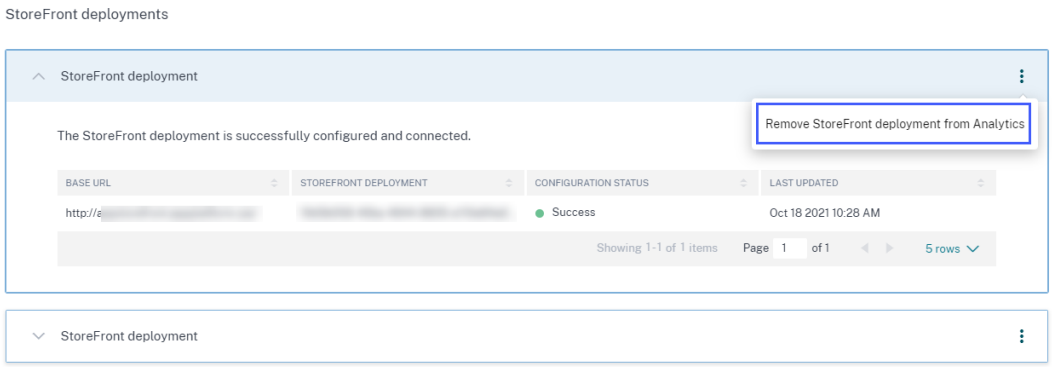
2. マルチサーバー展開を使用している場合は、次のコマンドを実行して変更を伝播し、StoreFront サーバーグループ内のすべてのサーバーから構成設定を削除します。

```
Publish-STFServerGroupConfiguration
```

3. 次のコマンドを実行して、構成設定が正常に削除されたことを確認します。設定が正常に削除された場合、このコマンドは何も返しません。

```
Get-STFCasConfiguration
```

4. Citrix Analytics に再度ログインし、[StoreFront 展開環境] セクションで **StoreFront** 展開環境を選択します。縦の省略記号（⋮）をクリックし、[**Analytics** から **StoreFront** 展開環境を削除] を選択します。



> 注
>
> 指定したコマンドを StoreFront 展開環境で実行してから、Citrix Analytics から削除します。コマンドを実行しなかった場合、Citrix Analytics は引き続きイベントを受信し、次のイベントプールサイクルで StoreFront 展開環境が再び追加されます。

HTTP プロキシを使用する **Web** サーバーでホストされる **StoreFront** 展開環境を構成する

StoreFront が Web プロキシを使用してインターネットに接続する Web サーバー上でホストされている場合は、Citrix Analytics に登録するようにストアを手動で構成する必要があります。この設定では、store web.config ファイルに<system.net>セクションを追加する必要があります。Citrix Analytics にイベントを送信する StoreFront 展開環境のすべてのストアを構成する必要があります。

store web.config ファイルに<system.net>セクションを追加する方法は 2 つあります。

- 1 つ以上のストアのストアプロキシ構成を PowerShell 経由で設定します (推奨される方法)。
- ストア web.config ファイルに<system.net>セクションを手動で追加します。

これらの方法について詳しくは、StoreFront ドキュメントの「Web プロキシを使用して Citrix Cloud に接続し、Citrix Analytics に登録するように StoreFront を構成する」を参照してください。

データガバナンス

December 7, 2023

このセクションでは、Citrix Analytics サービスによるログの収集、保存、および保持に関する情報を提供します。「定義」セクションで定義されていない大文字の用語は、Citrix エンドユーザーサービス契約で指定された意味を持ちます。

Citrix Analytics は、Citrix コンピューティング環境でのアクティビティに関する洞察を顧客に提供するように設計されています。Citrix Analytics を使用すると、セキュリティ管理者は、監視するログを選択し、ログに記録されたアクティビティに基づいて指示されたアクションを実行できます。これらのインサイトは、セキュリティ管理者がコンピューティング環境へのアクセスを管理し、お客様のコンピューティング環境にあるカスタマーコンテンツを保護するのに役立ちます。

データ所在地

Citrix Analytics ログはデータソースとは別に保持され、米国、欧州連合、およびアジア太平洋南部地域にある複数の Microsoft Azure Cloud 環境に集約されます。ログのストレージは、Citrix Cloud 管理者が組織を Citrix Cloud にオンボーディングするときに選択したホームリージョンによって異なります。たとえば、組織を Citrix Cloud にオンボーディングするときにヨーロッパリージョンを選択した場合、Citrix Analytics ログは欧州連合の Microsoft Azure 環境に格納されます。

詳しくは、「Citrix Cloud Services の顧客コンテンツとログの処理」および「地理的考慮事項」を参照してください。

データ収集

Citrix Cloud サービスは、ログを Citrix Analytics に送信するようにインストルメントされています。ログは、次のデータソースから収集されます。

- NetScaler ADC（オンプレミス）と NetScaler Application Delivery Management サブスクリプション
- Citrix Endpoint Management
- NetScaler Gateway (オンプレミス)
- Citrix ID プロバイダー
- Citrix Secure Browser
- Citrix Secure Private Access
- Citrix Virtual Apps and Desktops
- Citrix DaaS （旧 Citrix Virtual Apps and Desktops サービス）

- Microsoft Active Directory
- Microsoft Graph Security

データ送信

Citrix Cloud のログは、Citrix Analytics に安全に送信されます。顧客環境の管理者が Citrix Analytics を明示的に有効にすると、これらのログが分析され、顧客データベースに保存されます。Citrix Workspace Citrix Virtual Apps and Desktops
が構成されているデータソースにも同じことが当てはまります。

NetScaler ADC データソースの場合、ログ転送は、管理者が特定のデータソースに対して明示的に Citrix Analytics を有効にする場合にのみ開始されます。

データ管理

Citrix Analytics に送信されるログは、管理者がいつでもオンまたはオフにすることができます。

NetScaler ADC オンプレミスデータソースに対してオフにすると、特定の ADC データソースと Citrix Analytics 間の通信が停止します。

他のデータソースですべてオフにすると、特定のデータソースのログは分析されなくなり、Citrix Analytics に保存されなくなります。

データ保持

Citrix Analytics ログは、最大 13 か月または 396 日間、識別可能な形式で保持されます。すべてのログおよび関連する分析データ（ユーザーリスクプロファイル、ユーザーリスクスコアの詳細、ユーザーリスクイベントの詳細、ユーザーウォッチリスト、ユーザーアクション、ユーザープロファイルなど）は、この期間保持されます。

たとえば、2021 年 1 月 1 日にデータソースでアナリティクスを有効にした場合、デフォルトでは、2021 年 1 月 1 日に収集されたデータは、2022 年 1 月 31 日まで Citrix Analytics に保持されます。同様に、2021 年 1 月 15 日に収集されたデータは、2022 年 2 月 15 日まで保持されます。

このデータは、データソースのデータ処理をオフにした後や、Citrix Analytics からデータソースを削除した後でも、デフォルトのデータ保持期間にわたって保存されます。

Citrix Analytics は、サブスクリプションの有効期限または試用期間の 90 日後にすべてのカスタマーコンテンツを削除します。

データのエクスポート

このセクションでは、セキュリティのための Citrix Analytics とパフォーマンスのための Citrix Analytics からエクスポートされたデータについて説明します。

Citrix Analytics for Performance は、データソースからパフォーマンスメトリックを収集して分析します。

セルフサービス検索ページから CSV ファイルとしてデータをダウンロードできます。

Citrix Analytics for Security は、さまざまな製品（データソース）からユーザーイベントを収集します。これらのイベントは、ユーザーの危険で異常な動作を可視化するために処理されます。ユーザーのリスクインサイトとユーザーのイベントに関連するこれらの処理済みデータを、システム情報およびイベント管理 (SIEM) サービスにエクスポートできます。

現在、データは Citrix Analytics for Security から次の 2 つの方法でエクスポートできます。

- Citrix Analytics for Security を SIEM サービスと統合する
- セルフサービス検索ページからデータを CSV ファイルとしてダウンロードします。

Citrix Analytics for Security を SIEM サービスと統合すると、北行きの Kafka トピックまたは Logstash ベースのデータコネクタのいずれかを使用して、データが SIEM サービスに送信されます。

現在、次の SIEM サービスと統合できます。

- Splunk（Citrix Analytics アドオンを介して接続することにより）
- Elasticsearch や Microsoft Azure Sentinel などの Kafka トピックまたは Logstash ベースのデータコネクタをサポートする SIEM サービス

CSV ファイルを使用して SIEM サービスにデータをエクスポートすることもできます。[セルフサービス検索] ページでは、データソースのデータ (ユーザーイベント) を表示し、そのデータを CSV ファイルとしてダウンロードできます。CSV ファイルの詳細については、「セルフサービス検索」を参照してください。

> 重要
>
> SIEM サービスにデータがエクスポートされると、Citrix はエクスポートされたデータのセキュリティ、ストレージ、管理、および SIEM 環境での使用について責任を負いません。

Citrix Analytics for Security から SIEM サービスへのデータ転送をオンまたはオフにできます。

処理されたデータと SIEM 統合について詳しくは、「SIEM （セキュリティ情報およびイベント管理）の統合」および「SIEMの Citrix Analytics データ形式」を参照してください。

Citrix Services Security Exhibit

アクセスと認証、セキュリティプログラム管理、ビジネス継続性、インシデント管理など、Citrix Analytics に適用されるセキュリティ制御に関する詳細情報は、Citrix Services のセキュリティに関する展示会に含まれています。

定義

顧客コンテンツとは、Citrix がサービスを実行するためのアクセスを提供されているお客様の環境におけるストレージまたはデータのためにお客様のアカウントにアップロードされるデータを意味します。

ログ：パフォーマンス、安定性、使用状況、セキュリティ、およびサポートを測定するレコードを含む、サービスに関連するイベントのレコードを意味します。

サービスとは、Citrix Analytics の目的で上記に概説した Citrix Cloud クラウドサービスを意味します。

データ収集契約

お客様のデータを Citrix Analytics にアップロードし、Citrix Analytics の機能を使用することにより、お客様は、Citrix がお客様の Citrix 製品およびサービスに関する技術情報、ユーザー情報、または関連情報を収集、保存、送信、維持、処理、および使用することに同意し、同意するものとします。

Citrix は、受信した情報を常に Citrix プライバシーポリシーに従って取り扱います。

付録**:** 収集されたログ

- セキュリティログの Citrix Analytics
- パフォーマンス向け Citrix Analytics ログ

セキュリティログの **Citrix Analytics**

一般ログ

一般に、Citrix Analytics ログには次のヘッダー識別データポイントが含まれます。

- ヘッダーキー
- デバイス識別
- 識別
- IP アドレス
- 組織
- Product
- 製品バージョン
- システム時刻
- テナントの識別
- 種類
- ユーザー: 電子メール、ID、SAM アカウント名、ドメイン、UPN
- バージョン

Citrix Endpoint Management サービスログ

Citrix Endpoint Management サービスのログには、次のデータポイントが含まれています。

- コンプライアンス
- 企業所有
- デバイス ID
- デバイスモデル
- デバイスの種類
- 地理緯度
- 地理経度
- ホスト名
- IMEI
- IP アドレス
- ジェイル・ブロークン
- 前回のアクティビティ
- 管理モード
- オペレーティングシステム
- オペレーティングシステムバージョン
- プラットフォーム情報
- 理由
- シリアル番号
- 監視対象

Citrix Secure Private Access ログ

- AAA ユーザ名
- 認証ポリシーアクション名
- 認証セッション ID
- リクエスト URL
- URL カテゴリポリシー名
- VPN セッション ID

- 仮想サーバー IP
- AAA ユーザの電子メール ID
- 実際のテンプレートコード
- アプリ FQDN
- アプリ名
- アプリケーション名 Vserver LS
- アプリケーションフラグ
- 認証の種類
- 認証ステージ
- 認証ステータスコード
- バックエンドサーバー DST IPv4 アドレス
- バックエンドサーバー IPv4 アドレス
- バックエンドサーバー IPv6 アドレス
- カテゴリドメイン名
- カテゴリドメインソース
- クライアント IP
- クライアント MSS
- クライアント高速レトックスカウント
- クライアント TCP ジッター
- 再送信されたクライアント TCP パケット
- クライアント TCP RTO カウント
- クライアント TCP ゼロウィンドウカウント
- Clt フローフラグ Rx
- Clt フローフラグ Tx
- Clt TCP フラグ Rx
- Clt TCP フラグ Tx
- 接続チェーンホップカウント
- 接続チェーン ID
- 出力インターフェイス

- プロセス ID をエクスポート中
- フローフラグ Rx
- フローフラグ Tx
- HTTP コンテンツタイプ
- HTTP ドメイン名
- HTTP 要求認証
- HTTP 要求クッキー
- HTTP Req Forw FB
- HTTP Req Forw LB
- HTTP 要求ホスト
- HTTP 要求メソッド
- HTTP Req Rcv FB
- HTTP Req Rcv LB
- HTTP 要求リファラー
- HTTP リクエストの URL
- HTTP Req XForwarded For
- HTTP RES Forw FB
- HTTP Res Forw LB
- HTTP 解像度ロケーション
- HTTP 解像度 Rcv FB
- HTTP Res Rcv LB
- HTTP 解像度セットクッキー
- HTTP Rsp Len
- HTTP Rsp Status
- HTTP トランザクション終了時刻
- HTTP トランザクション ID
- IC Cont Grp Name
- IC フラグ
- IC ストアフラグなし

- IC ポリシー名
- Ingress インターフェイスクライアント
- NetScaler Gateway Service アプリ ID
- NetScaler Gateway Service アプリ名
- NetScaler Gateway Service アプリの種類
- NetScaler パーティション ID
- 観測ドメイン ID
- 観測ポイント ID
- 原点解像度ステータス
- オリジン Rsp レン
- プロトコル識別子
- レート制限識別子の名前
- レコードタイプ
- レスポンダーアクションタイプ
- レスポンスメディアタイプ
- Srv フローフラグ Rx
- Srv フローフラグ Tx
- サーブ高速レトックスカウント
- サーバー TCP ジッター
- 再送信されたサーバ TCP パケット
- サーバー TCP Rot カウント
- サーバー TCP ゼロウィンドウカウント
- SSL 暗号値 BE
- SSL 暗号値 FE
- SSL クライアント証明書サイズ BE
- SSL クライアント証明書サイズ FE
- SSL Clnt Cert Sig Hash BE
- SSL Clnt Cert Sig Hash FE
- SSL エラーアプリ名

- SSL エラーフラグ
- SSL フラグ
- SSL フラグ FE
- SSL ハンドシェイクエラーメッセージ
- SSL サーバ証明書サイズ BE
- SSL サーバ証明書サイズ FE
- SSL Session ID BE
- SSL セッション ID FE
- SSL Sig Hash Alg BE
- SSL Sig Hash Alg FE
- SSL Srvr Cert Sig Hash BE
- SSL Srvr Cert Sig Hash FE
- SSL iDomain Category
- SSL iDomain カテゴリグループ
- SSL ID ドメイン名
- SSL IDomain レピュテーション
- SSL i 実行アクション
- SSL iPolicy アクション
- SSL iReason for アクション
- SSL iURL セットが一致しました
- SSL iURL セットプライベート
- 加入者識別子
- Svr Tcp フラグ Rx
- Svr Tcp フラグ Tx
- テナント名
- Req 親スパン ID のトレース
- Req スパン ID のトレース
- トレーストレース ID
- トランスコルトダスト IPv4 アドレス

- トランスコルトダスト IPv6 アドレス
- トランス Clt Dst ポート
- トランス Clt フローエンドユーザーレックス
- トランス Clt フローエンドユーザー税
- トランス Clt フロー開始 Usec Rx
- トランス Clt フロー開始使用税
- トランス Clt IPv4 アドレス
- トランス Clt IPv6 アドレス
- トランスコルトパケット Tox Cnt Rex
- トランスコルトパケットトート Cnt Tx
- トランス・コルト RTT
- トランス Clt Src ポート
- トランス・コルト・トット・レックス 10 月 Cnt
- トランスコルトトート税 10 月 Cnt
- トランス情報
- トランスサーブ Dst ポート
- トランスサーブパケットトート Cnt Rx
- トランスサーブパケットトート Cnt Tx
- トランス Srv Src ポート
- トランス Svr フローエンドユーザー Rx
- Trans Svr フローエンドユーザー Tx
- Trans Svr Flow Start Usec Rx
- Trans Svr Flow Start Usec Tx
- Trans Svr RTT
- Trans Svr Tot Rx Oct Cnt
- Trans Svr Tot Tx Oct Cnt
- トランザクション ID
- URL カテゴリ
- URL カテゴリグループ

- URL カテゴリレピュテーション
- URL カテゴリアクションの理由
- 一致した URL セット
- URL セットプライベート
- URL オブジェクト ID
- VLAN 番号

Citrix Virtual Apps and Desktops および **Citrix DaaS** ログ

Citrix Virtual Apps and Desktops、および Citrix DaaS ログには、次のデータポイントが含まれます。

- アプリ名
- ブラウザー
- カスタマー ID
- 詳細: フォーマットサイズ、フォーマットタイプ、イニシエータ、結果
- デバイス ID
- デバイスの種類
- フィードバック
- フィードバック ID
- ファイル名
- [ファイルパス]
- ファイルサイズ
- Is like
- ジェイル・ブロークン
- ジョブの詳細: ファイル名、フォーマット、サイズ
- 位置: 推定、緯度、経度

  > 注
  >
  > 位置情報は都市レベルおよび国レベルで提供され、正確な地理的位置情報を表すものではありません。

- 長い CMD ライン
- モジュールファイルパス
- 操作

- オペレーティングシステム
- プラットフォームの追加情報
- プリンタ名
- 質問
- 質問 ID
- SaaS アプリケーション名
- セッションドメイン
- セッションサーバー名
- セッションユーザー名
- セッション GUID
- Timestamp
- タイムゾーン: バイアス、DST、名前
- 印刷部数の総数
- 総印刷ページ数
- 種類
- URL
- ユーザー エージェント

NetScaler ADC ログ

NetScaler ADC ログには、次のデータポイントが含まれています。

- コンテナ
- ファイル
- 形式
- 種類

Azure ログ用 **Citrix DaaS** スタンダード

Azure 向け Citrix DaaS Standard ログには、次のデータポイントが含まれています。

- アプリ名
- ブラウザー

- 詳細: フォーマットサイズ、フォーマットタイプ、イニシエータ、結果
- デバイス ID
- デバイスの種類
- ファイル名
- [ファイルパス]
- ファイルサイズ
- ジェイル・ブロークン
- ジョブの詳細: ファイル名、フォーマット、サイズ
- 位置: 推定、緯度、経度

  > 注
  >
  > 位置情報は都市レベルおよび国レベルで提供され、正確な地理的位置情報を表すものではありません。

- 長い CMD ライン
- モジュールファイルパス
- 操作
- オペレーティングシステム
- プラットフォームの追加情報
- プリンタ名
- SaaS アプリケーション名
- セッションドメイン
- セッションサーバー名
- セッションユーザー名
- セッション GUID
- Timestamp
- タイムゾーン: バイアス、DST、名前
- 種類
- URL
- ユーザー エージェント

Citrix アイデンティティプロバイダーのログ

- ユーザーログイン:
  - 認証ドメイン: 名前、製品、IdP タイプ、IdP 表示名
    - IdP プロパティ: アプリケーション、認証タイプ、顧客 ID、クライアント ID、ディレクトリ、発行者、ロゴ、リソース、TID
    - 拡張機能:
      - ワークスペース: 背景色、ヘッダーロゴ、ログオンロゴ、リンクの色、テキストの色、StoreFront ドメイン
      - ShareFile: カスタマー ID、カスタマージオ
      - 長寿命トークン: 有効、有効期限タイプ、絶対有効期限秒、スライディング有効期限秒
  - 認証結果: ユーザー名、エラーメッセージ
  - サインインメッセージ: クライアント ID、クライアント名
  - ユーザーの要求:AMR、アクセストークンハッシュ、Aud、認証時間、CIP Cred、認証エイリアス、認証ドメイン、グループ、製品、システムエイリアス、電子メール、
    検証済み E メール、Exp、ファミリー名、指定された名前、IAT、IdP、ISS、ロケール、名前、NBF、SID、サブ
    - 認証エイリアスの要求: 名前、値
    - ディレクトリコンテキスト: ドメイン、フォレスト、ID プロバイダ、テナント ID
    - ユーザー: 顧客、電子メール、OID、SID、UPN
    - IdP エクストラフィールド:Azure AD OID、Azure AD TID
- ユーザーログオフ: クライアント ID、クライアント名、ナンス、サブ
- クライアントアップデート: アクション、クライアント ID、クライアント名

NetScaler Gateway ログ

- トランザクションイベント:
  - ICA アプリケーション: レコードタイプ、実際のテンプレートコード、観測ドメイン ID、観測ポイント ID、エクスポートプロセス ID、ICA セッション GUID、MSI クライアント Cookie、フロー ID Rx、ICA フラグ、接続 ID、パディングオクテット 2、ICA デバイスシリアル番号、IP バージョン 4、プロトコル識別子、送信元 IPv4 アドレス Rx、宛先 IPv4 アドレス Rx、ソーストランスポートポート Rx、宛先トランスポートポート Rx、ICA アプリケーションの起動期間、ICA 起動メカニズム、ICA アプリケーションの起動時間、ICA プロセス ID の起動、ICA アプリケーション名、ICA アプリケーションモジュールパ

ス、ICA アプリケーションの終了タイプ、ICA アプリケーションの終了時間、アプリケーション名アプリケーション ID、ICA アプリケーションプロセス ID 終了、ICA アプリケーション

- ICA イベント: レコードタイプ、実際のテンプレートコード、ソース IPv4 アドレス Rx、宛先 IPv4 アドレス Rx、ICA セッション GUID、MSI クライアント Cookie、接続チェーン ID、ICA クライアントバージョン、ICA クライアントホスト名、ICA ユーザー名、ICA ドメイン名、ログオンチケットの設定、サーバー名、サーバーバージョン、フロー Id Rx、ICA フラグ、観察ポイント ID、エクスポートプロセス ID、監視ドメイン ID、接続 ID、ICA デバイスのシリアル番号、ICA セッションのセットアップ時間、ICA クライアント IP、NS ICA セッション状態のセットアップ、ソーストランスポートポート Rx、送信先トランスポートポート Rx、ICA クライアント起動ツール、ICA クライアントの種類、ICA 接続の優先度のセットアップ、NS ICA セッションサーバーポート、NS ICA セッションサーバ IP アドレス、IPv4、プロトコル識別子、接続チェーンホップカウント、アクセスタイプ
- ICA 更新: レコードタイプ、実際のテンプレートコード、観測ドメイン ID、観測ポイント ID、エクスポートプロセス ID、ICA セッション GUID、MSI クライアント Cookie、フロー ID Rx、ICA フラグ、接続 ID、ICA デバイスシリアル番号、IPv4、プロトコル識別子、パディングオクテット 2、ICA RTT、クライアント側の RX バイト、クライアント側パケット再送信、サーバー側パケット再送信、クライアント側 RTT、クライアント側ジッター、サーバー側ジッター、ICA ネットワーク更新開始時刻、ICA ネットワーク更新終了時刻、クライアント側 SRTT、サーバー側遅延、サーバー側遅延、ホスト遅延、クライアント側ゼロウィンドウ数、サーバー側ゼロウィンドウ数、クライアントサイド RTO カウント、サーバー側 RTO カウント、L7 クライアント遅延、L7 サーバー遅延、アプリケーション名アプリケーション ID、テナント名、ICA セッション更新開始秒、ICA セッション更新終了秒、ICA チャネル ID 1、ICA チャネル ID 2、ICA チャネル ID 2 バイト、ICA チャネル ID 3 バイト、ICA チャネル ID 3 バイト、ICA チャネル ID 4 バイト、ICA チャネル ID 5、ICA チャネル ID 5 バイト
- AppFlow 構成: レコードタイプ、実際のテンプレートコード、観測ドメイン ID、観測ポイント ID、エクスポートプロセス ID、システムルールフラグ 1、システム安全性インデックス、AppFlow プロファイル緩和フラグ、AppFlow プロファイルブロックフラグ、AppFlow プロファイルログフラグ、AppFlow プロファイル学習フラグ、AppFlow プロファイル統計フラグ、AppFlow プロファイル統計フラグ、AppFlow プロファイルなしフラグ、AppFlow アプリケーション名 ID、AppFlow プロファイル記号無効、AppFlow プロファイル符号ブロック数、AppFlow プロファイル符号ログ数、AppFlow プロファイル記号統計数、AppFlow 化身番号、AppFlow シーケンス番号、AppFlow プロファイル記号自動更新、AppFlow 安全性インデックス、AppFlow アプリケーション安全性インデックス、AppFlow プロファイル秒チェック安全性インデックス、AppFlow プロファイルタイプ、Iprep アプリケーション安全性インデックス、AppFlow プロファイル名、AppFlow シグネーム、AppFlow アプリケーション名 Ls、AppFlow シグルール ID1、AppFlow シグルール ID2、AppFlow シグルール ID3、AppFlow シグルール ID4、AppFlow シグルール ID5、AppFlow シグルール有効フラグ、AppFlow シグルールログフラグ、AppFlow シグルールファイル名、AppFlow シグルールカテゴリ 1、AppFlow シグルール Logstring1、AppFlow シグルールカテゴリ 2、AppFlow シグルール LogString2、AppFlow シグルールカテゴリ 3、AppFlow シグルールカテゴリ 4、AppFlow シグルール Logstring4、AppFlow シグルールカテゴリ 5、AppFlow Sig ルール logString5

- AppFlow: 実際のテンプレートコード、観測ドメイン ID、観測ポイント ID、エクスポートプロセス ID、トランザクション ID、Appfw 違反発生時間、アプリ名アプリ ID、appfw 違反の重大度、appfw 違反タイプ、appfw 違反場所、appfw 違反脅威インデックス、appfw NS 経度、appfw NS 緯度、ソース IPv4 アドレス Rx、appfw Http メソッド、Appfw アプリケーション脅威インデックス、appfw ブロックフラグ、appfw 変換フラグ、appfw 違反プロファイル名、appfw セッション ID、appfw Req URL、appfw 地理ロケーション、appfw 違反タイプ名 1、appfw 違反名の値 1、appfw シグカテゴリ 1、appfw 違反タイプ名 2、appfw 違反名前値 2、appfw シグカテゴリ 2、appfw 違反タイプ名 3、appfw 違反名の値 3、appfw シグカテゴリ 3、Appfw 要望 X 転送対用、Appfw アプリケーション名 Ls、アプリケーション名 Ps、Iprep カテゴリ、iprep 攻撃時間、Iprep レピュテーションスコア、Iprep NS 経度、Iprep NS 緯度、Iprep 重大度、Iprep HTTP メソッド、Iprep アプリ脅威インデックス、iprep 地理ロケーション、Tcp Syn 攻撃センター、Tcp 低速リスクセンター、TCP ゼロウィンドウセンター、Appfw ログ Expr 名、Appfw ログ Expr 値、Appfw Log Expr コメント
- VPN: 実際のテンプレートコード、観測ドメイン ID、アクセスインサイトフラグ、観測ポイント ID、エクスポートプロセス ID、アクセスインサイトステータスコード、アクセスインサイトのタイムスタンプ、認証期間、デバイスタイプ、デバイス ID、デバイスの場所、アプリ名アプリ ID、アプリ名アプリ Id、アプリ名アプリ Id1、ソーストランスポートポート Rx、宛先トランスポートポート Rx、認証ステージ、認証タイプ、VPN セッション ID、EPA ID、AAA ユーザ名、ポリシー名、認証エージェント名、グループ名、仮想サーバ FQDN、Csec 式、送信元 IPv4 アドレス Rx、宛先 IPv4 アドレス Rx、CUR ファクタポリシーラベル、次の要素ポリシーラベル、アプリケーション名 Ls、アプリケーション名 1 Ls、AAA ユーザ電子メール ID、ゲートウェイ IP、ゲートウェイポート、アプリケーションバイト数、VPN セッション状態、VPN セッションモード、SSO 認証方式、IIP アドレス、VPN 要求 URL、SSO 要求 URL、バックエンドサーバ名、VPN セッションログアウトモード、ログオンチケットファイル情報、STA チケット、セッション共有キー、リソース名、SNIP アドレス、一時 VPN セッション ID
- HTTP: 実際のテンプレートコード, HTTP 要求メソッド, HTTP 要求 URL, HTTP 要求ユーザエージェント, HTTP コンテンツタイプ, HTTP 要求ホスト, HTTP 要求承認, HTTP 要求クッキー, HTTP 要求リファラ, HTTP 解像度セットクッキー, IC 続き GRP 名, IC フラグ, IC Nostore フラグ, IC ポリシー名, 応答メディアタイプ, 入力インターフェイスクライアント, オリジン解像度ステータス、オリジン Rsp Len、Srv フローフラグ Rx、Srv フローフラグ Tx、フローフラグ Tx、フローフラグ Tx、アプリケーション名、観測ポイント ID、エクスポートプロセス ID、観測ドメイン ID、Http トランス終了時刻、トランザクション ID、Http Rsp ステータス、トランス clt Ipv4 アドレス、トランス clt dst Ipv4 アドレス、バックエンド Svr Ipv4 アドレス, Http Rsp Len, Trans Svr RTT, Trans Clt RTT, Http Req Rcv FB, Http Req Rcv LB, Http Res Rcv LB, Http Req Forw LB, Http Req Forw LB, Http Req X Forw 転送先、Http ドメイン名、HTTP Res ロケーション、プロトコル識別子、出力インターフェイス、バックエンド保存 IPv6 アドレス、SSL フラグ BE、SSL フラグ FE、SSL セッション IDBE、SSL セッション IDBE、SSL 暗号値 FE、SSL 暗号値 BE、SSL 署名ハッシュアルグ BE、SSL サーバー証明書署名ハッシュ BE、SSL サーバー証明書署名ハッシュ FE、SSL クライアント証明書署名ハッシュ FE、SSL クライアント証明書署名ハッシュ FE、SSL クライアント証明書署名ハッシュ BE、SSL サーバー証明書サイズ FE、SSL サーバー証明書サイズ BE、SSL クライアント証明書サイズ FE、SSL クライアント証明書サイズ BE、SSL エラーアプリケーション名、SSL エラーフラグ、SSL ハンドシェイクエラーメッセージ、

クライアント IP、仮想サーバー IP、接続チェーン ID、接続チェーンホップカウント、トランス clt TotT Rx Oct Cnt、トランス clt TotTx Oct Cnt、トランス clt Src ポート、トランス Srv Src ポート、トランス Srv Dst ポート、VLAN 番号、クライアント mss、トランス情報、トランス Clt フロー終了使用 Rx、トランス CLT フロー終了 Usec Tx、トランス clt フロー開始使用 Rx、トランス clt フロー開始使用 Tx、トランス Svr フロー終了使用 Rx、トランス Svr フロー終了使用 Tx、トランス Svr フロー開始 Usec、Trans Svr フロー開始 Usec Tx、Trans Svr Tot Rx Oct CNT、TransSvr Tit Tx Oct Cnt, clt フローフラグ Tx, clt フローフラグ Rx, トランス clt IPv6 アドレス, トランス CLT DST IPv6 アドレス, サブスクライバ識別子, SSLi ドメイン名, SSLi ドメインカテゴリ, SSLi ドメインカテゴリグループ, SSLI ドメインレピュテーション, SSLI ポリシーアクション, SSLI 実行アクション, SSLI アクションの理由, SSLI URL セット一致,SSLi URL セットプライベート、URL カテゴリ、URL カテゴリグループ、URL カテゴリレピュテーション、レスポンダアクションタイプ、一致した URL セット、URL セットプライベート、カテゴリドメイン名、カテゴリドメインソース、AAA ユーザ名、VPN セッション ID、テナント名

- メトリクスイベント:
  - vServer LB：バインドエンティティ名、エンティティ名、月サービスバインド、NetScaler ID、表現、スキーマタイプ、時間、CPU、GSLB サーバー、GSLB 仮想サーバー、インターフェイス、メモリプール、サーバーサービスグループ、サーバー Svc Cfg、vServer Authn、vServer Cr、vServer Cs、vServer LB：RATE Si Tet 要求バイト、RATE SiTot レスポンスバイト, RATE Si Tot レスポンス, RATE Si TotT clt Ttlb トランザクション, RATE Si Tott clt ttlb Pkt Rcvd, RATE Si TotT clt Pkt Sent, RATE Vsvr TotT Hits, Si Cur クライアント, Si Cur Conn 確立, Si Cur サーバ, Si Cur State, Si Tot リクエストバイト, Si Tot レスポンス, Si Tot レスポンス, Si Tott clt ttlb、Si Tott clt ttlb トランザクション、Si TotPkt Rcvd、Si TotPkt Sent Sent、Si TottLb イライラするトランザクション、Si TottTtlb 許容トランザクション、VSVR アクティブ SVC、VSVR TotTot ヒット、Vsvr TotReq Resp 無効、Vsvr TottReq Resp 無効なドロップ
  - CPU：バインドエンティティ名、エンティティ名、月サービスバインド、NetScaler ID、表現、スキーマタイプ、時間、Cc CPU 使用 GSLB サーバー、GSLB 仮想サーバー、インターフェイス、メモリプール、NetScaler、サーバーサービスグループ、サーバー SVC Cfg、vServer Authn、vServer Cr、vServer CS、vServer Lb、vServer SSL、仮想サーバーユーザー
  - サーバーサービスグループ: バインドエンティティ名、エンティティ名、月サービスバインド、NetScaler ID、表現、スキーマタイプ、時間、Cc CPU 使用率、GSLB サーバー、GSLB 仮想サーバー、インターフェイス、メモリプール、NetScaler、サーバー Svc Cfg、vServer Authn、vServer Cr、vServer CS、vServer Lb、vServer SSL、vServer ユーザー、サーバーサービスグループ：RATE Si Tot リクエストバイト, RATE Si Tot_Response バイト, RATE Si Tot_Response バイト, RATE Si Tott clt ttlb, RATE Si Tott clt Ttlb トランザクション, RATE Si Tott Si Tt SV ttfb トランザクション, RATE Si Tott Si Tvr ttfb トランザクション, RATE Si Tott Si Ttlb トランザクションイライラするトランザクション、RATE Si Tott Ttlb 許容トランザクション, Si Cur 状態, Si Tot リクエストバイト, Si Tot リクエスト, Si Tot レスポンスバイト, Si TotT clt Ttlb, Si TottClt Ttlb トランザクション, Si TotSvr ttfb, Si TotSvr Ttfb トランザクション, Si Tott Svr Ttlb トランザクション, Si Tott Svr Ttlb トランザクション, Si Tott Svr Ttlb トランザクション, Si Tots Svr Ttlb TotTtlb イライラするトランザクション、Si

