新機能

Citrix の目標は、Citrix Analytics のお客様が利用可能になったときに、新機能と製品アップデートを提供することです。新しいリリースはより多くの価値を提供するため、アップデートを遅らせる理由はありません。

お客様にとって、このプロセスは透過的です。最初のアップデートは Citrix の内部サイトにのみ適用され、その後、お客様の環境に段階的に適用されます。アップデートを段階的に波状に提供することで、製品の品質を確保し、可用性を最大化するのに役立ちます。

Citrix Analytics には、以下の製品またはサービスがあります。新機能と製品アップデートについては、各サービスに特化した「新機能」の記事を参照してください。

- シトリックス アナリティクス for セキュリティ
- シトリックス アナリティクス for パフォーマンス

このリリースノートでは、Citrix Analytics プラットフォームに特化した新機能と製品アップデートを強調しています。

September 21, 2023

PowerShellスクリプトを使用したStoreFront™オンボーディングの簡素化

前提条件の確認、StoreFrontのインストール、および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でこのスクリプトを管理者モードで実行して、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。

詳細については、StoreFront展開への接続を参照してください。

August 28, 2023

Microappsサービス（提供終了）

Citrix Microappsサービスは提供終了となり、ユーザーは利用できなくなりました。

August 01, 2023

Citrix Analytics - 利用状況 (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。

February 23, 2023

修正された問題

Citrix Virtual Apps and Desktops™ 2112 のリリース前は、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、これらの接続されたサイトは、**Virtual Apps and Desktops- Monitoring** サイトカードに表示されません。この問題は修正されました。

September 28, 2022

アラート通知用 Webhook

受信 Webhook URL が構成されている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するために Webhook を使用できます。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、イベント発生時に通知を受け取ることができます。詳細については、「アラート通知用 Webhook」を参照してください。

September 08, 2022

CSV エクスポートの制限が引き上げられました

CSV 形式で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制限が、10,000 行から 100,000 行に引き上げられました。詳細については、「イベントを CSV ファイルにエクスポート」を参照してください。

August 18, 2022

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、ダウンロードされた CSV ファイルでは Workspace アプリのバージョン値が **NA** (利用不可) と表示されていましたが、ページビューでは利用可能でした。この問題は修正されました。

August 10, 2022

サイト集約なしのStoreFrontオンボーディング

StoreFrontのサイト集約の依存関係は、**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。サイト集約にサイトが追加されていなくても、ワークスペースアプリケーションに**StoreFront展開の接続**オプションが表示されます。詳細については、Citrix Virtual Apps and Desktopsデータソースを参照してください。

April 05, 2022

Secure Workspace AccessがSecure Private Accessに名称変更されました

Analyticsのダッシュボードとレポートでは、ブランド変更された製品名に合わせて、すべての**Secure Workspace Access**ラベルが**Secure Private Access**に更新されました。

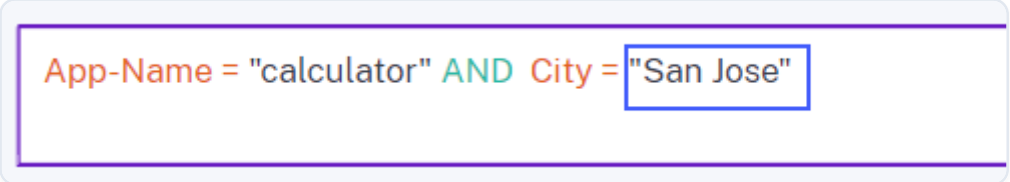
例えば、**データソース**ページと**セルフサービス検索ページ**では、**Secure Workspace Access**ラベルが**Secure Private Access**に名称変更されています。

March 21, 2022

修正された問題

- **検索**ページで、検索クエリの以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提案が機能しません。

  例えば、次のクエリでは、都市を`San Jose`として選択すると、自動提案が機能しなくなります。この問題は修正されました。



February 10, 2022

新機能

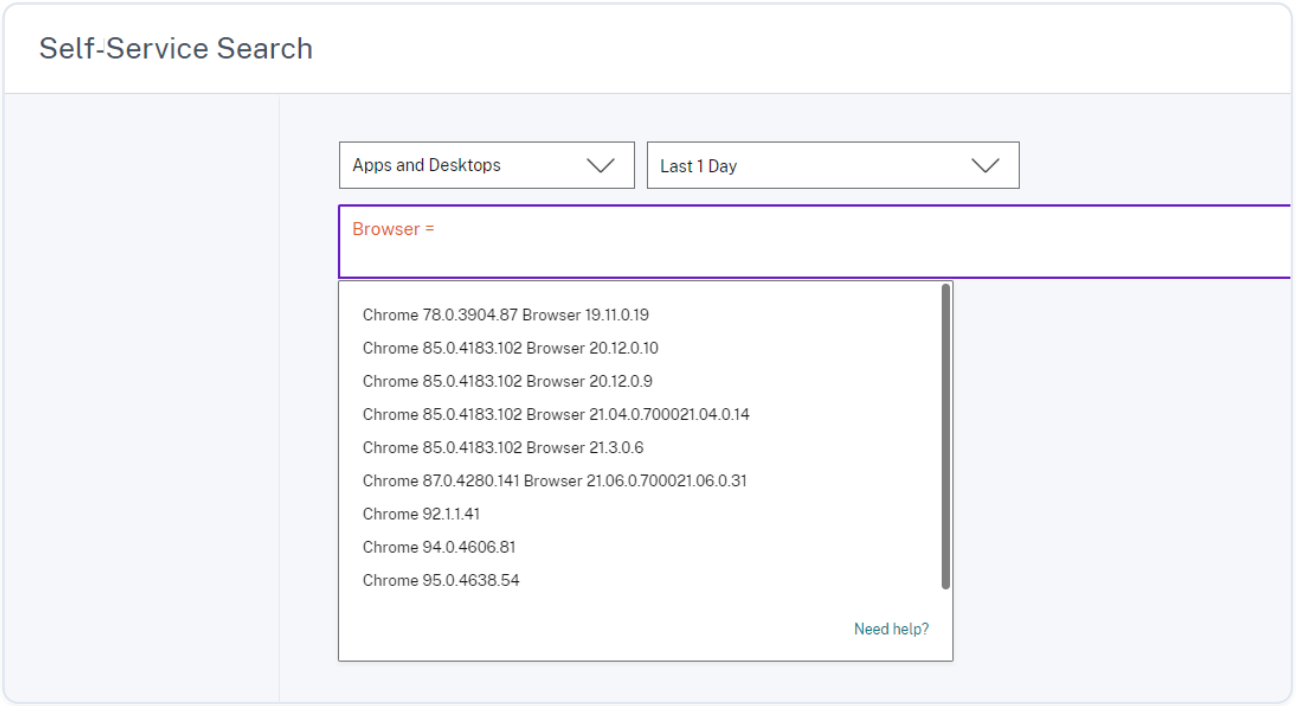
セルフサービス検索ボックスのディメンションの自動提案値

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、そのディメンションの値が自動的に表示されます。自動提案された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、レコードで利用可能な一致する値が自動提案されます。

ディメンションに提案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、過去の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提案されます。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。



December 20, 2021

新機能

アクセス制御はSecure Workspace Accessに名称変更されました

Analyticsのダッシュボードとレポートでは、ブランド変更された製品名に合わせて、すべての**Access Control**ラベルが**Secure Workspace Access**に更新されました。

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、**Access Control**ラベルが**Secure Workspace Access**に名称変更されました。

December 06, 2021

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

- Citrix Cloudに組織をオンボーディングする際に、ホームリージョンとしてアジア太平洋南部を選択し、Citrix Analyticsサービスを使用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は、ホームリージョンとしてアジア太平洋南部を選択した場合、組織のユーザーイベントとメタデータをアジア太平洋南部リージョンに保存するようになりました。詳細については、「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、「技術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。

August 19, 2021

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などの文字列型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。

July 14, 2021

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ない（空白でない）ことを確認できるようになりました。

注

この演算子は、App-Name、Browser、Countryなどの文字列型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。

June 07, 2021

非推奨の機能

Citrix Analytics デモ環境が削除されました

Security Analytics および Performance Analytics の **デモを試す** リンクは、Analytics の概要ページから削除されました。各サービス向けのデモ環境にはアクセスできなくなりました。Citrix Analytics のサービスへのアクセス方法の詳細については、はじめにを参照してください。

May 18, 2021

新機能

*演算子と!=演算子のサポート

検索クエリで、* 演算子を `!=` 演算子と組み合わせて使用できるようになり、ユーザーイベントを検索できます。例:

- 「John」という名前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、次のクエリを使用します。User-Name != John*
- 「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、次のクエリを使用します。User-Name != *Smith

> **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でも、クエリが見やすくなりました。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できます。以前は、複数行のクエリを表示するのが困難でした。

  複数行クエリ(/en-us/citrix-analytics/media/search-query-multi-line.png)

- Safariブラウザで確認されていたカーソルが飛ぶ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」(/ja-jp/citrix-analytics/self-service-search.html)を参照してください。

セルフサービス検索におけるチップ表示の再設計

- 再設計されたチップにより、選択した複数のファセットがより見やすくなりました。

  再設計されたチップ(/en-us/citrix-analytics/media/chips-multiple-facets-view.png)

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

修正された問題

- Citrix Directorで、**Go to Analytics**リンクが機能しません。この問題は、Citrix Cloudの欧州連合地域で組織をオンボーディングしたユーザーで確認されています。

March 31, 2021

Apps and Desktops検索クエリにおけるINおよびNOT IN演算子のサポート

Apps and Desktopsディメンション - `Device ID`、`Domain`、`Event-Type`、および`User-Name`では、次の演算子を使用できるようになりました。

- **IN**: 1つ以上の値に関連するイベントを取得するために、ディメンションに複数の値を割り当てます。
- **NOT IN**: ディメンションに複数の値を割り当て、指定され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。

March 18, 2021

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、NOT LIKE (!~) 演算子を使用できるようになりました。この演算子は、指定した一致パターンについてユーザーイベントをチェックします。イベント文字列内のどこにも指定されたパターンが含まれていないイベントを返します。

たとえば、クエリ `User-Name !~ “John”` は、John、John Smith、または「John」という一致する名前を含むその他のユーザーを除くイベントを表示します。

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。

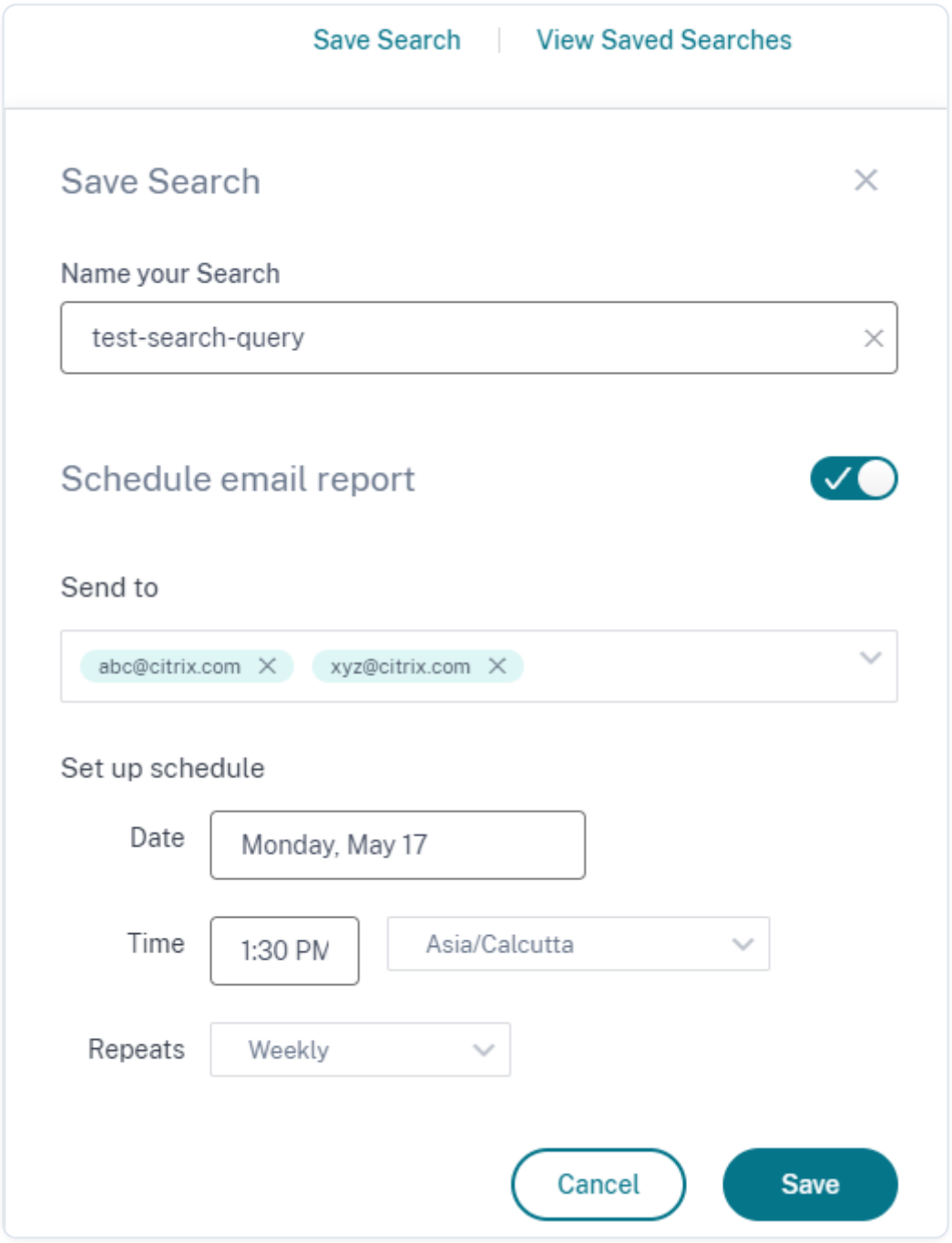
February 23, 2021

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、検索クエリを保存する際に、保存した検索クエリと対応する視覚的な概要レポートのコピーを自分自身や他のユーザーに送信するためのメール配信をスケジュールすることもできます。メールの送信を開始するには、日付、時刻、頻度（毎日、毎週、毎月）を設定します。以前に保存した検索クエリの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。



検索クエリの視覚的な概要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、他のユーザーとコピーを共有できるようになりました。ビジュアルサマリーレポートをPDFとしてダウンロードするには、**Export Visual Summary**をクリックします。

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（フィルター）。
- 検索イベントのタイムラインチャート、棒グラフ、またはグラフなどのビジュアルサマリー。

詳細については、「セルフサービス検索」(/ja-jp/citrix-analytics/self-service-search.html#export-visual-summary)を参照してください。

ビジュアルサマリーのエクスポート(/en-us/citrix-analytics/media/export-visual-summary.png)

November 12, 2020

新機能

セルフサービスクエリを保存する

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

- 適用された検索フィルター
- 選択されたデータソースと期間

セルフサービス検索の保存(/en-us/citrix-analytics/media/save-self-service-query.gif)

詳細については、「セルフサービス検索を保存する方法」(/ja-jp/citrix-analytics/self-service-search.html#how-to-save-the-self-service-search)を参照してください。

October 20, 2020

新機能

欧州連合地域でのCitrix Gatewayのサポート

Citrix Analyticsは、EU地域でのCitrix Gatewayをサポートするようになりました。詳細については、Citrix Gatewayデータソースを参照してください。

July 09, 2020

サポートの廃止

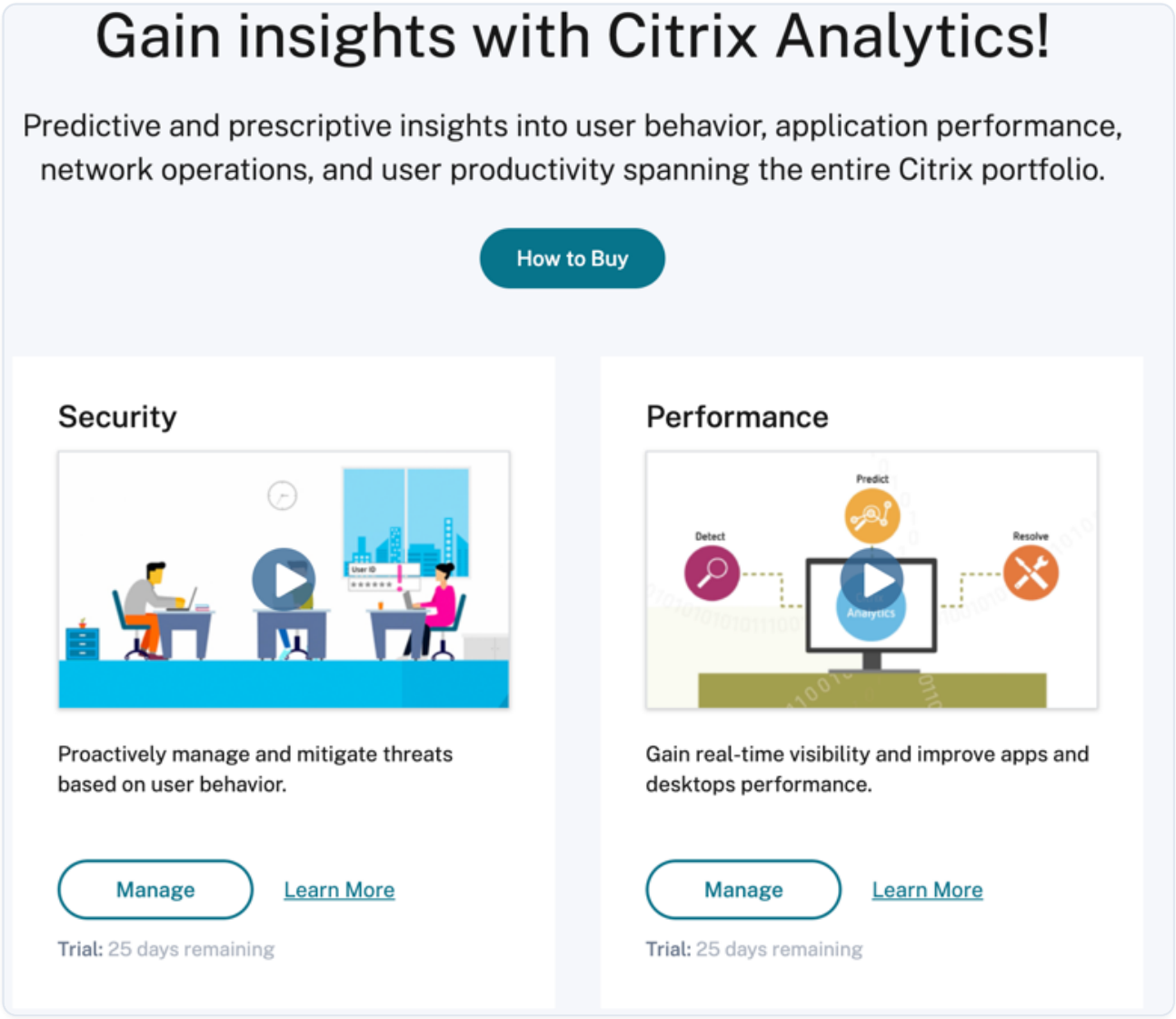
Microsoft Internet Explorer 11は、サポート対象ブラウザリストから削除されました。この廃止は、そのブラウザで確認されたセキュリティ脆弱性が原因です。サポート対象ブラウザのリストについては、システム要件を参照してください。

June 02, 2020

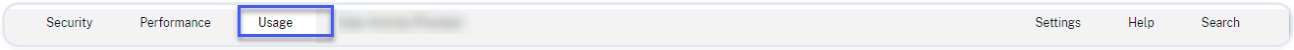
新機能

Analyticsの再設計された概要ページとトップバー

Analyticsの概要ページには、以前存在した**操作**タイルに代わる**使用状況**タイルが表示されます。また、**生産性**タイルはこのページから削除されました。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、トップバーでは、**使用状況**タブが**操作**タブに代わります。



February 20, 2020

新機能

Citrix Analytics サブスクリプションの提供

ユーザーに柔軟な購入オプションを提供するため、Citrix は現在、3つの個別のサブスクリプションベースの Citrix Analytics 製品を提供しています。Citrix Analytics は、お客様が購読するサービスに基づいて、独自のセキュリティまたはパフォーマンス（あるいはその両方）に関するインサイトを提供します。

以下の Citrix Analytics サブスクリプション製品を購入できます。

- シトリックス アナリティクス for セキュリティ
- シトリックス アナリティクス for パフォーマンス
- 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

以下のデータソースに新しいログが追加されました。

- シトリックス アイデンティティ プロバイダー
- シトリックス ゲートウェイ
- セキュア ブラウザ
- マイクロソフト グラフ セキュリティ
- マイクロソフト アクティブ ディレクトリ

詳細については、データガバナンス を参照してください。

修正された問題

- Internet Explorer 11 では、セルフサービス検索が正確に機能しません。そのため、検索クエリを入力して検索操作を実行できません。

January 09, 2020

修正された問題

- Citrix Analytics のウォークスルー機能が、欧州連合のホームリージョンにいるユーザーに対して機能しません。

December 18, 2019

修正された問題

Citrix Cloud ページの **Analytics** タイルに **View Service** ボタンが表示されていました。このボタンは、ユーザーエクスペリエンス向上のため、**Manage** に変更されました。

December 12, 2019

新機能

アジア太平洋南部での Microapps サービスイベントのサポート

Citrix Analyticsプラットフォームは、アジア太平洋南部リージョンのMicroapps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。詳細については、データガバナンスを参照してください。

> **注**
>
> Microapps サービスは Citrix Workspace の一部として提供されます。詳細については、「」のドキュメントを参照してください。(/ja-jp/citrix-microapps.html).

December 04, 2019

修正された問題

アジア太平洋南部地域の一部のユーザーは、ホームリージョンとして を選択してCitrix Cloudにオンボーディングしているにもかかわらず、Citrix Analyticsにサインインできません。

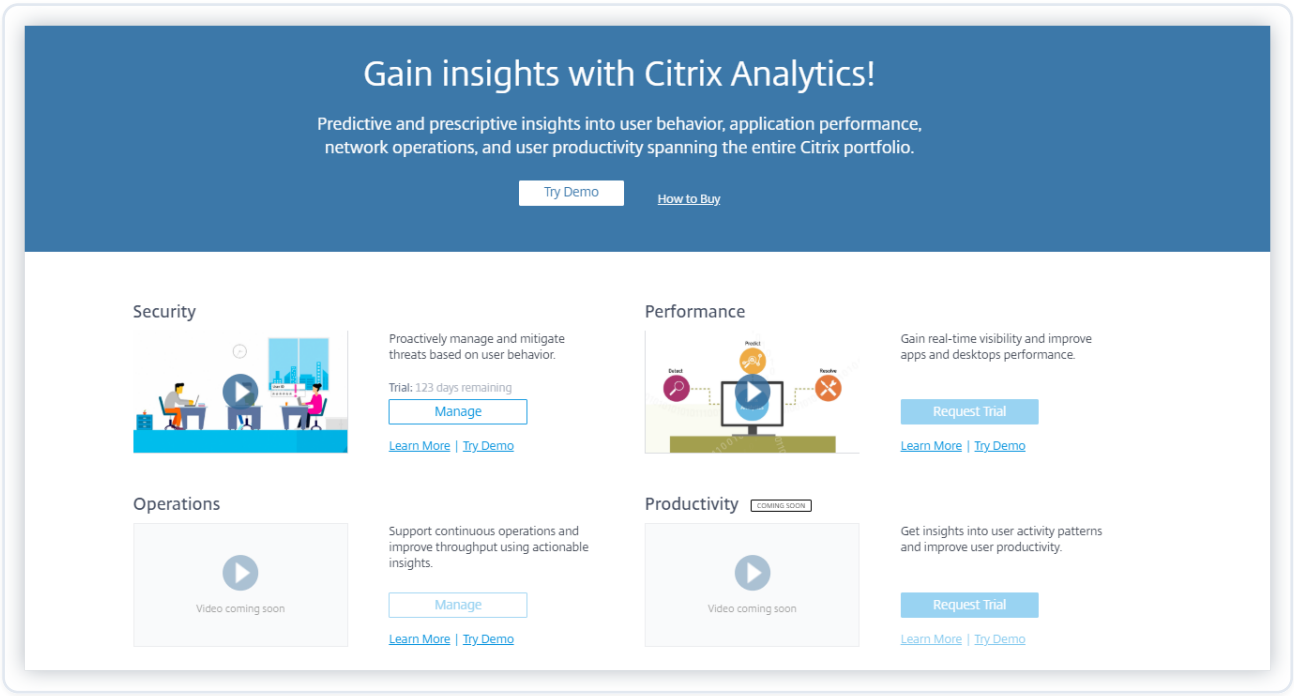
November 22, 2019

新機能

Analyticsの概要ページのデザイン変更

Analyticsの概要ページが再設計され、このページからすべてのAnalyticsサービスにアクセスできるようになりました。トライアルをリクエストしたり、デモを試したり、Analyticsサービスを管理したりできます。現在、Security AnalyticsとOperations Analyticsのみが一般提供されており、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、 > の順に選択します。



October 21, 2019

新機能

技術的なセキュリティの概要

技術的なセキュリティの概要では、Citrix Analyticsに関連するセキュリティのベストプラクティスについて説明しています。このドキュメントでは、Citrix Analyticsを使用する際に考慮すべきデータフロー、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。

September 11, 2019

修正された問題

- Citrix Cloudは、ユーザーを地域固有のCitrix Analyticsページにリダイレクトできません。

August 20, 2019

修正された問題

- Citrix Analytics のウォークスルー機能が、Microsoft Edge および Safari ブラウザで正確に読み込まれません。

July 31, 2019

新機能

欧州連合リージョンへの対応

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。Citrix Cloud に組織をオンボーディングする際に、ホームリージョンとして **欧州連合** を選択し、Citrix Analytics サービスを使用できます。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 リージョンの詳細については、「地理的考慮事項」を参照してください。

June 26, 2019

修正された問題

- Citrix Analytics が Internet Explorer 11 で正確に読み込まれません。

June 19, 2019

修正された問題

- Citrix Analytics が Microsoft Edge で正確に読み込まれません。

November 16, 2018

修正された問題

- 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** ナビゲーションバーがロードされず、ハンバーガーメニューにアクセスできなくなります。

October 10, 2018

アーキテクチャとプラットフォームの機能強化

このリリースでは、パフォーマンス、拡張性、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向上させるために、複数のアーキテクチャおよびプラットフォームの改善が行われました。

August 23, 2018

Citrix Analytics は、Citrix Cloud を介して提供されるクラウドサービスです。Citrix ポートフォリオ製品全体からデータを収集し、実用的なインサイトを提供することで、管理者が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るようにします。現在、Citrix Analytics は以下の分析サービスを提供しています。

- **Security Analytics**: ユーザーとエンティティの行動に関する情報を照合し、可視性を提供します。詳細については、「Security Analytics」を参照してください。
- **Operations Analytics**: ユーザーの活動（訪問したWebサイト、使用された帯域幅など）に関する情報を照合して提示します。詳細については、「Operations Analytics」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 統合製品ポートフォリオの一部として名称が変更されました。

当社の製品および製品ドキュメントで新しい名称に気づくかもしれません。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の詳細については、「Citrix product guide」を参照してください。 当社の製品およびそのドキュメントにおけるこの移行の実施は、現在進行中のプロセスです。

- 製品内のコンテンツやドキュメントには、以前の名称がまだ含まれている場合があります。たとえば、コンソールテキスト、メッセージ、ディレクトリ/ファイル名、スクリーンショット、図などで以前の名称のインスタンスが見られる場合があります。
- 一部の項目（コマンドなど）は、既存の顧客スクリプトを破損させないために、以前の名称を保持し続ける可能性があります。
- この製品のドキュメントからリンクされている関連製品ドキュメントやその他のリソース（ビデオやブログ投稿など）には、以前の名称がまだ含まれている場合があります。

既知の問題

この記事では、Citrix Analyticsの各サービス（パフォーマンスとセキュリティ）に共通する既知の問題について説明します。

各サービスに固有の問題については、対応する「既知の問題」の記事を参照してください: セキュリティ および パフォーマンス。

- **Gateway-First time access from new IP indicator** は、ゲートウェイ経由でサービスまたはアプリケーションに初めてログインするユーザーに対してトリガーされます。

データソース

データソースとは、Citrix Analyticsにデータを送信するクラウドサービスおよびオンプレミス製品のことです。

Citrix Analyticsは、以下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、Content CollaborationやEndpoint Managementなど、Citrix Cloudアカウントに関連付けられている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に接続するために一連の設定を実行する必要があります。たとえば、オンプレミスのGatewayインスタンスはApplication Delivery Managementに追加する必要があり、オンプレミスのVirtual Apps and DesktopsサイトはWorkspaceに追加するか、StoreFrontサーバーを設定する必要があります。
- **外部データソース**。Microsoft Graph Security、Microsoft Active Directoryなど、Citrix Analyticsと統合できるサードパーティアプリケーション。Citrix Analyticsは、これらの外部データソースから、統合が成功した後に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の提供形態によって、データソースは異なります。各提供形態でサポートされているデータソースを表示するには、以下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
- Citrix Analytics for Performanceでサポートされているデータソース

Citrix Gateway、Citrix DaaS（旧Citrix Virtual Apps and Desktopsサービス）、およびCitrix Virtual Apps and Desktopsのデータソースは、Citrix Analytics for SecurityとCitrix Analytics for Performanceの両方の提供形態でサポートされています。両方の提供形態に適用されるオンボーディング手順については、以下の記事を参照してください。

- Citrix Gatewayデータソース
- シトリックス バーチャル アプリケーションズ アンド デスクトップス データソース

Citrix Gateway データソース

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

ユーザーが Gateway を介してサービスや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、Citrix 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 の両方のサービスに適用されます。

前提条件

- Citrix Cloud で提供されている Citrix ADM を購読します。Citrix ADM の使用を開始する方法については、「Getting Started」を参照してください。
- 検証済みの Citrix ADM ライセンス。Citrix ADM ライセンスの詳細については、「Licenses」を参照してください。
- システム要件を確認し、要件が満たされていることを確認します。

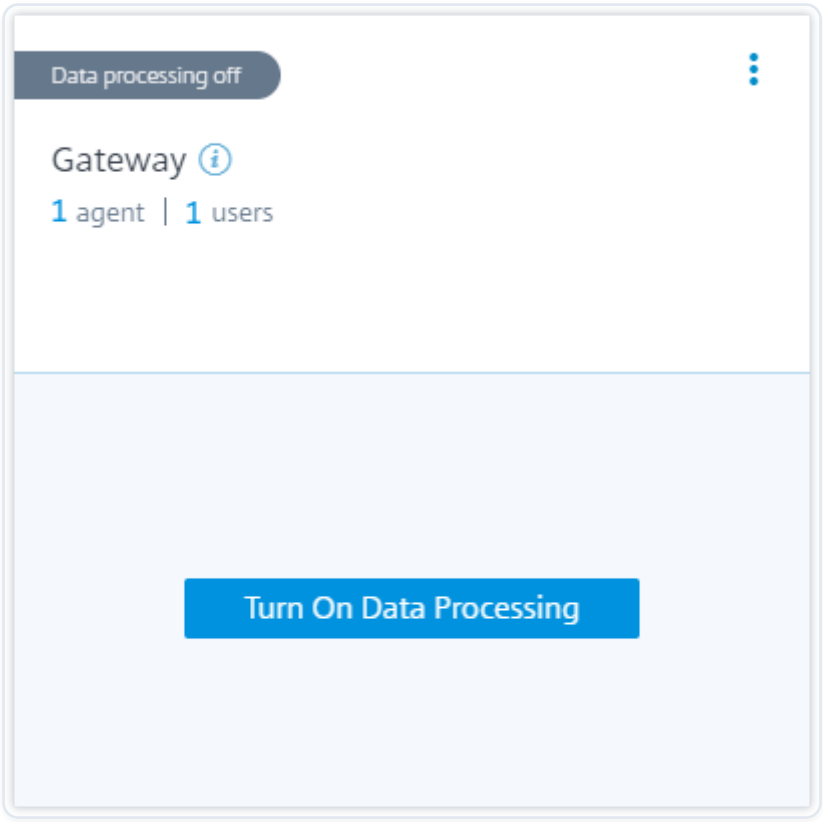
Citrix ADM に追加された Gateway データソース

Citrix Analytics は、Citrix ADM サービスにすでに追加されている Citrix ADM エージェントと Citrix 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：

上部のバーから、**設定** > **データソース** をクリックします。提供されているサービスに応じて、**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ーが Gateway サイトカードに表示されます。**データ処理をオンにする** をクリックして、Citrix Analytics がこのデータソースのデータ処理を開始できるようにします。

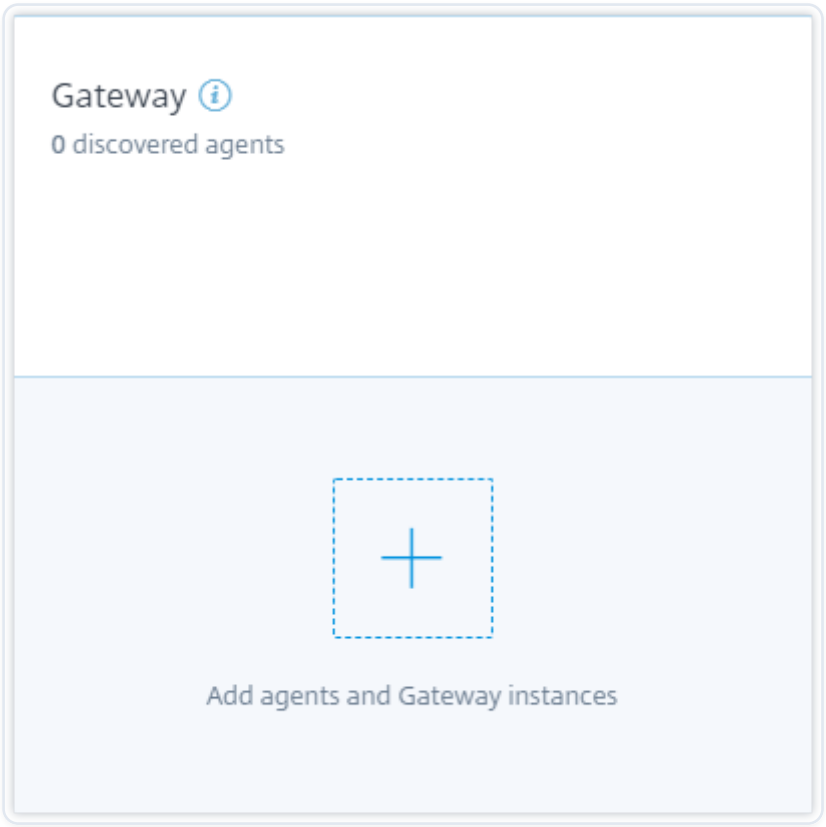


受信したイベントを表示できます。

Citrix ADM ServiceでCitrix Analyticsがまだ有効になっていない場合は、仮想サーバーでアナリティクスを有効にする統合プロセスを参照してください。

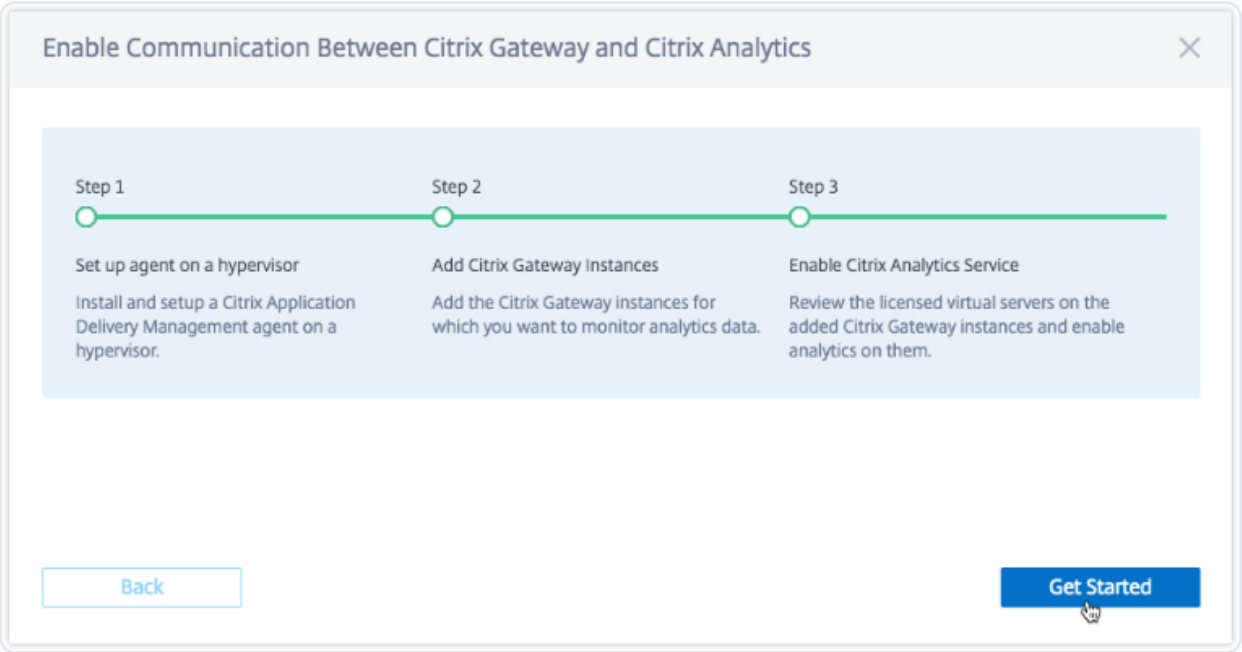
Citrix ADMに追加されていないGatewayデータソース

Citrix ADMエージェントとCitrix Gatewayインスタンスが Citrix 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**0個の検出されたエージェント**と表示されます。