Totttlb 許容するトランザクション

- サーバー SVC CFG：バインドエンティティ名、エンティティ名、月サービスバインド、NetScaler ID、表現、スキーマタイプ、時間、CPU 使用率、GSLB サーバー、GSLB 仮想サーバー、インターフェイス、メモリプール、NetScaler、vServer Authn、vServer Cr、vServer CS、vServer Lb、vServer SSL、vServer ユーザー、サーバー SVC Cfg：RATE Si Totot 要求バイト、RATESi Tot 要求, RATE Si Tot 応答バイト, RATE Si Tot 応答, Si Tott clt ttlb, RATE Si Tott Pkt rcvd, RATE Si Tott Pkt Si Pkt Si Tkt Sd, RATE Si Tott SVR Busy Err, RATE Si Tott SVR Tfb, RATE Si Tott Si Ttr Ttlb, RATE Si Tott svr ttlb Transactions, RATE SiTotTtlb イライラするトランザクション, RATE Si Tott ttlb 許容トランザクション, Si Cur 状態, Si Cur トランスポート, Si Tot リクエストバイト, Si Tot リクエスト, Si Tot レスポンスバイト, Si Tott clt ttlb, Si Tott clt Ttlb トランザクション, Si TotPkt Rcvd, Si Tott Pkt Sent Svr ビジーえーーーーーーーーーーーーーーーーーーーーーーーー Svr Ttfb トランザクション, Si TottSvr Ttlb, Si TotSvr Ttlb トランザクション, Si TottTtlb イライラするトランザクション, Si TottTtlb 許容トランザクション
- NetScaler：バインドエンティティ名、エンティティ名、月サービスバインド、NetScaler ID、表現、スキーマタイプ、時間、GSLB サーバー、GSLB 仮想サーバー、インターフェイス、メモリプール、サーバーサービスグループ、サーバー Svc Cfg、vServer Authn、vServer Cr、vServer CS、vServer Lb、vServer SSL、vServer ユーザー、NetScaler：RATE すべてニックトット Rx メガビット、RATE すべて NIC トット Rx メガビット、レート Dns トットクエリ、レート Dns トット Nxdmn エントリ、レート Http トット Gets、レート Http トットその他、レート Http トット投稿、レート Http トットリクエスト、レート Http トットリクエスト 1.0、レート Http トットリクエスト 1.1、レート Http トットリクエスト、レート Http トットリクエスト Rx レスポンスバイト、RATE Ip Tt Rx Mbit、RATE Ip TotT Rx バイト、RATE Ip Tt Rx Pits、RATE Ip Tt Tx バイト、RATE Ip Tt Tx バイト、RATE SSL Tt Dec バイト、RATE SSL TotT End バイト、RATE SSL Tt SSL 情報セッションヒット、RATE SSL トット SSL 情報合計送信カウント、レート Tcp エラー Rst、RATE Tcp Top クライアントオープン、レート Tcp Tt サーバーオープン、レート Tcp トット Rx バイト、レート Tcp トット Rx ポート、レート Tcp トット Syn、レート Tcp トット Tx バイト、レート Tcp トット Tx バイト、レート UDP トット Rx バイト、レート UDP トット Rx バイト、レート UDP トット Tx バイト、レート UDP トット Tx バイト、レート UDP トット Tx バイト、すべて NIC トット送信メガビット、CPU 使用、DNS トットクエリ、DNS トットネグ Nxdmn エントリ、Http トット取得, Http トットその他, Http トット投稿, Http トットリクエスト, Http トット Requests1.0, Http トットレスポンス, Http トット受信リクエストバイト, Http トット受信レスポンスバイト, IP トット受信メガビット, IP トット受信バイト, IP トット Rx Pkts, IP トット送信バイト, IP トット Pkt TS, Mem cur フリーサイズ, Mem Cur Free 実際のサイズ、メモリ CUR 使用サイズ、使用可能なメモリトット、管理追加 CPU 使用、管理 CPU 使用、管理 CPU 使用、SSL トット Dec バイト、SSL トット Enc バイト、SSL トット SSL 情報セッションヒット、SSL トット SSL 情報合計送信回数、システム CPU、Tcp Cur クライアントコネクト、TCP CUR クライアント接続終了、TCP CUR クライアント接続終了、TCP CUR クライアント接続テスト、TCP Cur サーバーコネン、TCP CUR サーバー接続終了、TCP CUR サーバー接続テスト、TCP エラー最初、TCP おっとクライアントオープン、TCP トットサーバーオープン、TCP トット受信バイト、TCP トット受信ピクツ、TCP トット同列、TCP トット Tx バイト、Tcp トット送信バイト、Tcp トット Tx Pkts、Ucp

トット受信バイト、Udp トット送信バイト、Udp トット送信バイト

- メモリプール：バインドエンティティ名、エンティティ名、月サービスバインド、NetScaler ID、スキーマタイプ、時間、CPU、Gslb サーバー、Gslb 仮想サーバー、インターフェイス、NetScaler、サーバーサービスグループ、サーバー Svc Cfg、vServer Authn、vServer Cr、vServer CS、vServer Lb、vServer SSL、vServer ユーザー、メモリプール：メモリコア割り当てサイズ、メモリエラーの割り当てに失敗しました。メモリメモリが使用可能
- 監視サービスバインド：バインドエンティティ名、エンティティ名、NetScalerId、schemaType、時間、CPU、Gslb サーバー、Gslb 仮想サーバー、インターフェイス、メモリプール、NetScaler、サーバーサービスグループ、サーバー Svc Cfg、vServer Authn、vServer Cr、vServer CS、Vserver Lb、vServer SSL、vServer ユーザー、月サービスバインディング：レート月 Toto プローブ、月トットプローブ
- インターフェイス：バインドエンティティ名、エンティティ名、月サービスバインド、NetScaler Id、スキーマタイプ、時間、CPU、Gslb サーバー、Gslb 仮想サーバー、メモリプール、NetScaler、サーバーサービスグループ、サーバー Svc Cfg、vServer Authn、vServer Cr、vServer Cs、Vserver Lb、vServer SSL、仮想サーバーユーザー、インターフェイス：レート NIC 合計受信バイト、RATE NIC tot 受信パケット、RATE NIC tot Tx バイト、RATE NIC tot Tx パケット、NIC tot Rx バイト、NIC ToT Rx パケット、NIC ToT Tx バイト、NIC ToT Tx パケット
- vServer CS：バインドエンティティ名、エンティティ名、月サービスバインド、NetScaler ID、スキーマタイプ、時間、CPU、Gslb サーバー、Gslb 仮想サーバー、メモリプール、NetScaler、サーバーサービスグループ、サーバー Svc Cfg、vServer Authn、vServer Cr、vServer CS、vServer Lb、vServer SSL、vServer ユーザー、vServer CS：RATE Si Totot 要求バイト、RATESi Tot リクエスト, RATE Si Tot レスポンスバイト, RATE Si Tot レスポンス, RATE Si Tott clt ttlb トランザクション, RATE Si Tott Pkt rcvd, RATE Si Tott Pkt Si Pkt 送信, RATE Si Tott ttlb イライラするトランザクション, RATE Si Tott ttlb 許容トランザクション, RATE Vsvr Tott Hits, Si Cur State, Si トット要求バイト数、SiTot リクエスト、Si Tot レスポンスバイト、Si Tot レスポンス、Si TotClt Ttlb トランザクション、Si TotPkt Rvd、Si TotPkt Sent、Si TottPit イライラするトランザクション、Si TottTlb 許容トランザクション、VSVR TotTotReq、VSVR TottReq Resp 無効ドロップされました

セキュリティで保護されたブラウザログ

- アプリケーションポスト:
  - 公開アプリケーションの前のログ: 認証、ブラウザ、ID の変更、作成済み、顧客名、宛先 URL、E-Tag、ゲートウェイサービス製品 ID、セッション ID、レガシーアイコン、アプリケーション名、ポリシー、公開アプリケーション ID、リージョン、リソースゾーン、リソースゾーン ID、サブスクリプション、セッションアイドルタイムアウト、セッションアイドルタイムアウト警告、ウォーターマーク、外部ホワイトリスト、ホワイトリスト内部、ホワイトリトリダイレクト

- 公開アプリケーションの後のログ: 認証、ブラウザ、ID の変更、作成済み、顧客名、宛先、E-Tag、ゲートウェイサービス製品 ID、セッション ID、レガシーアイコン、アプリケーション名、ポリシー、公開アプリケーション ID、リージョン、リソースゾーン、リソースゾーン ID、サブスクリプション、セッションアイドルタイムアウト、セッションアイドルタイムアウト警告、ウォーターマーク、ホワイトリスト外部 URL、ホワイトリスト内部 URL、ホワイトリトリダイレクト URL

- アプリケーションの削除:
  - 公開アプリケーションの前のログ: 認証、ブラウザ、ID の変更、作成済み、顧客名、宛先 URL、E-Tag、ゲートウェイサービス製品 ID、セッション ID、レガシーアイコン、アプリケーション名、ポリシー、公開アプリケーション ID、リージョン、リソースゾーン、リソースゾーン ID、サブスクリプション、セッションアイドルタイムアウト、セッションアイドルタイムアウト警告、ウォーターマーク、外部ホワイトリスト、ホワイトリスト内部、ホワイトリトリダイレクト
  - 公開アプリケーションの後のログ: 認証、ブラウザ、ID の変更、作成済み、顧客名、宛先、E-Tag、ゲートウェイサービス製品 ID、セッション ID、レガシーアイコン、アプリケーション名、ポリシー、公開アプリケーション ID、リージョン、リソースゾーン、リソースゾーン ID、サブスクリプション、セッションアイドルタイムアウト、セッションアイドルタイムアウト警告、ウォーターマーク、ホワイトリスト外部 URL、ホワイトリスト内部 URL、ホワイトリトリダイレクト URL

- アプリケーションの更新:
  - 公開アプリケーションの前のログ: 認証、ブラウザ、ID の変更、作成済み、顧客名、宛先 URL、E-Tag、ゲートウェイサービス製品 ID、セッション ID、レガシーアイコン、アプリケーション名、ポリシー、公開アプリケーション ID、リージョン、リソースゾーン、リソースゾーン ID、サブスクリプション、セッションアイドルタイムアウト、セッションアイドルタイムアウト警告、ウォーターマーク、外部ホワイトリスト、ホワイトリスト内部、ホワイトリトリダイレクト
  - 公開アプリケーションの後のログ: 認証、ブラウザ、ID の変更、作成済み、顧客名、宛先、E-Tag、ゲートウェイサービス製品 ID、セッション ID、レガシーアイコン、アプリケーション名、ポリシー、公開アプリケーション ID、リージョン、リソースゾーン、リソースゾーン ID、サブスクリプション、セッションアイドルタイムアウト、セッションアイドルタイムアウト警告、ウォーターマーク、ホワイトリスト外部 URL、ホワイトリスト内部 URL、ホワイトリトリダイレクト URL

- エンタイトルメントの作成:
  - エンタイトルメント作成前のログ: 承認済み、顧客 ID、データ保持日数、終了日、猶予期間日数、セッション ID、製品 SKU、数量、シリアル番号、開始日、状態、タイプ
  - エンタイトルメント作成後のログ: 承認済み、顧客 ID、データ保持日数、終了日、猶予期間日数、セッション ID、製品 SKU、数量、シリアル番号、開始日、状態、タイプ

- エンタイトルメントの更新:
  - エンタイトルメント更新前のログ: 承認済み、顧客 ID、データ保持日数、終了日、猶予期間日数、セッション ID、製品 SKU、数量、シリアル番号、開始日、状態、タイプ

  - エンタイトルメント更新後のログ: 承認済み、顧客 ID、データ保持日数、終了日、猶予期間日数、セッション ID、製品 SKU、数量、シリアル番号、開始日、状態、タイプ

- セッションアクセスホスト：ホスト、クライアント IP、日時、ホスト、セッション、ユーザー名を受け入れる
- セッション接続:
  - セッション接続前のログ: アプリケーション ID、アプリケーション名、ブラウザ、作成済み、顧客 ID、期間、セッション ID、IP アドレス、最終更新日、起動ソース、ユーザー名
  - セッション接続後のログ：アプリケーション ID、アプリケーション名、ブラウザ、作成済み、顧客 ID、期間、セッション ID、IP アドレス、最終更新日、起動ソース、ユーザー名
- セッションの起動:
  - セッション起動前のログ: アプリケーション ID、アプリケーション名、ブラウザ、作成済み、顧客 ID、期間、セッション ID、IP アドレス、最終更新日、起動ソース、ユーザー名
  - セッション起動後のログ：アプリケーション ID、アプリケーション名、ブラウザ、作成済み、顧客 ID、期間、セッション ID、IP アドレス、最終更新日、起動ソース、ユーザー名
- セッションティック:
  - セッションティック前のログ：アプリケーション ID、アプリケーション名、ブラウザ、作成済み、顧客 ID、期間、セッション ID、IP アドレス、最終更新日、起動ソース、ユーザー名
  - セッションティック後のログ：アプリケーション ID、アプリケーション名、ブラウザ、作成済み、顧客 ID、期間、セッション ID、IP アドレス、最終更新日、起動ソース、ユーザー名

Microsoft Graph セキュリティログ

- テナント ID
- ユーザー ID
- インジケータ ID
- インジケータ UUID
- イベント時間
- 時間を作成
- アラートのカテゴリ
- ログオンの場所
- ログオン IP
- ログオンの種類

- ユーザーアカウントタイプ
- ベンダー情報
- ベンダープロバイダ情報
- 脆弱性の状態
- 脆弱性の重大度

Microsoft Active Directory ログ

- テナント ID
- 時間を集める
- 種類
- ディレクトリコンテキスト
- グループ
- ユーザー情報
- ユーザーの種類
- アカウント名
- 不正なパスワードカウント
- 市区町村
- コモンネーム
- 会社
- 国
- パスワードの有効期限までの日数
- 部署
- 説明
- 表示名
- 識別名
- メール
- ファックス番号
- 名
- グループカテゴリ

- グループスコープ
- 自宅電話
- イニシャル
- IP フォン
- アカウントは有効になっていますか
- アカウントはロックされていか
- セキュリティグループか
- 姓
- マネージャー
- のメンバー
- 携帯電話
- ポケベル
- パスワードは期限切れにならない
- 物理的な配達所名
- 私書箱
- 郵便番号
- プライマリグループ ID
- 状態
- 番地
- 役職
- ユーザーアカウント制御
- ユーザーグループリスト
- ユーザー プリンシパル名
- 勤務先の電話番号

パフォーマンス向け **Citrix Analytics** ログ

- actionid
- actionreason
- actiontype

- adminfolder
- agentversion
- allocationtype
- applicationid
- applicationname
- applicationpath
- applicationtype
- applicationversion
- associateduserfullnames
- associatedusername
- associatedusernames
- associateduserupns
- authenticationduration
- autoreconnectcount
- autoreconnecttype
- AvgendPoint スループット受信バイト数
- AvgendPoint スループットバイトが送信されました
- blobcontainer
- blobendpoint
- blobpath
- brokerapplicationchanged
- brokerapplicationcreated
- brokerapplicationdeleted
- brokeringdate
- brokeringduration
- brokerloadindex
- brokerregistrationstarted
- browsername
- catalogchangeevent

- catalogcreatedevent
- catalogdeletedevent
- catalogid
- catalogname
- catalogsync
- clientaddress
- clientname
- clientplatform
- clientsessionvalidatedate
- clientversion
- collecteddate
- connectedviahostname
- connectedviaipaddress
- connectionid
- connectioninfo
- connectionstate
- connectiontype
- controllerdnsname
- cpu
- cpuindex
- createddate
- currentloadindexid
- currentpowerstate
- currentregistrationstate
- currentsessioncount
- datetime
- deliverygroupadded
- deliverygroupchanged
- deliverygroupdeleted

- deliverygroupid
- deliverygroupmaintenancemodechanged
- deliverygroupname
- deliverygroupsync
- deliverytype
- deregistrationreason
- desktopgroupdeletedevent
- desktopgroupid
- desktopgroupname
- desktopkind
- disconnectcode
- disconnectreason
- disk
- diskindex
- dnsname
- domainname
- effectiveloadindex
- enddate
- errormessage
- establishmentdate
- eventreporteddate
- eventtime
- exitcode
- failurecategory
- failurecode
- failuredata
- failuredate
- failurereason
- failuretype

- faultstate
- functionallevel
- gpoenddate
- gpostartdate
- hdxenddate
- hdxstartdate
- host
- hostedmachineid
- hostedmachinename
- hostingservername
- hypervisorconnectionchangedevent
- hypervisorconnectioncreatedevent
- hypervisorid
- hypervisorname
- hypervisorsync
- icartt
- icarttms
- id
- idletime
- inputbandwidthavailable
- inputbandwidthused
- instancecount
- interactiveenddate
- interactivestartdate
- ipaddress
- isassigned
- isinmaintenancemode
- ismachinephysical
- ispendingupdate

- ispreparing
- isremotepc
- issecureica
- lastderegisteredcode
- launchedviahostname
- launchedviaipaddress
- lifecyclestate
- linkSpeed
- logonduration
- logonenddate
- logonscriptsenddate
- logonscriptsstartdate
- logonstartdate
- long
- machineaddedtodesktopgroupevent
- machineassignedchanged
- machinecatalogchangedevent
- machinecreatedevent
- machinedeletedevent
- machinederegistrationevent
- machinednsname
- machinefaultstatechangeevent
- machinehardregistrationevent
- machineid
- machinemaintenancemodechangeevent
- machinename
- machinepvdstatechanged
- machineregistrationendedevent
- machineremovedfromdesktopgroupevent

- machinerole
- machinesid
- machineupdatedevent
- machinewindowsconnectionsettingchanged
- memory
- memoryindex
- modifieddate
- NGSConnector.ICAConnection.Start
- ngsConnector.ngs シンセティックメトリック
- ngsConnector.ngspassive メトリック
- ngsConnector.ngs システムメトリック
- network
- networkindex
- networklatency
- networkinfoperiodic
- ネットワークインターフェースタイプ
- ostype
- outputbandwidthavailable
- 使用された出力帯域幅
- path
- percentcpu
- persistentuserchanges
- powerstate
- processname
- profileloadenddate
- profileloadstartdate
- protocol
- provisioningschemeid
- provisioningtype

- publishedname
- registrationstate
- serversessionvalidatedate
- sessioncount
- sessionend
- sessionfailure
- sessionid
- sessionidlesince
- sessionindex
- sessionkey
- sessionstart
- sessionstate
- sessionsupport
- sessiontermination
- sessiontype
- sid
- 信号強度
- siteid
- sitename
- startdate
- totalmemory
- triggerinterval
- triggerlevel
- triggerperiod
- triggervalue
- usedmemory
- userid
- userinputdelay
- username

- usersid
- vdalogonDuration
- vdaprocessdata
- vdaresourceData
- version
- vmstartenddate
- vmstartstartdate
- windowsconnectionsetting
- xd.sessionStart

セキュリティの技術概要

April 12, 2024

Citrix Cloud でホストされている Analytics サービスは、Citrix ポートフォリオ製品とサードパーティ製品全体のデータを収集します。これらの製品はデータソースと呼ばれます。Citrix Analytics は、クラウドとオンプレミスの両方のデータソースをサポートします。このドキュメントの情報は、Citrix Analytics とそのデータソースに適用されます。

データフロー

Citrix Analytics は、顧客にサブスクライブされている Citrix Cloud データソースを自動的に検出します。ただし、オンプレミスのデータソースを Citrix Analytics と統合するには、追加の構成が必要です。たとえば、Citrix Analytics がサイトを検出する前に、Citrix Workspace に Citrix Virtual Apps and Desktops のサイトを追加する必要があります。同様に、オンプレミスの NetScaler Gateway では、NetScaler ADM エージェントを構成する必要があります。データソースで Citrix Analytics を有効にする方法について詳しくは、「Citrix データソースで分析を有効にする」を参照してください。

Microsoft Graph セキュリティや Microsoft Active Directory など、いくつかのサードパーティ製品を Citrix Analytics クスと統合できます。詳しくは、次のトピックを参照してください:

- Microsoft Graph セキュリティで分析を有効にする
- Microsoft の Active Directory と分析

Citrix Analytics は、リスクインテリジェンス情報を顧客所有の Splunk 環境に送信することもできます。この統合には、**Splunk** 環境に **Citrix Analytics Spunk** アドオンを展開して構成する必要があります。詳細については、「Splunk 統合」を参照してください。

お客様の同意なしに、Citrix Analytics はデータソースから受信したイベントを処理しません。データソースからのイベントを処理するには、Analytics 管理者がデータ処理を有効にする必要があります。Analytics によるデータ収集、保存、保持について詳しくは、「データガバナンス」を参照してください。

ネットワークの要件

- **Citrix Cloud** サービスの要件: Citrix Cloud サービスを使用するには、HTTPS ポート 443 を介して必要な Citrix アドレスに接続できる必要があります。詳細については、「インターネット接続の要件」を参照してください。
- **Citrix Analytics** の要件: Citrix Analytics を使用する前に、システム要件を確認してください 。Citrix Cloud の要件に加えて、Citrix Analytics サービスを使用するには、HTTPS ポート 443 を介して次のエンドポイントアドレスにアクセスできる必要があります。

エンドポイント	米国リージョン	欧州連合地域	アジア太平洋南部リージョン
管理者 UI	https://analytics.cloud.com/	https://analytics-eu.cloud.com/	https://analytics-aps.cloud.com/
管理用ユーザーインターフェイス (CDN)	https://cas-api-cdn-ep.azureedge.net/	https://cas-api-cdn-ep-eu.azureedge.net/	https://cas-api-cdn-ep-aps.azureedge.net/
API サービス	https://api.analytics.cloud.com/	https://api.analytics-eu.cloud.com/	https://api.analytics-aps.cloud.com/
API サービス (パフォーマンス分析)	https://api-a.was.cloud.com/	https://api-eu-a.was.cloud.com/	https://api-aps-a.was.cloud.com/
	https://api-b.was.cloud.com/	https://api-eu-b.was.cloud.com/	https://api-aps-b.was.cloud.com/
パブリック IP を取得	https://locus.analytics.cloud.com/	https://locus.analytics.cloud.com/	https://locus.analytics.cloud.com/

エンドポイント	米国リージョン	欧州連合地域	アジア太平洋南部リージョン
イベントハブ（NetScaler ADM エージェントには適用されません）	https://citrixanalyticseh-alias.servicebus.windows.net/ https://citrixanalyticseh2-alias.servicebus.windows.net/	https://citrixanalyticseheu-alias.servicebus.windows.net/	https://citrixanalyticsehaps-alias.servicebus.windows.net/
イベントハブ（NetScaler ADM エージェントの場合）	https://cas-eh-ns-alias.servicebus.windows.net/およびhttps://cas-eh-ns2-alias.servicebus.windows.net/	https://cas-eh-ns-eu-alias.servicebus.windows.net/	https://cas-eh-ns-aps-alias.servicebus.windows.net/
一括アップロード	https://casstoragebulk.blob.core.windows.net/	https://casstorebulkeu.blob.core.windows.net/	https://casstorebulkaps.blob.core.windows.net/

> 注
>
> Citrix Analytics は、前述のほとんどのエンドポイントで TLS 1.0 および TLS 1.1 のサポートを終了しました。

- **Citrix Cloud Connector** のインストール：Citrix Endpoint Management、Citrix Virtual Apps and Desktops、Microsoft Active Directory などの一部のデータソースでは、リソースの場所に Citrix Cloud Connector をインストールする必要があります。Citrix Cloud Connector は、Citrix Cloud とリソースの場所との間の通信チャネルです。Citrix Cloud Connector をインストールしたら、Web プロキシ設定を構成する必要があります。詳しくは、「Cloud Connector のプロキシとファイアウォールの構成」を参照してください。
- **SIEM** 統合のための **Citrix Analytics** エンドポイント：Citrix Analytics をセキュリティ情報およびイベント管理（SIEM）と統合するには、次のエンドポイントがネットワーク内の許可リストに含まれていることを確認します。

エンドポイント	米国リージョン	欧州連合地域	アジア太平洋南部リージョン
Kafka ブローカー	casnb-0.citrix.com:9094 casnb-1.citrix.com:9094 casnb-2.citrix.com:9094 casnb-3.citrix.com:9094	casnb-eu-0.citrix.com:9094 casnb-eu-1.citrix.com:9094 casnb-eu-2.citrix.com:9094	casnb-aps-0.citrix.com:9094 casnb-aps-1.citrix.com:9094 casnb-aps-2.citrix.com:9094

ID およびアクセス管理

- Citrix Analytics にアクセスするには、Citrix Cloud アカウントを使用する必要があります。デフォルトでは、Citrix ID プロバイダーを使用して、Citrix Cloud アカウントのすべてのユーザーの ID 情報を管理します。「ID とアクセス管理」で説明されているように、他の IDプロバイダを使用することもできます。
- Citrix Analytics は委任された管理者権限をサポートしています。エンタープライズの Analytics を管理するために、読み取り専用の管理者権限をユーザーに割り当てることができます。詳しくは、「管理者の役割の管理」を参照してください。

データ所在地

Citrix Cloud は Citrix Analytics コントロールプレーンを管理します。データソースから受信したデータは、複数の Microsoft Azure 環境に保存されます。これらの環境は、米国、欧州連合 (EU)、およびアジア太平洋南部リージョンにあります。ストレージの場所は、Citrix Cloud 管理者が組織を Citrix Cloud にオンボーディングするときに選択したホームリージョンによって異なります。詳しくは、次のトピックを参照してください:

- 地理的な考慮事項
- データガバナンス

データ保護

Citrix Analytics は、サブスクライブされた Citrix Cloud データソース、オンプレミスデータソース、およびサードパーティ製品からデータを受信します。受信したデータは、顧客が Citrix Cloud エンタイトルメントを持ち、Analytics 管理者がサブスクライブされた各データソースに対してデータ処理を明示的に有効にしている場合にのみ処理されます。

Citrix Analytics では、次のセキュリティ対策を使用してお客様のデータを保護します。

- アナリティクスユーザー用の Citrix Cloud 認証。詳細については、「ID とアクセス管理」を参照してください。
- データサービスとデータアクセスレイヤーによって実施されるテナントベースのデータアクセス制御。
- データレイクとデータウェアハウスのすべてのデータストアで、顧客またはテナントごとに強力なデータ分離を実現。
- プラットフォームおよびプラットフォーム内のパブリックエンドポイント (APT/入力/出力) に適用できる、さまざまなマイクロサービスとデータストア間の TLS 暗号化データ転送。
- TLS エンドポイントの高水準。TLS 1.0 と TLS 1.1 は無効になっています。
- 適切な Key Vault に保存されている暗号化キーとシークレットを使用して、暗号化されたデータストレージ。
- 顧客ログを保護しつつ、サービスの運用とサポートのための強力なユーザー管理アクセス制御。
- Azure Security Center とともに使用される脆弱性スキャン、侵入検知、マルウェア対策、ルートキットスキャン。

すべての Citrix Cloud サービスと同様に、データ収集はエンドユーザーサービス契約（EUSA）に厳密に適用されます。詳細については、次の契約書を参照してください。

- ユーザー規約
- Citrix プライバシーポリシー
- Citrix データ処理契約
- Citrix Services Security Exhibit
- Citrix Cloud Services：お客様のコンテンツとログの処理
- Citrix プライバシーとコンプライアンス情報

セキュリティ上の責任

Citrix の責任

Citrix は、Citrix Analytics をホストする Citrix が管理するクラウド環境に存在するすべてのインフラストラクチャとデータを保護する責任があります。Citrix は、セキュリティの脆弱性に対処するために、クラウド環境にソフトウェアアップデートとパッチを定期的に適用する責任があります。

顧客の責任

Citrix のお客様は、Citrix Analytics と統合されたデータソース、ポリシー適用ポイント、およびセキュリティ情報およびイベント管理（SIEM）システムを保護する責任があります。これには、次のものが含まれます。

- 顧客が所有、管理するオンプレミスのデータソース:
  - オンプレミスデータソース:Citrix Gateway、Citrix Virtual Apps and Desktops、Microsoft Active Directory
  - **SIEM**: SSplunk や、Kafka ブローカーを使用して Citrix Analytics からイベントを読み取るその他のサードパーティ製品。
- Citrix Analytics を含む Citrix Cloud サービスを管理するための、お客様が用意した管理者資格情報。
- Citrix Cloud サービスから電子メールまたは通知を受信する、顧客所有の管理者アカウント。
- Citrix ADM エージェントなどのエージェントを展開および統合するための、お客様から提供された管理者認証情報。これらのエージェントは、Citrix Analytics と通信するためにキーをローカルに保存するため、アクセスを制限する必要があります。
- **Splunk** の **Citrix Analytics** アドオンを構成するための **Citrix** アナリティクスが生成した認証情報。
- Windows、Mac、Android、iOS 上で実行され、Citrix Cloud または Citrix Workspace に接続し、データソースと統合されるエンドユーザーデバイス。

セキュリティ規定の詳細については、次のドキュメントを参照してください。

- セキュリティで保護された Citrix Cloud プラットフォームの展開ガイド
- Citrix Workspace のドキュメント
- Citrix DaaS（旧 Citrix Virtual Apps and Desktops サービス）の技術的セキュリティ概要
- Citrix Virtual Apps and Desktops のセキュリティに関する考慮事項
- StoreFront 展開ドキュメントを保護する
- Citrix Endpoint Management 技術セキュリティの概要
- Citrix Secure Private Access サービスのドキュメント
- NetScaler ADC のセキュアな導入ガイド
- NetScaler ADM のシステム要件

システム要件

September 21, 2023

Citrix Analytics の使用を開始する前に、ライセンス情報、ソフトウェア要件、およびブラウザー要件を確認する必要があります。

Citrix Analytics サブスクリプション

次の Analytics 製品を使用するには、有効なサブスクリプションが必要です。

- Citrix Analytics for Security
- Citrix Analytics for Performance

詳しくは、「Citrix Cloud サービス」を参照してください。

データソース要件

データソースは、Citrix Analytics にイベントを送信する製品です。使用している Citrix Analytics 製品によって、データソースは異なります。各オファリングでサポートされるデータソースを確認するには、次の記事を参照してください。

- Citrix Analytics for Security でサポートされているデータソース
- パフォーマンス向け Citrix Analytics でサポートされているデータソース

サポートされているブラウザー

Citrix Analytics にアクセスするには、ワークステーションでサポートされている次の Web ブラウザーが必要です。

- 最新バージョンの Google Chrome
- 最新バージョンの Mozilla Firefox
- 最新バージョンの Microsoft Edge
- 最新バージョンの Apple Safari

Citrix Analytics の管理者の役割を管理する

May 9, 2023

デフォルトでは、Citrix Cloud 管理者は、Citrix Cloud アカウントでサブスクライブされているすべてのサービスに対するフルアクセス権を持ちます。フルアクセス権があれば、管理者はサブスクライブされたサービスのすべての機能を使用できます。

フルアクセス権を持つ Citrix Cloud 管理者は、自分の Citrix Cloud アカウントに他の管理者を招待して、組織のサブスクライブ済みサービスを管理できます。その後、アクセス権限を定義して、サブスクライブされたサービスの特定の機能を管理できるようにすることができます。

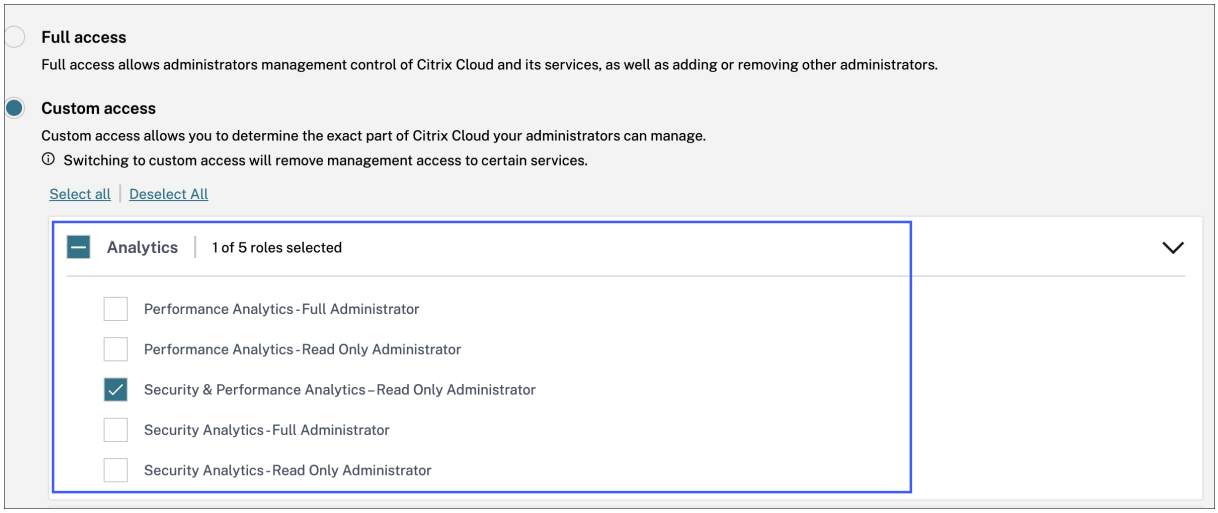
新しい管理者を追加するには次の 2 つの方法があります。

1. Citrix Identity および Azure AD /AActive Directory のユーザーとして個別に。詳しくは、「Citrix Cloud 管理者の管理」を参照してください。
2. Azure Active Directory リのグループを使用する。詳しくは、「管理者グループを管理する」を参照してください。

管理者は、Citrix Cloud、Active Directory、または Azure Active Directory アカウントを使用して Citrix Cloud にログインし、特定の機能にアクセスしたり、役割に応じてタスクを実行したりできます。

Citrix Analytics では、管理者に次のカスタムの役割を割り当てることができます。

役割	権限
Performance Analytics -すべての管理者	Performance Analytics の Citrix Cloud 管理者にフルアクセス権限を割り当てます。
Performance Analytics -読み取り専用管理者	Performance Analytics の Citrix Cloud 管理者に読み取り専用アクセス許可を割り当てます。
セキュリティとパフォーマンス分析-読み取り専用管理者	セキュリティ分析とパフォーマンス分析の両方の Citrix Cloud 管理者に読み取り専用アクセス許可を割り当てます。
セキュリティ分析-すべての管理者	セキュリティ分析の Citrix Cloud 管理者にフルアクセス権限を割り当てます。
セキュリティ分析-読み取り専用管理者	セキュリティ分析の Citrix Cloud 管理者に読み取り専用アクセス許可を割り当てます。



> メモ
>
> - 1 人の管理者に対して複数のロールを選択すると、より高いアクセス権を持つロールが有効になります。

> - ユーザーにユーザーとして直接、または Azure Active Directory グループを通じてアクセス権が付与された場合、そのユーザーに個別に付与されたアクセスが有効になります。
> - Azure Active Directory グループは、カスタム管理者としてのみ追加できます。フルアクセス管理者ロールはグループには使用できません。
> - 以前に使用可能だった読み取り専用管理者の役割を持つ管理者は、「セキュリティとパフォーマンス-読み取り専用管理者」に名前が変更されます。
> - セキュリティとパフォーマンス分析-読み取り専用管理者の役割とパフォーマンス分析-読み取り専用管理者の役割を持つ管理者は、Citrix Analytics から電子メール通知を受信しません。

オファリング固有のロールについて詳しくは、次の記事を参照してください。

- パフォーマンス分析の管理者ロールを管理する
- セキュリティ分析の管理者ロールを管理する

はじめに

April 12, 2024

このドキュメントでは、Citrix Analytics を初めて使用する方法について説明します。

ステップ **1**: **Citrix Cloud** にサインインする

Citrix Analytics を使用するには、Citrix Cloud アカウントが必要です。https://citrix.cloud.com にアクセスし、既存の Citrix Cloud アカウントでサインインします。