エージェントとGatewayインスタンスを検出するには、次の操作を行います。

1. Citrix ADMサービスサブスクリプションを既にお持ちの場合は、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. Citrix ADMサービスサブスクリプションをお持ちでない場合は、サブスクライブ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**の下で、**Application Delivery Management**タイルにある**管理**をクリックします。
    b. 画面の指示に従って、Citrix ADMのExpressアカウントを作成します。詳細については、Citrix ADM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に再度ログインし、**設定 > データソース > セキュリティ**をクリックします。
    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、**開始**をクリックします。



4. 次のタスクを実行します。

   - Citrix 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

- **Citrix 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 Server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がある仮想コンピューティングリソースを示します。

コンポーネント	要件
RAM	8 GB（パフォーマンス向上のため32 GBを推奨）
仮想CPU	4（パフォーマンス向上のため8仮想CPUを推奨）
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

コンポーネント	要件
スループット	1ギガbps

- **ポート要件**: Citrix ADMエージェントがCitrix Gatewayインスタンスと通信できるように、以下のポートが開いていることを確認してください。

タイプ	ポート	説明
TCP	80/443	エージェントからCitrix GatewayインスタンスへのNITRO通信用
TCP	22	エージェントからCitrix GatewayインスタンスへのSSH通信用。
UDP	4739	Citrix GatewayからエージェントへのAppFlow®通信用
ICMP	予約済みポートなし	エージェントからCitrix Gatewayインスタンスへのネットワーク到達性を検出するため。
SNMP	161, 162	Citrix GatewayインスタンスからエージェントへSNMPイベントを受信するため。
シスログ	514	Citrix 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ため。
TCP	5557	Citrix 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のため。

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

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

Citrix ADMエージェントとCitrix Analytics間の通信には、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てください。

エンドポイント	米国リージョン	EUリージョン	APSリージョン
イベントハブ	`https://cas-eh-ns-alias.servicebus.windows.net/`	`https://cas-eh-ns-eu-alias.servicebus.windows.net/`	`https://cas-eh-ns-aps-alias.servicebus.windows.net/`

エージェントをインストールしてセットアップする

Analyticsとデータセンター内のGatewayインスタンス間の通信を有効にするため、お使いのネットワーク環境にCitrix ADMサービスエージェントをインストールして構成します。

エンタープライズデータセンターの以下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。

- シトリックス ハイパーバイザー
- ヴイエムウェア ESXi
- マイクロソフト 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、次の手順を実行します。

1. エージェントイメージをダウンロードします。

   「**ハイパーバイザーにエージェントをセットアップ**」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。

   ハイパーバイザーを選択してください(/en-us/citrix-analytics/media/gateway-select-hypervisor.png)
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。

サービスURLとアクティベーションコードが生成され、次の図に示すようにUIに表示されます。(このプロセス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特定し、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際に、サービスURLとアクティベーションコードを入力します。

サービスURLとアクティベーションコードをコピー(/en-us/citrix-analytics/media/gateway-activation-codurl.png)

3. ハイパーバイザーにエージェントを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、以下を確認してください。
>
> - ハイパーバイザーが各エージェントに提供する必要がある仮想コンピューティングリソース（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ース: 1、スループット: 1 Gbps）があることを確認します。
> - エージェントがインターネットにアクセスできるように、DNS を構成します。

- Citrix Hypervisor で、次の操作を実行します。

  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。**コンソール**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設定します。

  エージェントのネットワーク構成(/en-us/citrix-analytics/media/gateway-agent-network-config.png)

  誤った値を入力した場合、または値を変更したい場合は、デフォルトの資格情報 `nsrecover` / `nsroot` を使用してシェルプロンプトにログオンします。次に、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。

  サービスURLとアクティベーションコードを貼り付けます(/en-us/citrix-analytics/media/gateway-url-code-agent.png)

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 `deployment_type.py` を実行します。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、次の操作を実行します。

  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。**コンソール**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設定します。

  エージェントのネットワーク構成(/en-us/citrix-analytics/media/gateway-agent-network-config.png)

  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ます。

  ログイン(/en-us/citrix-analytics/media/gateway-vmware-act-url-login.png)

  c. **/mps** ディレクトリに移動し、スクリプトを実行して、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。

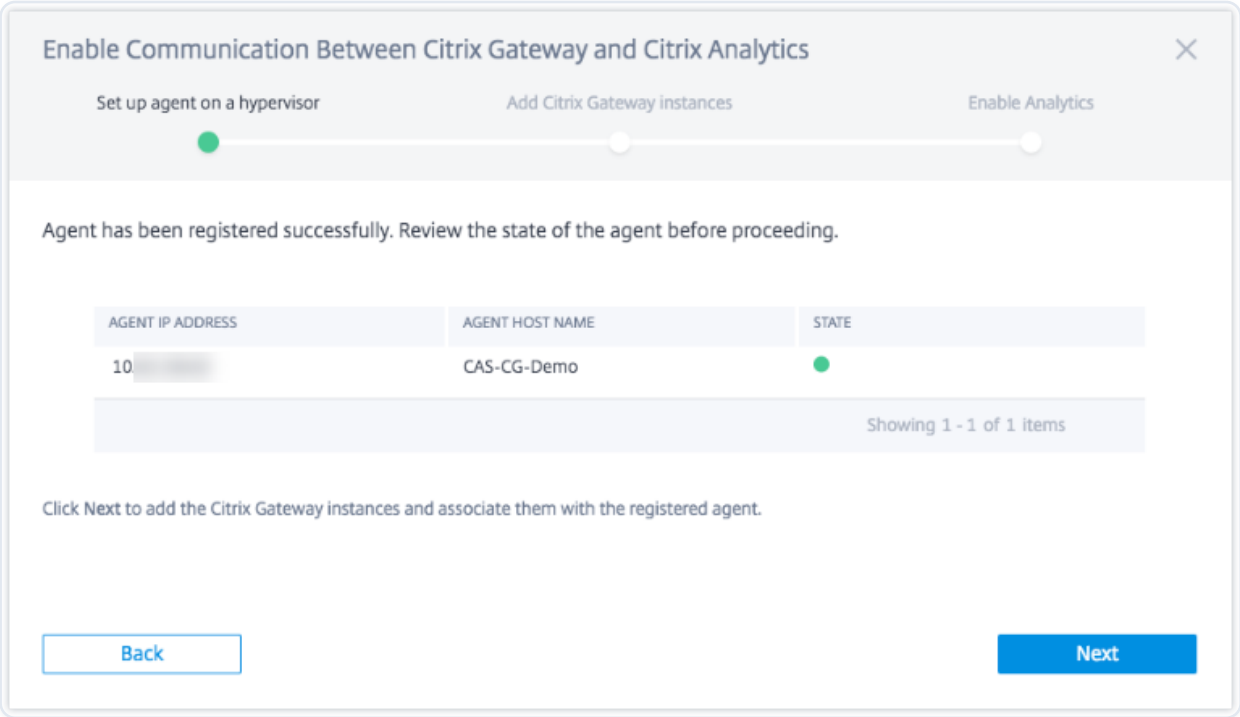
```
bash-3.2# cd /mps/
bash-3.2# ./deployment_type.py

--------------------------------------------------------------------------------
Citrix ADM Agent Registration with Citrix ADM Service. This menu allows you to s
pecify a cloud url and obtain an instance ID for your device.
--------------------------------------------------------------------------------
  Enter Service URL: agent.netscalermgmt.net
  Enter Activation Code : c56ba264-[redacted]5
```

> **注**
>
> 複数のエージェントをインストールするために同じイメージファイルを使用できます。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、「ハイパーバイザーにエージェントをセットアップ」ステップで、もう一度**イメージをダウンロード**をクリックします。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が成功すると、インストールプロセスを完了するためにエージェントが再起動します。エージェントが再起動したら、Citrix Analyticsにアクセスし、**エージェントを登録**をクリックして、エージェントのステータスを確認します。

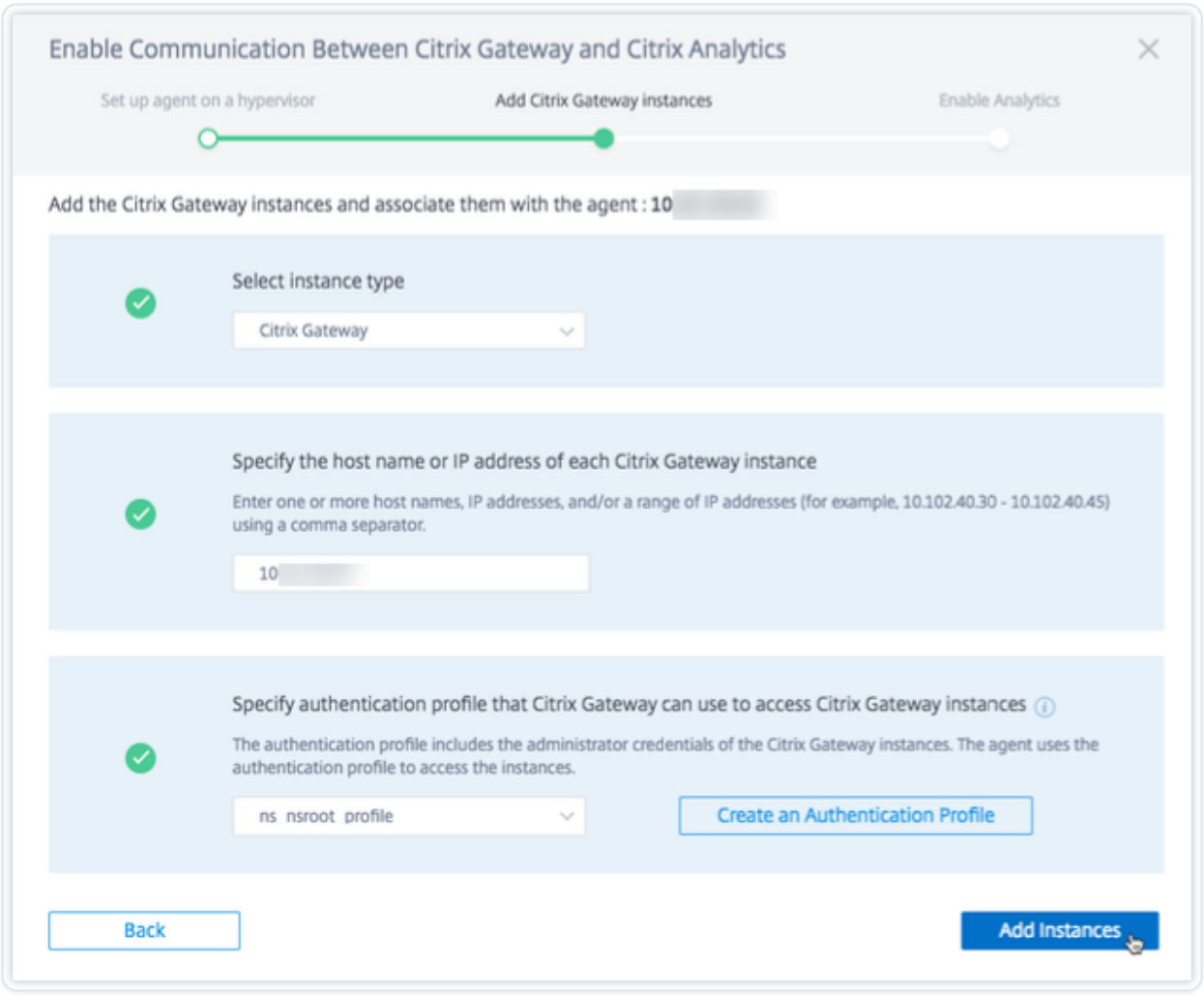


エージェントのステータスが、隣の緑色の点で示されるUP状態になったら、**次へ**をクリックして、サービスにインスタンスの追加を開始します。

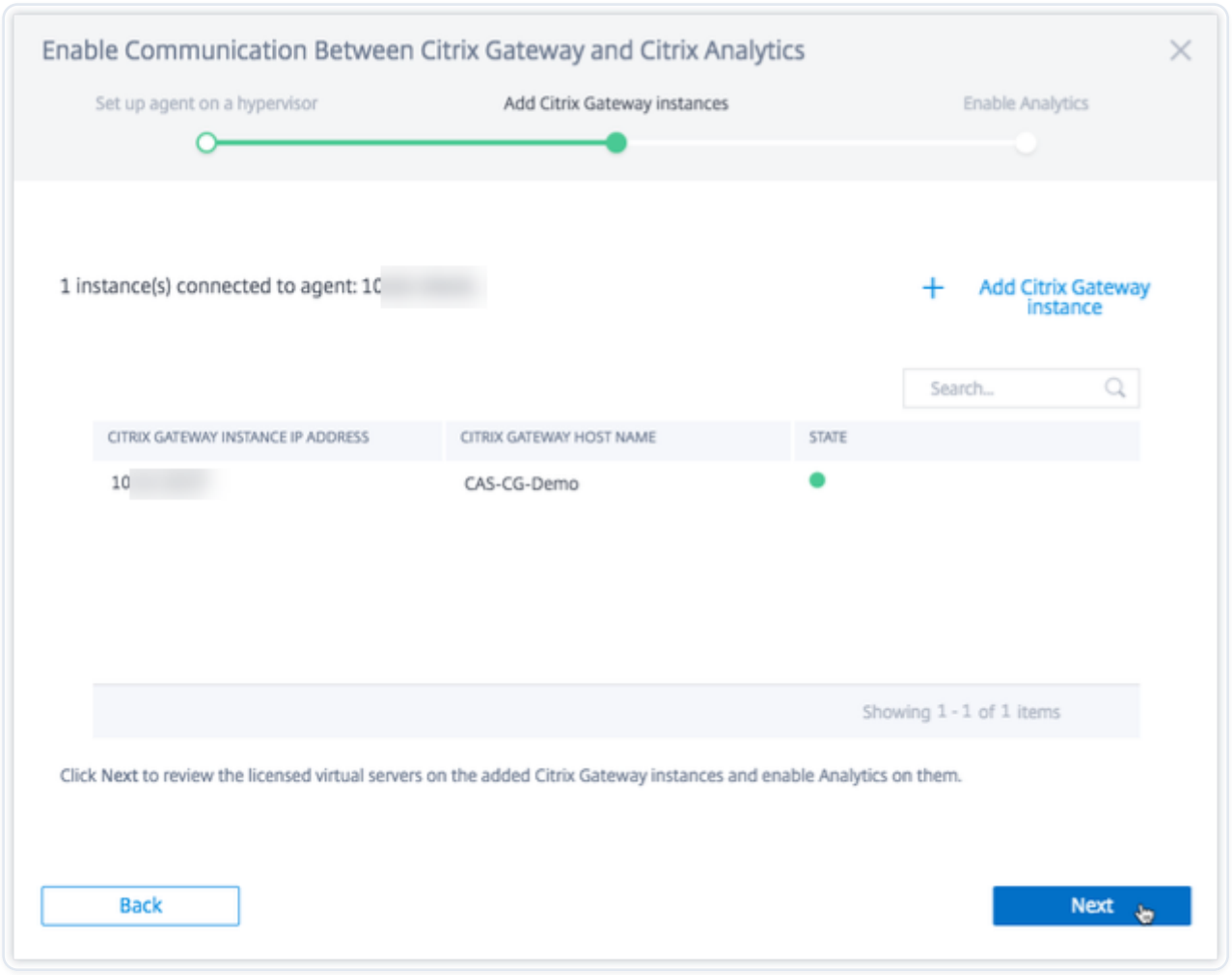
Citrix Gatewayインスタンスを追加する

インスタンスとは、Citrix Gatewayアプライアンスまたは仮想アプライアンスであり、Citrix Analyticsのデータソースとなります。

1. **Citrix Gatewayインスタンスの追加**ページで、インスタンスの種類を選択し、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資格情報です。その後、**インスタンスを追加**をクリックします。



インスタンスが追加されると、正常に検出されたインスタンスの数を確認できます。さらにインスタンスを追加するには、**Citrix Gatewayインスタンスを追加**をクリックします。



「**次へ**」をクリックして、アナリティクスを有効にします。

アナリティクスを有効にする

Citrix Analyticsは、追加されたCitrix Gatewayインスタンス上の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アナリティクスを有効にします。

「**アナリティクスを有効にする**」ページには、デフォルトでGatewayインスタンスからのすべてのライセンスされた仮想サーバーが表示されます。ライセンスされた仮想サーバーのリストを確認し、「**アナリティクスを有効にする**」をクリックして、仮想サーバーでアナリティクスを有効にします。

> 「**注**」
>
> 仮想サーバー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。

アナリティクスを有効にする(/en-us/citrix-analytics/media/gateway-enable-analytics.png)

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。

アナリティクスを有効にする(/en-us/citrix-analytics/media/gateway-data-source-added.png)

オンボーディングビデオを見る

次のビデオは、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。

<iframe src="https://www.youtube.com/embed/Bw_CXAUHINk" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>

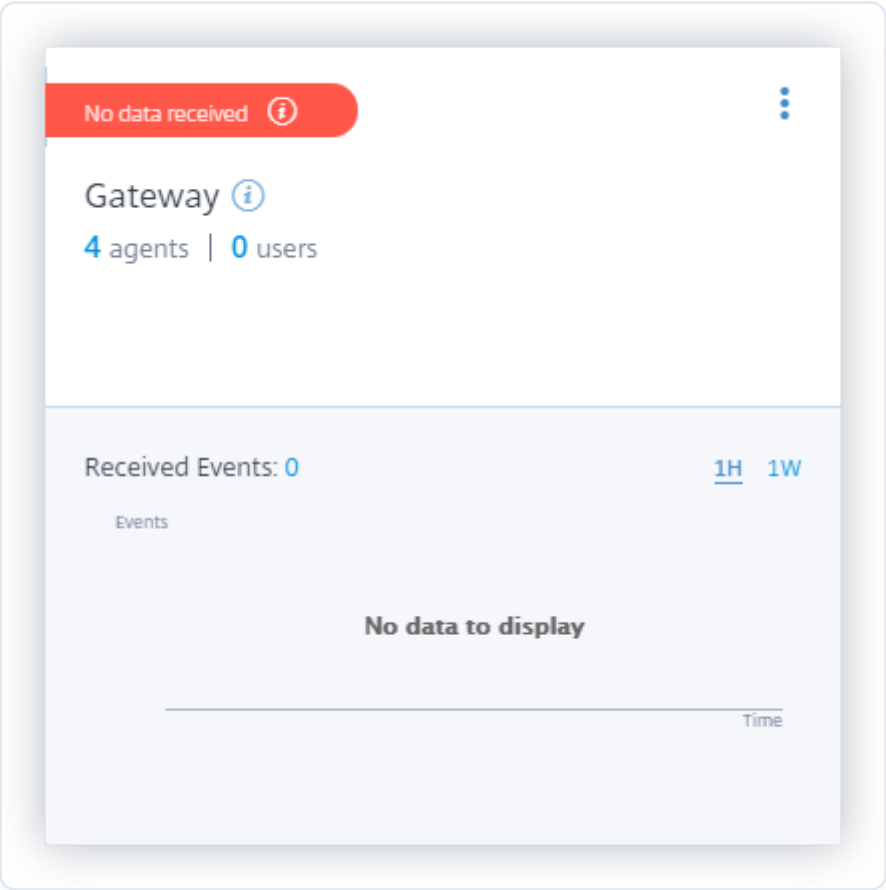
受信したイベント、ユーザー、エージェントを表示する

サイトカードには、Gatewayユーザー数、Citrix ADMエージェント数、およびデータソースから受信したイベント数が、デフォルトの時間選択である過去1時間分表示されます。1週間（**1W**）を選択してデータを表示することもできます。「**ユーザー**」ページで表示するには、ユーザー数をクリックします。Citrix Gatewayインスタンスとエージェントを表示するには、エージェント数をクリックします。