Citrix Cloud アカウントをお持ちでない場合は、最初に Citrix Cloud アカウントを作成するか、組織内の他のユーザーが作成した既存のアカウントに参加する必要があります。詳細なプロセスと手順については、「Citrix Cloud へのサインアップ」を参照してください。

ステップ **2:** アナリティクスにアクセスする

Analytics には、次のいずれかの方法でアクセスできます。

- **Citrix Analytics** サービスの試用版をリクエストしてください。Citrix Cloud にサインインした後、［利用可能なサービス］セクションの［分析］タイルで［管理］をクリックすると、分析の概要ページが表示されます。

  概要ページには、Analytics サービス (** セキュリティとパフォーマンス **) が表示されます。

  - セキュリティ分析とパフォーマンス分析の場合は、「試用版をリクエスト」をクリックしてサービスの試用版を使用してください。リクエストが承認され、トライアルが利用可能になると、メールが届きます。試用版は最長で 60 日間使用できます。サービストライアルの詳細については、「Citrix Cloud サービストライアル」を参照してください。

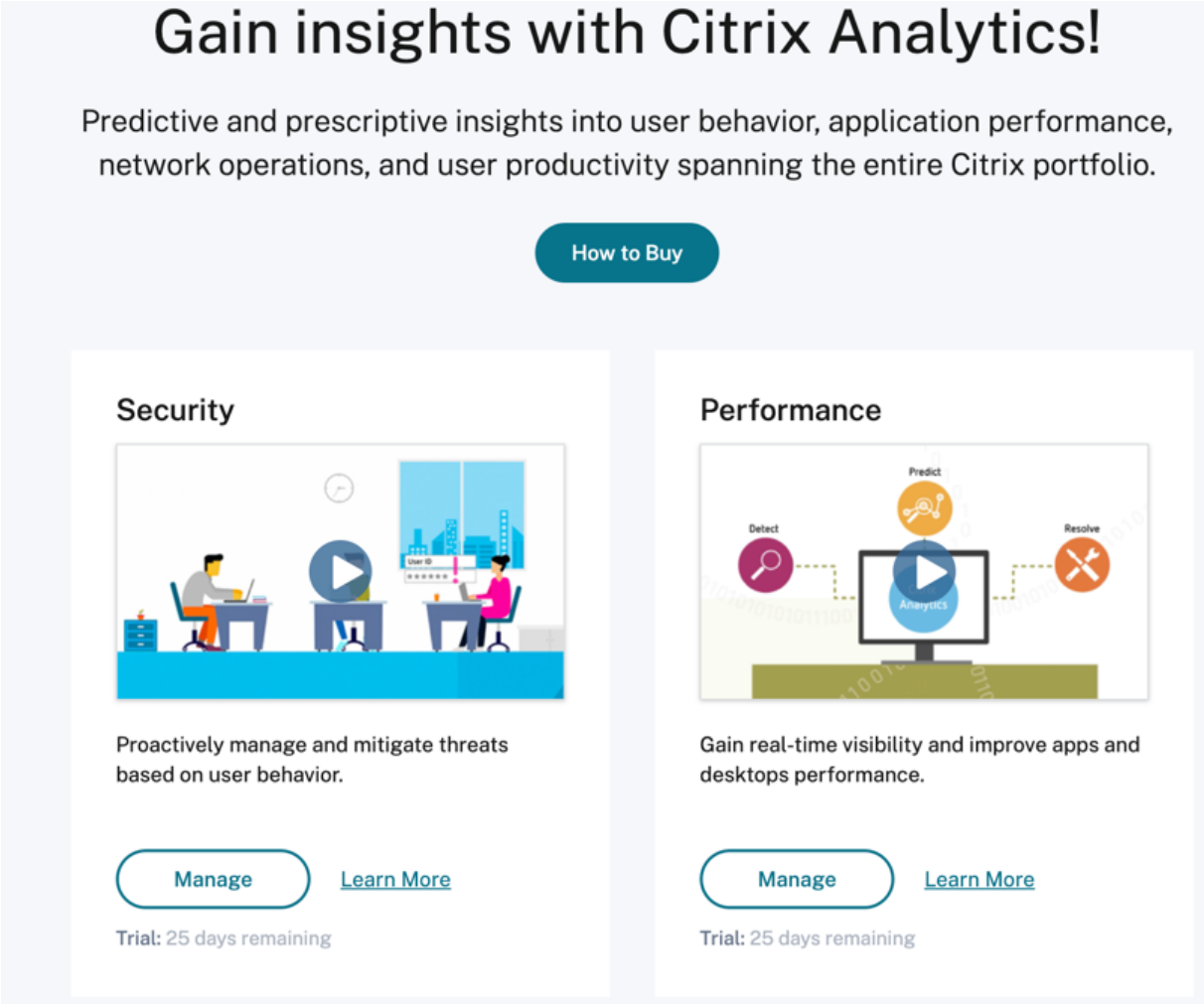
［Citrix Cloud］ページで、［分析］タイルが［マイサービス］セクションに移動します。

- **Citrix Analytics** スを購読します。以下の Citrix Analytics サブスクリプションを購入できます。
  - Citrix Analytics for Security
  - Citrix Analytics for Performance
  - セキュリティとパフォーマンスのための Citrix Analytics

  Citrix Analytics for Security および Citrix Analytics for Performance は、Citrix Workspace パッケージ（ワークスペーススタンダード、ワークスペースプレミアム、およびワークスペースプレミアムプラス）のアドオンサービスとして提供されます。詳しくは、「Citrix Cloud サービス」を参照してください。

ステップ **3: Analytics** の管理

Security Analytics と Performance Analytics では、必要なサブスクリプションを取得するか、トライアルへのアクセスを許可されると、アナリティクスの概要ページで、サービスの [トライアルのリクエスト] ボタンが [管理] に変わります。「管理」をクリックすると、各オファリングに対応するユーザーダッシュボードが表示されます。



アナリティクスは、Citrix Cloud アカウントに関連付けられている Citrix Cloud サービス（データソース）を自動的に検出します。検出されたデータソースを表示するには、[設定**] > [**データソース] をクリックし、必要なタブ ([セキュリティ] または [パフォーマンス]) をクリックします。

Analytics の各サービスの詳細については、以下を参照してください

- Citrix Analytics for Security
- Citrix Analytics for Performance

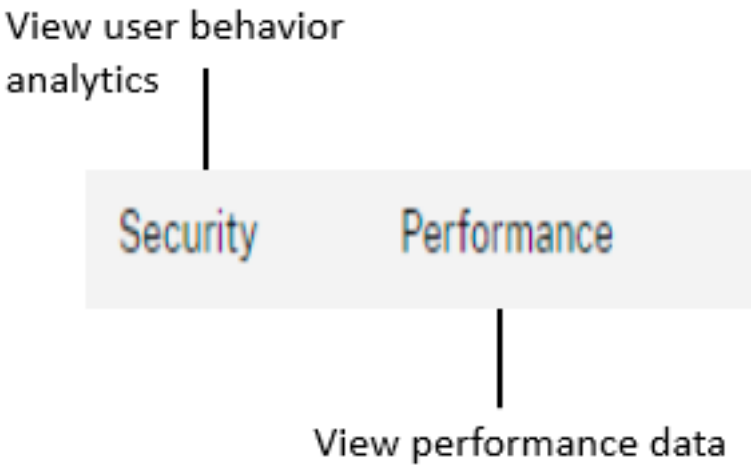
利用方法

May 10, 2022

Analytics ユーザーインターフェイスの主なコントロールについて理解しておきます。

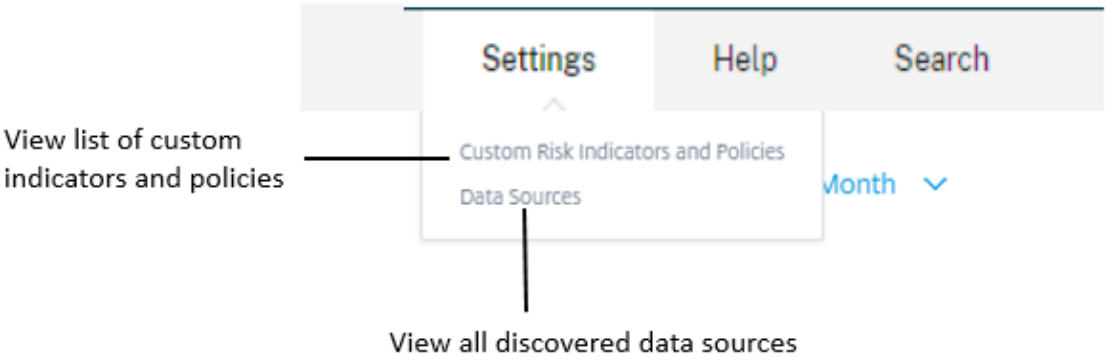
トップバー

トップバーからさまざまな Analytics オファリングに移動します。

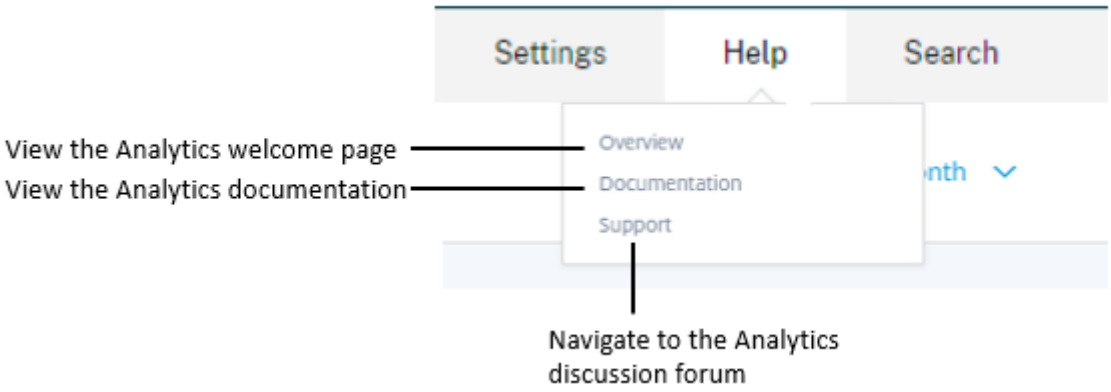


設定メニュー

[設定] メニューから、[インジケータとポリシー] ページまたは [データソース] ページに移動します。

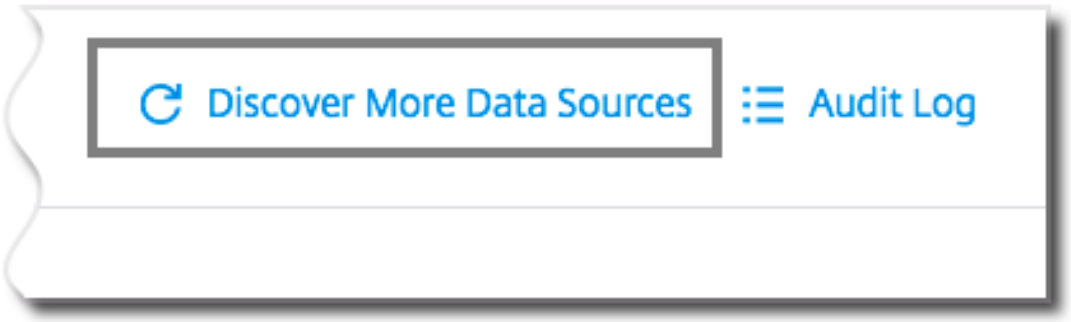


[ヘルプ] メニュー



より多くのデータソースを検出する

新しく追加したデータソース、または以前に削除したデータソースを検出します。



監査ログ

Analytics で生成されたすべてのイベントを一覧表示する [監査ログ] ページに移動します。

セルフサービス検索

December 7, 2023

セルフサービス検索とは何ですか

セルフサービス検索機能を使用すると、データソースから受信したユーザーイベントを検索してフィルタリングできます。基礎となるユーザーイベントとその属性を調べることができます。これらのイベントは、データの問題を特定し、トラブルシューティングするのに役立ちます。検索ページには、データソースのさまざまなファセット (ディメンション) と指標が表示されます。検索クエリを定義し、フィルタを適用して、定義した基準に一致するイベントを表示できます。デフォルトでは、セルフサービス検索ページには、過去 1 日のユーザーイベントが表示されます。

現在、セルフサービス検索機能は、次のデータソースで使用できます。

- Authentication
- Gateway
- Secure Browser
- Secure Private Access
- アプリケーションとデスクトップ
- パフォーマンスユーザー、マシン、セッション

また、定義したポリシーに一致するイベントに対してセルフサービス検索を実行することもできます。詳細については、ポリシーのセルフサービス検索を参照してください。

セルフサービス検索にアクセスする方法

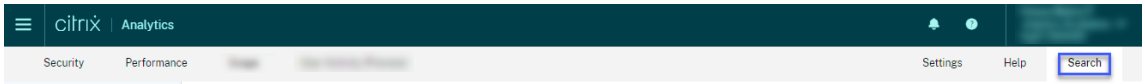
次のオプションを使用して、セルフサービス検索にアクセスできます。

- トップバー: トップバーの [検索] をクリックすると、選択したデータソースのすべてのユーザーイベントが表示されます。
- ユーザープロファイルページのリスクタイムライン:[イベント検索] をクリックして、各ユーザーのイベントを表示します。

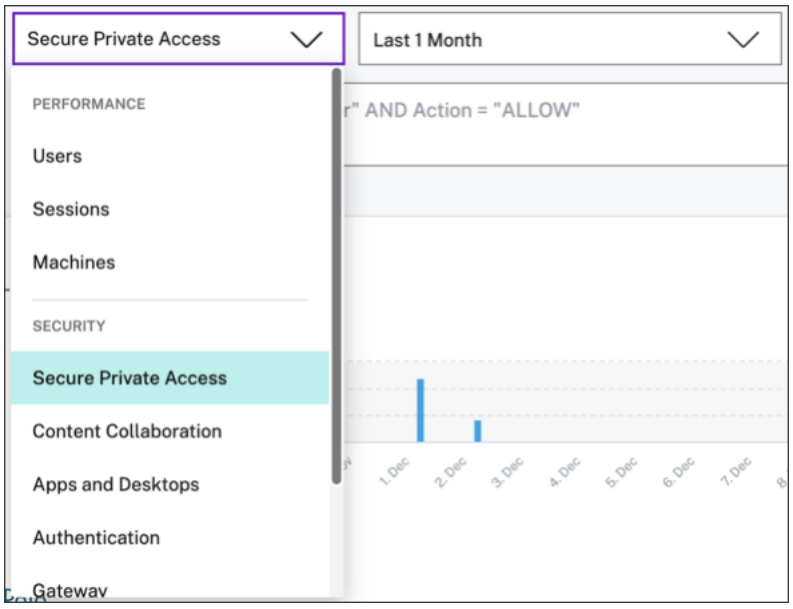
トップバーからのセルフサービス検索

ユーザーインターフェイスの任意の場所からセルフサービス検索ページに移動するには、このオプションを使用します。

1. [検索（Search）] をクリックして、セルフサービスページを表示します。



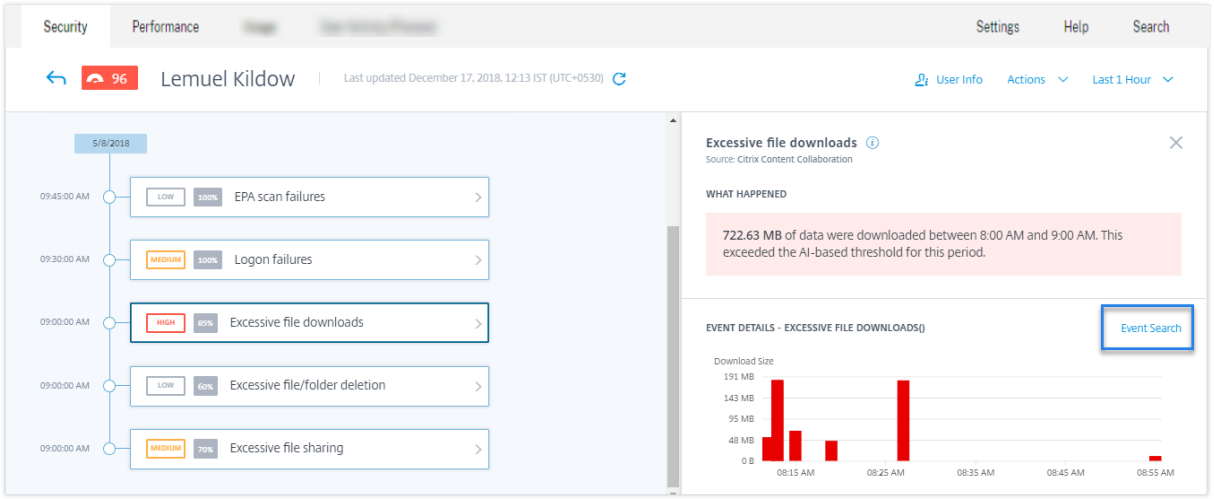
2. データソースと期間を選択して、対応するイベントを表示します。



ユーザーのリスクタイムラインからのセルフサービス検索

リスク指標に関連付けられたユーザーイベントを表示する場合は、このオプションを使用します。

ユーザーのタイムラインからリスク指標を選択すると、右側のペインにリスク指標情報セクションが表示されます。[イベント検索] をクリックして、セルフサービス検索ページで、ユーザーおよびデータソース (リスク指標がトリガーされる) に関連付けられたイベントを調べます。



ユーザーリスクタイムラインの詳細については、「リスクタイムライン」を参照してください。

セルフサービス検索の使用方法

セルフサービス検索ページの次の機能を使用します。

- イベントをフィルタリングするファセット 。
- 検索ボックスにクエリを入力し 、イベントをフィルタリングします。
- 期間を選択するための時間セレクタ 。
- タイムラインの詳細 。イベントグラフを表示します。
- イベントデータを使用して 、イベントを表示します。
- CSV 形式にエクスポートして 、検索イベントを CSV ファイルとしてダウンロードします。
- ビジュアルサマリーをエクスポートして 、検索クエリのビジュアルサマリーレポートをダウンロードします。
- イベントを複数の列で並べ替えるには 、複数列でソートします。

ファセットを使用してイベントをフィルタリングする

ファセットは、イベントを構成するデータポイントの要約です。ファセットはデータソースによって異なります。たとえば、Secure Private Access データソースのファセットは、評判、アクション、場所、およびカテゴリグループです。一方、アプリとデスクトップのファセットは、イベントタイプ、ドメイン、プラットフォームです。

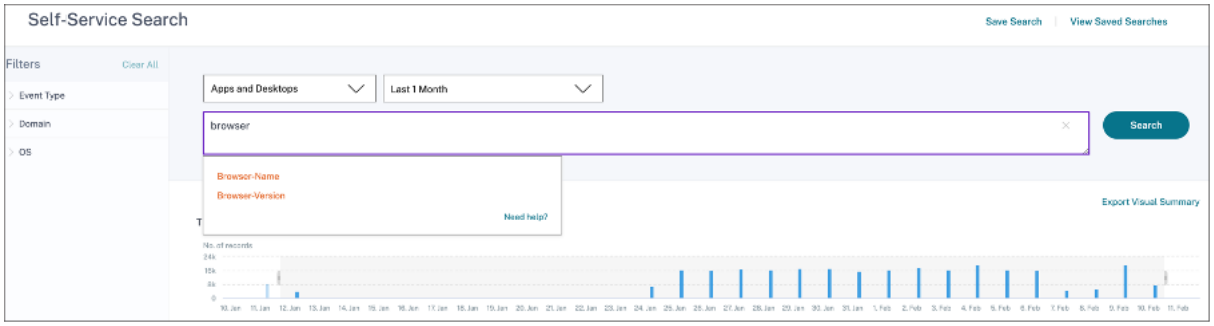
ファセットを選択して、検索結果をフィルタリングします。選択したファセットがチップとして表示されます。

各データソースに対応するファセットについて詳しくは、この記事で前述したデータソースのセルフサービス検索の記事を参照してください。

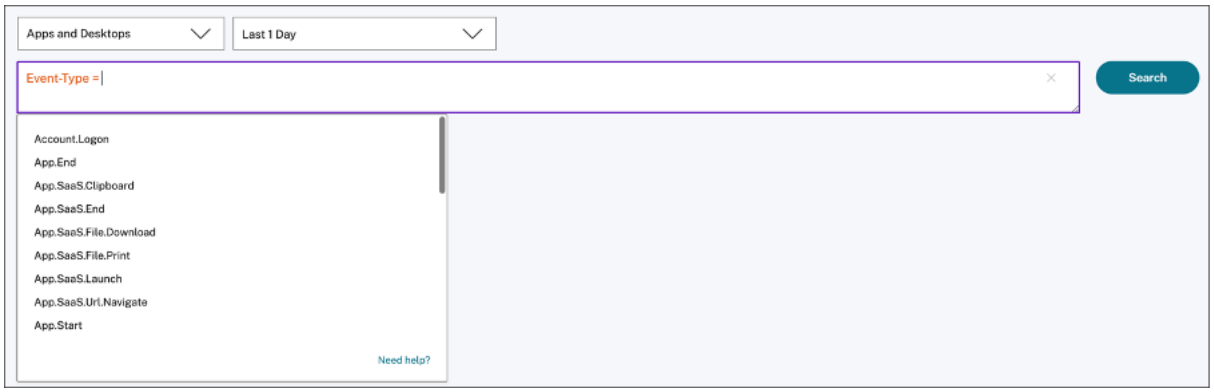
検索ボックスで検索クエリを使用してイベントをフィルタリングする

検索ボックスにカーソルを置くと、ユーザーイベントに基づいたディメンションのリストが検索ボックスに表示されます。これらのディメンションは、データソースによって異なります。ディメンションと有効な演算子を使用して 、検索条件を定義し、必要なイベントを検索します。

たとえば、アプリとデスクトップのセルフサービス検索では、Browserディメンションに対して次の値が取得されます。ディメンションを使用してクエリを入力し、期間を選択して、[検索] をクリックします。



特定のディメンション（Event-TypeやClipboard-Operationなど）を有効な演算子と一緒に選択すると、ディメンションの値が自動的に表示されます。推奨オプションから値を選択するか、要件に応じて新しい値を入力できます。



検索クエリでサポートされる演算子　検索クエリで次の演算子を使用して、検索結果を絞り込みます。

演算子	説明	例	出力
:	検索ディメンションに値を割り当てます。	User-Name : John	ユーザー John のイベントを表示します。
=	検索ディメンションに値を割り当てます。	User-Name = John	ユーザー John のイベントを表示します。
~	類似した値を持つイベントを検索します。	User-Name ~ test	類似のユーザー名を持つイベントを表示します。

演算子	説明	例	出力
" "	値をスペースで区切って囲みます。	User-Name = “John Smith”	ユーザー John Smith のイベントを表示します。
< >	リレーショナル値を検索します。	Data Volume > 100	データボリュームが 100 GB を超えるイベントを表示します。
AND	指定した条件が真であるイベントを検索します。	User-Name : John AND Data Volume > 100	データボリュームが 100 GB を超えるユーザー John のイベントを表示します。
! ~	指定した一致するパターンについてイベントをチェックします。この NOT LIKE 演算子は、イベント文字列のどこにも一致するパターンを含まないイベントを返します。	ユーザー名! ~ ジョン	John、John Smith、または一致する名前「John」を含むユーザー以外のユーザーのイベントを表示します。
! =	イベントで、指定した文字列が正確にチェックされます。この NOT EQUAL 演算子は、イベント文字列のどこにも正確な文字列を含まないイベントを返します。	国!= 米国	米国以外の国のイベントを表示します。
*	指定した文字列に一致するイベントを検索します。現在、*演算子は次の演算子、:、=および!=でのみサポートされています。検索結果では大文字と小文字が区別されます。	User-Name = John*	John で始まるすべてのユーザー名のイベントを表示します。
		User-Name = *John*	John を含むすべてのユーザー名のイベントを表示します。
		User-Name = *Smith	Smith で終わるすべてのユーザー名のイベントを表示します。

演算子	説明	例	出力
		ユーザー名:John*	John で始まるすべてのユーザー名のイベントを表示します。
		ユーザー名:*John*	John を含むすべてのユーザー名のイベントを表示します。
		ユーザー名:*Smith	Smith で終わるすべてのユーザー名のイベントを表示します。
		ユーザー名! = ジョン *	John で始まるすべてのユーザー名のイベントを表示します。
		ユーザー名! = * スミス	Smith で終わらないすべてのユーザー名のイベントを表示します。
IN	検索ディメンションに複数の値を割り当てて、1 つ以上の値に関連するイベントを取得します。注：現在、この演算子は、アプリとデスクトップ -Device ID、Domain、Event-Typeおよび User-Name のディメンションで使用できます。この演算子は、文字列値にのみ適用されます。	ユーザーネーム IN (ジョン、ケビン)	ジョンまたはケビンに関連するすべてのイベントを見つける。

演算子	説明	例	出力
NOT IN	検索ディメンションに複数の値を割り当てて、指定した値を含まないイベントを検索します。注：現在、この演算子は、アプリとデスクトップ -Device ID、Domain、Event-TypeおよびUser-Nameのディメンションで使用できます。この演算子は、文字列値にのみ適用されます。	User-Name NOT IN (John, Kevin)	John と Kevin 以外のすべてのユーザーのイベントを検索します。
IS EMPTY	ディメンションの NULL 値または空の値をチェックします。この演算子は、App-Name、Browser、Countryなどの文字列タイプのディメンションでのみ機能します。Upload-File-Size、Download-File-Size、Client-IP などの非文字列 (数値) タイプのディメンションには使用できません。	Country IS EMPTY	国名が利用できない、または空である (指定されていない) イベントを検索します。

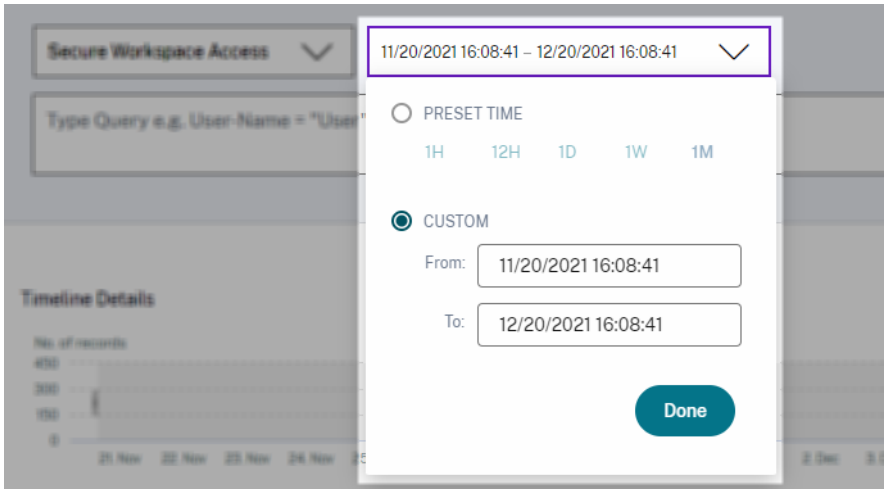
演算子	説明	例	出力
IS NOT EMPTY	ディメンションの NULL 値でない値または特定の値がないかどうかをチェックします。この演算子は、App-Name、Browser、Countryなどの文字列タイプのディメンションでのみ機能します。Upload-File-Size、Download-File-Size、Client-IP などの非文字列 (数値) タイプのディメンションには使用できません。	Country IS NOT EMPTY	国名が利用可能または指定されているイベントを検索します。
OR	どちらかまたは両方の条件に該当する値を検索します。	(ユーザー名 = John* またはユーザー名 = *Smith) およびイベントタイプ = 「Session.Logon」	John で始まる、または Smith Session.Logon で終わるすべてのユーザー名のイベントを表示します。

> 注
>
> **NOT EQUAL** 演算子では、クエリーのディメンションの値を入力するときに、データ・ソースのセルフ・サービス検索ページで使用可能な正確な値を使用します。寸法値では、大文字と小文字が区別されます。

データソースの検索クエリを指定する方法の詳細については、この記事で前述したデータソースのセルフサービス検索の記事を参照してください。

イベントを表示する時間を選択

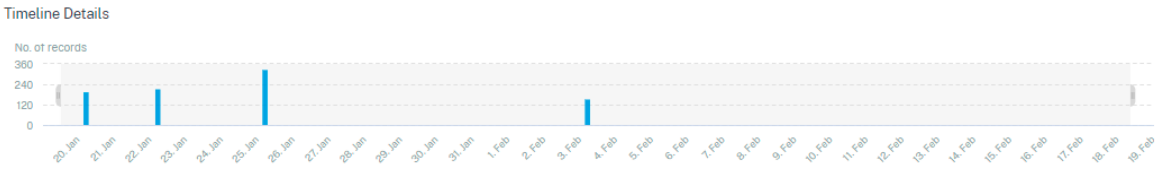
プリセット時間を選択するか、カスタムの時間範囲を入力して [検索（Search）] をクリックしてイベントを表示します。



タイムラインの詳細を表示する

タイムラインには、選択した期間のユーザーイベントがグラフィカルに表示されます。セレクタバーを移動して時間範囲を選択し、選択した時間範囲に対応するイベントを表示します。

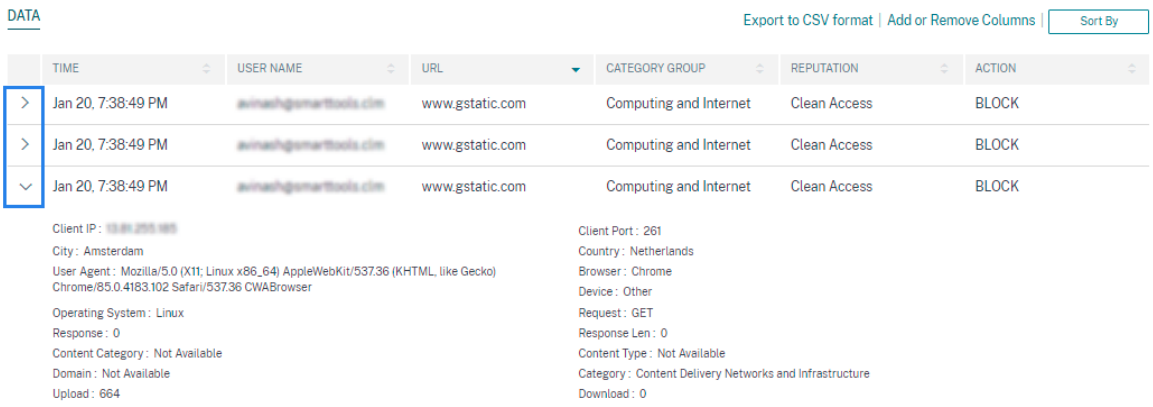
この図は、アクセスデータのタイムラインの詳細を示しています。



イベントを見る

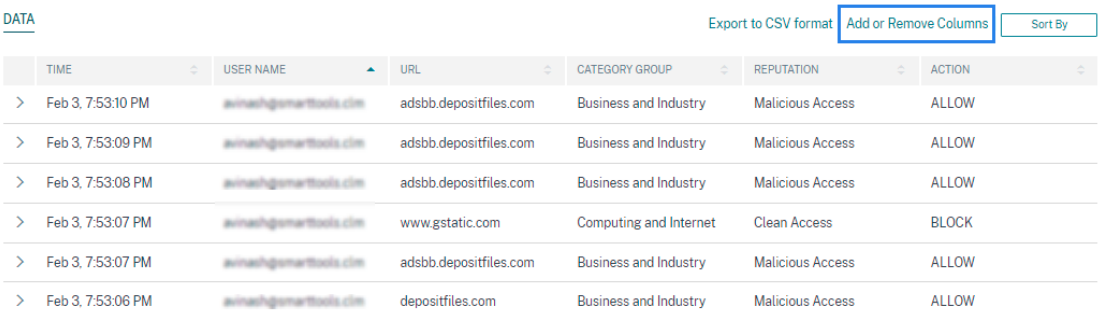
ユーザーイベントに関する詳細情報を表示できます。**DATA** テーブルで、各列の矢印をクリックして、ユーザーイベントの詳細を表示します。

この図は、ユーザーのアクセスデータに関する詳細を示しています。

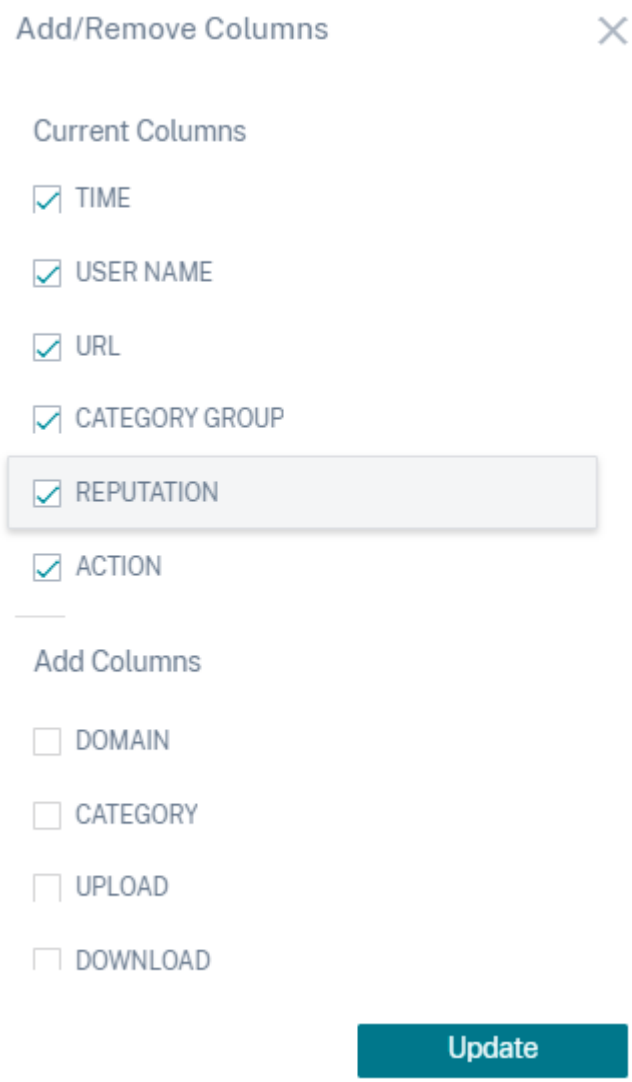


列を追加または削除する　イベントテーブルの列を追加または削除して、対応するデータポイントを表示または非表示にすることができます。以下を実行します：

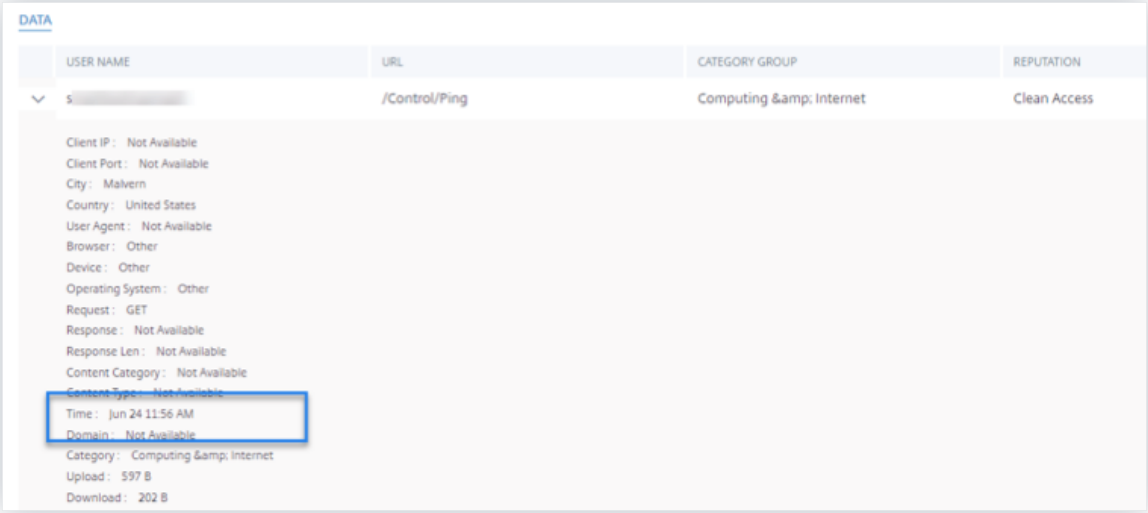
1. [列の追加または削除] をクリックします。



2. リストからデータ要素を選択または選択解除し、「更新」をクリックします。

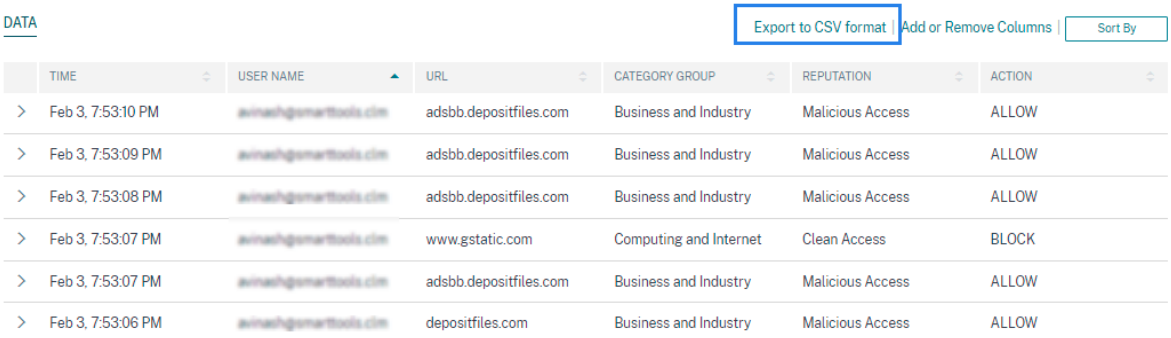


リストからデータポイントを選択解除すると、対応する列がイベントテーブルから削除されます。ただし、ユーザーのイベント行を展開すると、そのデータポイントを表示できます。たとえば、リストから **TIME** データポイントを選択解除すると、**TIME** 列がイベントテーブルから削除されます。時間レコードを表示するには、ユーザのイベント行を展開します。



イベントを **CSV** ファイルにエクスポートする

検索結果を CSV ファイルにエクスポートし、参照用に保存します。[**CSV** 形式にエクスポート（**Export to CSV format**）] をクリックしてイベントをエクスポートし、生成された CSV ファイルをダウンロードします。**CSV** 形式へのエクスポート機能を使用して、**10** 万行をエクスポートできます。



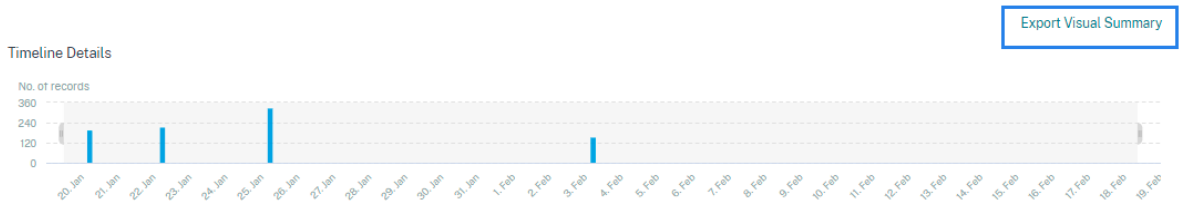
ビジュアルサマリーを書き出す

検索クエリのビジュアルサマリーレポートをダウンロードし、他のユーザー、管理者、またはエグゼクティブチームとコピーを共有できます。

ビジュアルサマリーをエクスポートをクリックして、ビジュアルサマリーレポートを PDF としてダウンロードします。レポートには、次の情報が含まれています。

- 選択した期間のイベントに対して指定した検索クエリ。
- 選択した期間のイベントに適用したファセット（フィルタ）。
- 選択した期間の検索イベントのタイムラインチャート、棒グラフ、グラフなどの視覚的なサマリー。

データソースの場合、データが棒グラフ、タイムラインの詳細などのビジュアル形式で表示される場合にのみ、ビジュアルサマリーレポートをダウンロードできます。それ以外の場合、このオプションは使用できません。たとえば、アプリとデスクトップ、セッションなどのデータソースのビジュアルサマリーレポートをダウンロードして、データをタイムラインの詳細と棒グラフとして表示できます。Users や Machines などのデータソースの場合、データは表形式でのみ表示されます。したがって、ビジュアルサマリーレポートをダウンロードすることはできません。

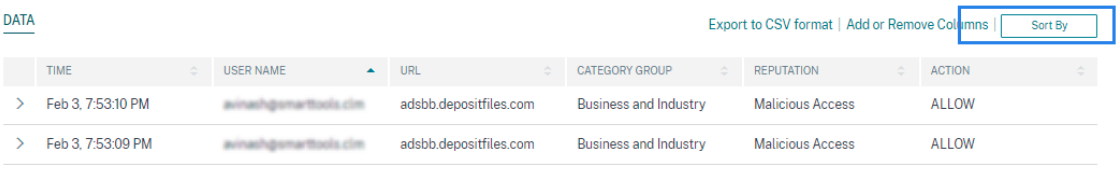


複数列の並べ替え

並べ替えは、データの整理に役立ち、可視性を高めます。セルフサービス検索ページで、ユーザーイベントを 1 つ以上の列で並べ替えることができます。列は、ユーザー名、日付と時刻、URL などのさまざまなデータ要素の値を表します。これらのデータ要素は、選択したデータソースによって異なります。

複数列の並べ替えを実行するには、次の操作を行います。

1. [並べ替え] をクリックします。



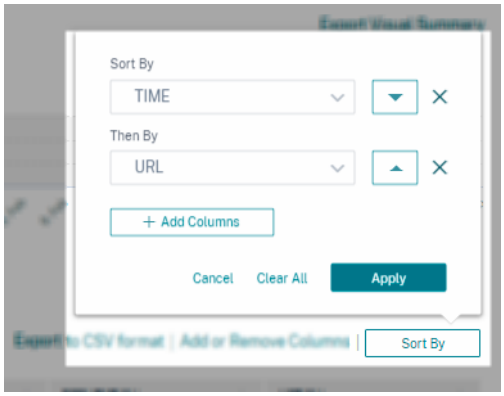
2. [並べ替え基準] リストから列を選択します。
3. 列内のイベントを並べ替えるには、昇順 (上矢印) または降順 (下矢印) の並べ替え順序を選択します。
4. [**+** 列の追加] をクリックします。
5. [次の項目] リストから別の列を選択します。
6. 列内のイベントをソートするには、ソート順として、昇順（上矢印）または降順（下方向エラー）を選択します。

   > 注
   >
   > 最大 6 つの列を追加して、並べ替えを実行できます。

7. [適用] をクリックします。

8. 上記の設定を適用しない場合は、[キャンセル] をクリックします。選択した列の値を削除するには、「すべてクリア」**(Clear All**) をクリックします。

次の例は、Secure Private Access イベントに対する複数列のソートを示しています。イベントは、時刻 (新しい順)、URL (アルファベット順) の順にソートされます。



または、**Shift** キーを使用して複数列の並べ替えを実行することもできます。**Shift** キーを押しながら列見出しをクリックして、ユーザーイベントを並べ替えます。

セルフサービス検索を保存する方法

管理者は、セルフサービスクエリを保存できます。この機能により、分析やトラブルシューティングで頻繁に使用するクエリを書き換える時間と労力を節約できます。次のオプションは、クエリーとともに保存されます。

- 適用された検索フィルタ
- 選択したデータソースと期間

セルフサービスクエリを保存するには、次の手順を実行します。

1. 必要なデータソースと期間を選択します。
2. 検索バーにクエリを入力します。
3. 必要なフィルターを適用します。
4. [検索を保存] をクリックします。
5. カスタムクエリを保存する名前を指定します。

   > (注
   >
   >) クエリ名が一意であることを確認します。それ以外の場合、クエリは保存されません。

6. 検索クエリレポートのコピーを自分や他のユーザーに定期的に送信する場合は、**[**電子メールレポートのスケジュール] ボタンを有効にします。詳細については、「検索クエリのメールをスケジュールする」を参照してください。

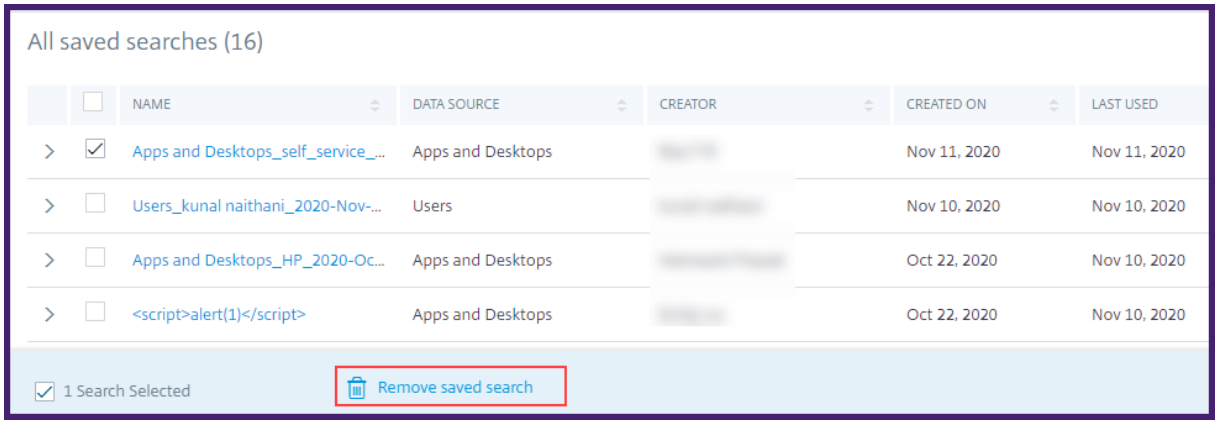
7. [保存] をクリックします。

保存した検索を表示するには、次の手順に従います。

1. [保存された検索の表示] をクリックします。
2. 検索クエリの名前をクリックします。

保存した検索を削除するには:

1. [保存された検索の表示] をクリックします。
2. 保存した検索クエリを選択します。
3. [保存された検索条件を削除] をクリックします。



保存済み検索を変更するには、次の操作を行います。

1. [保存された検索の表示] をクリックします。
2. 保存した検索クエリの名前をクリックします。
3. 要件に基づいて、検索クエリまたはファセットの選択を変更します。
4. [検索の更新] **>** [保存] をクリックして、変更した検索を同じ検索クエリ名で更新して保存します。
5. 変更した検索を新しい名前で保存する場合は、下矢印をクリックし、[新しい検索として保存] **>** [名前を付けて保存] をクリックします。

検索を新しい名前に置き換えると、検索は新しいエントリとして保存されます。置換時に既存の検索名を保持すると、変更された検索データが既存の検索データを上書きします。

> 注
>
> - クエリの所有者のみが、保存された検索を変更または削除できます。
> - 保存した検索リンクアドレスをコピーして、他のユーザーと共有することができます。

検索クエリのメールをスケジュールする

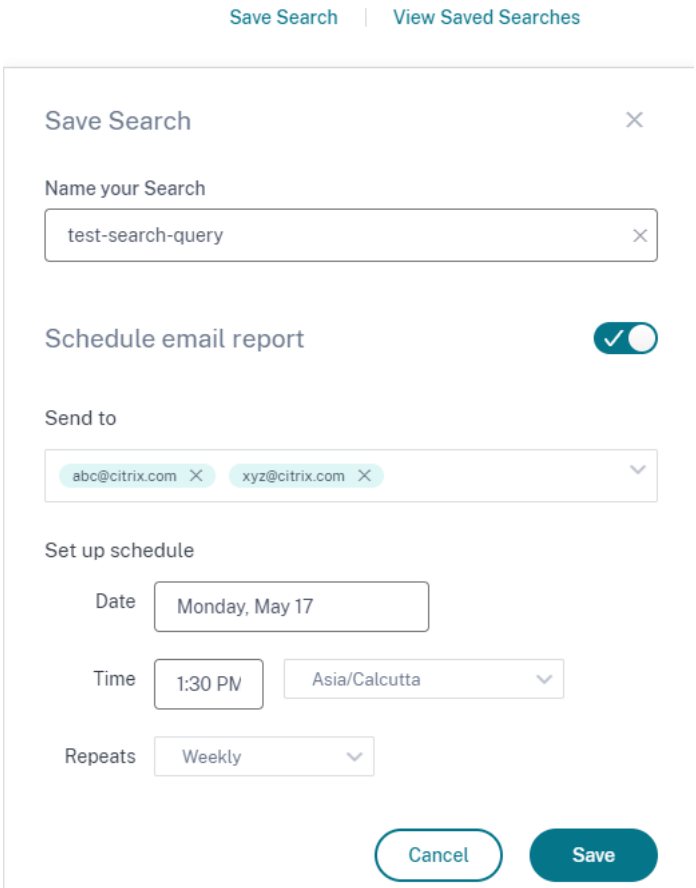
メール配信スケジュールを設定することで、検索クエリレポートのコピーを自分や他のユーザーに定期的に送信できます。

このオプションは、検索クエリレポートに棒グラフ、タイムラインの詳細などのビジュアル形式のデータが含まれている場合にのみ使用できます。そうしないと、メール配信をスケジュールできません。たとえば、[アプリとデスクトップ]、[セッション] などのデータソースの電子メールをスケジュールして、タイムラインの詳細と棒グラフとしてデータを表示できます。Users や Machines などのデータソースの場合、データは表形式でのみ表示されます。したがって、メールをスケジュールすることはできません。

検索クエリの保存中にメールをスケジュールする

検索クエリの保存中に、電子メール配信スケジュールを次のように設定します。

1. [検索の保存] ダイアログボックスで、[電子メールレポートのスケジュール] ボタンを有効にします。



2. 受信者の電子メールアドレスを入力または貼り付けます。

> 注
>
> メールグループはサポートされていません。

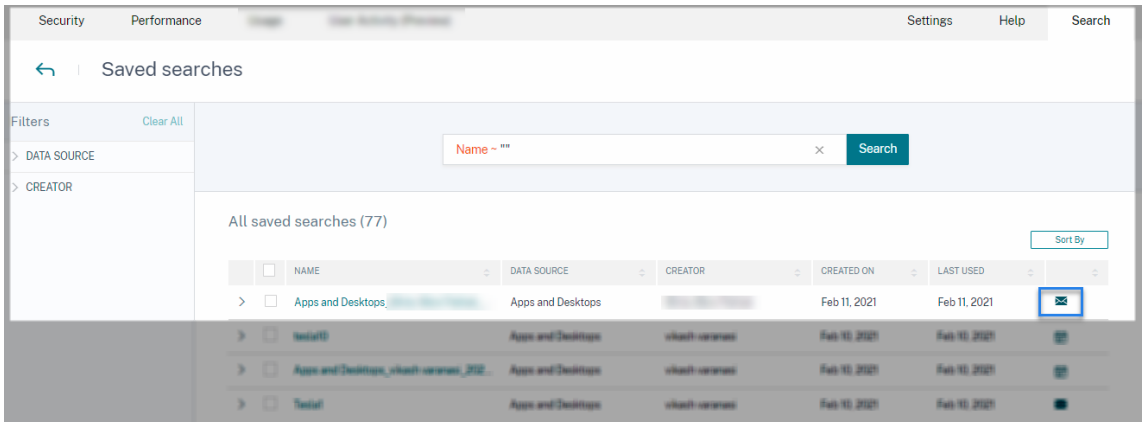
3. メール配信の日付と時刻を設定します。
4. 配信頻度（毎日、毎週、または毎月）を選択します。
5. [保存] をクリックします。

すでに保存されている検索クエリのメールをスケジュールする

以前に保存した検索クエリの電子メール配信スケジュールを設定する場合は、次の操作を行います。

1. [保存された検索の表示] をクリックします。
2. 作成した検索クエリに移動します。[このクエリを電子メールで送信] アイコンをクリックします。

> 注
>
> 保存した検索クエリの電子メール配信をスケジュールできるのは、クエリの所有者だけです。



3. [電子メールレポートをスケジュールする] ボタンを有効にします。
4. 受信者の電子メールアドレスを入力または貼り付けます。

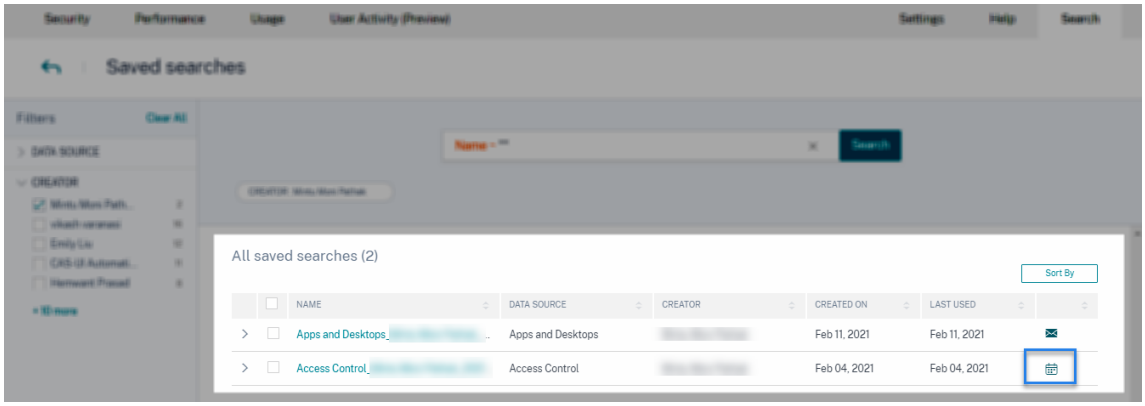
> 注
>
> メールグループはサポートされていません。

5. メール配信の日付と時刻を設定します。
6. 配信頻度（毎日、毎週、または毎月）を選択します。
7. [保存] をクリックします。

検索クエリのメール配信スケジュールを停止する

1. [保存された検索の表示] をクリックします。
2. 作成した検索クエリに移動します。[メール配信スケジュールの表示] アイコンをクリックします。

   > 注
   >
   > 保存した検索クエリの電子メールスケジュールを停止できるのは、クエリの所有者だけです。



3. [電子メールレポートのスケジュール] ボタンを無効にします。
4. [保存] をクリックします。

メールコンテンツ

受信者は、「Citrix Cloud-通知 < donotreplynotifications@citrix.com >」から検索クエリレポートに関する電子メールを受信します。レポートは PDF ドキュメントとして添付されます。メールは、[電子メールレポートのスケジュール] 設定で定義した一定の間隔で送信されます。

検索クエリレポートには、次の情報が含まれています。

- 選択した期間のイベントに対して指定した検索クエリ。
- イベントに適用したファセット (フィルタ)。
- タイムラインチャート、棒グラフ、検索イベントのグラフなどの視覚的なサマリー。

フルアクセス管理者および読み取り専用アクセス管理者の権限

- フルアクセス権を持つ Citrix Cloud 管理者は、[検索] ページで使用できるすべての機能を使用できます。
- 読み取り専用アクセス権を持つ Citrix Cloud 管理者の場合、[検索] ページでは次のアクティビティのみを実行できます。
  - データソースと期間を選択して、検索結果を表示します。

- 検索クエリを入力し、検索結果を表示します。
- 他の管理者の保存済み検索結果を表示します。
- ビジュアルサマリーをエクスポートし、検索結果を CSV ファイルとしてダウンロードします。

管理者の役割について詳しくは、「Citrix Analytics の管理者の役割の管理」を参照してください。

アラート設定

December 7, 2023

Citrix Analytics は、アラートポリシー基準に基づいてアラートを生成します。Citrix Analytics for Security and Performance からのアラート通知を電子メールと Webhook 経由で受信するように構成できます。

- メール配布リスト
- アラート通知用 webhook

Citrix Analytics for Security からのアラートに関する電子メール通知をフォーマットできます。

- エンドユーザーのメール設定

メール配布リスト

December 7, 2023

管理者への通知」アクションを手動で、またはポリシーを作成して適用すると、選択した管理者にリスク指標に関する通知が送信されます。

> 重要
>
> 組織内の Citrix Cloud ドメインおよびその他の非 Citrix Cloud ドメインから管理者を選択できます。

適切な管理者グループに通知を送信するには、その管理者の電子メールアドレスを使用して配布リストを作成します。

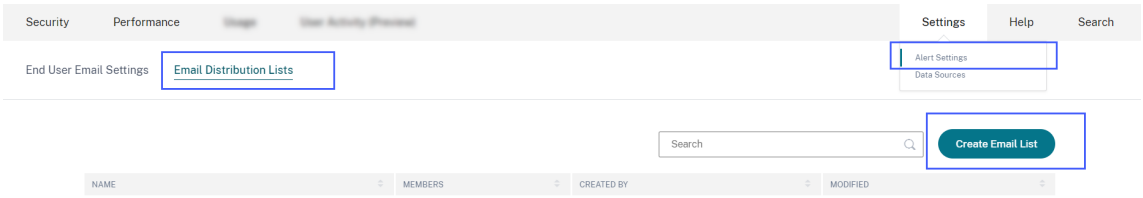
電子メール配布リストでは、次の操作を実行できます。

- 組織内の異なるドメインのメンバーを含む共通のメール配布リストを作成します。
- メンバー全員に一斉に通知する。
- 異なるドメインから管理者を選択する時間と労力を節約できます。
- 新しいメンバーの追加や既存のメンバーの削除などの要件に基づいて、電子メール配布リストを管理および管理します。

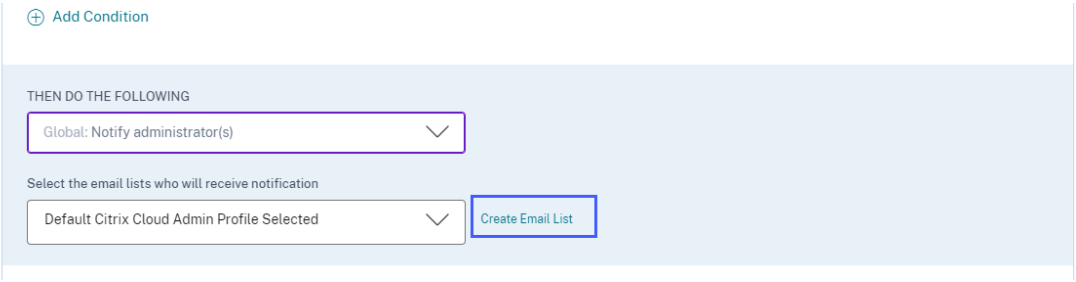
電子メール配布リストの作成

電子メール配布リストを作成するには、次の手順を実行します。

1. 設定 **>** アラート設定 **>** 電子メール配布リスト **>** 電子メールリストの作成をクリックします。



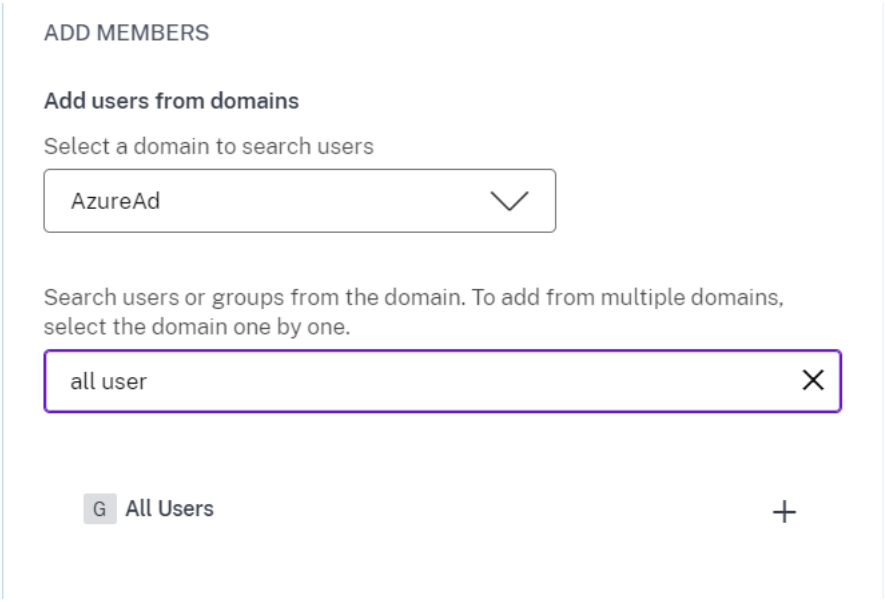
または、ポリシーからメール配布リストを作成することもできます。既存のポリシーを変更するか、ポリシーを作成して、[管理者に通知] アクションを選択します。[メーリングリストの作成] リンクをクリックします。



2. 電子メール配布リストの名前と説明を入力して、その目的を特定します。
3. 電子メール配布リストにメンバーを追加するには、次のオプションを使用します。
   - ドメインからユーザーを追加する。このオプションを使用するには、ドメインが Citrix Cloud に接続されている必要があります。
   - 電子メールアドレスでユーザーを追加します。選択したドメイン外のユーザーを追加する場合は、このオプションを使用します。
4. ドメインからユーザーを追加するには、ドメインを選択し、ユーザーまたはユーザーグループを検索します。

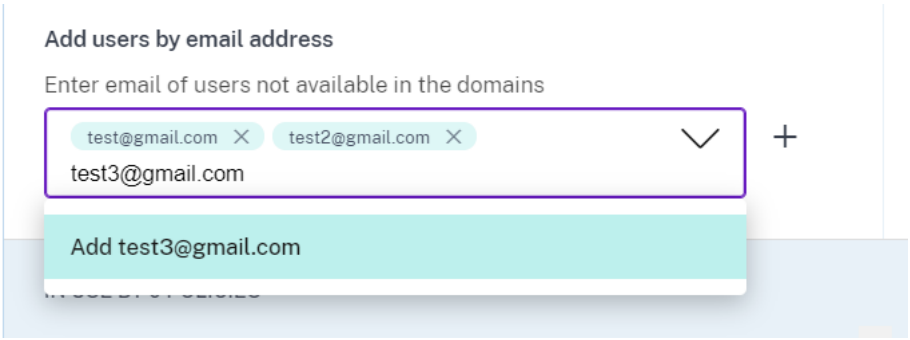
   > 注
   >
   > また、ドメインを 1 つずつ選択して、複数のドメインからユーザーとユーザーグループを追加することもできます。ドメインごとに、ユーザーまたはユーザーグループを検索して追加します。

5. ユーザーまたはユーザーグループの横にある [**Add**] アイコンをクリックします。



6. 選択したドメインで使用できないユーザーを追加するには、ユーザーの電子メールアドレスまたは電子メール配布リストを入力します。

> 注
>
> 電子メール配布リストを入力する前に、組織のネットワーク外から電子メール配布リストにアクセスできることを確認してください。組織の内部にあるメール配布リストを追加すると、そのリストのメンバーは Citrix Analytics からの通知を受信できなくなります。



7. [電子メールリストの作成] をクリックします。

メール配布リストの表示

メール配布リストを表示するには、[設定] **>** [アラート設定] **>** [メール配布リスト] をクリックします。

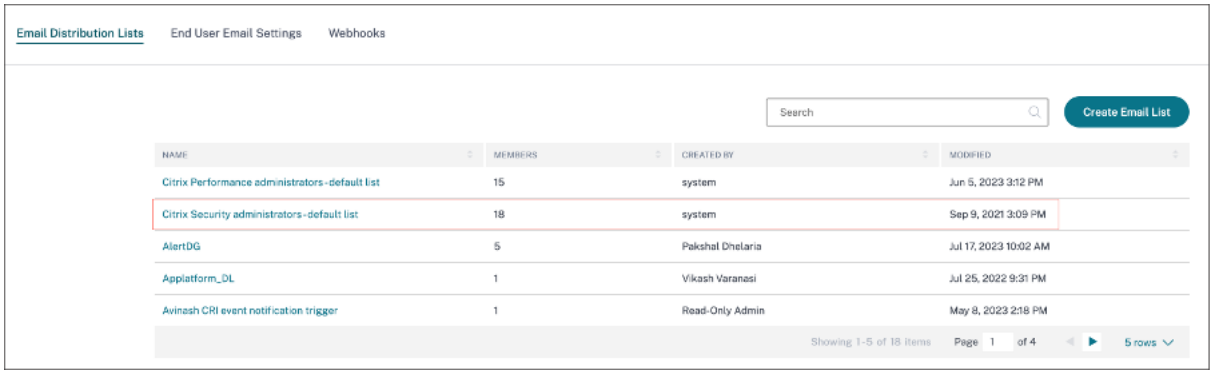
このページには、アカウントで作成されたすべてのメール配布リストが表示されます。電子メール配布リストを選択して、メンバーを表示したり、リストを変更したりします。

アカウントには、既定で作成されたメール配布リストが表示されます。これには、Citrix Cloud アカウントで電子メ

ール通知オプションが有効になっている **Citrix** Cloud 管理者が含まれます。既定のリストは削除または変更できません。

> 注
>
> デフォルトのメール配布リストでは、Citrix Analytics はメール通知が有効になっている管理者に関する情報をキャッシュします。キャッシュは 24 時間に 1 回更新されます。そのため、管理者が電子メール通知の設定を変更した場合、この変更は Citrix Analytics で 24 時間後に更新されます。
>
> たとえば、Citrix Cloud 管理者が電子メール通知を有効にした場合、通知の受信はすぐではなく 24 時間後に開始されます。同様に、Citrix Cloud 管理者がメール通知を無効にした場合、24 時間後に通知の受信を停止します。

セキュリティ管理者向けのデフォルトの配布リストには、Citrix **Cloud** アカウントでメール通知オプションを有効にしているフル管理者とカスタム管理者の両方が含まれるようになりました。



メール配布リストを変更する

電子メール配布リストを変更するには、次の手順を実行します。

1. 設定 **>** アラート設定 **>** メール配布リストをクリックします。
2. 変更する電子メール配布リストをクリックします。
3. 電子メール配布リストで、名前、説明、メンバーの追加や削除など、必要な詳細情報を更新します。
4. [変更の保存] をクリックします。

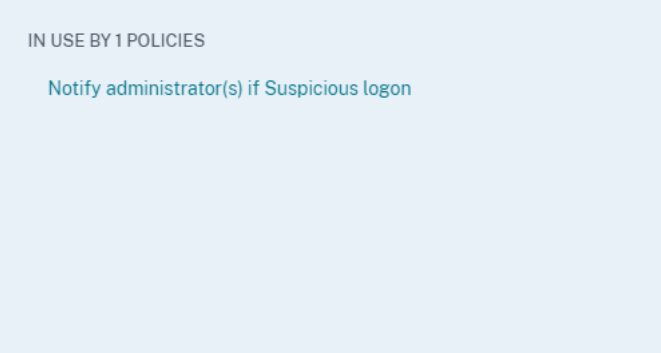
メール配布リストを削除する

メール配布リストは、どのポリシーにもリンクされていない場合にのみ削除できます。一部のポリシーにリンクされている場合は、関連するポリシーからメール配布リストを削除する必要があります。

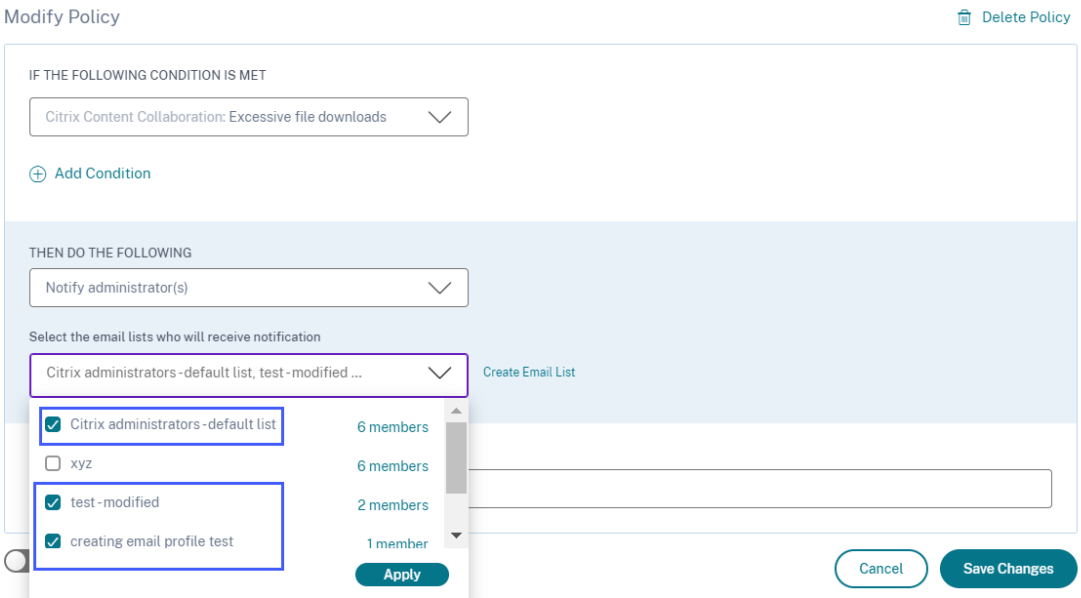
メール配布リストを削除するには、次の手順を実行します。

1. 設定 **>** アラート設定 **>** メール配布リストをクリックします。

2. 削除するメール配布リストをクリックします。
3. 電子メール配布リストで、関連するポリシーを表示します。



4. ポリシーをクリックして開き、メール配布リストを削除します。また、必要に応じてポリシーを削除することもできます。



5. [変更を保存] をクリックし、電子メール配布リストに戻ります。
6. 電子メール配布リストを開き、[削除] アイコンをクリックします。

アラート通知用 **webhook**

June 19, 2023

Webhook を使用して、受信 Webhook URL が設定されている任意のサードパーティアプリケーションに Citrix Analytics のアラート通知を送信できます。Webhook は、サービスプロバイダーアプリケーションとコンシューマ