データソースページ(/en-us/citrix-analytics/media/gateway-discover-status.png)

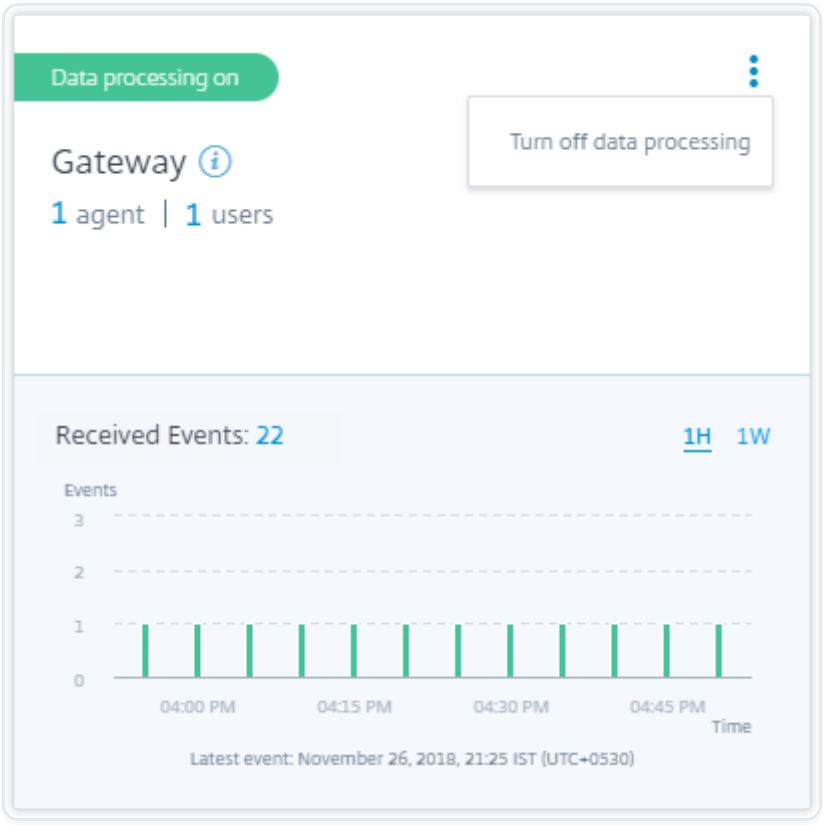
データ処理を有効にすると、サイトカードに「**データが受信されていません**」というステータスが表示されることがあります。このステータスが表示される理由は2つあります。

1. データ処理を初めて有効にした場合、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、ステータスは「**データ処理オン**」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**」ページを更新してください。
2. Analyticsが過去1時間以内にデータソースからイベントを受信していません。

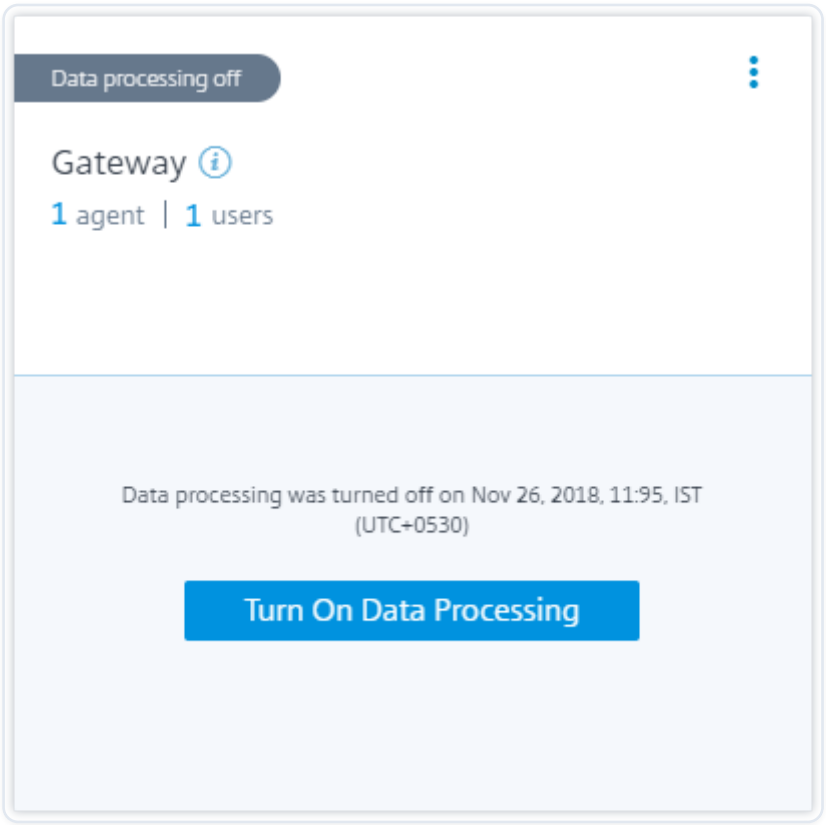


データ処理のオン/オフを切り替える

データ処理を停止するには、サイトカードの縦三点リーダー (⋮) 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、このデータソースのデータ処理を停止します。

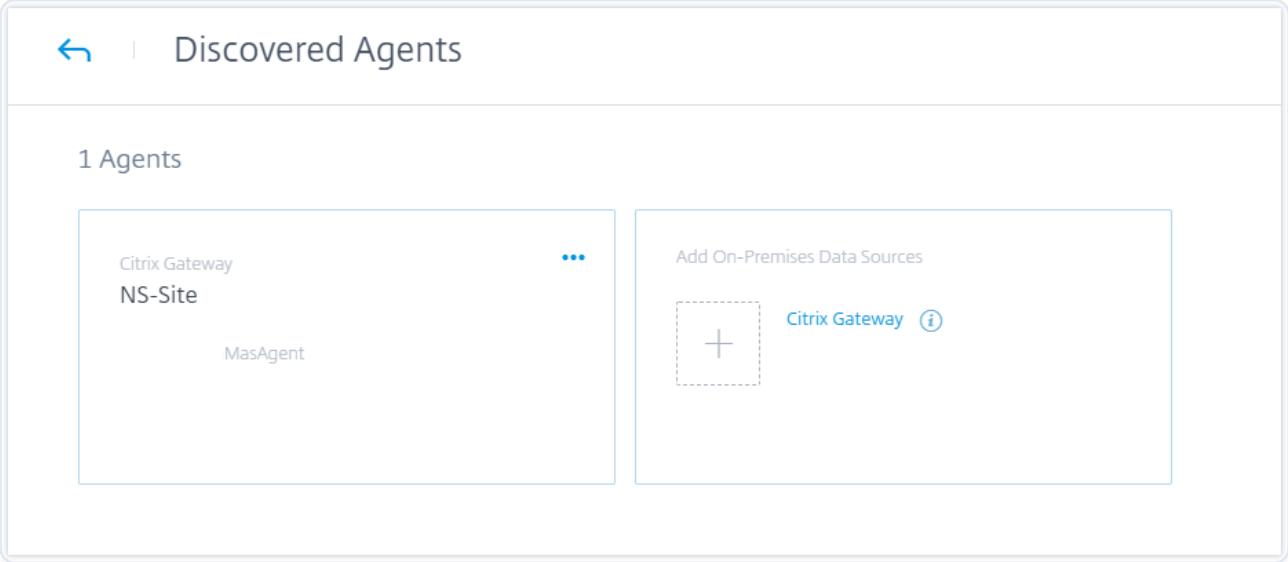


データ処理を再度有効にするには、「**データ処理をオンにする**」をクリックします。



Gatewayインスタンスを追加する

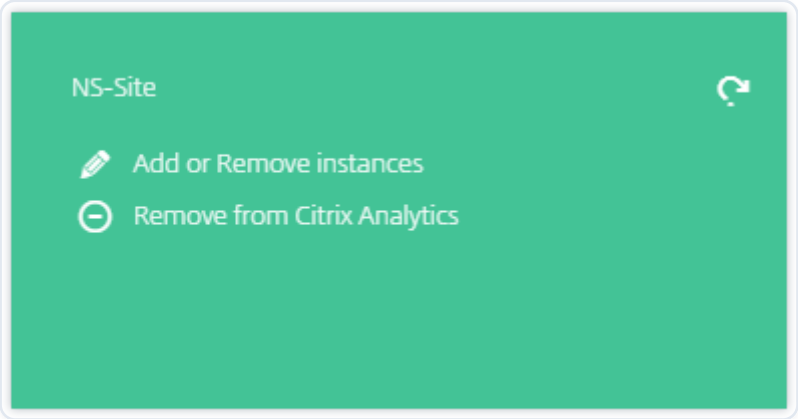
Gatewayインスタンスを追加する場合は、Gatewayサイトカードのエージェント数をクリックして「**検出されたエージェント**」ページを表示します。「**オンプレミスデータソースの追加**」タイルから「**Citrix Gateway**」をクリックします。



データソースの管理

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。また、エージェントとその関連インスタンスを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、次のいずれかを実行します。



- **インスタンスの追加または削除**。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で構成されている仮想サーバーでAnalyticsを有効にできます。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関連付けを解除すると、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**。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収集を停止します。ただし、以前に処理されたすべてのデータは保持期間中に利用可能です。

シトリックス バーチャルアプリおよびデスクトップ™ データソース

この記事では、StoreFront を使用してオンプレミスの Citrix Virtual 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。この記事で説明するオンボーディング手順は、Citrix Analytics for Performance (Performance Analytics) と Citrix Analytics for Security (Security Analytics) の両方のサービスに適用されます。

各サービスに固有のオンボーディング手順については、以下の記事を参照してください。

- オンプレミスの Citrix Virtual Apps and Desktops サイトを Citrix Analytics for Performance で構成する
- Citrix Analytics for Security 用に Citrix Virtual Apps and Desktops および Citrix DaaS データソースを構成する

StoreFront を使用して Citrix Virtual Apps and Desktops オンプレミスサイトをオンボーディングする

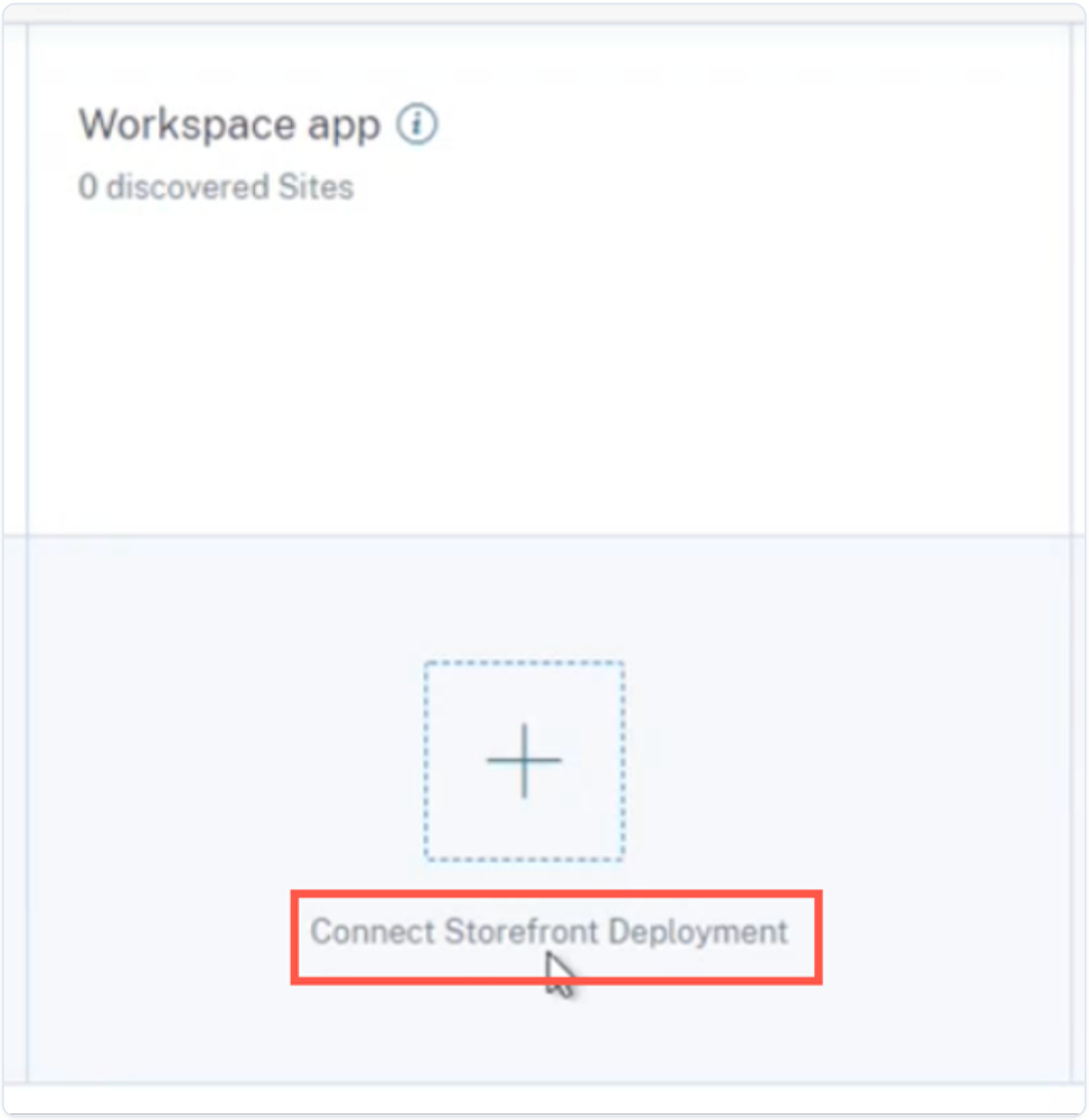
組織がオンプレミスの StoreFront™ 展開を使用している場合、Citrix Workspace™ アプリがイベントを Citrix Analytics に送信できるように、StoreFront サーバーを構成する必要があります。Citrix Analytics はイベントを処理し、Citrix IT インフラストラクチャのパフォーマンスとユーザーの行動に関する実用的なインサイトを提供します。

Citrix Analytics 用の StoreFront 展開の構成方法の詳細については、StoreFront ドキュメントの Citrix Analytics サービス の記事を参照してください。

以前は、Citrix Apps and Desktops オンプレミスサイトを使用しているお客様は、Citrix Analytics for Security™ および Performance のオンプレミスサイトをオンボーディングするためにサイト集約の使用を強制されていました。

サイト集約に依存せずに、Citrix Apps and Desktops 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。

サイト集約にサイトが追加されていなくても、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、以下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展開では、アウトバウンドインターネット接続用にポート443を開放する必要があります。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サーバーでホストされている場合、各ストアのプロキシは、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使用しません。詳細については、HTTPプロキシを使用するWebサーバーでホストされているStoreFront展開を構成するを参照してください。
- StoreFront展開は、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互換ブラウザのWebサイト用Citrix Receiver™。

    注

    HTML5ユーザーの場合、StoreFrontで特定の構成が有効になっていると、Citrix Virtual Apps and Desktopsはイベントを起動できます。構成手順については、Citrix Workspace app for HTML5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については、StoreFrontで追加のポリシーを構成する必要があります。詳細については、Citrix Workspace app for HTML5ドキュメントのPDF印刷の記事を参照してください。
  - Windows用Citrix Workspaceアプリ1907以降。
  - Linux用Citrix Workspaceアプリ2006以降。
  - Mac用Citrix Workspaceアプリ2006以降
- Citrix Virtual Apps and Desktops 7 1912 LTSRを使用している場合、サポートされるStoreFrontバージョンは1912です。

StoreFront展開に接続する

StoreFront展開には、次の方法で接続できます。

- **Apps and Desktops – Workspace app**サイトカードと**Apps and Desktops – Monitoring**サイトカードを使用する
- **Recommendations**パネルを使用する

Apps and Desktops – Workspace appサイトカードとApps and Desktops – Monitoringサイトカードを使用して接続する

1. **Settings > Data Sources > Security**に移動します。**Apps and Desktops- Workspace app**サイトカードで、縦の省略記号 (⋮) をクリックし、**Connect StoreFront deployment**を選択します。

   ストアセキュリティを接続(/en-us/citrix-analytics/media/store-front-site-card-1.png)

2. **Settings > Data Sources > Performance**に移動します。**Apps and Desktops- Monitoring**サイトカードで、縦の省略記号 (⋮) をクリックし、**Connect StoreFront deployment**を選択します。

   ストアパフォーマンスを接続(/en-us/citrix-analytics/media/cvad-performance-sf-connect.png)

   StoreFrontオンボーディングウィザードまたは**Connect StoreFront Deployment**ポップアップが表示されます。

3. **Download package**をクリックします。

   StoreFrontオンボーディングウィザード(/en-us/citrix-analytics/media/sf-onboarding-wizard.png)

   > **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管してください。

4. StoreFront展開を構成するには、,

   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内でそのフォルダーに移動します。
   c. StoreFrontをオンボードするには、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

      StoreFront管理者モード(/en-us/citrix-analytics/media/sf-admin-mode.png)

      その他のオプションまたは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Citrix Analytics Service GUIにStoreFrontサイトが表示されない場合は、iisresetコマンドを実行します。

f. Citrix Analytics Service GUIにログインし、Cluster 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検証します。

g. 設定が完了したら、Citrix Analyticsにログインして、接続されているStoreFront展開を表示します。

5. 設定が正常に完了したら、**完了**をクリックします。
6. Citrix Analyticsがデータを処理できるように、**データ処理を有効にする**をクリックします。

PowerShellスクリプト

Citrix Analytics Service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、StoreFrontのインストール、および構成の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。

StoreFront管理者モード(/en-us/citrix-analytics/media/sf-admin-mode.png)

お客様は、このPowerShellスクリプトをStoreFrontで実行して、オンボード、デボード、セルフチェックの実行、トラブルシューティングを行い、Citrix Analytics Service GUIへのオンボーディングが成功したかどうかを確認できます。お客様がスクリプトを初めて実行すると、発行元を確認するための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、オプションを選択します。