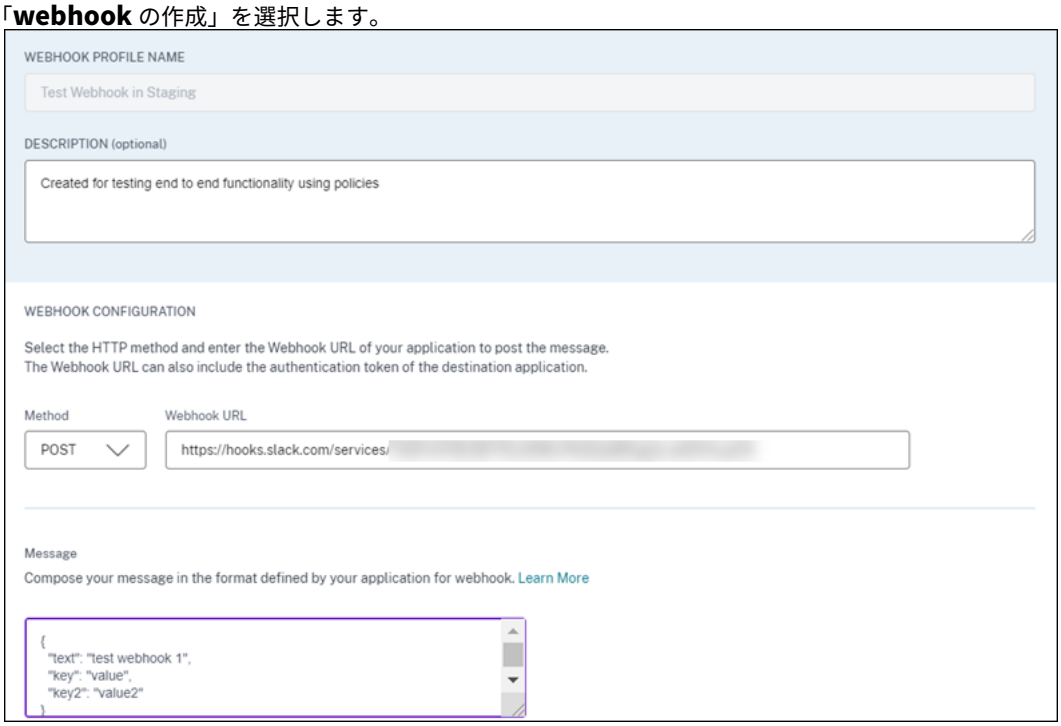
ーアプリケーション間のリアルタイムメッセージングを可能にする HTTP コールバックです。アラート通知はリアルタイムで送信されるため、イベントが発生すると通知されます。

Citrix Analytics がアラートをトリガーすると、関連する Webhook がアラートメッセージをターゲットアプリケーションの URL に送信します。アラートは、HTTP POST または PUT リクエストを通じて JSON ペイロードの形式で送信されます。たとえば、ユーザーがリスク指標をトリガーしたり、VDI マシンのパフォーマンスが低下したりした場合に、アラート通知を Slack チャンネルに送信する webhook を設定できます。
アラート管理用に Webhook を設定すると、アプリケーションでリアルタイムの通知を受け取ることができます。セキュリティリスクを軽減したり、Citrix Virtual Apps and Desktops 環境のパフォーマンスを改善したりするために、タイムリーなアクションを実行できます。

Webhook プロファイルの作成

Citrix Analytics でウェブフックプロファイルを作成するには:

1. Citrix Analytics にログインします。
2. 購読しているサービスに応じて、「管理」をクリックして「セキュリティ分析」または「パフォーマンス分析」にアクセスします。
3. トップバーから [設定] > [アラート設定**] > [Webhook**] をクリックします。
4. 「**webhook** の作成」を選択します。



5. プロファイル名と webhook の説明を入力して、目的を特定します。
6. アラートメッセージを送信するアプリケーションの HTTP メソッドと webhook URL を選択します。

> 注:
> 通常、送信 webhook は HTTP POST リクエストを介して送信されます。アプリケーションの webhook URL に認証トークンを含めることもできます。

7. Webhook URL に送信するアラートに関するメッセージを入力します。メッセージは、ターゲットアプリケーションで定義されている JSON や XML などの形式で構造化する必要があります。詳細については、Webhook の例を参照してください。
8. (オプション) メッセージのヘッダーキーと値を入力します。ヘッダーには、ペイロードをアプリケーションへ安全に送信するための認証トークンやその他のカスタムキーと値のペアを含めることができます。
9. Webhook の設定を検証するには、「テスト」をクリックします。
   このテストでは、送信 Webhook URL、ペイロード構造、およびヘッダーキーを検証します。構成に問題が見つからない場合は、「テスト成功」のメッセージが表示されます。

webhook の設定例

このセクションでは、Slack や Microsoft Teams などのサードパーティアプリケーションにアラートを送信するように webhook を設定する例を紹介します。

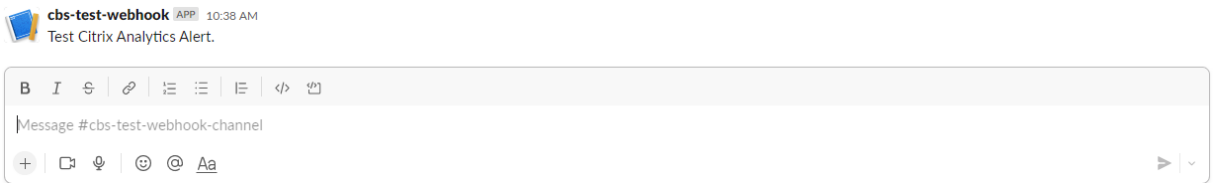
> 注:
> Webhook URL の取得方法と Webhook に必要な設定については、サードパーティアプリケーションの製品ドキュメントを参照してください。

Slack にアラートメッセージを送る

Slack では、アラートを送信する前に次のタスクを完了していることを確認してください。

1. Citrix Analytics 用の Slack アプリをまだ作成していない場合は、作成してください。
2. アプリでは、受信 webhook 機能を有効にして、受信 webhook を作成します。
3. アプリがメッセージを投稿するチャンネルを選択します。
4. アプリを認証すると、メッセージを送信するための Webhook URL が取得されます。
   詳細については、「受信 webhook の入門」を参照してください。

サンプルメッセージ形式 `curl --location --request POST 'WEBHOOK URL'--header 'Content-Type: application/json'--data-raw '{ "text": "Test Citrix Analytics Alert." }`

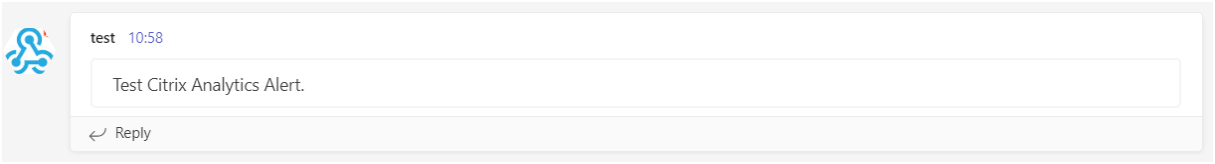
出力 

Microsoft Teams にアラートメッセージを送信する

Microsoft Teams では、アラートを送信する前に次のタスクを完了していることを確認してください。

1. Teams グループを作成していない場合は、Teams 内に作成してください。
2. Webhook コネクタを作成します。メッセージの作成と送信の記事で説明されている手順を参照してください。
3. webhook の URL を取得します。

サンプルメッセージ形式 `curl --location --request POST 'WEBHOOK URL'--header 'Content-Type: application/json'--data-raw '{ "text": "Test Citrix Analytics Alert." }`

出力 

セキュリティのための **Citrix Analytics**（セキュリティ分析）

February 14, 2024

ネットワーク上のどこでも、いつでも、どのデバイスからでも作業できるという利点により、ユーザーが孤立した企業オフィスでしか作業しない場合よりも、機密性の高い企業データが漏洩する危険性が高くなります。悪意のあるユーザーは、大きな攻撃対象領域を標的にしています。IT チームは、セキュリティを損なうことなく、優れたユーザーエクスペリエンスを提供する責任を負っています。Citrix Analytics for Security は、ユーザーセキュリティに重点を置いてこのギャップを埋めるのに役立ちます。

セキュリティ分析って何ですか

Citrix Analytics for Security は、Citrix Virtual Apps and Desktops ユーザー、Citrix DaaS（旧シトリ Citrix Virtual Apps and Desktops サービス）ユーザー、および Citrix Workspace ユーザーの動作を継続的に評価しま

す。企業の機密情報を保護するための措置を講じています。ネットワーク、仮想化されたアプリケーション、およびデスクトップツールにわたるデータの集約と関連付けにより、ユーザーのセキュリティ脅威に対処するための貴重な洞察とより焦点を絞ったアクションを生成できます。また、機械学習は、悪意のあるユーザーの行動を特定するための高度に予測的なアプローチをサポートしています。

機能

- Citrix 製品およびパートナーインテグレーション全体から得られるインサイトを合理化しました。詳細については、「セルフサービス検索」を参照してください。
- 使いやすいダッシュボードにより、ユーザーの行動を完全に把握できます。詳細については、「ユーザーダッシュボード」を参照してください。
- 機械学習と自動化されたアクションによるカスタマイズされたポリシーを使用して、悪意のあるユーザーの行動を検出して軽減します。詳細については、「ポリシーとアクション」を参照してください。
- 企業ネットワークへの初期認証後、ユーザーの行動を継続的に監視することで、徹底したセキュリティと優れたユーザーエクスペリエンスのバランスをとることができます。詳細については、「継続的なリスク評価」を参照してください。

ダッシュボード

ユーザーまたはエンティティの動作に関する詳細を、次のセキュリティダッシュボードに表示できます。

- ユーザー: 組織全体のユーザー行動パターンを可視化します。
- [ユーザーアクセス]: アクセスされた危険なドメインの数と、ネットワーク内のユーザーがアップロードおよびダウンロードしたデータの量を要約します。
- App Access: ネットワーク内のユーザーがアクセスしたドメイン、URL、アプリの詳細を要約します。

- アクセス保証の場所: Citrix Virtual Apps and Desktops ユーザーと Citrix DaaS ユーザーのアクセスの詳細とログオンの詳細が要約されます。
- レポート: オンボーディングされたデータソースのディメンションと指標に基づいてカスタムレポートを作成します。

次の操作

- システム要件: 開始する前に満たす必要のある最小要件。
- データソース:Analytics がサポートする製品について把握します。
- データガバナンス:Analytics によるログの収集、保存、保持について把握します。
- はじめに: 組織で Analytics の使用を開始する方法

パフォーマンス向け **Citrix Analytics**（パフォーマンス分析）

September 21, 2023

パフォーマンス分析とは何ですか

パフォーマンス分析は、アプリおよびデスクトップ環境の主要パフォーマンス指標を追跡、集計、および視覚化できるようにする Citrix Analytics 製品です。

- Performance Analytics は、サイトのパフォーマンス指標を、見やすいユーザーエクスペリエンスとインフラストラクチャダッシュボードに集約します。ダッシュボードは、ユーザーエクスペリエンスを分析し、アプリとデスクトップサイトの使用を最適化するのに役立ちます。
- パフォーマンス分析は、マルチサイトの集約とレポートをサポートしています。クラウドとオンプレミスのセットアップ全体のパフォーマンスメトリクスを集約します。そのため、環境内のすべてのサイトのデータを 1 つのコンソールで表示できます。
- パフォーマンス分析は、ユーザーのパフォーマンス要因を定量化し、これらの要因に基づいてユーザーを分類します。障害、画面の遅れ、セッションログオンの遅延、およびその他のパフォーマンス指標のトラブルシューティングに役立つ実用的な洞察を提供します。
- パフォーマンス分析では、メトリックを検索してフィルタリングし、パフォーマンスの問題に直面している特定のユーザーまたはセッションに絞り込むことができます。

パフォーマンス分析の使用方法

ユーザーエクスペリエンスダッシュボード

[ユーザーエクスペリエンス] ダッシュボードには、セッションの応答性、セッションログオン時間、セッションの失敗、セッションの再接続などの要因に関するサイトのパフォーマンスが表示されます。これらを組み合わせてユーザーエクスペリエンスを定義します。

組織内の仮想アプリケーションおよびデスクトップの複数のユーザーをサポートしており、アプリまたはデスクトップの起動中に遅延が発生することがある場合には、ログオン時間メトリックで問題の洞察を得ることができます。ドリルダウンは、問題の原因となる要因を特定するのに役立ちます。

インフラストラクチャダッシュボード

インフラストラクチャダッシュボードには、サイト内のコンピュータのステータスと正常性が表示されます。ユーザーダッシュボードとインフラストラクチャダッシュボードを併用すると、リソースの可用性をプロアクティブにチェックし、サイトのパフォーマンスのボトルネックを特定するのに役立ちます。

- ユーザーまたはセッションの傾向が低下し、サイトにログインしているユーザーまたはセッションの数が減少している場合は、このインジケータを使用して、ハイパーバイザーが再起動されたかどうか、またはマシンの数が不足しているかどうかを確認します。
- セッションの起動に失敗するケースが複数ある場合は、ドリルダウンして失敗の原因を特定します。ライセンス数が不足しているか、Delivery Controller へのマシン接続に問題がある可能性があります。

> 注:
>
> インフラストラクチャ分析ダッシュボードは、現在 [プレビュー] の下にあります。

Performance Analytics を使用すると、問題を迅速に分析し、トラブルシューティングして解決し、アプリケーションとデスクトップの最適なサービスレベルを維持できます。

Getting Started

前提条件

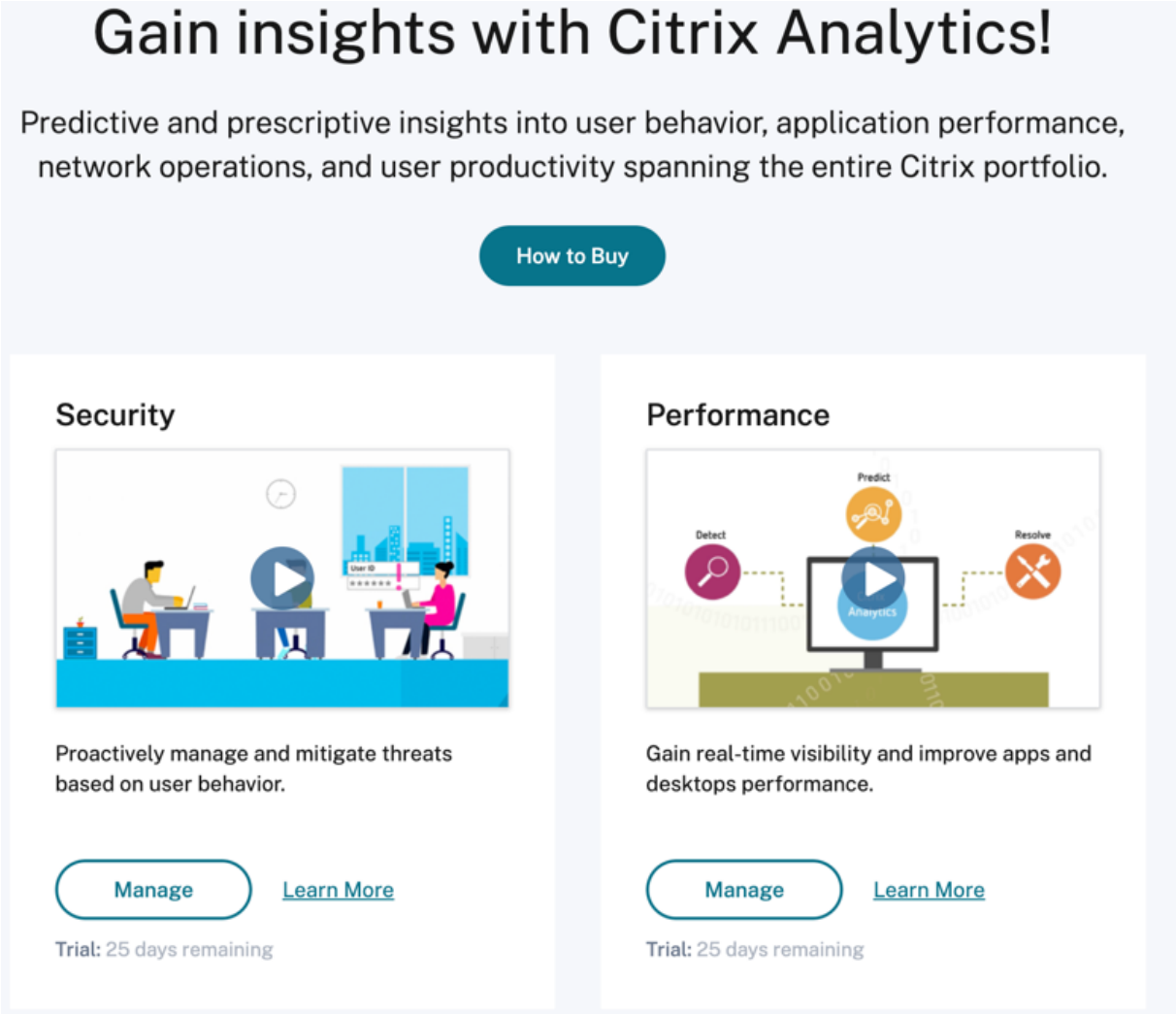
1. お使いのワークステーションに、サポートされているブラウザの記事に記載されているサポートされている Web ブラウザがあるかどうかを確認します 。システム要件について詳しくは、「Citrix Analytics のシステム要件 」を参照してください。
2. アナリティクスサービスを使用するには、Citrix Cloud アカウントが必要です。Citrix Cloud アカウントを作成する方法の詳細については、「Citrix Cloud へのサインアップ」を参照してください。https://citrix.cloud.com にアクセスし、Citrix Cloud アカウントでサインインします。

3. Citrix Analytics for Performance は、サブスクリプションベースのオファリングとして、スタンドアロンオファリングとして、または Citrix Analytics for Security にバンドルされています。Citrix Analytics for Performance をサブスクライブする方法については、「https://www.citrix.com/products/citrix-analytics-performance.html)」を参照してください。
4. サポートされているバージョンのデータソースについては、「データソース 」の記事を参照してください。
5. Citrix Profile Management をすべてのマシンにインストールする必要があります。
6. エンドユーザーエクスペリエンス監視 (EUEM) サービスが実行されており、対応するポリシーがすべてのマシンで構成されている必要があります。詳細については、「エンドユーザーの監視ポリシー設定」を参照してください。
7. 監視サービスが帯域幅や遅延の統計などのマシン関連のパフォーマンスメトリックを収集できるようにするには、**Performance Analytics** ポリシーの **VDA** データ収集をマシンで［許可］に設定する必要があります。詳細については、「パフォーマンス分析のデータ収集のポリシー」を参照してください。
8. Citrix Studio のプロセス監視ポリシーを有効にすると、［マシン統計］**>**［プロセス］タブでリソースを大量に消費するプロセスを可視化できます。
   詳細については、「プロセス監視を有効にする」を参照してください。
9. すべてのエンドポイント (またはプロキシが設定されている場合はプロキシ) から次の URL にアクセスできることを確認します。

エンドポイント	米国リージョン	欧州連合地域	アジア太平洋南部リージョン
Citrix キー登録	https://trust.citrixnetworkapi.net	https://trust.citrixnetworkapi.net	https://trust.citrixnetworkapi.net
Citrix Cloud	https://trust.citrixworkspacesapi.net	https://trust-eu.citrixworkspacesapi.net	https://trust-aps.citrixworkspacesapi.net
Citrix Analytics	https://api.was.cloud.com	https://api-eu.was.cloud.com	https://api-aps.was.cloud.com
一括アップロード	https://citrixanalyticseh-alias.servicebus.windows.net/	https://citrixanalyticsehec-alias.servicebus.windows.net/	https://citrixanalyticsehaps-alias.servicebus.windows.net/

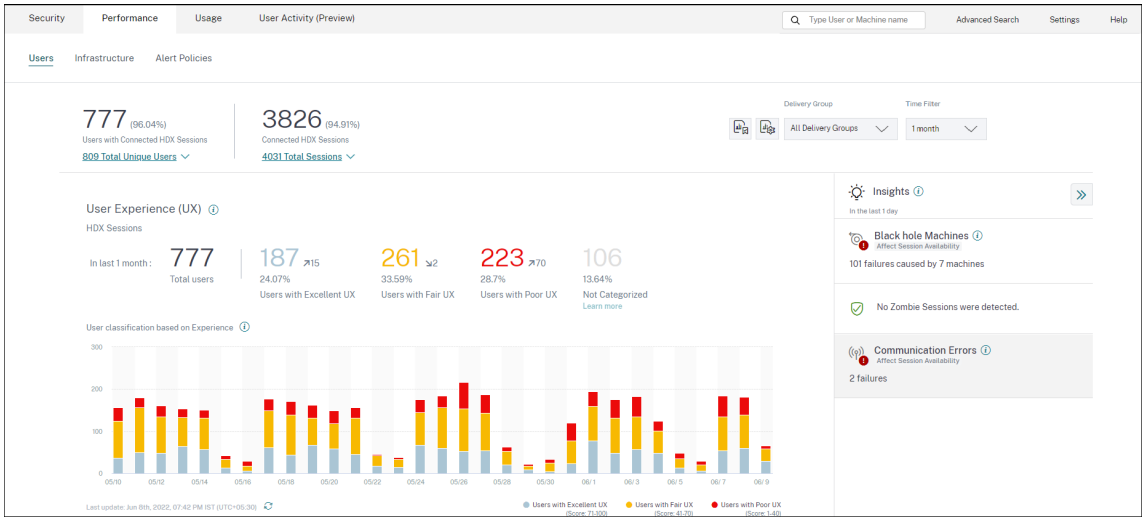
アクセス

1. Citrix Cloud にログオンします。Analytics サービスタイルを探して、[管理] をクリックします。概要ページには、Analytics ポートフォリオで使用可能なオファリングが表示されます。
2. パフォーマンスオファリングで、オファリングの試用版を使用するには、[トライアルのリクエスト] をクリックします。パフォーマンス向け Citrix Analytics オファリングを購入した場合は、代わりに［管理］リンクをクリックします。



。

1. Citrix Analytics for Performance が開き、ダッシュボードにユーザーエクスペリエンスとインフラストラクチャパフォーマンス分析が表示されます。



アジア太平洋南地域からのアクセス　Citrix Analytics for Performance は、アジア太平洋南部（APS）地域のトライアル版のお客様とサブスクリプションベースのお客様向けに自動的にオンボーディングされるようになりました。Citrix Cloud でサポートされているリージョンの詳細については、「地理的考慮事項」を参照してください。

APS リージョンからパフォーマンス分析にアクセスするには、テナントを Citrix Cloud にオンボーディングする際にアジア太平洋南部リージョンを選択します。Citrix Cloud にログオンし、Citrix Cloud の APS リージョンでテナントを選択します。`https://analytics-aps.cloud.com` URL を使用して、Citrix Analytics クラウドサービスにアクセスします。

- Citrix Analytics for Performance は、組織のユーザーイベントとメタデータをホームリージョンとして選択すると、アジア太平洋南部リージョンに保存されるようになりました。詳しくは、「データガバナンス」を参照してください。
- アジア太平洋南部リージョンのネットワーク要件については、「テクニカルセキュリティの概要」を参照してください。

データソースの設定

パフォーマンス分析を使用して、オンプレミスまたはクラウドサイトを監視できます。このオファリングは、純粋なオンプレミスのお客様、クラウドのお客様、またはオンプレミスとクラウドサイトが混在するハイブリッドのお客様のいずれでも使用できます。

パフォーマンス分析は、Citrix DaaS（旧 Citrix Virtual Apps and Desktops サービス）を自動的に検出します。オンプレミスのお客様の場合は、

- まず、Citrix Virtual Apps and Desktops サイトをパフォーマンス分析にオンボードします。
- パフォーマンス分析でネットワーク関連の情報を取得するには、オンプレミスの NetScaler Gateway もオンボードする必要があります。

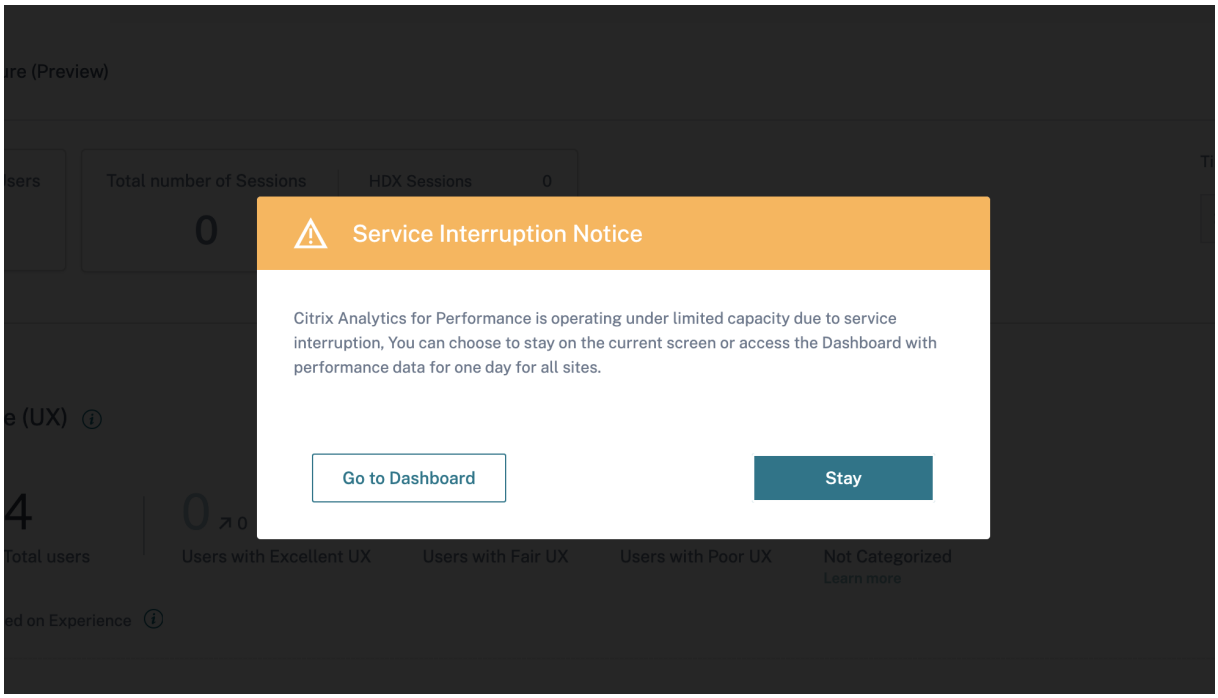
「データソース」の記事の説明に従って、必要なデータソースを構成します 。

> 注:
>
> - パフォーマンス向上の Citrix Analytics は、「パフォーマンス向け Citrix Analytics で収集されるログ」に記載されているように、データポイントのログを収集して保存します。
> - パフォーマンス向け Citrix Analytics サービスの推奨される制限は、制限の記事に記載されています 。

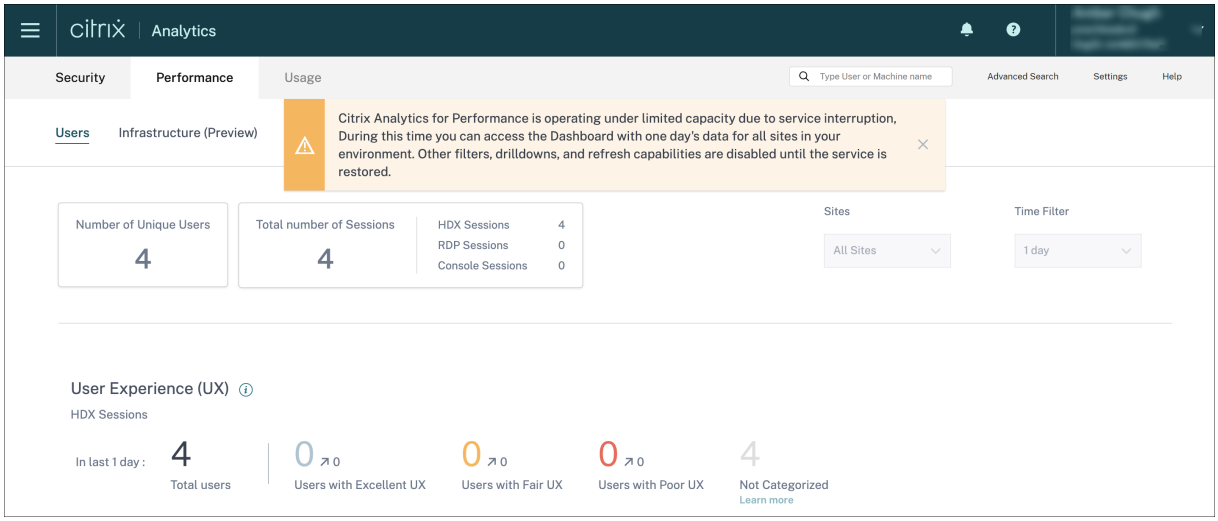
サービス継続性

サービスが中断した場合、Citrix Analytics for Performance は限られた容量で動作します。

管理者は、現在の画面で利用可能なデータを維持して表示するか、ダウングレードモードでダッシュボードに移動するかを選択できます。



ダウングレードモードでは、ユーザーは過去 1 日のすべてのサイトのデータを含むダッシュボードに切り替わります。いずれの場合も、サービスが通常の動作に復元されるまで、すべてのフィルタとドリルダウンは無効になります。



この更新により、製品の耐障害性が向上し、サービスレベルアグリーメントとの整合性が向上します。

セキュリティとパフォーマンスに関する **Citrix Analytics** トラブルシューティング

December 7, 2023

このセクションでは、Citrix Analytics for Security を使用するときに発生する可能性のある次の問題を解決する方法について説明します。

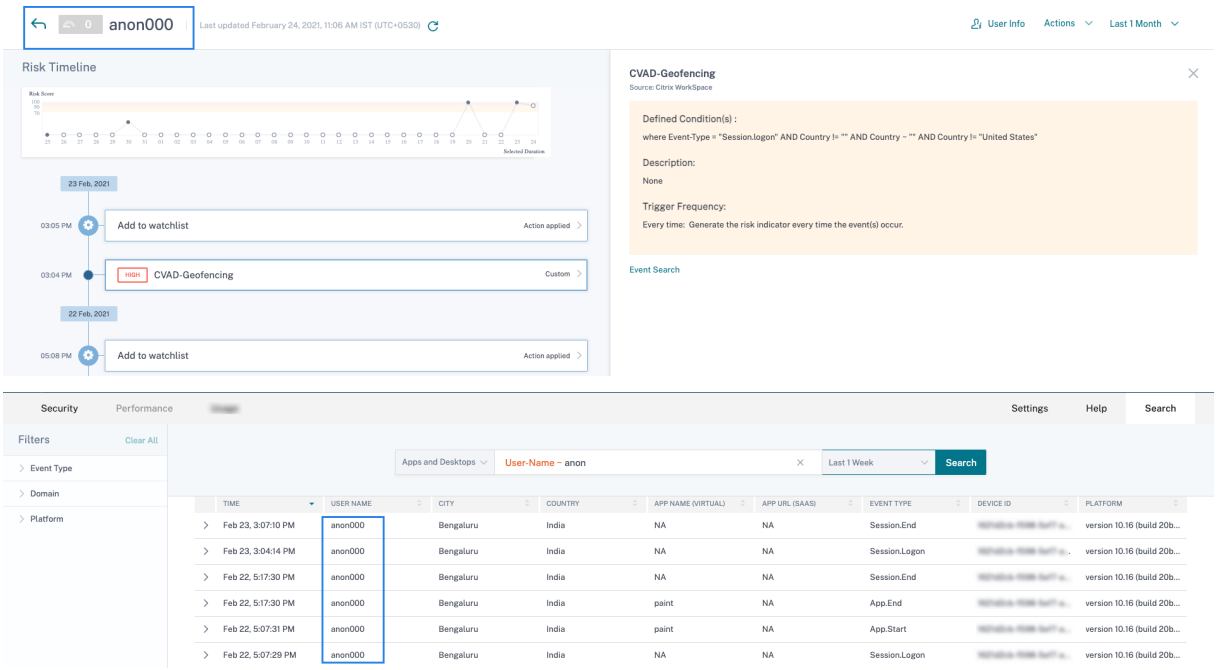
- 匿名ユーザーを正当なユーザーとして検証します。
- データソースからのイベント転送の問題をトラブルシューティングします。
- Virtual Apps and Desktops イベント、SaaS イベントをトリガーし、Citrix Analytics for Security へのイベント送信を検証します。
- Session Recording サーバーが接続に失敗する。
- Splunk 用 Citrix Analytics アドオンの設定に関する問題

匿名ユーザーを正当なユーザーとして検証する

August 22, 2022

管理者として、Citrix Analytics for Citrix Virtual Apps and Desktops Security で一部のユーザーおよび Citrix DaaS （以前の Citrix Virtual Apps and Desktops サービス）ユーザーが匿名として表示されることがあります。これらのユーザーは、検出されたユーザーとして識別されます。ただし、ユーザー名 anonXYZ （「XYZ」は 3 桁の数字を表します）は、次のページに表示されます。

- ユーザー
- ユーザーのタイムライン
- リスクの高いユーザー
- アプリとデスクトップデータソースのセルフサービス検索



そのようなユーザーが表示されたら、次のことを知りたいかもしれません。

- これらのユーザーは誰ですか?
- これらのユーザーは本質的に合法的で悪意のあるのですか?
- それらを検証するには?
- これらのユーザーに対して適用する必要があるアクションは何ですか?