PowerShellスクリプトは常に実行されます(/en-us/citrix-analytics/media/powershell-script-always-run.png)

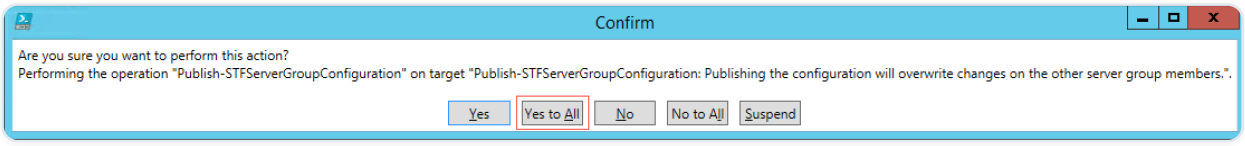
PowerShellスクリプトは、StoreFrontConfiguration.jsonファイル、いくつかのCCAuth、およびdllファイルとともに、zipファイル内の**Connect StoreFront Deployment**ページで入手できます。PowerShellスクリプトのログは、**Downloads**フォルダーのcas-logsファイルに保存されます。

PowerShellスクリプトは、次のパラメーターをサポートしています。

- **SelfCheck**: **SelfCheck**パラメーターは、StoreFrontの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するために使用されます。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。**selfcheck**を実行するには、次のコマンドを使用します。

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

- **OnboardStorefront**: **OnboardStoreFront**パラメーターは、Citrix Analytics Service構成のセットアップ準備状況を検証するために、セルフチェックを迅速に実行します。セットアップの準備ができていれば、Citrix Analytics Service構成をインポートし、変更をサーバーグループ内の他のサーバーに公開します。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StoreFront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ためのポップアップが表示されます。**Yes to All**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、StoreFrontがCitrix Analytics Service 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、認証のために秘密キーが必要です。この秘密キーを生成するには、CCAuthおよびdllファイルと、ダウンロードしたJSONファイルで利用可能な資格情報が必要です。

> **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 Service 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 Service GUIに表示されない場合は、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ためにIISRESETを実行する必要があります。

> **OnboardStoreFront**を実行するには、次のコマンドを使用します。

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

- **IsOnboarded**: **IsOnboarded**パラメーターは、StoreFrontがCitrix Analytics Service 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前に1分間待機しますが、StoreFrontが正常にオンボーディングされた後、GUIに表示されるまでに最大5分かかる場合があります。これを検証するには、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およびdllファイルの依存関係もあります。**IsOnboarded**を実行するには、次のコマンドを使用します。

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

- **Troubleshoot**: 5分間待ってもStoreFrontサイトがCitrix Analytics Service GUIに表示されない場合は、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ためにIISRESETを実行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、**Troubleshoot**パラメーターを使用します。これは、接続の問題をトラブルシューティングし、ログを収集するのに役立ちます。**Troubleshoot**を実行するには、次のコマンドを使用します。

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

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

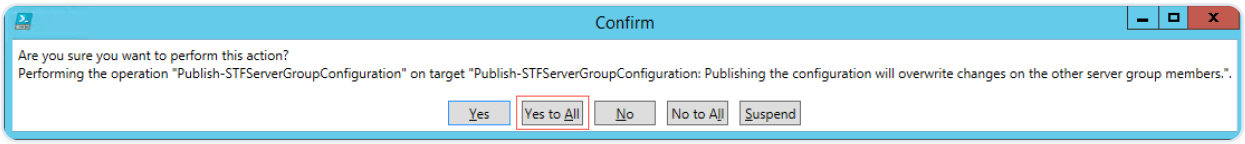
  - **ユースケース1**: セルフチェックの一環としてcurlAnalyticsが失敗した場合、ファイアウォールルールが作成されます。このファイアウォールルールは443ポートを開放し、Analyticsへの接続性を検証します。接続できない場合、Analyticsサーバーに到達できないことを意味し、スクリプトはここで終了します。Citrix Analytics Serviceへの接続が復元されたら、スクリプトを再実行してください。
  - **ユースケース2**: cURLが正常に実行されたにもかかわらず、StoreFrontサイトがGUIに反映されない場合、管理者はDownload DebugViewからDebugViewツールzipファイルをダウンロードし、解凍して**Downloads**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 Serviceがすでに構成されている場合、まずそれをアンインストールします。詳細ログを有効にします。その後、DebugViewツールを起動し、Citrix Analytics Service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取得し、Citrix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、問題を発見して解決を試みます。ログはDebugViewフォルダー内にログファイルとして生成され、保存されます。

  Citrix管理者と以下の3つのログファイルを共有する必要があります。

  - DebugViewログファイル (Downloads\DebugView\log)
  - 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、**Downloads > 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行する際に、`PublishConfiguration`コマンドが自動的に実行されます。PublishConfigurationコマンドは、StoreFront構成をそのStoreFront内のすべてのサーバーに公開するのに役立ちます。このアクションを確認するための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。

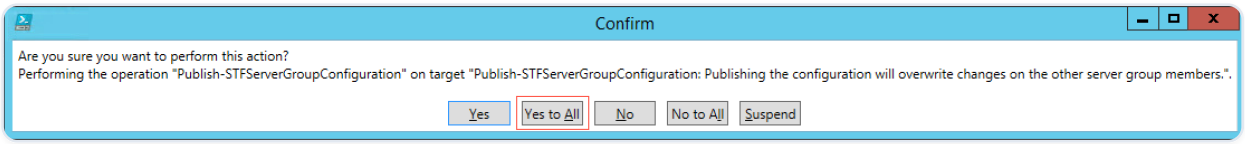


- **DeboardStoreFront**: DeboardStoreFrontパラメータは、Citrix Analytics ServiceからStoreFrontサーバーをデボードするために使用されます。DeboardStoreFrontを実行するには、次のコマンドを使用します。

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

  PowerShellスクリプトは、まずStoreFrontからすべてのCitrix Analytics Service構成を削除し、削除が成功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、存在する場合は構成を公開して、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、DeleteSiteOnboardedを呼び出します。サイトがCitrix Analytics Service GUIから削除されない場合は、StoreFront DeploymentでStoreFrontサイトを、およびStoreFront Deploymentの下にあるWorkspace Applicationサイトカードから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StoreFront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ための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。



「推奨事項」パネルを使用して接続

データソースページの**推奨事項**パネルは、データソースのオンボーディングの重要性についてユーザーに情報を提供します。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、また、利用可能なすべてのデータソースをオンボーディングしたことを確認および保証するためのオプションも提供されます。

1. Security Analytics製品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. Performance Analytics製品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**ページで、StoreFront展開をオンボーディングするための**推奨事項**パネルの情報と推奨事項を確認します。

   推奨事項パネルを確認する(/en-us/citrix-analytics/media/review-recommedations-panel.png)

> **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に送信できるようになります。

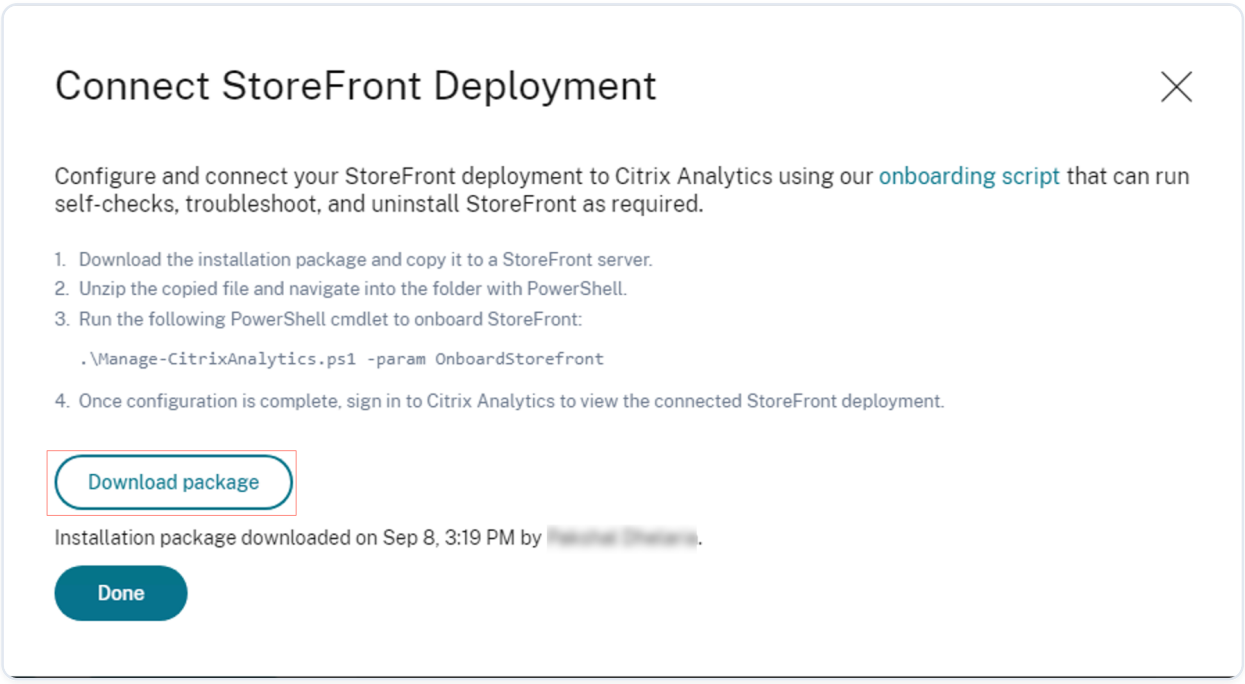
4. **オンボーディングを開始**をクリックします。**展開されたStoreFrontインスタンスの指定**ページが表示されます。

   StoreFrontインスタンスを指定する(/en-us/citrix-analytics/media/specify-sf-instances.png)

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、**展開されたStoreFrontインスタンスの総数**を指定します。

> **注:**
>
> **展開された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展開の接続**ポップアップが表示されます。
7. **StoreFront展開の接続**ページで、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。



> **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管してください。
>
> 1つのパッケージをダウンロードし、それを使用して1つのStoreFrontグループのみをオンボードできます。複数のStoreFrontグループがある場合は、各StoreFrontグループ用に個別にパッケージを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完了したら、パッケージを再度ダウンロードし、次のStoreFrontグループのオンボーディングを続行してください。
>
> 何らかの問題により、1つのパッケージを使用してStoreFrontのオンボーディングが2日以内に正常に完了しなかった場合、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。パッケージ内のキーは、2日以内に正常にオンボードされないと期限切れになるためです。

8. StoreFront展開を構成するには、,
   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内でそのフォルダーに移動します。
   c. StoreFrontをオンボードするには、次のコマンドを実行します。

      ```
      .\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スクリプトで利用可能なクラスターIDをログに記録し、確認します。
   g. 構成が完了したら、Citrix Analyticsにログインして、接続されたStoreFront展開を表示します。
9. 設定が成功したら、**完了**をクリックします。

推奨事項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ストア展開の数を取得します。**推奨事項**パネルが表示され、オンボーディングさ

れたStoreFront展開を確認できます。**推奨事項**パネルのメッセージを確認し、**完了としてマーク**をクリックできます。

> **注**
>
> **推奨事項**パネルとメッセージは、宣言されたすべてのStoreFront展開がオンボーディングされた場合にのみ消えます。

1. Citrix Analyticsがデータを処理できるように、**データ処理をオンにする**をクリックします。

推奨事項パネルを確認する

推奨事項パネルで、宣言されたStoreFront展開の数とオンボーディングされたStoreFront展開の数を比較できます。

宣言されたStoreFront展開の数がオンボーディングされたStoreFront展開の数と同じ場合、すべてのStoreFront展開がオンボーディングされたことを示す**すべてオンボーディング済み**メッセージが表示されます。**推奨事項**パネルのメッセージを確認し、**完了としてマーク**をクリックできます。

> **注**
>
> さらにStoreFront展開をオンボーディングしたい場合は、**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展開を接続**ポップアップが再度表示されます。

> オンボーディングされたStoreFrontインスタンスを確認する(/en-us/citrix-analytics/media/review-onboarded-sf-instances.png)

宣言されたStoreFront展開の数がオンボーディングされたStoreFront展開の数より少ない場合は、**カウントを編集**をクリックすると、**展開されたStoreFrontインスタンスを指定**ページが表示されます。その後、**展開されたStoreFrontインスタンスの合計数**を入力し、**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展開を接続**ポップアップが再度表示されます。さらにStoreFront展開をオンボーディングするには、手順に従ってください。

> **注:**

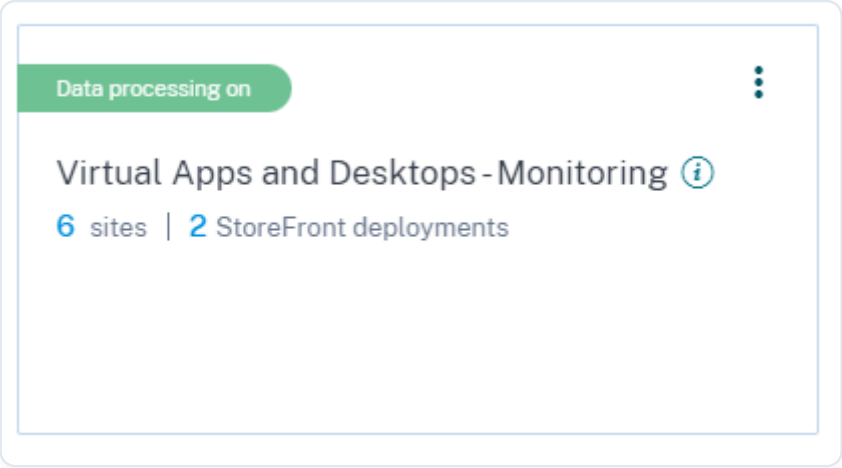
> **展開されたStoreFrontインスタンスの合計数**は、StoreFrontグループの合計数であり、個々のStoreFrontサーバーの数ではありません。

> StoreFrontオンボーディングを完了する(/en-us/citrix-analytics/media/complete-storefront-onboarding.png)

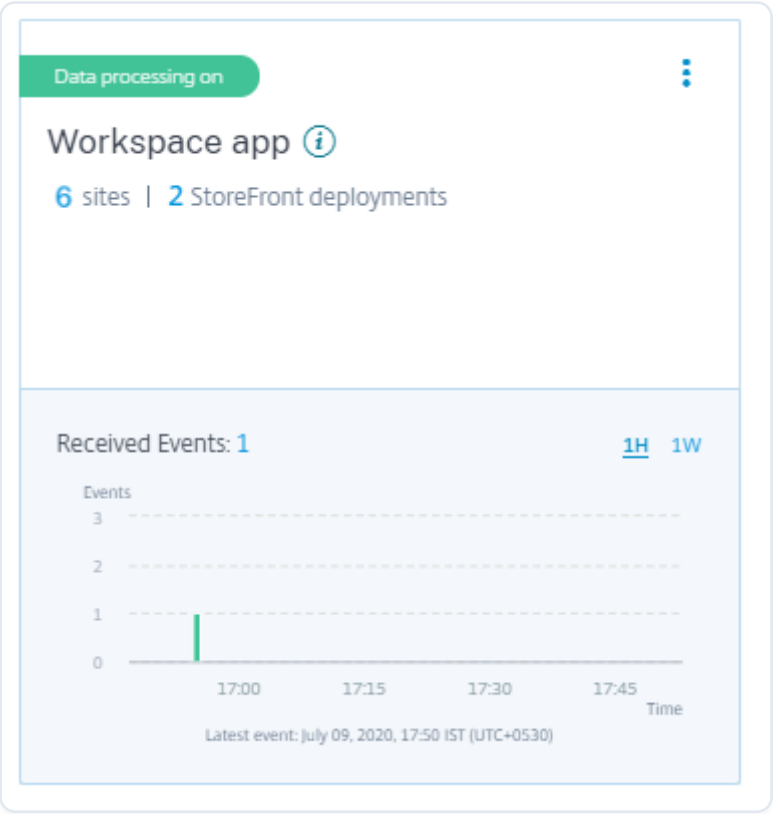
接続されているStoreFront展開を表示

StoreFront展開は、構成が成功し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と接続を確立したStoreFront展開の数が表示されます。

- Performance Analyticsサービスを使用している場合、**Apps and Desktops- Monitoring**サイトカードに次の情報が表示されます。

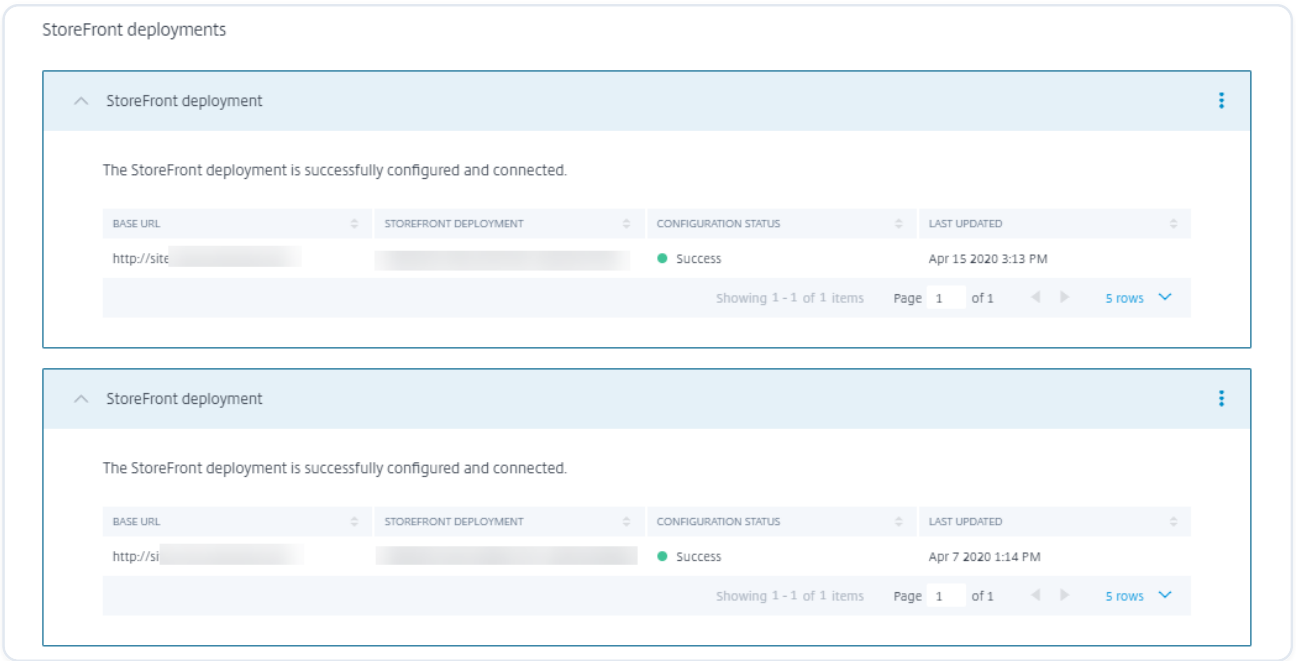


- Security Analyticsサービスを使用している場合、**Workspace app**サイトカードに次の情報が表示されます。



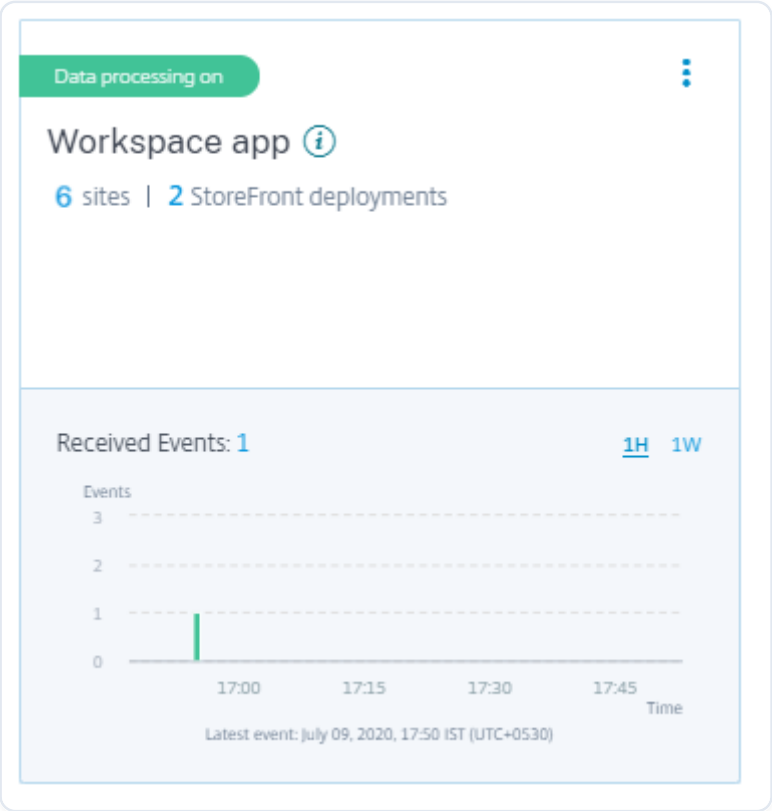
サイトカード上のStoreFront展開の数をクリックして、サーバーグループを表示します。