Citrix IT 環境では、次のシナリオで匿名ユーザーが表示されます。

- 公開済みのセキュアブラウザアプリをユーザーが使用している場合
- ユーザーが認証されていないストアを使用している場合

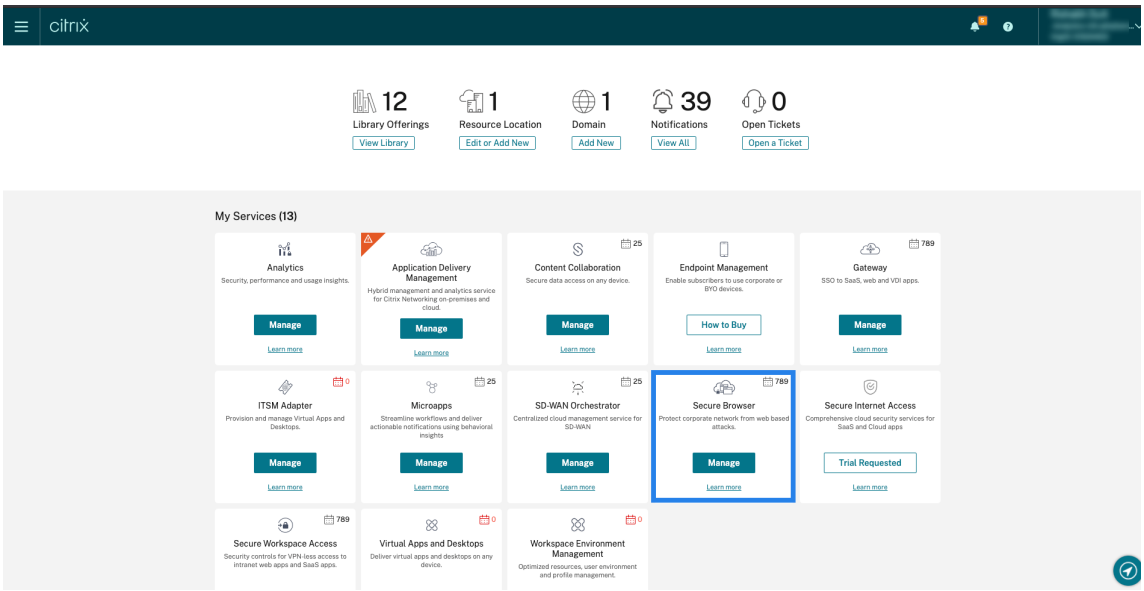
公開済みのセキュアブラウザアプリを使用しているユーザー

セキュアブラウザアプリは、Citrix Secure Browser サービスを使用して公開される Web アプリです。これらのアプリは、Web ブラウジングイベントを隔離し、ブラウザベースの攻撃から企業ネットワークを保護します。詳細については、「セキュリティで保護されたブラウザサービス」を参照してください。

セキュアブラウザアプリは、の匿名セッション機能を使用します Citrix DaaS。

Citrix Cloud アカウントでセキュアブラウザが構成されているかどうかを確認するには:

1. Citrix Cloud にサインインします。
2. [セキュアブラウザ] カードで、[管理] をクリックします。



3. [管理] ページで、公開されているセキュアなブラウザアプリを確認します。

ユーザーが Web ブラウザを使用して Citrix Receiver for Web サイトを介して StoreFront ストアにアクセスし、公開されているセキュリティで保護されたブラウザアプリを使用している場合、ユーザーの ID は非表示になります。したがって、Citrix Analytics はユーザーを匿名として表示します。

ユーザーがデバイスにインストールされている Citrix Receiver アプリまたは Citrix Workspace アプリを介して StoreFront ストアにアクセスし、公開されているセキュリティで保護されたブラウザアプリを使用する場合、Citrix Analytics StoreFront で指定されたユーザー名としてユーザーを表示します。

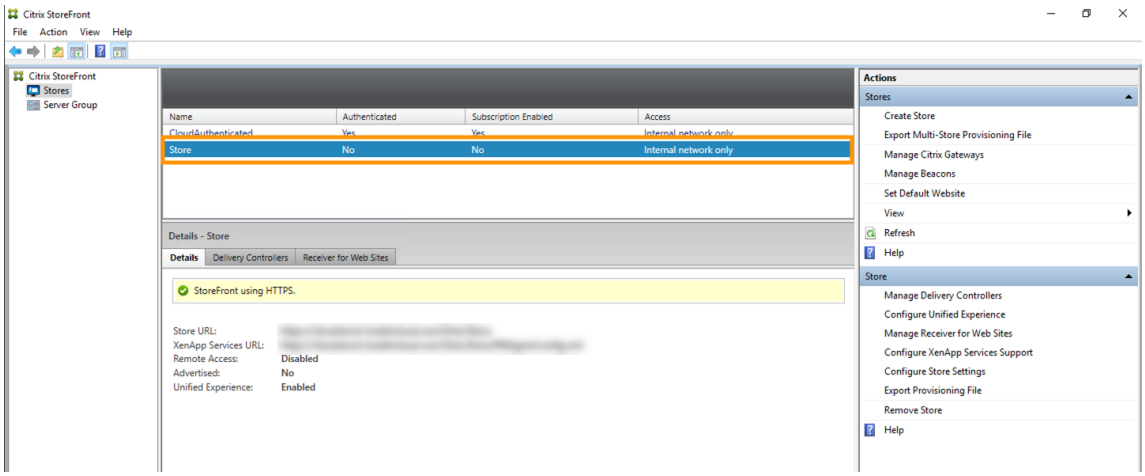
したがって、そのユーザーを組織の正当なユーザーと見なすことができます。危険な動作がユーザーに関連付けられていない場合は、アクションを適用する必要はありません。

認証されていないストアを使用しているユーザー

認証されていないストアは Citrix StoreFront の機能で、お客様が管理するストアに適用されます。この機能は、認証されていない (匿名) ユーザーのアクセスをサポートします。

組織に認証されていないストアがあるかどうかを確認するには、次の手順を実行します。

1. Citrix Studio を起動します。
2. [ストア] をクリックします。
3. ストアの場合は、[認証済み] 列で認証ステータスを確認します。



ストアが認証されておらず、ユーザーがその非認証ストアにアクセスしている場合、ユーザー ID は匿名のままになります。したがって、Citrix Analytics はユーザーを匿名として表示します。このユーザーを組織の正当なユーザーと見なすことができます。危険な動作がユーザーに関連付けられていない場合は、アクションを適用する必要はありません。

データソースからのイベント転送に関する問題のトラブルシューティング

April 12, 2024

このセクションでは、Citrix Analytics for Security でのデータ転送に関する問題のトラブルシューティングに役立ちます。データソースがユーザーイベントを正確に送信できない場合、ユーザーやリスク指標の検出不能などの問題が発生する可能性があります。

チェックリスト

シーケンス	チェック
1	Security Analytics を使用するための正しい資格を持っていますか?
2	そのデータソースはホームリージョンでサポートされていますか?
3	ご使用の環境は、すべてのシステム要件を満たしていますか。
4	Analytics ですべてのデータソースが検出され、データ処理が有効になっていますか?
5	データソースでのユーザーアクティビティは、Analytics にイベントを正確に送信していますか?
6	仮想アプリケーションとデスクトップのイベントは Analytics に送信されますか。
7	ユーザーイベントは Analytics のセルフサービス検索ページに表示されていますか?
8	ユーザーは Analytics によって検出されていますか?

チェック **1-**セキュリティアナリティクスを使用するための正しいエンタイトルメントがありますか**?**

Citrix Analytics for Security は、サブスクリプションベースのサービスです。詳しくは、「はじめに」を参照してください。

チェック **2-**データソースはご使用のホームリージョンでサポートされていますか

Citrix Analytics for Security は、次のホームリージョンでサポートされています。

- 米国（米国）
- 欧州連合 (EU)
- アジア太平洋南部 (APS)

組織の場所に応じて、いずれかのホームリージョンの Citrix Cloud にオンボーディングできます。

ただし、一部のホームリージョンではサポートされていないデータソースもあります。[データソース](/en-us/security-analytics/data-sources.html)）は、Citrix Analytics for Security がユーザーイベントを受信する製品のことです。

データソースがサポートされていないホームリージョンで組織が Citrix Cloud にオンボーディングされている場合、データソースからユーザーイベントは取得されません。

次の表を使用して、データソースと、そのデータソースがサポートされているリージョンを表示します。

データソース	米国リージョンでのサポート	EU リージョンでのサポート	APS リージョンでサポートされています
Citrix Endpoint Management	はい	はい	はい
NetScaler Gateway (オンプレミス)	はい	はい	はい
Citrix ID プロバイダー	はい	はい	はい
Citrix Secure Browser	はい	はい	はい
Citrix Secure Private Access	はい	番号	番号
Citrix DaaS（旧称: Citrix Virtual Apps and Desktops サービス）	はい	はい	はい
Citrix Virtual Apps and Desktops オンプレミス	はい	はい	はい
Microsoft Active Directory	はい	はい	はい
Microsoft Graph Security	はい	はい	はい

チェック **3-**ご使用の環境がすべてのシステム要件を満たしていますか

Citrix Analytics は、データソースからユーザーイベントを受信するまでに数分かかる場合があります。データソースサイトカードにユーザーイベントが表示されない場合は、環境が前提条件とシステム要件を満たしていることを確認してください。

前提条件

1. Citrix Cloud サブスクリプションはすべてアクティブである必要があります。[Citrix Cloud] ページで、すべての Citrix Cloud サービスがアクティブであることを確認します。
2. オンプレミスで使用している場合は Citrix Virtual Apps and Desktops、Citrix Workspace にサイトを追加し、サイトアグリゲーションを構成する必要があります。Citrix Analytics は、Citrix Workspace に追加されたサイトを自動的に検出します。詳細については、「ワークスペースでのオンプレミスの仮想アプリケーションおよびデスクトップの集約」を参照してください。
3. サイトで StoreFront 展開環境を使用している場合は、Citrix Workspace アプリがユーザーイベントを Citrix Analytics に送信できるように StoreFront サーバーを構成します。StoreFront のバージョンが 1906 以降であることを確認します。StoreFront サーバーを構成しない場合、Citrix Analytics Citrix Virtual

Apps and Desktops はオンプレミスからのユーザーイベントの受信に失敗します。StoreFront の展開環境を構成するには、StoreFront のドキュメントの「Citrix Analytics サービス」

4. Citrix Virtual Apps and DesktopsCitrix DaaS ユーザーとユーザーは、指定したバージョンの Citrix Workspace アプリまたは Citrix Receiver をエンドポイントで使用する必要があります。そうしないと、Analytics はユーザーエンドポイントからユーザーイベントを受信しません。Citrix Workspace アプリまたは Citrix Receiver のサポートされるバージョンのリストは、Citrix Virtual Apps and Desktops および Citrix DaaS データソースで確認できます。
5. 公開されたセキュアブラウザセッションからユーザーのイベントを受信するには、セキュアブラウザでホスト名トラッキング設定を有効にします。デフォルトでは、この設定は無効になっています。詳細については、「公開されたセキュリティで保護されたブラウザーを管理する」を参照してください。
6. 次の記事で説明されているように、データソースをオンボーディングします。
    - Citrix Endpoint Management データソース
    - NetScaler Gateway データソース
    - Citrix Secure Private Access データソース
    - Citrix Virtual Apps and Desktops および Citrix DaaS データソース
    - Microsoft Active Directory 統合
    - Microsoft Graph セキュリティ統合

チェック **4-Analytics** ですべてのデータソースが検出され、データ処理が有効になっていますか

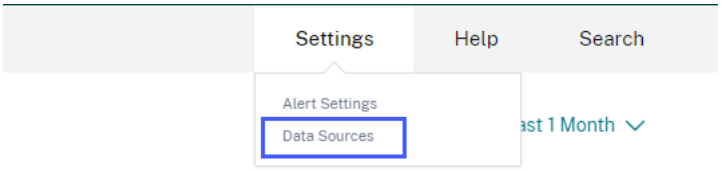
すべてのデータソースが検出され、そのデータソースのデータ処理が有効になっていることを確認します。データソースのデータ処理を有効にしないと、そのデータソースを使用しているユーザーは検出されません。このような状況では、潜在的なセキュリティリスクが生じる可能性があります。

データ処理を有効にすると、Citrix Analytics でユーザーイベントが確実に処理されます。Citrix Analytics にイベントが送信されるのは、ユーザーがデータソースをアクティブに使用している場合のみです。

> 注
>
> Citrix Analytics は、お客様の環境から積極的にデータを取得しません。

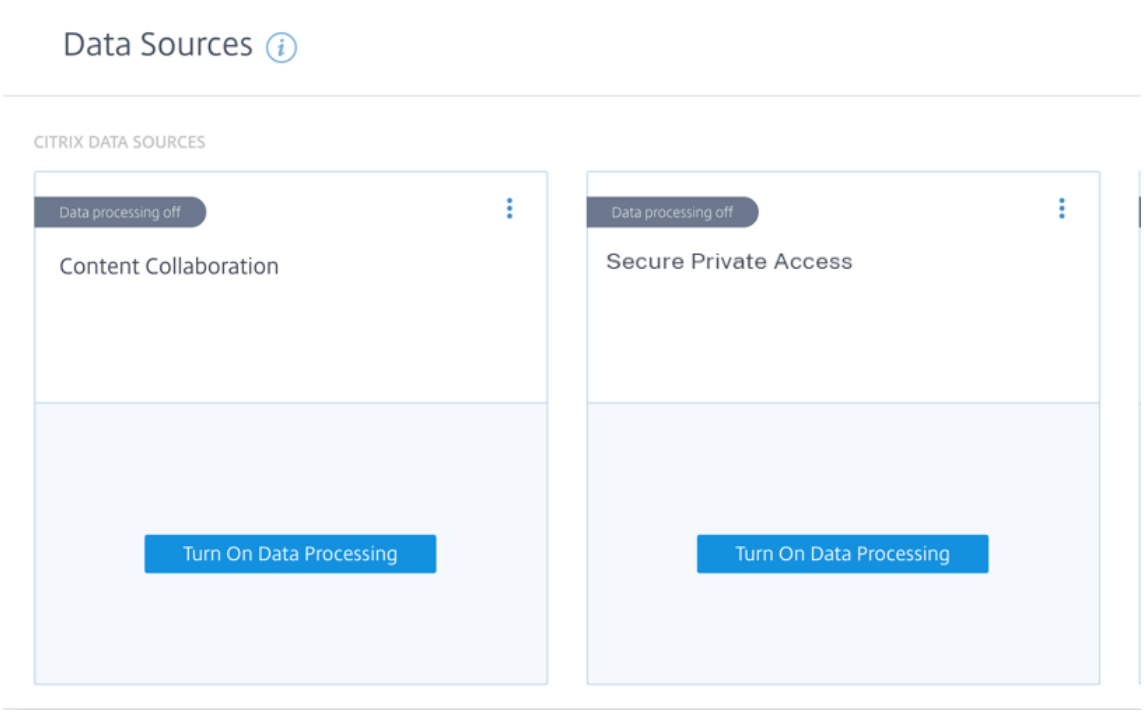
データソースを検出して分析を有効にするには、次の操作を行います。

1. [設定] > [データソース] > [セキュリティ] をクリックして、検出されたデータソースを表示します。Citrix Analytics は、ユーザーが Citrix Cloud アカウントにサブスクライブしているデータソースを自動的に検出します。

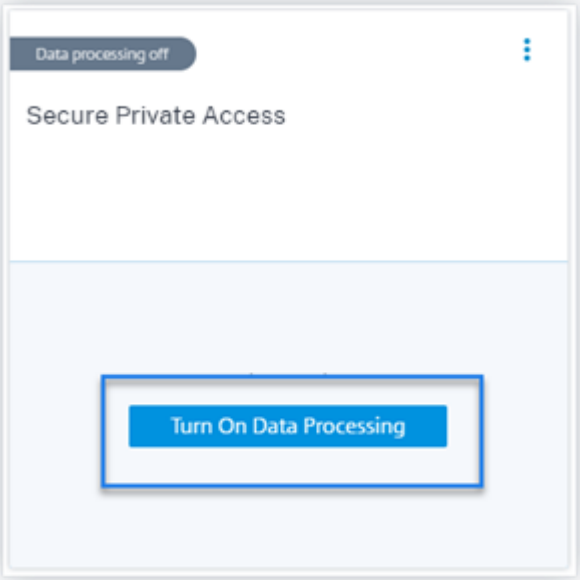


2. [データソース] ページに、検出されたデータソースがサイトカードとして表示されます。デフォルトでは、データ処理はオフになっています。

> 重要
>
> Citrix Analytics は、お客様の同意を得た後、お客様のデータを処理します。



3. Citrix Analytics でイベントを処理するサイトカードの［データ処理をオンにする］をクリックします。たとえば、Citrix Secure Private Access サイトカードの [データ処理を有効にする] をクリックします。



4. データ処理を有効にすると、Citrix Analytics はデータソースのイベントを処理します。サイトカードのステータスが [データ処理] に変わります。選択した期間に基づいて、ユーザー数と受信したイベントを表示できます。

5. 検出されたすべてのデータソースについて、「はじめに 」に記載されている手順に従って分析を有効にします。

チェック **5-**データソースでのユーザーアクティビティは、**Analytics** にイベントを正確に送信していますか

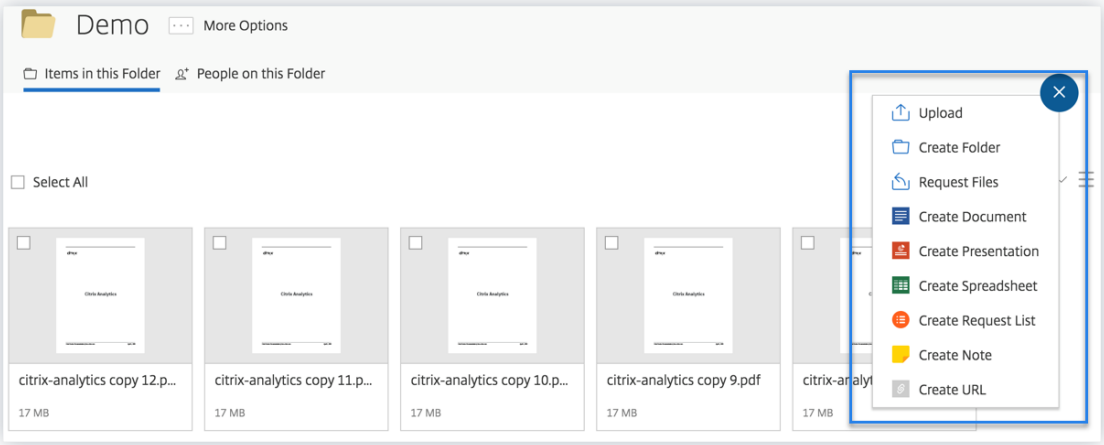
Citrix Analytics は、ユーザーがデータソースをアクティブに使用しているときに、データソースからユーザーイベントを受信します。ユーザーは、イベントを生成するために、データソースに対して何らかのアクティビティを実行する必要があります。たとえば、Apps and Desktops データソースからイベントを受信するには、Apps and Desktops ユーザーは一部のファイルを共有、アップロード、またはダウンロードする必要があります。

> 注
>
> Citrix Analytics は、お客様の環境から積極的にデータを取得しません。

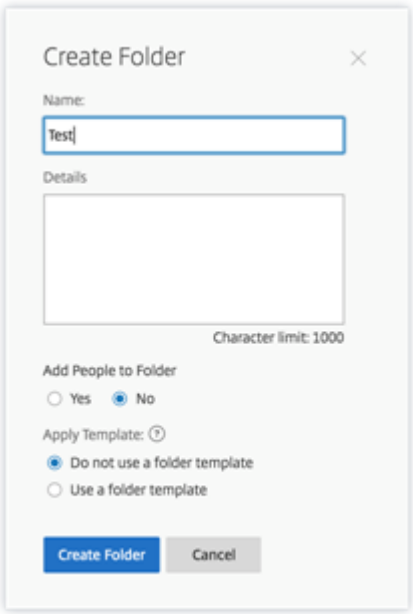
Citrix Analytics でデータソースのユーザーイベントが表示されない場合、その時点でユーザーがアクティブではない可能性が高くなります。

Citrix Analytics がユーザーイベントを正確に受信したことを確認するには、次のアクティビティを実行します。このアクティビティでは、Citrix アプリとデスクトップのデータソースを使用します。サブスクリプションに基づいて、他の Citrix 製品（データソース）を使用して同様のアクティビティを実行できます。

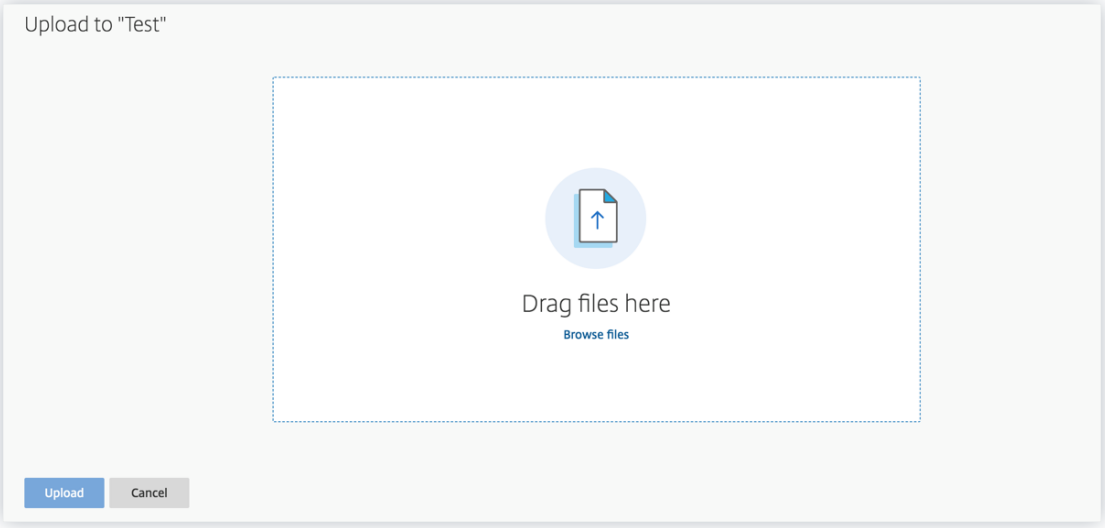
1. Citrix アプリとデスクトップサービスにログオンします。
2. フォルダーの作成、ファイルのダウンロード、ファイルのアップロード、ファイルの削除など、通常のユーザーアクティビティを実行します。



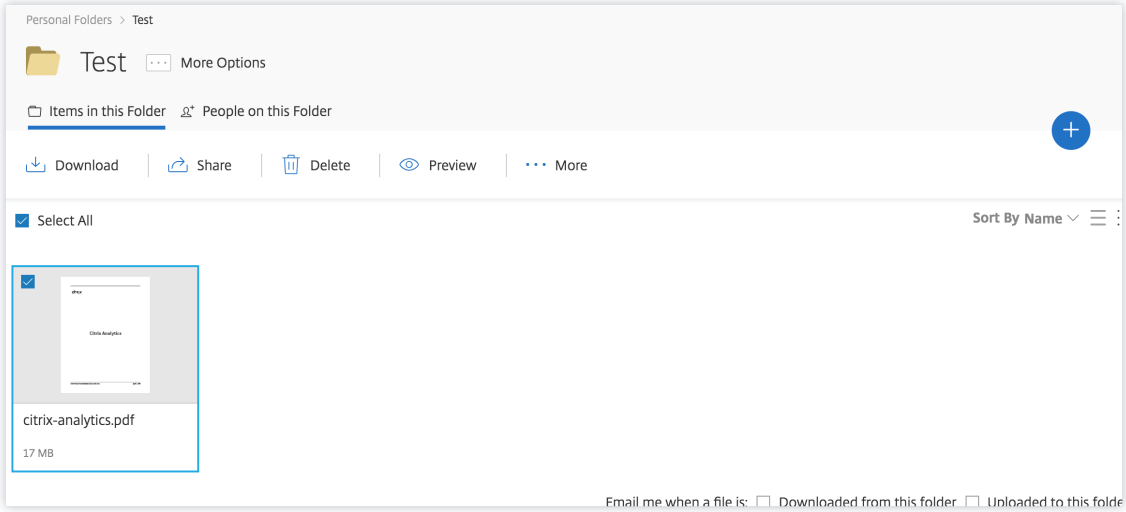
3. たとえば、Test フォルダーを作成します。



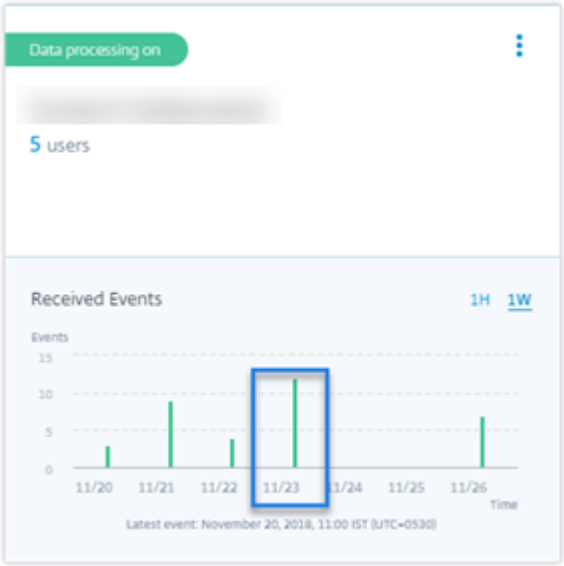
4. ローカルファイルをいくつかアップロードします。



5. フォルダ内のファイルをいくつか削除します。



6. Citrix Analytics に戻り、［データソース］ページの［アプリとデスクトップ］サイドカードを確認します。Citrix Analytics は、アプリとデスクトップのデータソースからユーザーイベントを受信し、サイトカードに表示します。



チェック **6:** 仮想アプリケーションとデスクトップのイベントは **Analytics** に送信されますか**?**

一部のバージョンの Citrix Workspace アプリまたは Citrix Receiver クライアントは、ユーザーイベントを Citrix Analytics に送信できません。ユーザーがこれらのクライアントを介して仮想アプリケーションやデスクトップを起動すると、サポートされているイベントが実行されるまで、Citrix Analytics はユーザーを検出できません。

たとえば、Linux 2006 以降の Citrix Workspace アプリは、**SaaS アプリケーションの起動イベントと SaaS アプリケーション終了イベントを Citrix** Analytics に送信しません。Linux 向け Citrix Workspace アプリを使用して SaaS アプリを起動したユーザーは、Citrix Analytics では検出されません。

サポートされるイベント

各クライアントバージョンでサポートされるユーザーイベントを確認するには、次の表を参照してください。

- はい-イベントはクライアントから Citrix Analytics に送信されます。
- いいえ-イベントはクライアントから Citrix Analytics に送信されません。
- **NA**-イベントはクライアントには適用されません。

イベント	Windows 1907 以降用のワークスペースアプリ	Mac 向け Work-space アプリ 1910.2 以降	Linux 2006 以降用のワークスペースアプリ	Android 用ワークスペースアプリ-Google Play で利用可能な最新バージョン	iOS 用ワークスペースアプリ-Apple App Store で入手可能な最新バージョン	Chrome 用ワークスペースアプリ-Chrome Web Store で入手可能な最新バージョン	HTML5 2007 以降用のワークスペースアプリ
アカウントログオン	はい	はい	はい	はい	はい	番号	番号
セッションログオン	はい	はい	はい	はい	はい	はい	はい
セッションの起動	はい	はい	はい	はい	はい	はい	はい
セッション終了	はい	はい	はい	はい	はい	はい	はい
アプリ開始	はい	はい	はい	番号	はい	はい	はい
アプリ終了	はい	はい	はい	番号	はい	はい	はい
ファイルのダウンロード	はい	はい	はい	番号	番号	はい	はい
印刷	番号	はい	はい	番号	番号	はい	はい
SaaS アプリケーションの起動	はい	はい	番号	番号	番号	番号	番号
SaaS アプリ終了	はい	はい	番号	番号	番号	番号	番号

イベント	Windows 1907 以降用のワークスペースアプリ	Mac 向け Work-space アプリ 1910.2 以降	Linux 2006 以降用のワークスペースアプリ	Android 用ワークスペースアプリ-Google Play で利用可能な最新バージョン	iOS 用ワークスペースアプリ-Apple App Store で入手可能な最新バージョン	Chrome 用ワークスペースアプリ-Chrome Web Store で入手可能な最新バージョン	HTML5 2007 以降用のワークスペースアプリ
SaaS アプリ URL ナビゲーション	はい	はい	番号	番号	番号	番号	番号
SaaS アプリのクリップボードへのアクセス	はい	はい	番号	番号	番号	番号	番号
SaaS アプリファイルのダウンロード	はい	はい	番号	番号	番号	番号	番号
SaaS アプリファイル印刷	はい	はい	番号	番号	番号	番号	番号

イベントの送信状態に基づいて、次の問題が発生する可能性があります。

- ユーザーがクライアントを使用して Citrix Virtual Apps and Desktops または Citrix DaaS に接続すると、サポートされているイベント（アクティビティ）が実行されるまで、Citrix Analytics でユーザーが検出されないことがあります。たとえば、アプリケーションの開始と SaaS アプリケーションの起動という 2 つのユーザーイベントについて考えてみます。iOS 向け Citrix Workspace アプリを使用しているユーザーの場合、Citrix Analytics はアプリケーション開始イベントを受信しますが、SaaS アプリ起動イベントは受信しません。したがって、ユーザーが仮想アプリケーションを起動すると、アプリケーション開始イベントが Citrix Analytics に送信され、ユーザーが検出されます。ただし、ユーザーが SaaS アプリケーションを起動した場合、Citrix Analytics は SaaS アプリケーションの起動イベントを受信せず、ユーザーは検出されません。検出されたユーザの詳細については、検出されたユーザを参照してください。
- テーブルで「いいえ」とマークされたイベントは、セルフサービス検索ページに表示されません。セルフサービスページの使用方法については、「セルフサービス検索について」を参照してください。

推奨

Analytics のメリットを最大限に活用するには、次をお勧めします。

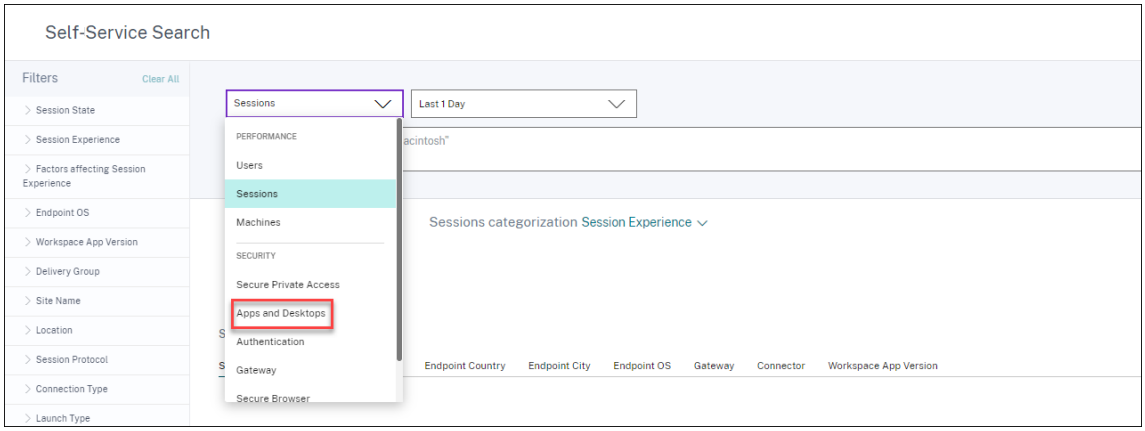
- **Windows** ユーザー: Windows 1907 以降の Citrix Workspace Citrix Virtual Apps and Desktops および Citrix DaaS アプリを使用してに接続します。
- **Mac** ユーザー: **Mac**1910.2 以降の Mac 向け Citrix Citrix Virtual Apps and Desktops および Citrix DaaS Workspace アプリを使用して接続します。

チェック **7-Analytics** のセルフサービス検索ページにユーザーイベントが表示されていますか

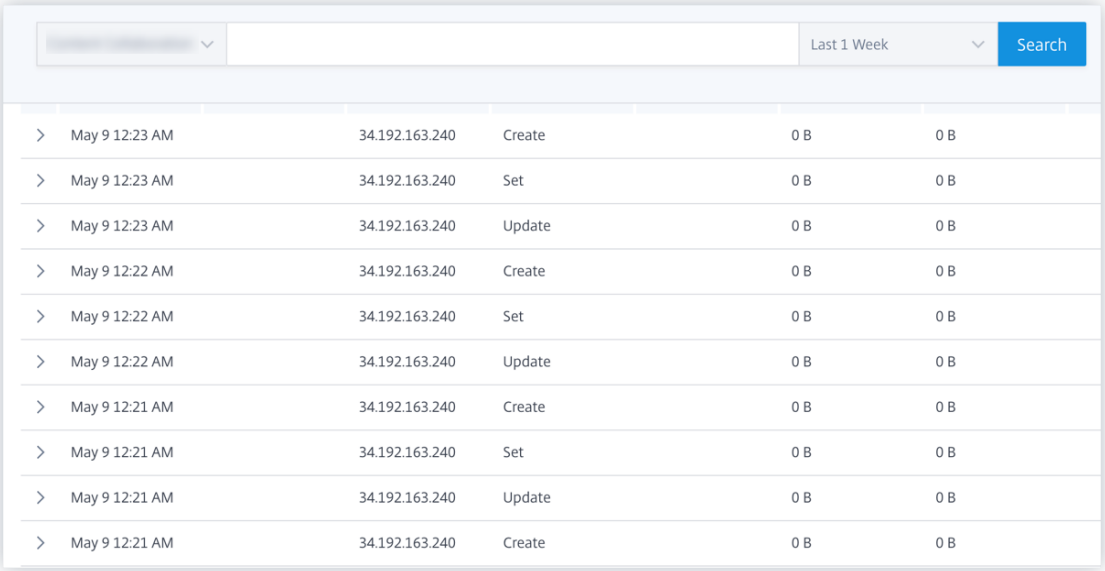
この最終チェックを実行して、イベントが Citrix Analytics に正確に送信されていることを確認します。

1. トップバーの [詳細検索] をクリックして、セルフサービス検索ページに移動します。

2. データソースを選択して、対応する検索ページとイベントを表示します。



3. アプリとデスクトップのイベントに関連するデータを表示するには、リストから **[**** アプリとデスクトップ] を選択し、期間を選択して、[検索] をクリックします。**

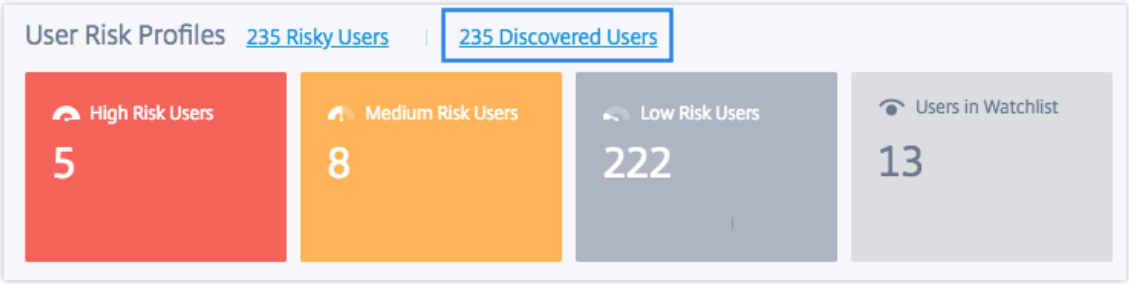


詳細については、「セルフサービス検索」を参照してください。

チェック **8-**ユーザーは **Analytics** によって検出されていますか

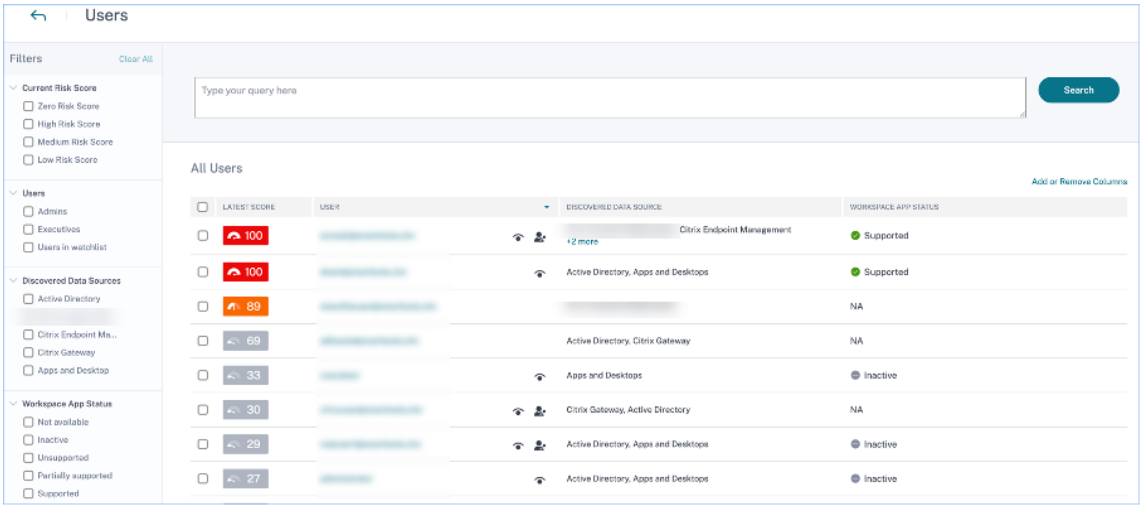
イベントが Citrix Analytics に流れ始めると、イベントを生成したユーザーが検出され、［ユーザー］ダッシュボードに表示されます。このプロセスは、通常、ダッシュボードに表示できるようになるまでに約数分かかります。

1. ［ユーザー］ダッシュボードの［検出されたユーザー **］リンクをクリックすると、Citrix Analytics によって検出されたユーザーの完全なリストが表示されます。