各StoreFront展開は、ベースURLとServerGroupIDによって表されます。



Security Analyticsサービスを使用している場合、サイトカードには受信したイベントに関する次の情報も表示されます。

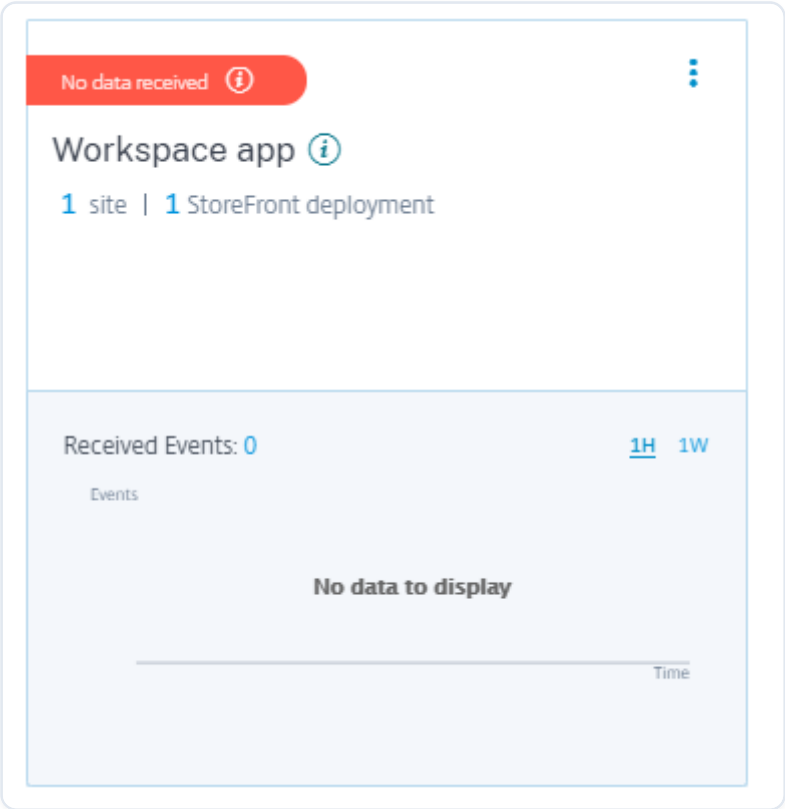
- StoreFront展開から過去1時間に受信したイベント（デフォルトの時間選択）。1週間（1 W）を選択してデータを表示することもできます。受信したイベントの数をクリックすると、セルフサービス検索ページでイベントを表示できます。



- データ処理を有効にした後、サイトカードに**データが受信されていません**というステータスが表示される場合があります。このステータスが表示される理由は2つあります。

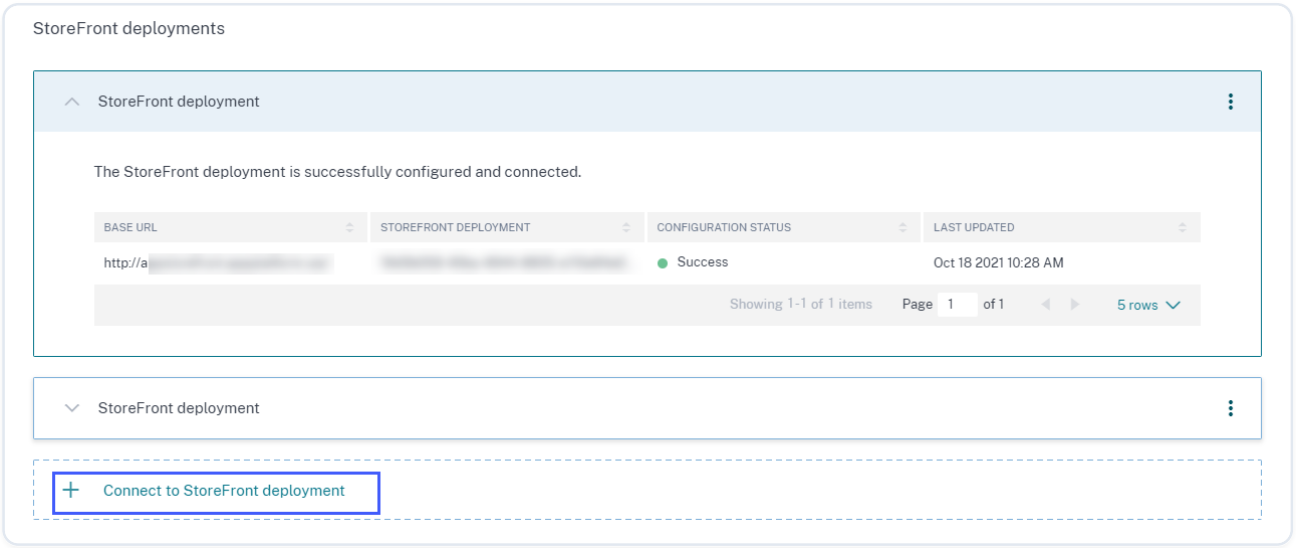
  a. 初めてデータ処理を有効にした場合、イベントがCitrix Analyticsのイベントハブに到達するまでに時間がかかります。Citrix Analyticsがイベントを受信すると、ステータスは**データ処理中**に変わります。しばらくしてもステータスが変わらない場合は、**データソース**ページを更新してください。

  b. Citrix Analyticsは、過去1時間、データソースからイベントを受信していません。



StoreFront展開の追加または削除

StoreFront展開を追加するには、**StoreFront展開**セクションで**StoreFront展開に接続**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展開を構成します。



構成済みのStoreFront展開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から削除したいStoreFront展開に移動します。StoreFrontサーバーから構成設定を削除するには、次のコマンドを実行します。

```
Remove-STFCasConfiguration
```

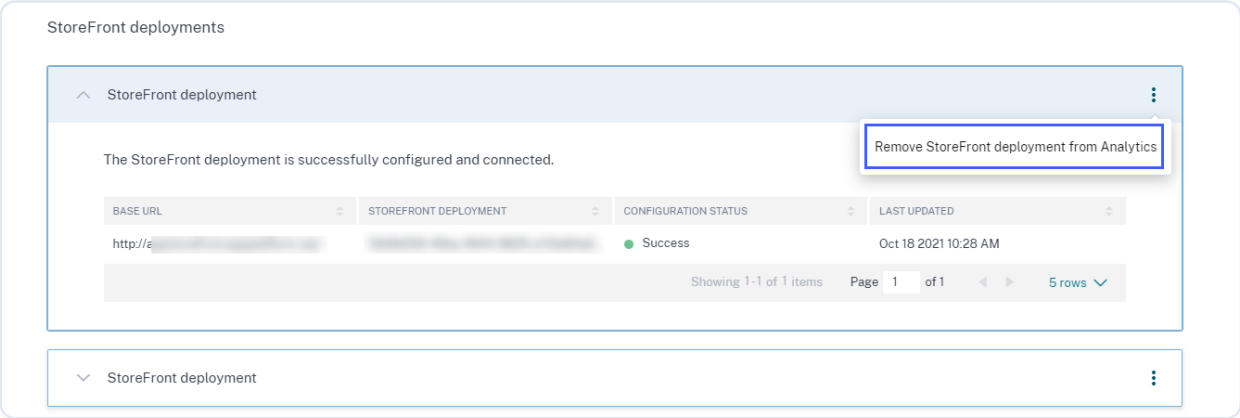
2. マルチサーバー展開を使用している場合は、変更を伝播し、StoreFrontサーバーグループ内のすべてのサーバーから構成設定を削除するために、次のコマンドを実行します。

```
Publish-STFServerGroupConfiguration
```

3. 構成設定が正常に削除されたことを確認するには、次のコマンドを実行します。設定が正常に削除された場合、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**セクションでStoreFront展開を選択します。縦の省略記号 (⋮) をクリックし、**AnalyticsからStoreFront展開を削除**を選択します。



注

Citrix Analyticsから削除する前に、StoreFront展開で指定されたコマンドを実行してください。コマンドの実行に失敗すると、Citrix Analyticsは引き続きイベントを受信し、次のイベントポーリングサイクルでStoreFront展開が再度追加されます。

HTTPプロキシを使用するWebサーバーでホストされているStoreFront展開を構成する

StoreFrontがインターネットに接続するためにWebプロキシを使用するWebサーバーでホストされている場合、ストアをCitrix Analyticsに登録するには手動で構成する必要があります。この構成では、ストアの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展開上のすべてのストアを構成する必要があります。

ストアの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つまたは複数のストアに対して、PowerShell を介してストアプロキシ構成を設定します (推奨される方法)。
- ストアの web.config ファイルに `<system.net>` セクションを手動で追加します。

これらの方法の詳細については、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」記事を参照してください。

データガバナンス

技術セキュリティの概要

Citrix Cloud™でホストされているサービスは、Citrixポートフォリオ製品およびサードパーティ製品全体から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ています。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、顧客がサブスクライブしているCitrix Cloudデータソースを自動的に検出します。しかし、オンプレミスのデータソースをCitrix Analyticsと統合するには、追加の設定が必要です。たとえば、Citrix Analyticsがサイトを検出する前に、Citrix Virtual Apps and Desktopsサイトを Citrix Workspaceに追加する必要があります。同様に、オンプレミスのCitrix Gatewayでは、Citrix 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を有効にする方法の詳細については、「CitrixデータソースでAnalyticsを有効にする」を参照してください。

Microsoft Graph SecurityやMicrosoft Active Directoryなどのいくつかのサードパーティ製品をCitrix Analyticsと統合できます。詳細については、以下のトピックを参照してください。

- Microsoft Graph SecurityでAnalyticsを有効にする
- Microsoft Active DirectoryとAnalyticsを統合する

Citrix Analyticsは、顧客が所有するSplunk環境にリスクインテリジェンス情報を送信することもできます。この統合には、Splunk環境に**Citrix Analytics Add-on for Spunk**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。

顧客の同意なしに、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、および保持の詳細については、「データガバナンス」を参照してください。

ネットワーク要件

- **Citrix Cloudサービス要件**: 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要件」を参照してください。

- **Citrix Analytics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を介して以下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	欧州連合リージョン	アジア太平洋南部リージョン
管理UI	`https://analytics.cloud.com/`	`https://analytics-eu.cloud.com/`	`https://analytics-aps.cloud.com/`
管理UI (CDN)	`https://cas-api-cdn-ep-h9apa4bsccg0gfe7.a02.azurefd.net/`	`https://cas-api-cdn-ep-eu-g5d6bhadh5gvd0fh.a02.azurefd.net/`	`https://cas-api-cdn-ep-aps-a0fwd8c3d7bbfxdt.a02.azurefd.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-ap-s-a.was.cloud.com/`
	`https://api-b.was.cloud.com/`	`https://api-eu-b.was.cloud.com/`	`https://api-ap-s-b.was.cloud.com/`
パブリック IP の取得	`https://locus.analytics.cloud.com/`	`https://locus.analytics.cloud.com/`	`https://locus.analytics.cloud.com/`
イベントハブ (Citrix ADM エージェントには適用されません)	`https://citrixanalyticseh-alias.servicebus.windows.net/`	`https://citrixanalyticseheu-alias.servicebus.windows.net/`	`https://citrixanalyticsehaps-alias.servicebus.windows.net/`
	`https://citrixanalyticseh2-`	`https://citrixanalyticseh2eu-`	

エンドポイント	米国リージョン	欧州連合リージョン	アジア太平洋南部リージョン
	`alias.servicebus.windows.net/`	`alias.servicebus.windows.net/`	
	`https://citrixanalyticseh3-alias.servicebus.windows.net/`		
イベントハブ (Citrix ADMエージェント用)	`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、ほとんどの以前のエンドポイントについて 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 とリソースの場所間の通信チャネルです。Citrix Cloud Connector をインストールした後、Web プロキシ設定を構成する必要があります。詳細については、「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 統合用の 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の許可リストに含まれていることを確認してください。

エンドポイント	米国リージョン	欧州連合地域	アジア太平洋南部地域
Kafka ブローカー	`casnb-0.citrix.com:9094`	`casnb-eu-0.citrix.com:9094`	`casnb-aps-0.citrix.com:9094`
	`casnb-1.citrix.com:9094`	`casnb-eu-1.citrix.com:9094`	`casnb-aps-1.citrix.com:9094`
	`casnb-2.citrix.com:9094`	`casnb-eu-2.citrix.com:9094`	`casnb-aps-2.citrix.com:9094`
	`casnb-3.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 Cloud は Citrix Identity プロバイダーを使用して、Citrix Cloud アカウント内のすべてのユーザーの ID 情報を管理します。ID およびアクセス管理 に記載されているように、他の ID プロバイダー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。企業内でAnalyticsを管理するために、ユーザーに読み取り専用の管理者権限を割り当てることができます。詳細については、「管理者ロールの管理」を参照してください。

データレジデンシー

Citrix Cloudは、Citrix Analyticsの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、およびアジア太平洋南部地域にあります。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際に選択したホームリージョンによって異なります。詳細については、以下のトピックを参照してください。

- 地理的考慮事項

- 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の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は、以下のセキュリティ対策を使用して顧客のデータを保護します。

- Analyticsユーザー向けのCitrix Cloud認証。詳細については、「IDおよびアクセス管理」を参照してください。
- データサービスおよびデータアクセスレイヤーによって適用されるテナントベースのデータアクセス制御。
- データレイクおよびデータウェアハウス内のすべてのデータストアにおける、顧客またはテナントごとの強力なデータ分離。
- プラットフォームのパブリックエンドポイント（APTs/入力/出力）およびプラットフォーム内で適用される、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エンドポイントにおける高い標準。TLS 1.0および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た暗号化データストレージ。
- 顧客ログを保護しながら、サービス運用およびサポートのための強力なユーザー管理アクセス制御。
- 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は、Azure Security Centerと併用されます。

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) に厳密に従います。詳細については、以下の契約を参照してください。

- ユーザー契約
- Citrixプライバシーポリシー
- Citrixデータ処理契約
- Citrixサービスセキュリティ補足資料
- Citrix Cloud Services: お客様のコンテンツとログの処理
- Citrixプライバシーおよびコンプライアンス情報

セキュリティの責任

Citrixの責任

Citrixは、Citrix Analyticsをホスト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のセキュリティを確保する責任を負います。Citrixは、セキュリティの脆弱性に対処するために、クラウド環境に定期的なソフトウェアアップデートとパッチを適用する責任を負います。

お客様の責任

Citrixのお客様は、Citrix Analyticsと統合されているデータソース、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) システムのセキュリティを確保する責任があります。これには以下が含まれます。

- お客様が所有および管理するオンプレミスデータソース:
  - **オンプレミスデータソース**: シトリックス ゲートウェイ、シトリックス バーチャル アプリケーションズ アンド デスクトップ、マイクロソフト アクティブ ディレクトリ
  - **SIEM**: Splunk および Citrix Analytics からイベントを読み取るために Kafka ブローカーを使用す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、お客様が提供する管理者資格情報。
- Citrix Cloud サービスからメールまたは通知を受信する、お客様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が提供する管理者資格情報。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、これらのエージェントへのアクセスは制限する必要があります。
- **Citrix Analytics Add-on for Splunk** を構成するための、Citrix Analytics が生成した資格情報。
- Citrix Cloud または Citrix Workspace™ に接続し、データソースと統合するために、Windows、Mac、Android、iOS で動作するエンドユーザーデバイス。

セキュリティプロビジョニングの詳細については、以下のドキュメントを参照してください。

- Citrix Cloud Platform のセキュアな展開ガイド
- Citrix Workspace ドキュメント
- Citrix DaaS (旧 Citrix Virtual Apps and Desktops サービス) の技術セキュリティ概要
- Citrix Virtual Apps and Desktops のセキュリティに関する考慮事項

- StoreFront 展開のセキュリティ保護に関するドキュメント
- Citrix Endpoint Management の技術セキュリティ概要
- Citrix Secure Private Access サービスドキュメント
- Citrix ADC のセキュアな展開ガイド
- Citrix ADM システム要件(/ja-jp/citrix-application-delivery-management-service/system-requirements.html)

システム要件

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、およびブラウザ要件を確認する必要があります。

Citrix Analytics のサブスクリプション

以下の 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。

- シトリックス アナリティクス フォー セキュリティ
- シトリックス アナリティクス フォー パフォーマンス

詳細については、Citrix Cloud services を参照してください。

データソースの要件

データソースとは、Citrix Analytics にイベントを送信する製品です。使用している Citrix Analytics のサービスに応じて、データソースは異なります。各サービスでサポートされているデータソースを表示するには、以下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
- Citrix Analytics for Performance 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

Citrix Analytics にアクセスするには、ワークステーションに以下のサポートされているWebブラウザが必要です。

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

Citrix Analytics の管理者ロールを管理する

注:

2023 年 7 月以降、Microsoft は Azure Active Directory (Azure AD) を Microsoft Entra ID に名称変更しました。このドキュメントでは、Azure Active Directory、Azure AD、または AAD へのすべての参照は、Microsoft Entra ID を指します。

デフォルトでは、Citrix Cloud™ 管理者は、Citrix Cloud アカウント上のすべてのサブスクライブ済みサービスに対するフルアクセス権限を持っています。フルアクセス権限を持つ管理者は、サブスクライブ済み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 管理者として、組織のサブスクライブ済みサービスを管理するために、他の管理者を Citrix Cloud アカウントに招待できます。その後、彼らのアクセス権限を定義し、サブスクライブ済みサービス内の特定の機能を管理できるようにすることができます。

新しい管理者は、次の 2 つの方法で追加できます。

1. Citrix Identity および Azure AD/Active Directory からのユーザーとして個別に。詳細については、「Citrix Cloud 管理者の管理」を参照してください。
2. Azure Active Directory のグループを使用する。詳細については、「管理者グループの管理」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、そのロールに応じて特定の機能にアクセスしたり、タスクを実行したりできます。

Citrix Analytics では、管理者に対して以下のカスタムロールを割り当てることができます。

ロール	権限
Performance Analytics - フル管理者	Performance Analytics の Citrix Cloud 管理者にフルアクセス権限を割り当てます。

ロール	権限
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権限を割り当てます。
Security & Performance Analytics - 読み取り専用管理者	Security AnalyticsとPerformance Analyticsの両方のCitrix Cloud管理者に読み取り専用アクセス権限を割り当てます。
Security Analytics - フル管理者	Security AnalyticsのCitrix Cloud管理者にフルアクセス権限を割り当てます。
Security Analytics - 読み取り専用管理者	Security AnalyticsのCitrix Cloud管理者に読み取り専用アクセス権限を割り当てます。

Analytics管理者ロール(/en-us/citrix-analytics/media/analytics-rbac.png)

注

- 管理者に対して複数のロールを選択した場合、より高いアクセス権を持つロールが適用されます。
- ユーザーが直接ユーザーとして、かつAzure Active Directoryグループを介してアクセス権を付与された場合、ユーザーに個別に付与されたアクセス権が適用されます。
- 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では利用できません。
- 以前利用可能だった**読み取り専用管理者**ロールを持つ管理者は、**Security & Performance - 読み取り専用管理者**に名称変更されました。
- **Security & Performance Analytics - 読み取り専用管理者**ロールと**Performance Analytics - 読み取り専用管理者**ロールを持つ管理者は、Citrix Analyticsからのメール通知を受け取りません。

オファリング固有のロールの詳細については、以下の記事を参照してください。

- Performance Analytics の管理者ロールを管理する
- Security Analytics の管理者ロールを管理する

使用開始

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てください。

Citrix Cloud アカウントをお持ちでない場合は、まず 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。詳細な手順については、「Sign Up for Citrix Cloud」を参照してください。

ステップ 2: Analytics へのアクセスを取得する

Analytics には、次のいずれかの方法でアクセスできます。

- **Citrix Analytics オファリングのトライアルをリクエストする**。Citrix Cloud にサインインした後、**Available Services** セクションの **Analytics** タイルで、**Manage** をクリックして Analytics の概要ページを表示します。

  概要ページには、Analytics のオファリングである **Security** と **Performance** が表示されます。

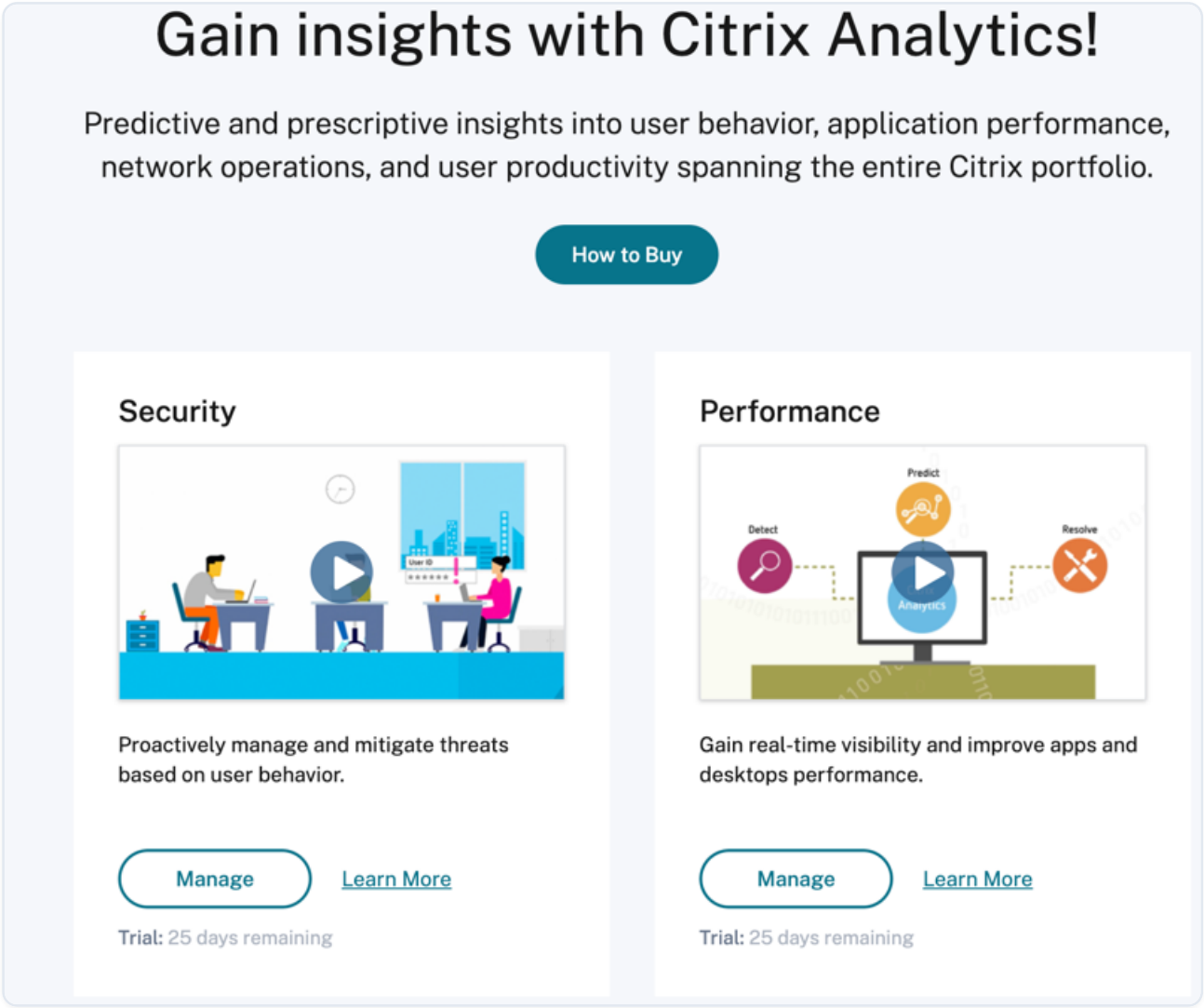
  - Security Analytics および Performance Analytics の場合、**Request Trial** をクリックして、オファリングのトライアルバージョンを使用します。リクエストが承認され、トライアルが利用可能になると、メールが届きます。トライアルは最大 60 日間使用できます。サービス試用版の詳細については、「Citrix Cloud Service Trials」を参照してください。

  Citrix Cloud ページで、**Analytics** タイルが **My Services** セクションに移動します。
- **Citrix Analytics を購読する**。次の Citrix Analytics サブスクリプションを購入できます。
  - Citrix Analytics セキュリティ™
  - Citrix Analytics パフォーマンス™
  - Citrix Analytics セキュリティおよびパフォーマンス

Citrix Analytics for SecurityとCitrix Analytics for Performanceは、Citrix Workspaceパッケージ（Workspace Standard、Workspace Premium、Workspace Premium Plus）のアドオンサービスとして提供されます。詳細については、Citrix Cloud servicesを参照してください。

ステップ 3: Analyticsの管理

Security AnalyticsとPerformance Analyticsの場合、必要なサブスクリプションをお持ちの場合、または試用版へのアクセスが許可されている場合、Analyticsの概要ページで、その製品の**試用版をリクエスト**ボタンが**管理**に変わります。**管理**をクリックして、各製品に対応するユーザーダッシュボードを表示します。



Analytics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。

各Analytics製品の詳細については、以下を参照してください。

- Citrix Analytics for セキュリティ

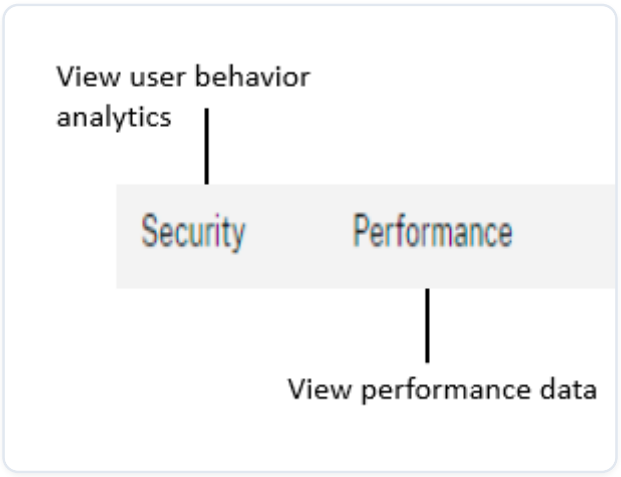
- Citrix Analytics for パフォーマンス

操作方法

Analyticsユーザーインターフェイスの主要なコントロールに慣れてください。

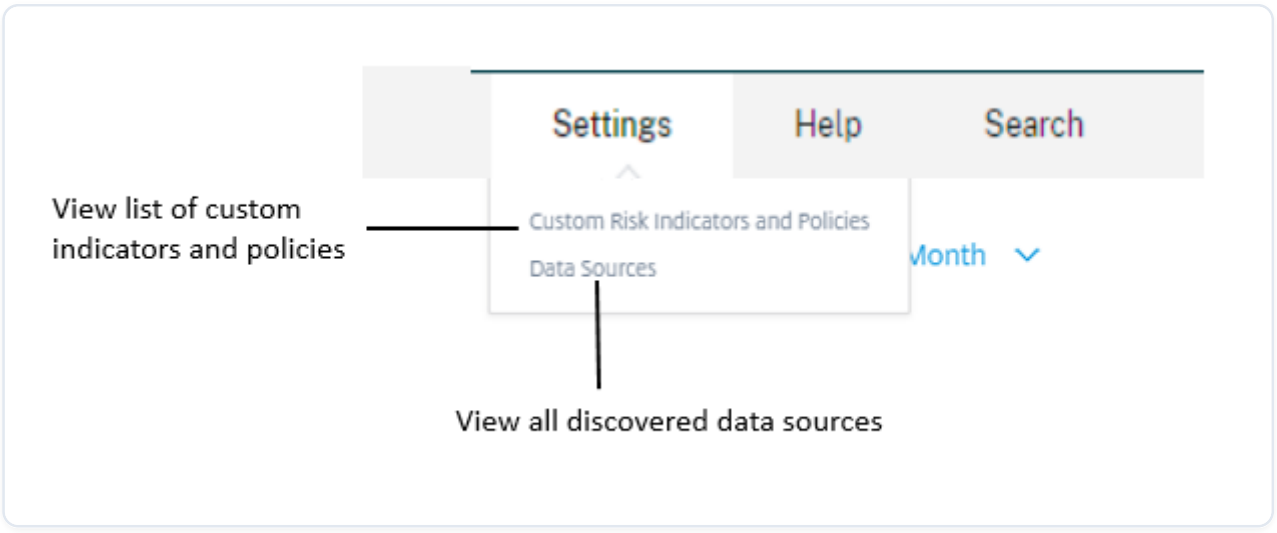
トップバー

トップバーからさまざまなAnalyticsの機能に移動します。

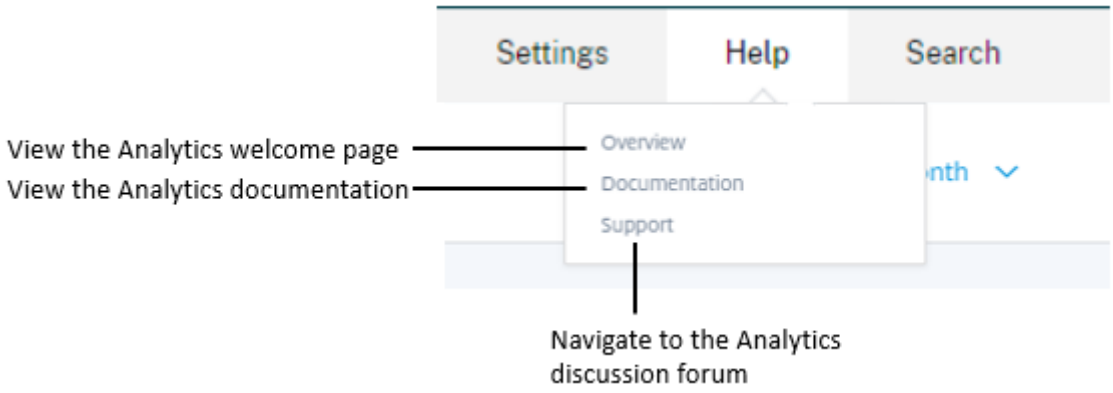


設定メニュー

設定メニューから、インジケーター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。

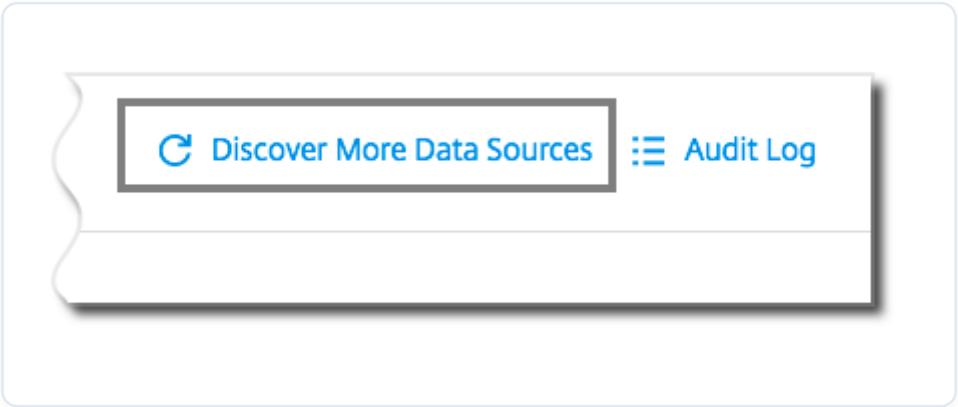


ヘルプメニュー



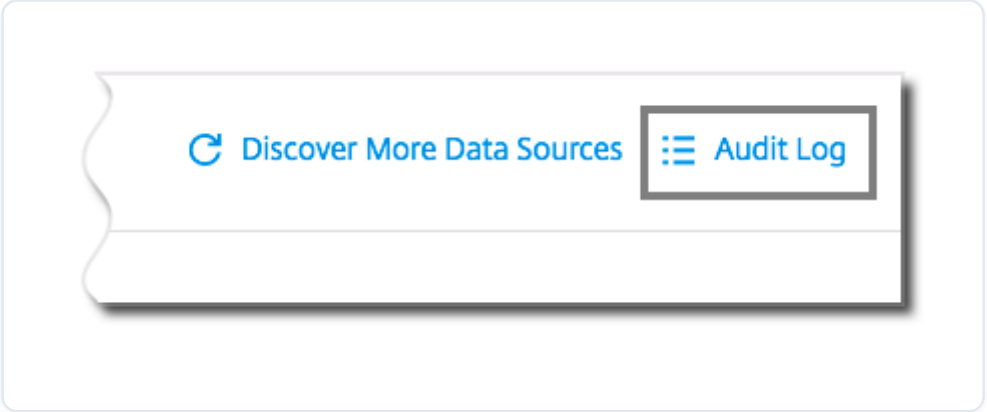
その他のデータソースを見つける

新しく追加されたデータソースまたは以前に削除されたデータソースを見つけます。



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

アラート設定

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

- 電子メール配信リスト(/ja-jp/citrix-analytics/alert-settings/email-distribution-lists.html)
- アラート通知用Webhook(/ja-jp/citrix-analytics/alert-settings/webhook-for-alerts.html)

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

- エンドユーザーの電子メール設定(/ja-jp/security-analytics/email-settings.html)

メール配布リスト

手動で、またはポリシーを作成して **Notify administrator(s)** アクションを適用すると、選択された管理者に対してリスクインジケーター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Citrix Cloud以外のドメインから管理者を選択できます。

> 適切な管理者のグループに通知を送信するには、彼らのメールアドレスを使用して配布リストを作成します。

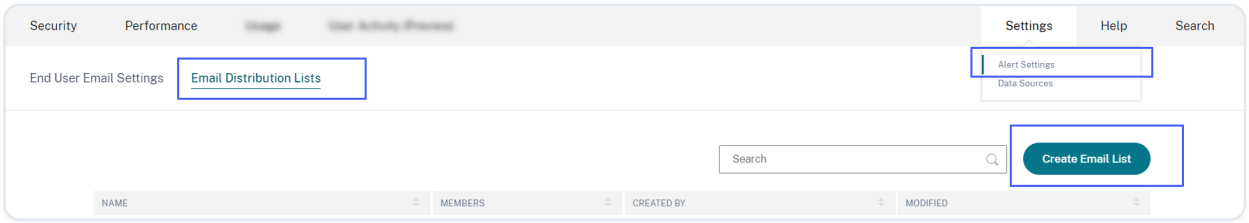
メール配布リストを使用すると、次のことができます。

- 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する。
- すべてのメンバーに一度に通知する。
- 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する。
- 新しいメンバーの追加や既存メンバーの削除など、要件に基づいてメール配布リストを管理および維持する。

メール配布リストの作成

メール配布リストを作成するには：

1. **設定 > アラート設定 > メール配信リスト > 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 **Notify administrator(s)** アクションを選択します。**Create Email List** リンクをクリックします。

   ポリシーからメールリストを作成(/en-us/citrix-analytics/media/create-email-list-policy.png)

2. メール配信リストの目的を識別するために、名前と説明を入力します。
3. メール配信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**。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。
   - **メールアドレスでユーザーを追加**。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**
   >
   > 複数のドメインからユーザーやユーザーグループを追加することもできます。その場合は、ドメインを1つずつ選択します。各ドメインで、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**追加**アイコンをクリックします。

   ドメインからメンバーを追加(/en-us/citrix-analytics/media/add-domain-users.png)

6. 選択したドメインで利用できないユーザーを追加するには、ユーザーのメールアドレスまたはメール配信リストを入力します。

> **注**
>
> メール配信リストを入力する前に、組織のネットワーク外からメール配信リストにアクセスできることを確認してください。組織内部のメール配信リストを追加した場合、そのリストのメンバーはCitrix Analyticsからの通知を受け取ることができません。