2. ユーザーページには、過去 31 日間に検出されたすべてのユーザーのリストが表示されます。リスク指標の発生を表示する期間を選択します。

> 注:
>
> 31 日を超える値を設定しようとすると、「日付範囲が無効です」というエラーメッセージが表示されます。開始日から終了日までの最大許容範囲は **31** 日です。



イベントが正常に送信されると、Citrix Analytics 環境は期待どおりに動作しています。リスク指標は、異常が検出されたときに生成されます。

Virtual Apps and Desktops イベント、**SaaS** イベントのトリガー、およびイベント送信の検証

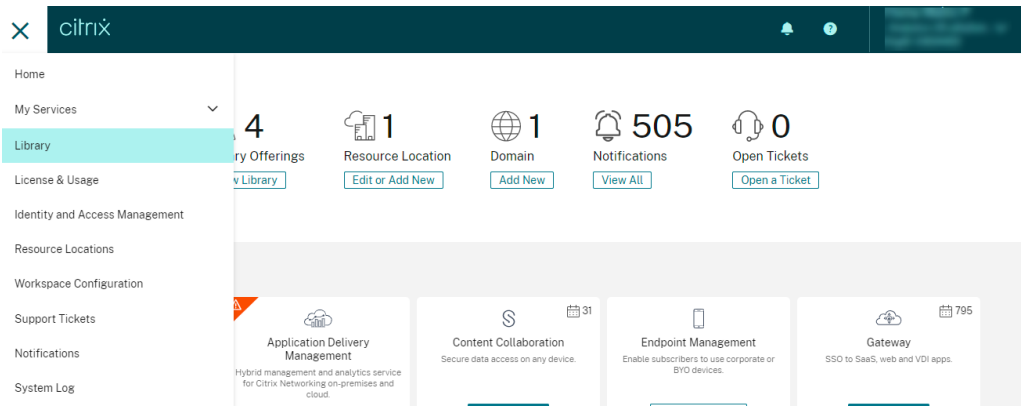
April 12, 2024

このセクションでは、アプリとデスクトップのイベント、SaaS イベントをトリガーし、Citrix Analytics for Security がこれらのユーザーイベントをアクティブに受信していることを確認する手順について説明します。

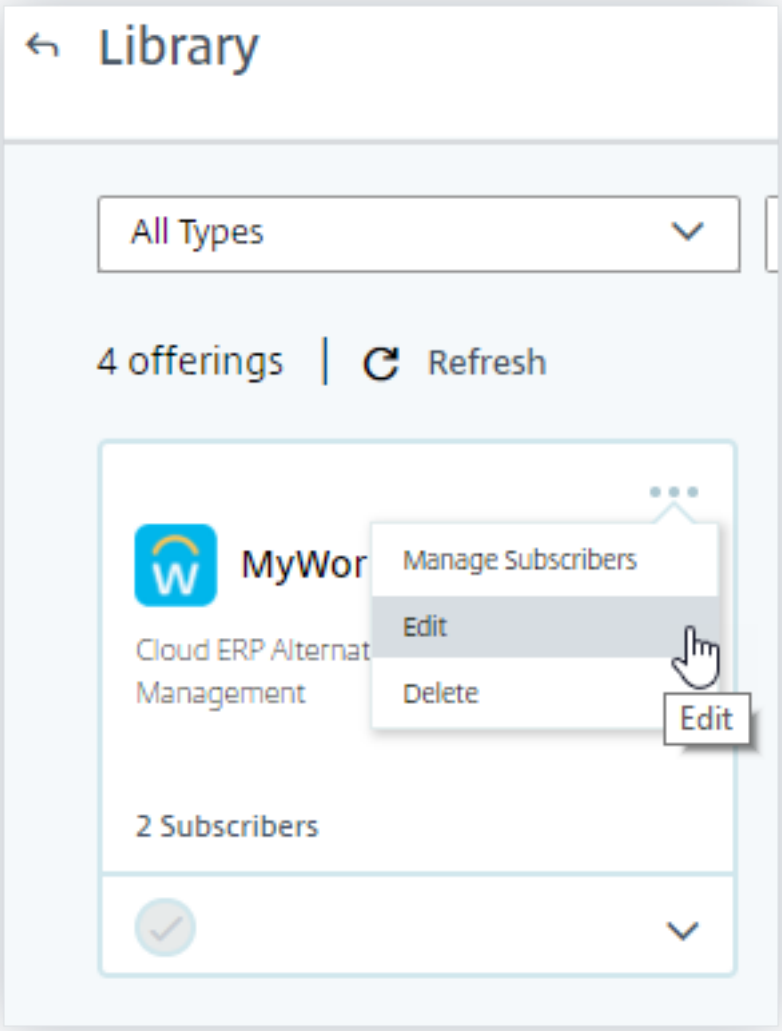
前提条件

- オンプレミスを使用している場合は Citrix Virtual Apps and Desktops、オンプレミスサイトを Citrix Analytics にオンボーディングし、サイトカードからデータ処理を有効にします。Citrix DaaS（以前の Citrix Virtual Apps and Desktops サービス）を使用している場合は、サイトカードから直接データ処理を有効にします。詳しくは、「Citrix Virtual Apps and Desktops」および「Citrix DaaS データソース」を参照してください。
- イベントが Citrix Analytics に正確に送信されるように、ユーザーのエンドポイントデバイスで正しいバージョンの Citrix Workspace アプリまたは Citrix Receiver を使用します。詳しくは、「Citrix Virtual Apps and Desktops」および「Citrix DaaS データソース」を参照してください。
- 仮想デスクトップから印刷イベントをトリガーする前に、アプリとデスクトップ環境でプリンターが構成およびプロビジョニングされていることを確認します。プリンタの管理について詳しくは、「印刷」を参照してください。

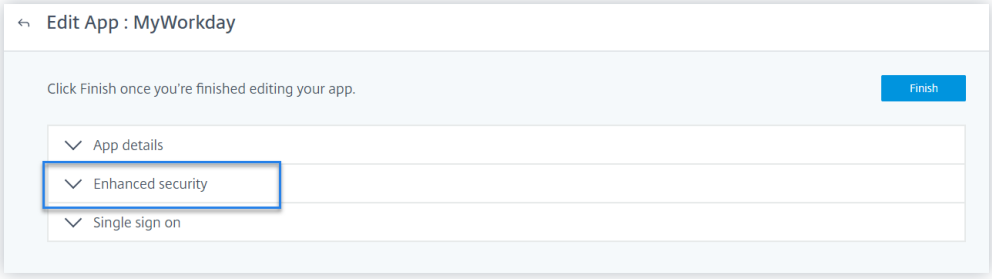
- SaaS アプリケーションの起動、SaaS アプリケーション URL ナビゲーション、SaaS アプリケーションファイルのダウンロードなどの SaaS イベントをトリガーするには、Workspace から構成された SaaS アプリを使用する必要があります。一般的に使用される SaaS アプリケーションには、Salesforce、Workday、Concur、GoTo ミーティングなどがあります。
  - 構成済みの SaaS アプリがない場合は、SaaS アプリを構成して公開する必要があります。詳細については、「サービスとしてのソフトウェアアプリのサポート」を参照してください。SaaS アプリケーションを構成するときは、次のセキュリティオプションが無効になっていることを確認します。
    * クリップボードへのアクセスを制限する
    * 印刷を制限
    * ナビゲーションを制限する
    * ダウンロードを制限する
  - Workspace から設定済みの SaaS アプリを使用してイベントをトリガーする場合は、SaaS アプリに対して指定した拡張セキュリティオプションが無効になっていることを確認します。
    1. Citrix Cloud アカウントに移動し、［ライブラリ］を選択します。



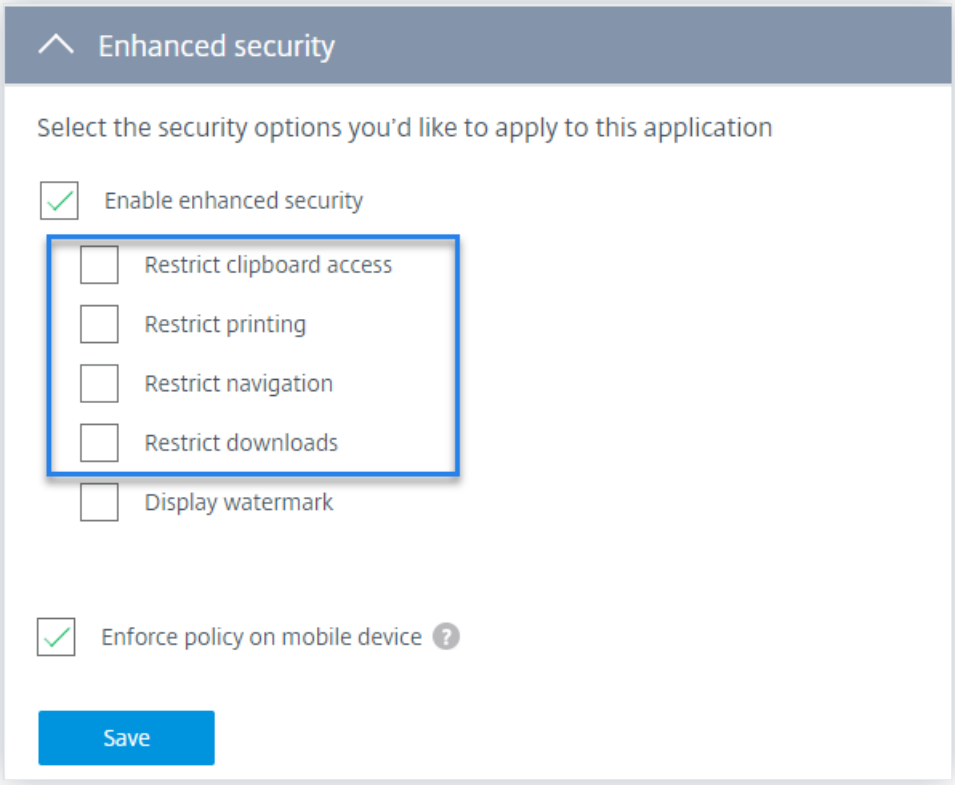
    2. [ライブラリ] ページで、イベントの検証に使用する SaaS アプリを特定します。たとえば、Workday と入力します。
    3. 楕円をクリックし、[編集] を選択します。



4. [アプリケーションの編集] ページで、[強化されたセキュリティ] の下矢印をクリックします。



5. 次のセキュリティオプションが選択されていないことを確認します。



既知の問題

一部のバージョンの Citrix Workspace アプリと Citrix Receiver では、一部のイベントを Citrix Analytics に送信できませんしたがって、Citrix Analytics は、これらのイベントに関する洞察を提供したり、リスク指標を生成したりすることはできません。この問題とその回避策の詳細については、既知の問題である CAS-16151を参照してください。

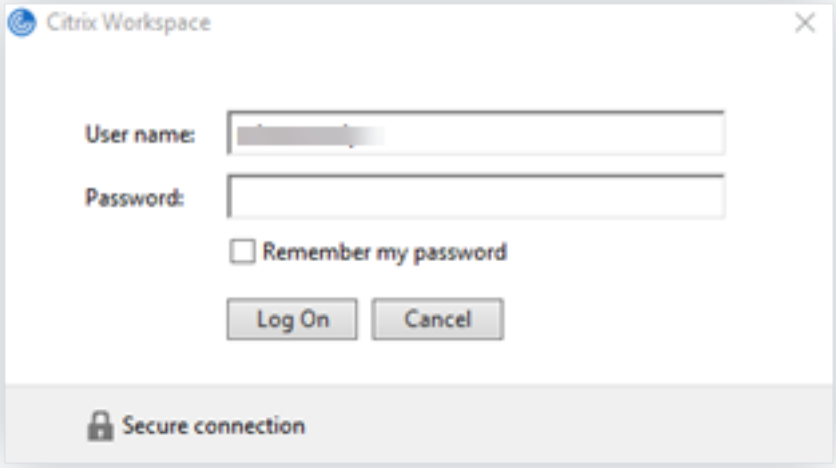
手順

次の手順を順番に実行して、アプリとデスクトップ環境でイベントをトリガーし、Citrix Analytics for Security がこれらのイベントをアクティブに受信していることを確認します。

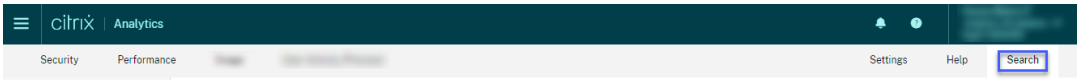
> 注
>
> - イベントが Citrix Analytics に到達するまでに時間がかかる場合があります。トリガーされたイベントが表示されない場合は、［Citrix Analytics］ページを更新します。
> - この手順では、SaaS イベントをトリガーするために、Workday アプリを例として使用します。Workspace から設定済みの任意の SaaS アプリを使用して SaaS イベントをトリガーできます。

- アカウントログオン

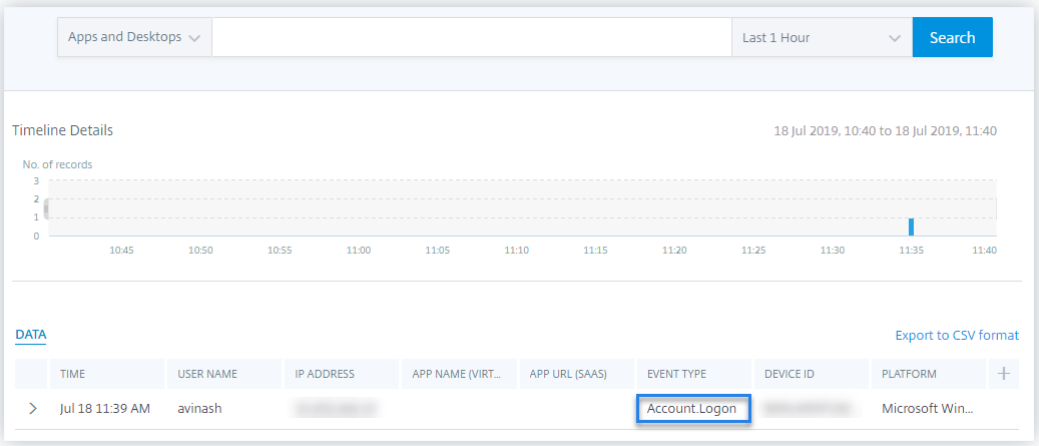
1. Citrix Workspace アプリまたは Citrix Receiver を起動して、ワークスペースまたは StoreFront にアクセスします。
2. 資格情報を入力して、Citrix Workspace アプリまたは Citrix Receiver にログオンします。



3. Citrix Analytics に移動します。
4. [検索] をクリックし、リストから [アプリとデスクトップ] を選択します。



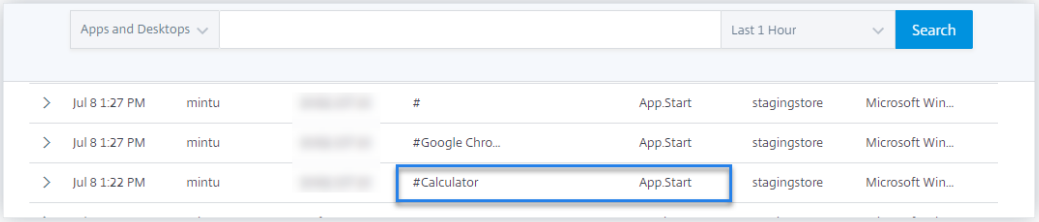
5. 検索ページで、**Account.Logon** イベントのデータを表示します。行を展開して、イベントの詳細を表示します。



- アプリ開始

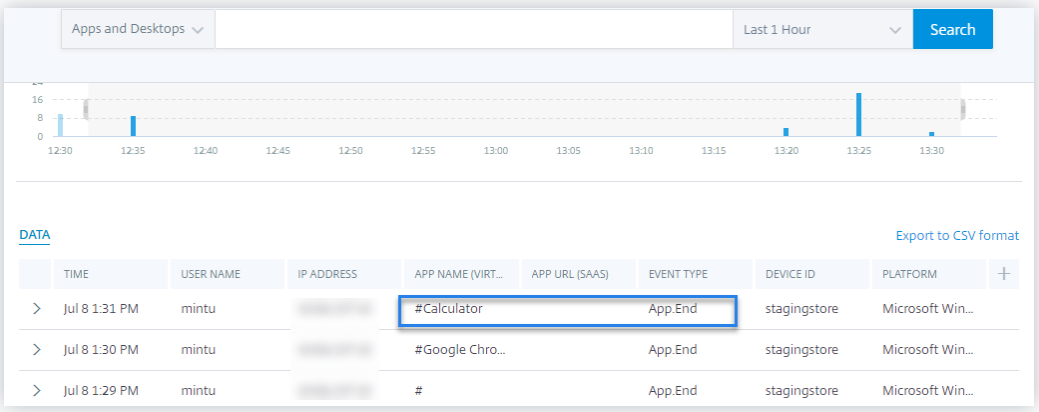
1. Citrix Workspace アプリまたは Citrix Receiver を起動して、ワークスペースまたは StoreFront にアクセスします。

2. 電卓などのアプリケーションを起動します。
3. Citrix Analytics に移動します。
4. [検索] をクリックし、[アプリとデスクトップ] を選択します。
5. 検索ページで、**App.Start** イベントデータのデータを表示します。行を展開して、イベントの詳細を表示します。



- アプリ終了

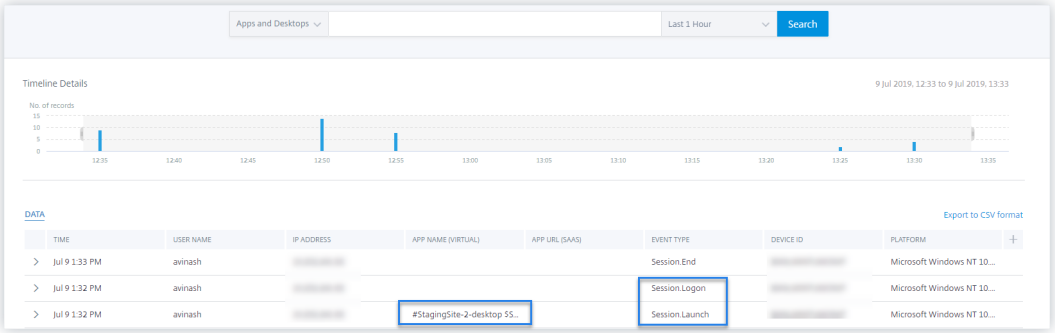
1. ワークスペースまたは StoreFront ですでに起動している計算ツールを閉じます。
2. Citrix Analytics に移動します。
3. [検索] をクリックし、[アプリとデスクトップ] を選択します。
4. 検索ページで、**App.End** イベントデータのデータを表示します。行を展開して、イベントの詳細を表示します。



- セッションログオンとセッション起動

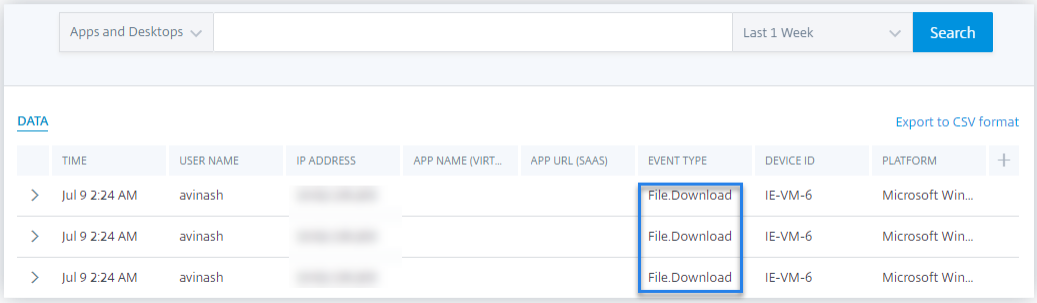
1. Citrix Workspace アプリまたは Citrix Receiver を起動して、ワークスペースまたは StoreFront にアクセスします。
2. 仮想デスクトップを起動します。
3. Citrix Analytics に移動します。
4. [検索] をクリックし、[アプリとデスクトップ] を選択します。

5. 検索ページで、**Session.Logon** および Session.Launch** イベントのデータを表示します。行を展開して、イベントの詳細を表示します。



- ファイルのダウンロード

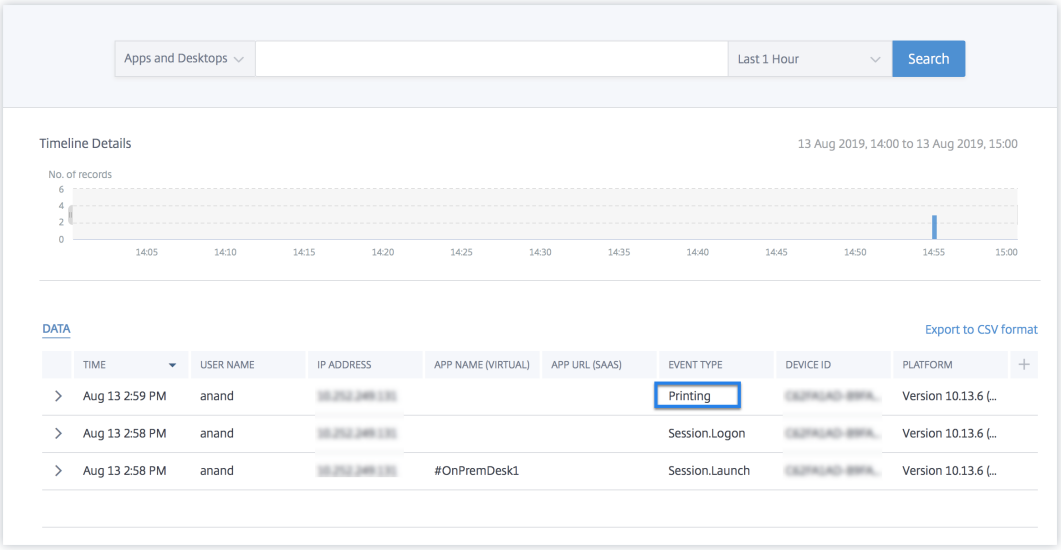
1. Citrix Workspace アプリまたは Citrix Receiver を起動して、ワークスペースまたは StoreFront にアクセスします。
2. 仮想デスクトップを起動します。
3. 仮想デスクトップからローカルコンピュータにファイルをコピーします。
4. Citrix Analytics に移動します。
5. [検索] をクリックし、[アプリとデスクトップ] を選択します。
6. 検索ページで、**File.Download** イベントのデータを表示します。行を展開して、イベントの詳細を表示します。



- 印刷

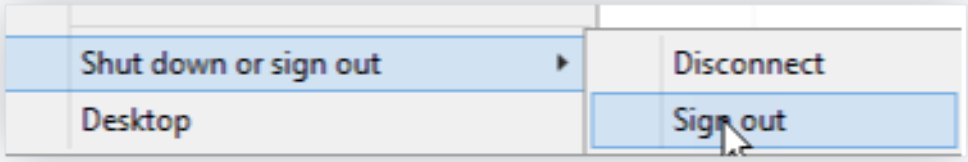
1. Citrix Workspace アプリまたは Citrix Receiver を起動してワークスペースにアクセスします。
2. 仮想デスクトップを起動します。
3. 仮想デスクトップで構成されたプリンタを使用して、ドキュメントを印刷します。
4. Citrix Analytics に移動します。
5. [検索] をクリックし、[アプリとデスクトップ] を選択します。

6. [検索] ページで、**Printing** イベントのデータを表示します。行を展開して、イベントの詳細を表示します。

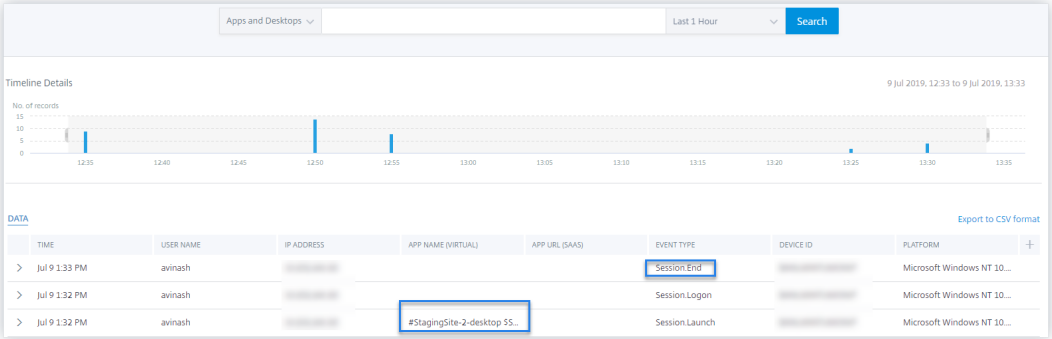


- セッション終了

1. 仮想デスクトップからサインアウトします。たとえば、Windows 仮想デスクトップを使用している場合は、[サインアウト] オプションを選択します。



2. Citrix Analytics に移動します。
3. [検索] をクリックし、[アプリとデスクトップ] を選択します。
4. 検索ページで、**Session.End** イベントのデータを表示します。行を展開して、イベントの詳細を表示します。

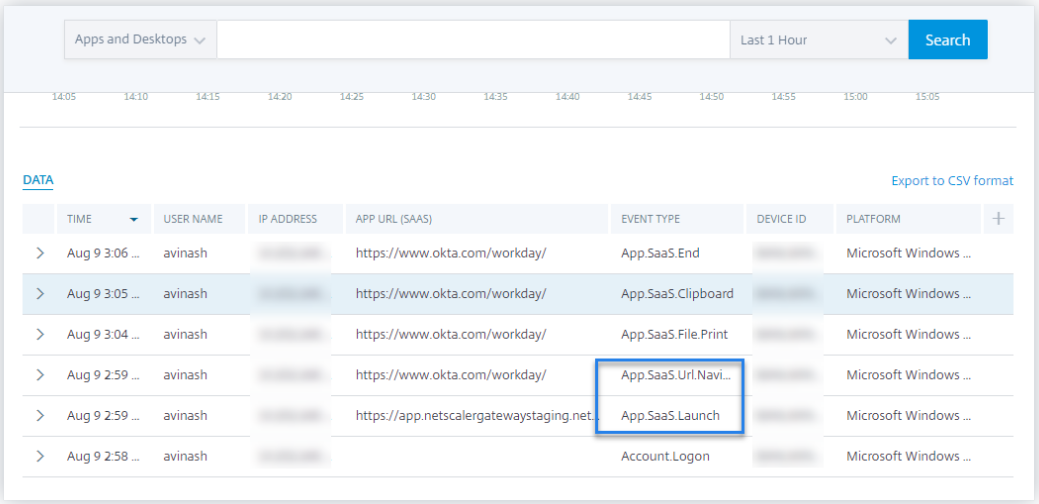


- **SaaS** アプリケーションの起動と **SaaS** アプリケーション **URL** ナビゲーション

  1. Citrix Workspace アプリまたは Citrix Receiver を起動して、ワークスペースまたは StoreFront にアクセスします。
  2. Workday などの SaaS アプリケーションを起動し、[Workday] ページが読み込まれるまで待ちます。Workday の Web ページ内を移動します。

     > 注
     >
     > [セキュリティの強化] セクションの [ナビゲーションの制限] オプションが無効になっていることを確認します。詳細については、「前提条件」を参照してください。

  3. Citrix Analytics に移動します。
  4. [検索] をクリックし、[アプリとデスクトップ] を選択します。
  5. 検索ページで、**app.saas.Launch** イベントと app.saas.url.Navigation** イベントのデータを表示します。行を展開して、イベントの詳細を表示します。



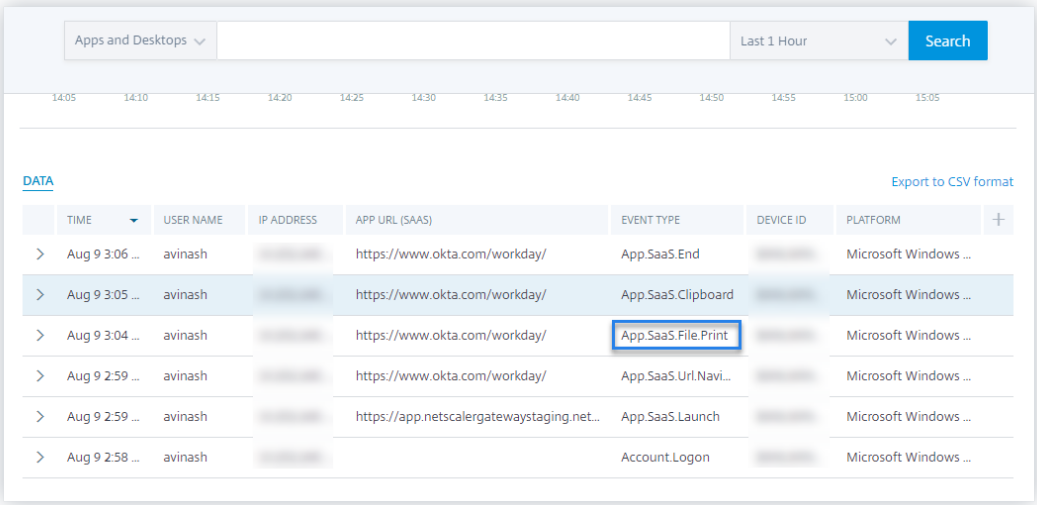
- **SaaS** アプリファイル印刷

  1. 現在表示している [Workday] ページを印刷します。

     > 注
     >
     > [セキュリティの強化] セクションの [印刷を制限する] オプションが無効になっていることを確認します。詳細については、「前提条件」を参照してください。

  2. Citrix Analytics に移動します。
  3. [検索] をクリックし、[アプリとデスクトップ] を選択します。

4. 検索ページで、**app.Saas.File.Print** イベントのデータを表示します。行を展開して、イベントの詳細を表示します。

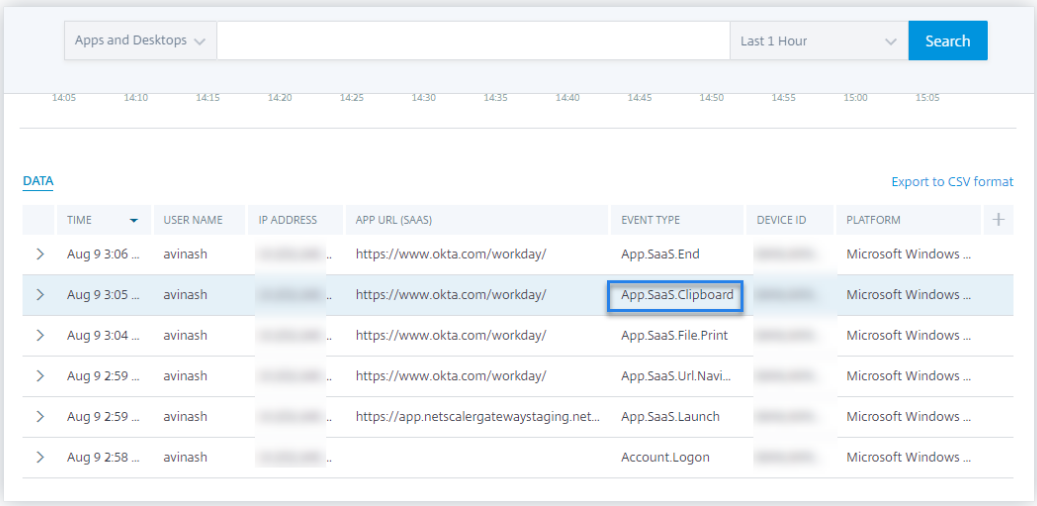


- **SaaS** アプリのクリップボードへのアクセス

1. [Workday] ページから、テキストをシステムのクリップボードにコピーします。

> 注
>
> [セキュリティの強化] セクションの [クリップボードへのアクセスを制限する] オプションが無効になっていることを確認します。詳細については、「前提条件」を参照してください。

2. Citrix Analytics に移動します。
3. [検索] をクリックし、[アプリとデスクトップ] を選択します。
4. 検索ページで、**app.SaaS.Clipboard** イベントのデータを表示します。行を展開して、イベントの詳細を表示します。

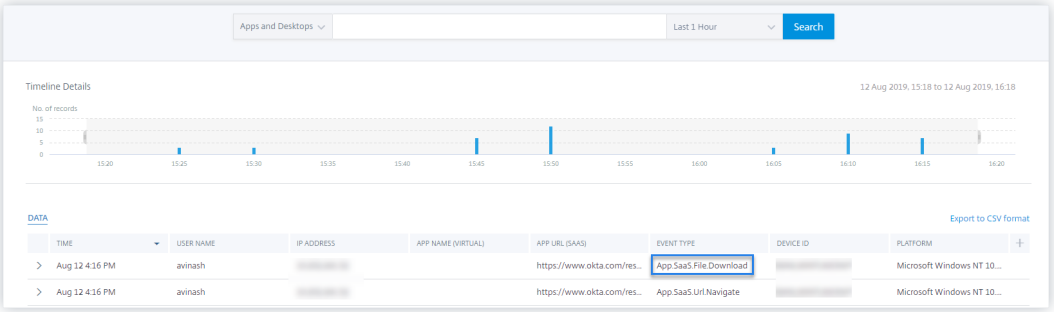


- **SaaS** アプリファイルのダウンロード

  1. [Workday] ページで、ホワイトペーパーなどの公開ドキュメントを検索し、そのドキュメントをダウンロードします。

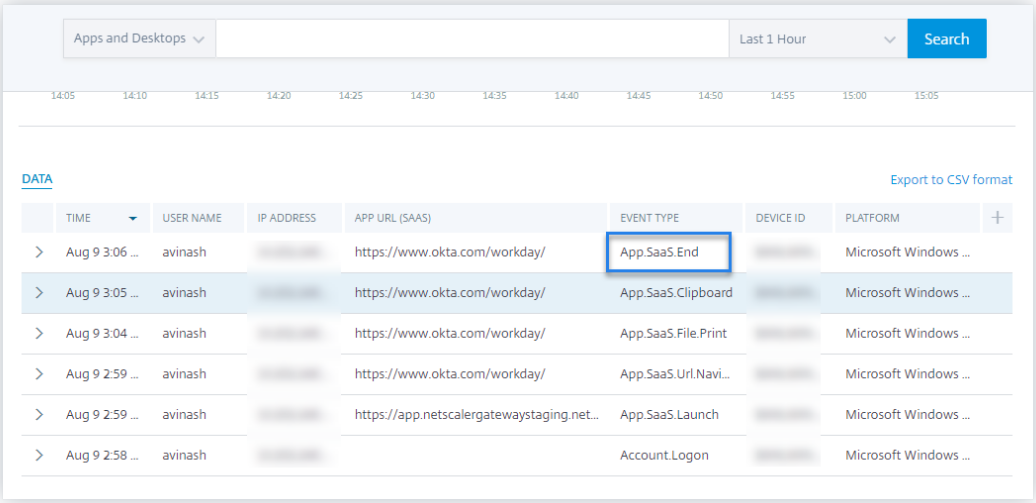
     > 注
     >
     > [セキュリティの強化] セクションの [ダウンロードを制限する] オプションが無効になっていることを確認します。詳細については、「前提条件」を参照してください。

  2. Citrix Analytics に移動します。
  3. [検索] をクリックし、[アプリとデスクトップ] を選択します。
  4. [検索] ページで、**app.saas.file.Download** イベントのデータを表示します。行を展開して、イベントの詳細を表示します。