> メールでメンバーを追加(/en-us/citrix-analytics/media/add-members-emails.png)

7. **メールリストの作成**をクリックします。

メール配信リストの表示

メール配信リストを表示するには、 **> >** の順にクリックします。

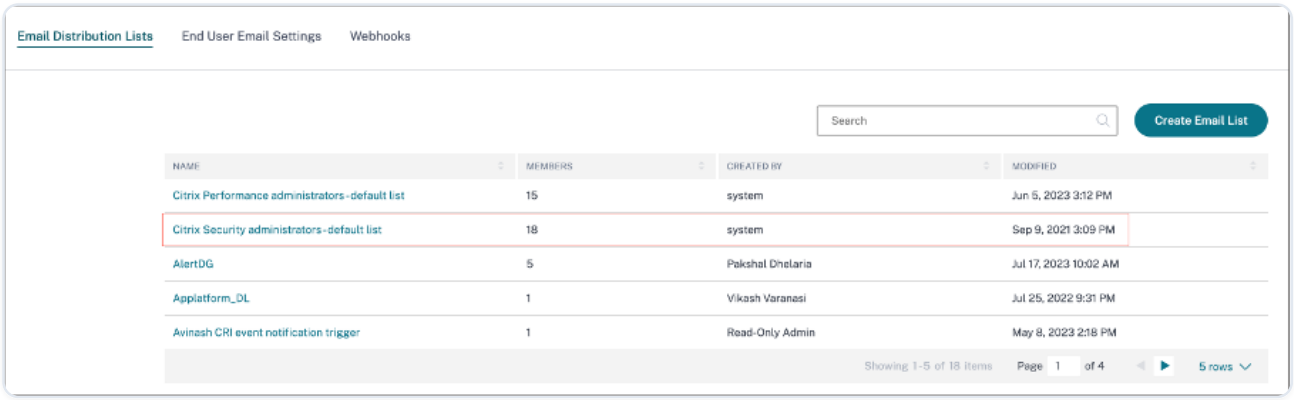
このページには、アカウントで作成されたすべてのメール配信リストが表示されます。メール配信リストを選択して、メンバーを表示したり、リストを変更したりできます。

アカウントには、デフォルトで作成されたメール配信リストが表示されます。これには、Citrix Cloudアカウントで 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。デフォルトのリストを削除または変更することはできません。

> **注**
>
> デフォルトのメール配信リストの場合、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時間ごとに1回更新されます。そのため、管理者がメール通知設定を変更した場合、この変更は24時間後にCitrix Analyticsに更新されます。

> たとえば、Citrix Cloud管理者がメール通知を有効にした場合、通知は即時ではなく24時間後に届き始めます。同様に、Citrix Cloud管理者がメール通知を無効にした場合、通知は24時間後に届かなくなります。

> セキュリティ管理者向けのデフォルトの配信リストには、Citrix Cloudアカウントで オプションが有効になっ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。



メール配信リストの変更

メール配信リストを変更するには：

1. **> >** の順にクリックします。
2. 変更するメール配信リストをクリックします。
3. メール配信リストで、名前、説明などの必要な詳細を更新し、メンバーを追加または削除します。
4. をクリックします。

メール配信リストを削除する

メール配信リストは、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。いくつかのポリシーにリンクされている場合は、まず関連付けられているポリシーからメール配信リストを削除する必要があります。

メール配信リストを削除するには：

1. 「**設定 > アラート設定 > メール配信リスト**」をクリックします。
2. 削除したいメール配信リストをクリックします。
3. メール配信リストで、関連付けられているポリシーを表示します。

   メール関連ポリシー(/en-us/citrix-analytics/media/email-associated-policies.png)
4. ポリシーをクリックして開き、メール配信リストを削除します。必要に応じて、ポリシーを削除することもできます。

   ポリシーからメールを削除(/en-us/citrix-analytics/media/remove-email-policy.png)
5. 「**変更を保存**」をクリックして、メール配信リストに戻ります。
6. メール配信リストを開き、「**削除**」アイコンをクリックします。

アラート通知用Webhook

Webhook を使用して、受信 Webhook URL が設定されているサードパーティ製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、イベント発生時に通知を受け取ることができます。

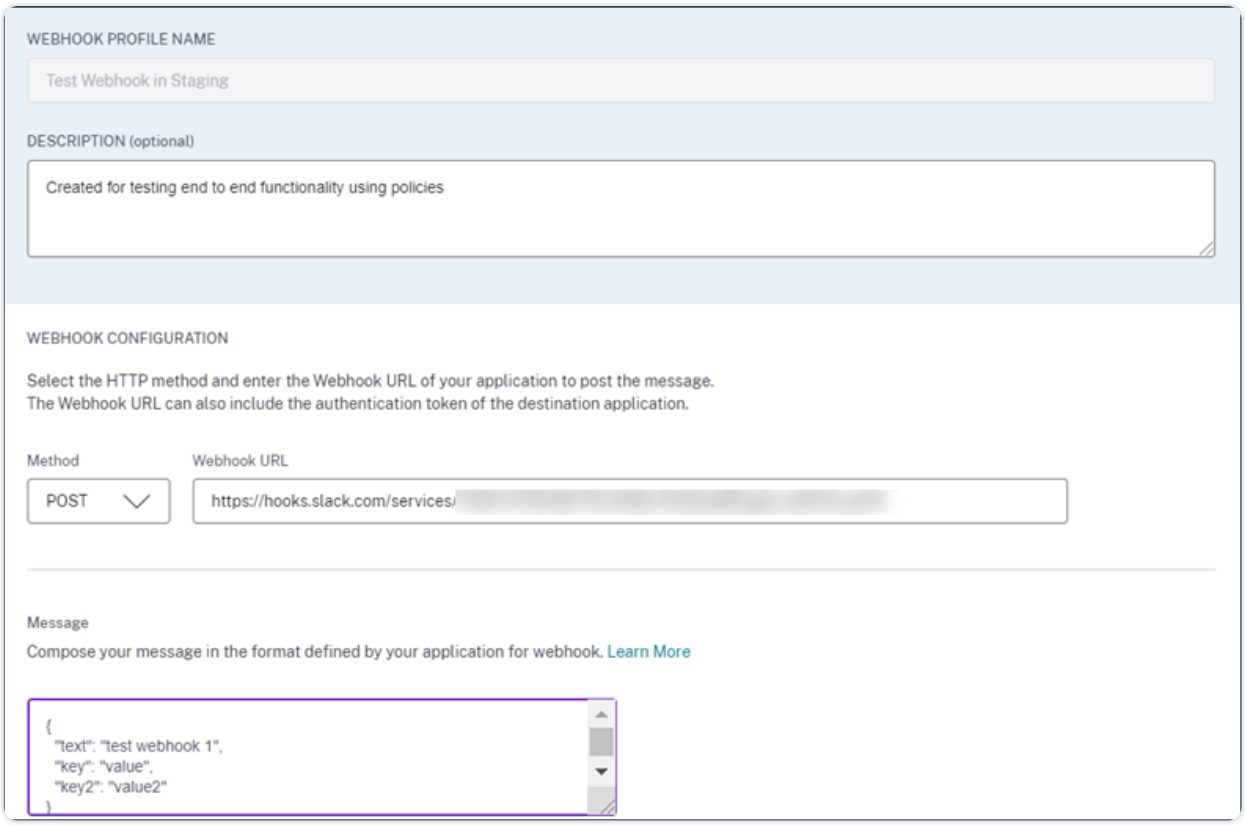
Citrix Analytics がアラートをトリガーすると、関連付けられた Webhook がターゲットアプリケーションの URL にアラートメッセージを送信します。アラートは、HTTP POST または PUT リクエストを介して JSON ペイロードの形式で送信されます。たとえば、ユーザーがリスクインジケーターをトリガーしたり、VDI マシンのパフォーマンスが低下したりした場合、Webhook を設定してアラート通知を Slack チャネルに送信できます。 アラート管理のために Webhook を設定すると、アプリケーションでリアルタイム通知を受け取ることができます。セキュリティリスクを軽減したり、Citrix Virtual Apps and Desktops™ 展開のパフォーマンスを向上させたりするために、タイムリーな措置を講じることができます。

Webhook プロファイルの作成

Citrix Analytics で Webhook プロファイルを作成するには:

1. Citrix Analytics にサインインします。
2. ご契約のサービスに応じて、 をクリックして Security Analytics または Performance Analytics にアクセスします。
3. 上部のバーから、 **> >** をクリックします。

4. を選択します。



5. プロファイル名と Webhook の目的を識別するための説明を入力します。
6. アラートメッセージを送信するための HTTP メソッドとアプリケーションの Webhook URL を選択します。
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 または XML などの形式で構造化されている必要があります。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に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 の構成を検証するには、 をクリックします。 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が検証されます。構成に問題がない場合、「テスト成功」メッセージが表示されます。

Webhook 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ための Webhook の設定例を示します。

Slack にアラートメッセージを送信する

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

1. まだお持ちでない場合は、Citrix Analytics 用の Slack アプリを作成します。
2. アプリケーションで、受信 Webhook 機能を有効にし、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ネルを選択します。
4. アプリを承認すると、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 の使用開始」を参照してください。

メッセージ形式の例

```
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

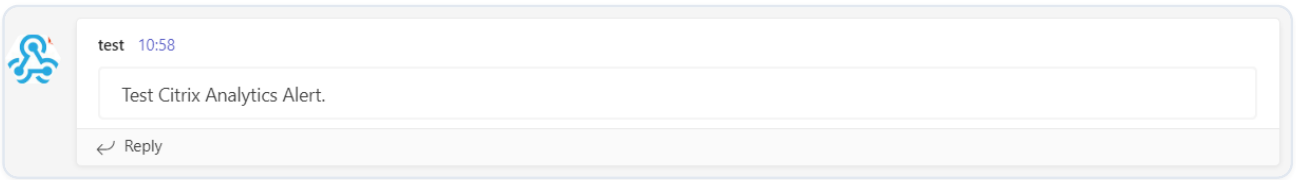
Microsoft Teams でアラートを送信する前に、以下のタスクを完了していることを確認してください。

1. Teams内にTeamsグループがまだない場合は作成します。
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に記載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。

メッセージ形式の例

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

出力



Citrix Analytics for セキュリティ™ (セキュリティ アナリティクス)

いつでも、どこからでも、どのデバイスからでも、どのネットワークからでも仕事ができるという利点により、ユーザーが隔離された企業オフィスからのみ作業していた頃よりも、機密性の高い企業データがより危険にさらされています。悪意のあるユーザーは、標的とする広範な攻撃対象領域を持っています。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ことを求められています。Citrix Analytics for Securityは、ユーザーセキュリティに焦点を当てることで、そのギャップを埋めるのに役立ちます。

Security Analyticsとは何か?

Citrix Analytics for Securityは、Citrix Virtual Apps and Desktops™ユーザー、Citrix DaaS（旧Citrix Virtual Apps and Desktopsサービス）ユーザー、およびCitrix Workspace™ユーザーの行動を継続的に評価します。機密性の高い企業情報を保護するためのアクションを適用します。ネットワーク、仮想化されたアプリケーション、デスクトップツール全体でのデータの集約と相関により、貴重な洞察と、ユーザーセキュリティの脅威に対処するためのより焦点を絞ったアクションの生成が可能になります。また、機械学習は、悪意のあるユーザー行動を特定するための非常に予測的なアプローチをサポートします。

機能

- Citrix製品およびパートナー統合全体からの合理化されたインサイト。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。
- わかりやすいダッシュボードは、ユーザー行動の全体像を提供します。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を備えた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行動を検出し、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回認証後のユーザー行動の継続的な監視は、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取ります。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

以下のセキュリティダッシュボードで、ユーザーまたはエンティティの行動に関する詳細を表示できます。

- 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。
- アクセス保証ロケーション: Citrix Virtual Apps and DesktopsユーザーおよびCitrix DaaSユーザーのアクセス詳細とログオン詳細を要約します。
- レポート: オンボードされたデータソースから利用可能なディメンションとメトリックに基づいてカスタムレポートを作成します。

次のステップ

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

シトリックス アナリティクス for パフォーマンス™ (パフォーマンス分析)

パフォーマンス分析とは

Performance Analyticsは、Citrix Analyticsが提供するサービスで、Apps and Desktops環境の主要なパフォーマンス指標を追跡、集計、視覚化できます。

- Performance Analyticsは、サイトのパフォーマンスメトリックを見やすいユーザーエクスペリエンス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に集計します。これらのダッシュボードは、ユーザーエクスペリエンスを分析し、Apps and Desktopsサイトの使用状況を最適化するのに役立ちます。
- Performance Analyticsは、マルチサイトの集計とレポート作成をサポートしています。クラウドおよびオンプレミス環境全体のパフォーマンスメトリックを集計します。そのため、環境内のすべてのサイトのデータを単一のコンソールで表示できます。
- Performance Analytics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、画面の遅延、セッションログオンの遅延、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インサイトを提供します。
- Performance Analyticsを使用すると、メトリックを検索およびフィルタリングして、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。

Performance Analytics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は、セッションの応答性、セッションログオン期間、セッション障害、セッション再接続など、ユーザーエクスペリエンスを構成する要因に関するサイトのパフォーマンスを表示します。

組織内で仮想アプリとデスクトップの複数のユーザーをサポートしており、アプリやデスクトップの起動時に時々遅延が発生する場合、ログオン期間メトリックは、その問題に関するインサイトを提供できます。ドリルダウンすることで、問題の原因となっている要因を特定できます。

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は、サイト内のマシンのステータスと正常性を表示します。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一緒に使用すると、リソースの可用性を事前に確認し、サイトのパフォーマンス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を示し、サイトにログオ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、この指標を使用して、ハイパーバイザーが再起動されたか、マシンの数が不足しているかを確認します。
- セッションの起動に失敗するケースがいくつか見られる場合は、ドリルダウンして障害の原因を特定します。ライセンス数の不足、またはDelivery Controllerへのマシン接続の問題が原因である可能性があります。

> **注記:**
>
> **Infrastructure Analytics Dashboard** は現在プレビュー中です。

> 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。

はじめに

前提条件

1. 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対象のWebブラウザが搭載されているか確認してください。システム要件については、Citrix Analyticsシステム要件の記事を参照してください。
2. Analytics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アカウントの作成方法の詳細については、Citrix Cloudに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、スタンドアロン製品として、またはCitrix Analytics for Securityとバンドルされたサブスクリプションベースの製品として利用できます。Citrix Analytics for Performanceを購読するには、`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データソースのバージョンは、データソースの記事で確認できます。
5. Citrix Profile Managementは、すべてのマシンにインストールされている必要があります。

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、**Performance AnalyticsのVDAデータ収集**ポリシーがマシンで **許可** に設定されている必要があります。詳細については、Performance Analyticsのデータ収集ポリシーを参照してください。
8. Citrix Studioからプロセス監視ポリシーを有効にして、**マシン統計 > プロセス**タブでリソース消費量の多いプロセスを可視化します。 詳細については、プロセス監視の有効化を参照してください。
9. すべてのエンドポイントから（またはプロキシが構成されている場合はプロキシから）次のURLへのアクセスを確保してください。

エンドポイント	米国リージョン	欧州連合リージョン	アジア太平洋南部リージョン
シトリックスキー登録	`https://trust.citrixnetworkapi.net`	`https://trust.citrixnetworkapi.net`	`https://trust.citrixnetworkapi.net`
シトリックスクラウド	`https://trust.citrixworkspacesapi.net`	`https://trust-eu.citrixworkspacesapi.net`	`https://trust-aps.citrixworkspacesapi.net`
シトリックス アナリティクス	`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://citrixanalyticseheu-alias.servicebus.windows.net/`	`https://citrixanalyticsehaps-alias.servicebus.windows.net/`
一括アップロード	`https://citrixanalyticseh2-alias.servicebus.windows.net/`	`https://citrixanalyticseh2eu-alias.servicebus.windows.net/`	

エンドポイント	米国リージョン	欧州連合リージョン	アジア太平洋南部リージョン
一括アップロード	`https://citrixanalyticseh3-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、**管理**をクリックします。概要ページには、Analytics ポートフォリオで利用可能なサービスが表示されます。
2. **パフォーマンス**サービスで、サービスの試用版を使用するには、**トライアルをリクエスト**をクリックします。Citrix Analytics for Performance サービスを購入済みの場合は、代わりに**管理**リンクをクリックします。

パフォーマンス分析(/en-us/citrix-analytics/media/pa-ftu.png)。

1. Citrix Analytics for Performance が開き、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を表示するダッシュボードが表示されます。

アジア太平洋南部リージョンからのアクセス

Citrix Analytics for Performance は、試用版のお客様およびサブスクリプションベースのお客様向けに、アジア太平洋南部 (APS) リージョンで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に関する詳細については、地理的考慮事項を参照してください。

APS リージョンから Performance Analytics 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 Cloud Service にアクセスします。

- Citrix Analytics for Performance は、ホームリージョンとしてアジア太平洋南部リージョンを選択した場合、組織のユーザーイベントとメタデータをこのリージョンに保存するようになりました。詳細については、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、技術セキュリティの概要を参照してください。

データソースの構成

Performance Analytics 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。このサービスは、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を組み合わせたハイブリッドのお客様のいずれの場合でも利用できます。

Performance Analytics は、Citrix DaaS (旧称 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、

- まず、Citrix Virtual Apps and Desktops サイトを Performance Analytics にオンボーディングします。
- Performance Analytics でネットワーク関連情報を取得するには、オンプレミスの Citrix Gateway もオンボーディングする必要があります。

データソースの記事で説明されているように、必要なデータソースを構成します。

> **注:**
>
> - Citrix Analytics for Performance は、Citrix Analytics for Performance 用に収集されるログに記載されているデータポイントのログを収集および保存します。
> - Citrix Analytics for Performance サービスの推奨制限は、制限の記事に記載されています。

サービス継続性

サービス中断が発生した場合、Citrix Analytics for Performance は制限された機能で動作します。

管理者は、**滞在**して現在の画面で利用可能なデータを表示するか、ダウングレードモードで**ダッシュボードへ移動**するかを選択できます。

読み取りレジリエンスダイアログ(/en-us/citrix-analytics/media/pa-read-resiliency-dialog.png)

ダウングレードモードでは、ユーザーは過去1日間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、すべてのフィルターとドリルダウンは無効になります。

読み取りレジリエンス(/en-us/citrix-analytics/media/pa-read-resiliency.png)

このアップデートにより、製品の回復性が向上し、サービスレベル契約との整合性が高まります。

Citrix Analytics for Security and Performance のトラブルシューティング

匿名ユーザーの正規ユーザーとしての検証

データソースからのイベント送信に関する問題のトラブルシューティング

Virtual Apps and Desktops イベント、SaaS イベントのトリガーとイベント送信の検証

構成済みSession Recordingサーバーの接続失敗

Splunk 用 Citrix Analytics アドオンの構成に関する問題

StoreFront™ サーバーと Citrix Analytics の接続不可

よくある質問

用語集