- **SaaS** アプリ終了

  1. [Workday] ページを閉じます。
  2. Citrix Analytics に移動します。
  3. [検索] をクリックし、[アプリとデスクトップ] を選択します。
  4. 検索ページで、**App.Saas.End** イベントのデータを表示します。行を展開して、イベントの詳細を表示します。



- **VDA.Print**

  前提条件

  印刷イベントをトリガーする前に、「Citrix DaaS の印刷テレメトリの有効化」を参照してください。

  印刷イベントをトリガーするには、次のアクションを実行します。

  1. テキストドキュメントをメモ帳または印刷が許可されているその他のアプリで開きます。
  2. [ファイル] **>** [印刷] をクリックするか、**Ctrl+P** を押します。
  3. [プリンタの選択] でプリンタを選択し、[適用] をクリックして印刷します。

- **VDA** クリップボード

  前提条件

  印刷イベントをトリガーする前に、「Citrix DaaS のクリップボードテレメトリの有効化」を参照してください。

  クリップボードイベントをトリガーするには、次のアクションを実行します。

  1. メモ帳または任意のテキストエディタでテキストドキュメントを開きます。
  2. コピーするコンテンツを選択します。
  3. [コピー] を右クリックするか、Ctrl+C を押します。

構成された **Session Recording** サーバーが接続に失敗する

July 15, 2022

構成後、Session Recording サーバーが Citrix Analytics に接続できない。したがって、**Session Recording** サイトカードに構成済みのサーバーが表示されません。

この問題のトラブルシューティングを行うには、次の操作を行います。

1. 設定した Session Recording サーバーで、次の PowerShell コマンドを実行して、クライアントマシン識別 (CMID) を確認します。

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

2. CMID が空の場合、指定したパスに次のレジストリファイルを追加します。

レジストリ名	レジストリのパス	キー型	値
AuditorUniqueID	Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\	文字列	UUID を入力します。
EnableCASUseAuditorUniqueID	Computer/HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/SmartAuditor/Server/	REG_DWORD	1

3. 次のサービスを再起動します:

   - Citrix Session Recording Analytics サービス
   - Citrix Session Recording ストレージマネージャー

Splunk 用 Citrix Analytics アドオンの設定に関する問題

July 15, 2022

Citrix Analytics アドオン設定を使用できません

Splunk Forwarder または Splunk スタンドアロン環境に Splunk 用 Citrix **Analytics** アドオンをインストールした後、**[設定] > [データ入力]** に **[Citrix Analytics アドオン]** 設定が表示されません。

理由

この問題は、サポートされていない Splunk 環境に Splunk 用 Citrix Analytics アドオンをインストールすると発生します。

解決された問題

サポートされている Splunk 環境に Splunk 用 Citrix Analytics アドオンをインストールします。サポートされるバージョンの詳細については、「Splunk 統合」を参照してください。

Splunk ダッシュボードにはデータがありません

Splunk Forwarder または Splunk スタンドアロン環境に Splunk 用 Citrix Analytics アドオンをインストールして構成すると、Splunk ダッシュボードにシトリックスアナリティクスからのデータが表示されません。

チェック

この問題のトラブルシューティングを行うには、Splunk Forwarder または Splunk スタンドアロン環境で以下を確認します。

1. Splunk 統合の前提条件が満たされていることを確認します 。
2. ［設定］**>** ［データ入力］**>** ［**Citrix Analytics** アドオン］Citrix Analytics の構成の詳細が利用可能であることを確認します 。
3. 構成の詳細が利用できる場合は、次のクエリを実行して、SSplunk 向け Citrix Analytics アドオンに関連するエラーがないかログを確認します。

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

4. エラーが見つからない場合、SSplunk 向け Citrix Analytics アドオンは期待どおりに動作しています。ログにエラーが見つかった場合は、次のいずれかの原因が考えられます。

   - Splunk 環境と Citrix Analytics Kafka エンドポイント間の接続を確立できませんでした。この問題は、ファイアウォールの設定が原因である可能性があります。

     修正方法: この問題を解決するには、ネットワーク管理者に問い合わせてください。

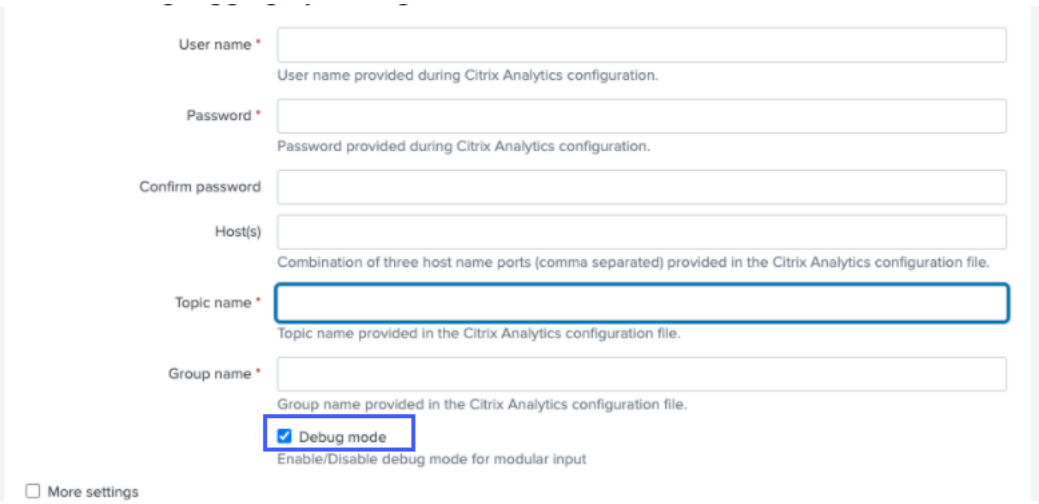
   - ［設定］**>** ［データ入力］**>** ［**Citrix Analytics** アドオン］の構成の詳細

     修正：ユーザー名、パスワード、ホストエンドポイント、トピック、コンシューマーグループなどの Citrix Analytics 構成の詳細が、Citrix Analytics 構成ファイルに従って正しく入力されていることを確認します。詳しくは、「Splunk 用の Citrix Analytics アドオンを構成する」を参照してください。

5. 前述のログから問題の原因が見つからず、さらに調査する場合は、次の手順を実行します。

   a) 設定］**>**［データ入力］**>**［**Citrix Analytics** アドオン］でデバッグモードを有効にします

   > 注
   >
   > デフォルトでは、**Debug** モードは無効になっています。このモードを有効にすると、生成されるログが多すぎます。したがって、このオプションは必要な場合にのみ使用し、デバッグタスクが完了したら無効にしてください。



   b) 生成されたデバッグログを次の場所で探し、エラーがないか確認します。

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

   c) (オプション)Splunk 用 Citrix Analytics `splunk cmd python cas_siem_consumer_debug.py` アドオンで使用できるデバッグスクリプトを使用します。このスクリプトは、Splunk 環境と接続チェックの詳細を含むログファイルを生成します。この詳細を使用して、問題をデバッグできます。以下のコマンドを使用してスクリプトを実行します。

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

エラーメッセージ

Splunk 用 Citrix Analytics アドオンに関連するログに、次のエラーが表示される場合があります。

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

このエラーは、ネットワーク接続の問題または認証の問題が原因で発生します。

この問題をデバッグするには、次の手順を実行します。

1. Splunk Forwarder または Splunk スタンドアロン環境で、デバッグモードを有効にしてデバッグログを取得します。前のステップ 5.a を参照してください。
2. 次のクエリを実行して、デバッグログで認証の問題を検出します。

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

3. デバッグログに認証の問題が見つからない場合、エラーはネットワーク接続の問題が原因です。
4. telnet または前のステップ 5.c で説明したデバッグスクリプトを使用して、問題を検出して解決します。

2.0.0 より前のバージョンからのアドオンのアップグレードが失敗する

Splunk Forwarder または Splunk スタンドアロン環境で、Splunk 用 Citrix Analytics アドオンを 2.0.0 より前のバージョンから最新バージョンにアップグレードすると 、アップグレードが失敗します。

解決された問題

1. Citrix Analytics Splunk /bin アドオンインストールフォルダーのフォルダー内にある以下のファイルとフォルダーを削除します。
   - cd $SPLUNK_HOME$/etc/apps/TA_CTXS_AS/bin
   - rm -rf splunklib
   - rm -rf mac
   - rm -rf linux_x64
   - rm CARoot.pem
   - rm certificate.pem
2. Splunk フォワーダまたは Splunk スタンドアロン環境を再起動します。

StoreFront サーバーを **Citrix Analytics** と接続

January 5, 2023

Citrix Analytics から StoreFront サーバーに構成設定をインポートすると、StoreFront サーバーは Citrix Analytics への接続に失敗します。

StoreFront サーバーに構成設定をインポートする方法については、「StoreFront を使用した Virtual Apps and Desktops サイトのオンボード」を参照してください。

CAS Onboarding Assistant は、この記事で説明されている問題の確認とトラブルシューティングに役立ちます。詳しくは、「Citrix Analytics サービス（CAS）オンボーディングアシスタント」を参照してください。

この問題のトラブルシューティングを行うには、次の操作を行います。

1. StoreFront サーバーで、Citrix Analytics 地域固有のエンドポイントに ping を実行して 、StoreFront サーバーと Citrix Analytics サーバー間の接続をテストします。また、前提条件が満たされていることを確認します 。

   > 注
   >
   > StoreFront サーバーでは、地域固有のエンドポイントに直接 ping を実行するか、Web ブラウザーを開いて地域固有のエンドポイントにアクセスすることで、接続をテストできます。

2. StoreFront サーバーで詳細ログを有効にして、ログをトレースします。詳細ロギングについて詳しくは、CTX139592 の記事を参照してください。
3. インターネットインフォメーションサービス (IIS) マネージャを開き、次の点を確認します。
   - StoreFront サイトが IIS のデフォルトサイトの下にある場合、IIS は StoreFront サイトを再起動します。
   - StoreFront サイトが他のドライバーにあるか、デフォルトサイトにない場合は、コマンドウィンドウを開いて次のように入力します `iisreset`。
4. 次のコマンドを実行して、Citrix Analytics の設定をインポートします。

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

5. 次のコマンドを実行して、インポートした設定を確認します。

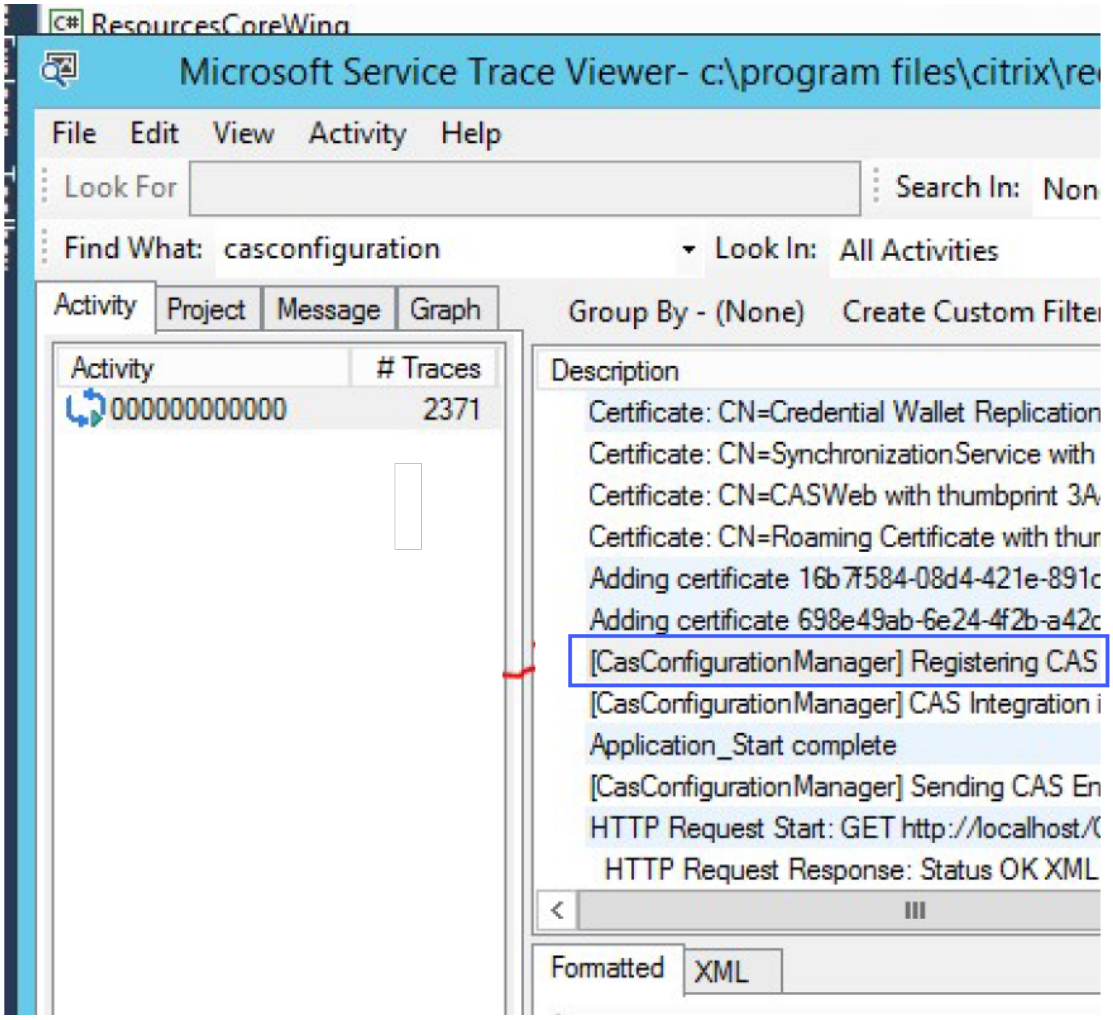
   ```
   1 Get-STFCasConfiguration
   ```

6. StoreFront サイトが他のドライバー内にあるか、デフォルトサイトの下にない場合は、コマンドウィンドウを開きます。StoreFront サイトに Citrix Analytics の設定を読み取らせるには `iisreset` を入力します
7. StoreFront の詳細ログファイルを次の場所から取得します。

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

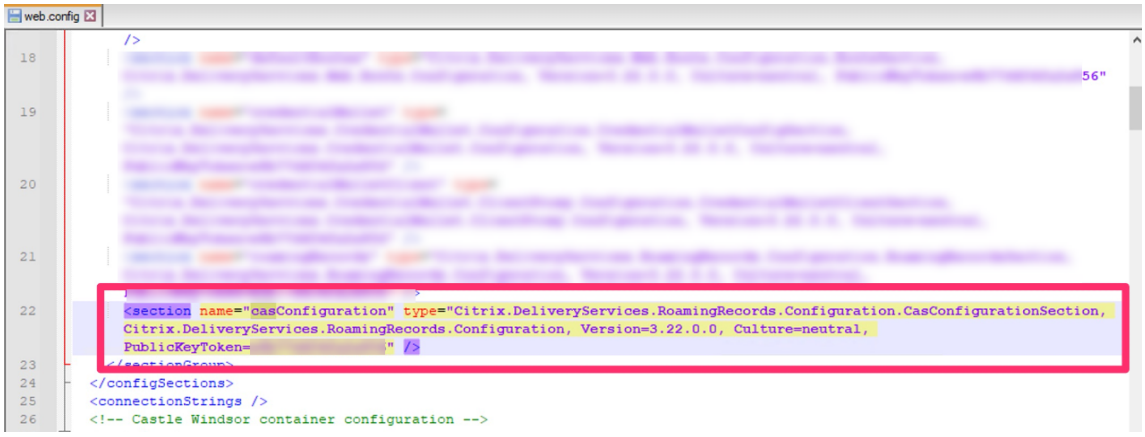
   上記の場所には、イベントビューアで開くことができる複数の svclog ファイルがあります。
8. Microsoft サービストレースビューアを使用して、次のログを開きます。
   - StoreFront ログ
   - ローミングサイトの詳細ログ

9. ログで、**CASConfigurationManager** セクションと Citrix Analytics サーバー情報が利用可能であることを確認します。



10. CASConfigurationManager セクションが使用できない場合は、にあるローミングサイトの web.config `roaming site\folder`ファイルを開きます。

11. `web.config` ファイルで［**CASConfiguration**］セクションを探し、Citrix Analytics サーバーの情報が利用可能であることを確認します。



12. StoreFront サーバーがインストールされている Windows サーバーマシンで、以下を確認します。

    - TLS 1.2 クライアントは有効になっています。
    - 次の暗号スイートのうち少なくとも 1 つが有効になっている。
        - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
        - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
        - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
        - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

    TLS 暗号スイートの順序を設定する方法については、Microsoft のドキュメントを参照してください。

13. Windows Server 2012 マシンを使用している場合は、Diffie-Hellman Exchange (ECDHE/DHE) が有効になっていることを確認します。

14. StoreFront サーバーがインストールされている Windows Server マシンに、Microsoft のドキュメントに記載されているレジストリ設定が含まれている必要があることを確認します。

    > 重要
    >
    > : グループポリシーを使用して TLS/SSL 暗号スイートを更新します。TLS/SSL 暗号スイートを手動で変更しないでください。グループポリシーの使用方法の詳細については、Microsoft のドキュメントを参照してください。

    たとえば、Windows Server マシンで次のレジストリ設定を使用できる必要があります。

    TLS 1.2 クライアント**:**

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

```



```
<!--NeedCopy-->
```

Diffie-Hellman KEAs:

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

<!--NeedCopy-->
```

AES-128/AES-256 暗号**:**

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

<!--NeedCopy-->
```

SHA256/SHA384 ハッシュ**:**

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

<!--NeedCopy-->
```

よくある質問

November 26, 2023

データソース

データソースって何ですか**?**

データソースは、Citrix Analytics にデータを送信する Citrix のサービスおよび製品です。

詳細: データソース

データソースを追加するにはどうすればいいですか

Citrix Analytics にログオンした後、［ようこそ］画面で［はじめに］を選択して、データソースを Citrix Analytics に追加します。または、[設定] **>** [データソース] に移動して、データソースを追加することもできます。

NetScaler ADM エージェント

オンプレミスのハイパーバイザーにエージェントをインストールするための最小リソース要件は何ですか**?**

8 GB RAM、4 仮想 CPU、120 GB ストレージ、1 仮想ネットワークインターフェイス、1 Gbps スループット

プロビジョニング中に **NetScaler ADM** エージェントに追加のディスクを割り当てる必要がありますか

いいえ、ディスクを追加する必要はありません。エージェントは、Citrix Analytics とエンタープライズデータセンターのインスタンスとの間の仲介としてのみ使用されます。追加のディスクを必要とするインベントリや分析データは保存されません。

エージェントにログオンするためのデフォルトの認証情報は何ですか

エージェントにログオンするためのデフォルトの認証情報は`nsrecover`/`nsroot`です。これにより、エージェントのシェルプロンプトにログオンします。

間違った値を入力した場合、エージェントのネットワーク設定を変更するにはどうすればいいですか

ハイパーバイザーのエージェントコンソールにログオンし、資格情報 `nsrecover`/`nsroot`を使用してシェルプロンプトにアクセスし、コマンド`networkconfig`を実行します。

サービス **URL** とアクティベーションコードが必要なのはなぜですか

エージェントは、サービス URL を使用してサービスを検索し、アクティベーションコードを使用してエージェントをサービスに登録します。

エージェントコンソールでサービス **URL** を間違って入力した場合、どうすれば再入力できますか

資格情報`nsrecover`/`nsroot`を使用してエージェントのシェルプロンプトにログオンし、次のように入力します。`deployment_type.py` このスクリプトを使用すると、サービス URL とアクティベーションコードを再入力できます。

新しいアクティベーションコードはどうやって入手できますか

NetScaler ADM サービスから新しいアクティベーションコードを取得できます。NetScaler ADM サービスにログオンし、[ネットワーク**] > [**エージェント] に移動します。[エージェント] ページの **[**アクションの選択**]** リストから、[アクティベーションコードの生成] を選択します。

アクティベーションコードを複数のエージェントで再利用できますか**?**

いいえ、あなたはできません。

NetScaler ADM エージェントはいくつインストールする必要がありますか

エージェントの数は、データセンターのマネージドインスタンスの数と合計スループットによって異なります。Citrix では、各データセンターに少なくとも 1 つのエージェントをインストールすることをお勧めします。

複数の **NetScaler ADM** エージェントをインストールするにはどうすればいいですか

[データソース] ページで、NetScaler Gateway の横にあるプラス（+）記号をクリックし、指示に従って別のエージェントをインストールします。

または、NetScaler ADM GUI にアクセスして [ネットワーク] > [エージェント] に移動し、[エージェントの設定] をクリックして、複数のエージェントをインストールすることもできます。

高可用性セットアップで **2** つのエージェントをインストールできますか**?**

いいえ、あなたはできません。

エージェントの登録に失敗した場合の対処方法

- エージェントがインターネットにアクセスできることを確認します (DNS の設定)。
- アクティベーションコードを正しくコピーしたことを確認してください。
- サービス URL が正しく入力されていることを確認してください。
- 必要なポートが開いていることを確認してください。

登録は成功しましたが、エージェントが正常に動作しているかどうかはどうすればわかりますか

エージェントが正常に動作しているかどうかを確認するには、次の操作を行います。

- エージェントが正常に登録されたら、NetScaler ADM にアクセスし、[ネットワーク**] > [**エージェント] に移動します。このページで検出されたエージェントを表示できます。エージェントが正常に動作している場合、ステータスは緑色のアイコンで示されます。実行中でない場合、状態は赤いアイコンで示されます。
- エージェントのシェルプロンプトにログオンし、`ps -ax | grep mas`と`ps -ax | grep ulfd`コマンドを実行します。次のプロセスが実行中であることを確認します。

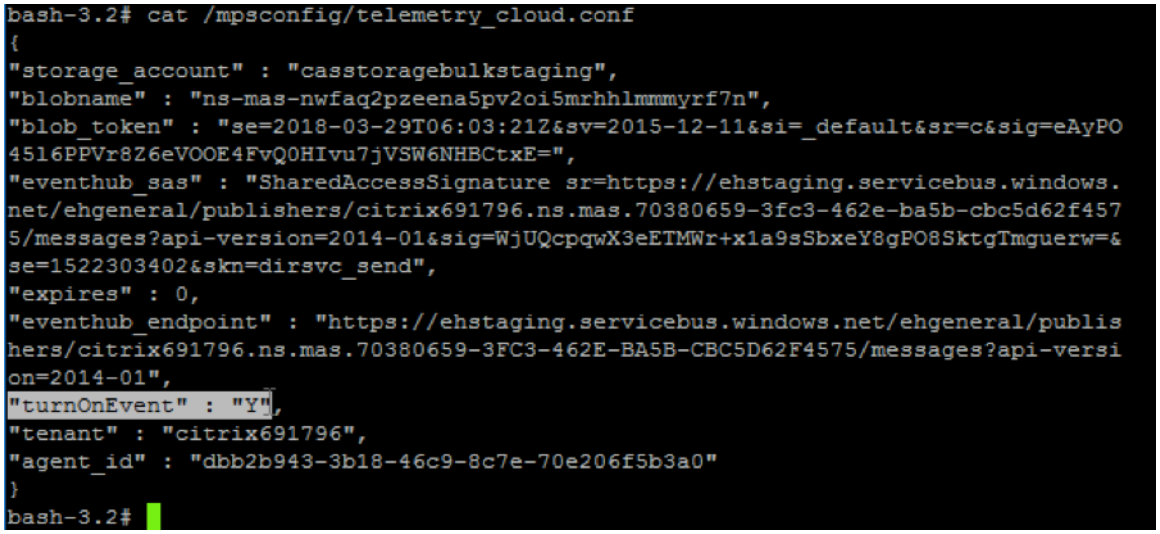
- 実行されていないプロセスがある場合は、コマンド **masd restart** を実行します。すべてのデーモンを起動するには時間がかかる場合があります (1 分程度)。
- エージェントの登録が成功したら、`/mpsconfig`で`agent.conf`が作成されていることを確認してください。

NetScaler Gateway インスタンスのオンボード

NetScaler Gateway インスタンスは **Citrix Analytics** に追加されますが、エージェントで **Analytics** が有効になっているかどうかはどうすればわかりますか

エージェントのシェルプロンプトを使用して、エージェントで分析が有効になっているかどうかを確認できます。エージェントでアナリティクスが正常に有効になっている場合、`turnOnEvent`パラメータは`/mpsconfig/telemetry_cloud.conf`ファイル内で`Y`に設定されます。

エージェントのシェルプロンプトにログオンし、cat `/mpsconfig/telemetry_cloud.conf`コマンドを実行し、`turnOnEvent`パラメータの値を確認します。



誤って **NetScaler Gateway** オンボーディングウィザードを閉じてしまいました。設定は最初から始める必要がありますか

いいえ。Citrix Analytics は進行状況を保存し、［データソース］**>**［設定］ページにタイルとして不完全な構成を表示します。[セットアップを続行] をクリックして設定を完了します。

Virtual Apps and Desktops サイトのオンボーディング

データ処理をオフにするにはどうすればいいですか

サイトから Citrix Analytics へのデータ処理を一時的に無効にする場合は、［サイト］カードをクリックし、［データ処理を無効にする］をクリックします。

自分のサイトを **Workspace** に追加して「**Test STA**」をクリックすると、テストが失敗します。どのように対処すればよいですか**?**

NetScaler Gateway とクラウドコネクタの間に接続の問題がある可能性があります。トラブルシューティングを行うには、Citrixサポート Knowledge Center CTX232517 を参照してください 。

Citrix Analytics のヘルプはどこで入手できますか

https://discussions.citrix.com/forum/1710-citrix-analytics/ にある Citrix Analytics ディスカッションフォーラムで、質問をしたり、Citrix Analytics 専門家と連絡を取ったりすることができます。

フォーラムに参加するには、Citrix ID でサインインする必要があります。

アクセス保証—ジオロケーション

位置情報の詳細は **Analytics** によってどのように導き出されますか

Citrix Analytics は、ワークスペースクライアントが起動されたデバイスの IP アドレスを使用します。Citrix Analytics は、サードパーティの IP 位置情報データプロバイダーを利用して、IP アドレスからユーザーの位置情報を導き出します。セッションログオンを実行すると、ユーザーの場所 (IPv4 アドレス) が国または都市に解決され、マッピングが定期的に更新されます。組織は、国によって定義されたこれらの場所を使用して、ビジネスを行わない場所からのアクセスパターンを監視できます。

ユーザーの位置情報を導き出す精度はどれくらいですか

Citrix Analytics は、サードパーティの IP 位置情報データプロバイダーを利用して、IP アドレスからユーザーの位置情報を導き出します。GeoIP サービスは、ほとんどの場合、適切な都市または場所に解決できますが、GeoIP ルックアップが完全に正確になることはありません。ユーザーに表示されている場所が、アクセスした正確な場所と異なる場合があります。

IP GeoPoint のドキュメントによると、カバレッジレベルは世界中で割り当てられている IP アドレス (IPv4 ルーティング可能な IP アドレス) の約 99.99% です。位置の精度に関しては、必須のロケーションフィールド (国、州、都市、郵便番号) のそれぞれに [信頼係数] が付いています。

位置の決定が不正確になるのはどのような場合ですか

位置情報データの精度は、デバイスがインターネットに接続する方法によって異なります。デバイスは次の方法でインターネットに接続できます。

- モバイルゲートウェイ
- VPN またはホスティング施設
- 地域または国際的なプロキシ/アノニマイザーサーバー

このような場合、IP ジオロケーションプロバイダソフトウェアを使用しても、ジオロケーションデータは正確ではありません。

サポートされている **Citrix Workspace** アプリのバージョンは何ですか

オペレーティングシステムがセキュリティのために Citrix Analytics に **IP** アドレス属性を送信するために必要な **Citrix** Workspace アプリの最小バージョンがあります。詳細については、[マトリックス表または利用できないと特定された場所を参照してください](/ja-jp/security-analytics/access-assurance-location.html#locations-identified-as-not-available) 。

地質学的詳細を受け取らないのはどのような場合ですか

ジオロケーションの詳細を表示するには、「利用できないと識別されたロケーション」セクションで詳細を参照してください。

Citrix Analytics がユーザーの位置を報告するために使用する地理位置情報サービスは何ですか？ **IP** の間違った場所を報告するにはどうすればいいですか

Citrix Analytics は、Neustar ファイルベースの位置情報サービスを使用して 、着信アクセス用の位置情報データを提供します。公開されている IP 訂正ページがあり、訂正要求を自己提出するために使用できます。修正リクエストが送信されると、そのリクエストは Neustar によって正確性が確認され、処理されます。

GeoIP プロバイダは、できるだけ正確な情報を表示するのに役立ちます。残念ながら、GeoIP の本質的な性質により、GeoIP データが不正確になる場合があります。

用語集

April 12, 2024

- アクション: 不審なイベントに対するクローズドループ応答。アクションは、今後異常なイベントが発生するのを防ぐために適用されます。詳細情報。
- **Cloud Access Security Broker (CASB)**: クラウドサービスコンシューマーとクラウドサービスプロバイダーの間に配置される、オンプレミスまたはクラウドベースのセキュリティポリシー適用ポイント。CASB は、クラウドベースのリソースにアクセスする際に、エンタープライズセキュリティポリシーを組み合わせて介入します。また、組織がオンプレミスインフラストラクチャのセキュリティ制御をクラウドに拡張するのにも役立ちます。
- **NetScaler ADC**（アプリケーション **Delivery Controller**）: ファイアウォールと 1 つ以上のアプリケーションサーバーの間に戦略的に配置された、データセンター内に存在するネットワークデバイス。サーバー間の負荷分散を処理し、エンタープライズアプリケーションのエンドユーザーのパフォーマンスとセキュリティを最適化します。詳細情報。
- **NetScaler ADM**（アプリケーションデリバリ管理）: 一元化されたネットワーク管理、分析、オーケストレーションソリューション。管理者は、1 つのプラットフォームから、スケールアウトアプリケーションアーキテクチャのネットワークサービスを表示、自動化、管理できます。詳細情報。
- **NetScaler ADM** エージェント: NetScaler ADM とデータセンター内の管理対象インスタンス間の通信を可能にするプロキシ。詳細情報。
- **Citrix Analytics**: サービスや製品（オンプレミスとクラウド）にまたがるデータを収集し、実用的な洞察を生成するクラウドサービスです。これにより、管理者はユーザーやアプリケーションのセキュリティ脅威にプロアクティブに対処し、アプリのパフォーマンスを向上させ、継続的な運用をサポートできます。詳細情報。

- **Citrix Cloud**：任意のクラウドまたはインフラストラクチャ（オンプレミス、パブリッククラウド、プライベートクラウド、ハイブリッドクラウド）上の Citrix Cloud Connector を介してリソースに接続するプラットフォーム。詳細情報。
- **NetScaler Gateway**：リモートアクセスインフラストラクチャを統合して、データセンター、クラウド、または SaaS として提供されるすべてのアプリケーションにわたってシングルサインオンを提供する統合リモートアクセスソリューションです。もっと詳しく知る。
- **Citrix Hypervisor**：アプリケーション、デスクトップ、およびサーバーの仮想化インフラストラクチャ向けに最適化された仮想化管理プラットフォームです。詳細情報。
- **Citrix Workspace** アプリ（旧称 Citrix Receiver）：スマートフォン、タブレット、PC、Mac など、あらゆるデバイスからアプリケーション、デスクトップ、およびデータへのシームレスで安全なアクセスを提供するクライアントソフトウェアです。詳細情報。
- **DLP (Data Loss Prevention)**: ファイル、電子メール、パケット、アプリケーション、データストアなどのオブジェクトに含まれる情報を分類するための一連のテクノロジーと検査手法を記述したソリューションです。また、オブジェクトはストレージ内、使用中、またはネットワーク上に存在することもできます。DLP ツールは、ログ、レポート、分類、再配置、タグ付け、暗号化などのポリシーを動的に適用できます。DLP ツールは、エンタープライズデータ権利管理保護を適用することもできます。詳細情報。
- **DNS (**ドメインネームシステム**)**: インターネットドメイン名を検索し、インターネットプロトコル (IP) アドレスに変換するために使用されるネットワークサービス。DNS は、エンティティの物理的な場所に関係なく、ユーザーが指定した Web サイト名を、マシンが提供する IP アドレスに対応付けて、Web サイトを特定します。
- データ処理：データソースから Citrix Analytics にデータを処理する方法です。詳細情報。
- データソース：Citrix Analytics にデータを送信する製品またはサービス。データソースは内部でも外部でもかまいません。[もっと詳しく] /en-us/citrix-analytics/data-sources.html)。
- データのエクスポート：Citrix Analytics からデータを受け取り、洞察を提供する製品またはサービス。詳細情報。
- 検出されたユーザー: 組織内でデータソースを使用しているユーザーの総数。詳細情報。
- **FQDN**（完全修飾ドメイン名）：内部（StoreFront）および外部（NetScaler ADC）アクセス用の完全なドメイン名。
- 機械学習: 明示的にプログラムされずに知識を抽出するデータ分析テクノロジーの一種。アプリケーション、センサー、ネットワーク、デバイス、アプライアンスなど、さまざまなソースからのデータが、機械学習システムに入力されます。システムはデータを使用し、アルゴリズムを適用して独自のロジックを構築し、問題の解決、洞察の導出、または予測を行います。
- **Microsoft Graph** セキュリティ: 顧客のセキュリティと組織のデータをつなぐゲートウェイ。アクションを実行する必要がある場合に、確認しやすいアラートと修復オプションを提供します。詳細情報。
- パフォーマンス分析: 組織全体のユーザーセッションの詳細を可視化するサービスです。詳細情報。
- ポリシー: ユーザーのリスクプロファイルにアクションを適用するために満たす一連の条件。詳細情報。

- リスク指標: 組織が特定の時点で抱えているビジネスリスクへのエクスポージャーのレベルに関する情報を提供するメトリック。詳細情報。
- リスクスコア: あらかじめ決められた監視期間中に、ユーザーまたはエンティティが IT インフラストラクチャにもたらすリスクの総レベルを示す動的な値です。詳細情報。
- リスクタイムライン: ユーザーまたはエンティティのリスクの高い行動を記録することで、管理者はリスクプロファイルを精査し、データ使用量、デバイス使用量、アプリケーション使用状況、場所の使用状況を把握できます。詳細情報。
- 危険なユーザー: 危険な行動をとった、または危険な行動を示したユーザー。詳細情報。
- セキュリティ分析: セキュリティ監視や脅威ハンティングなど、説得力のあるセキュリティ成果を達成するために使用されるデータの高度な分析。詳細情報。
- **Secure Private Access**: シングルサインオン、リモートアクセス、コンテンツ検査を、エンドツーエンドのアクセス制御のための単一のソリューションに統合するサービスです。詳細情報。
- **Splunk**: Citrix Analytics からインテリジェントなデータを受け取り、潜在的なビジネスリスクに関する洞察を提供する SIEM（セキュリティ情報およびイベント管理）ソフトウェア。詳細情報。
- **UBA**（**User Behavior Analytics**）: ユーザーのアクティビティと行動をピアグループ分析と組み合わせてベースライン化し、潜在的な侵入や悪意のあるアクティビティを検出するプロセス。
- **Watchlist**: 管理者が疑わしいアクティビティを監視したいユーザーまたはエンティティのリスト。詳細情報。